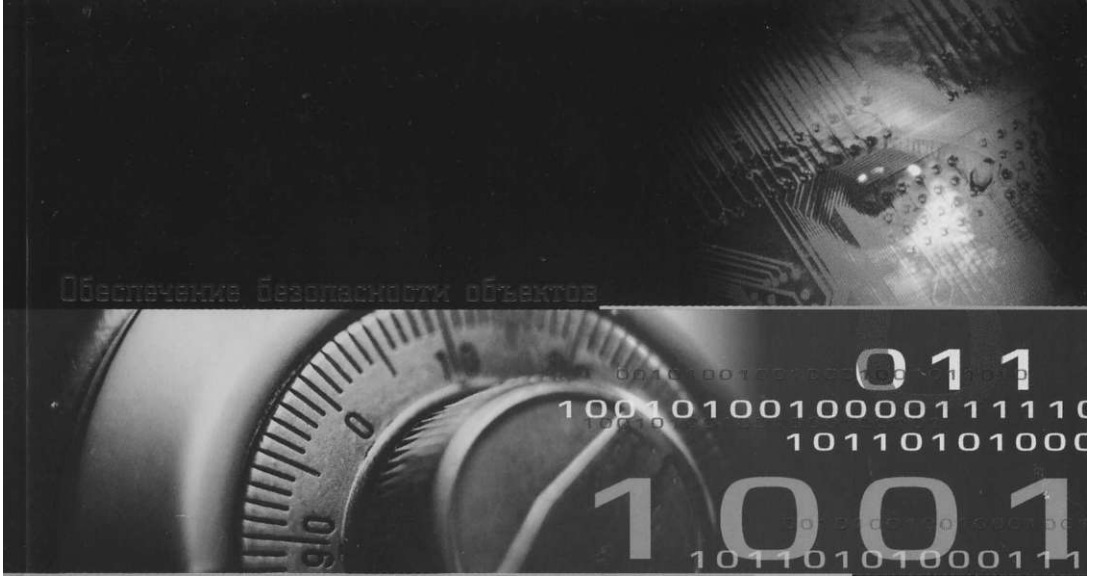


В. А. Ворона
В. А. Тихонов

Системы контроля и управления доступом

Горячая линия–Телеком

Обеспечение безопасности объектов

В. А. Ворона
В. А. Тихонов

Системы контроля и управления доступом

Москва
Горячая линия - Телеком
2010

УДК 004.78:681.139.3
ББК 32.965
В83

Серия «Обеспечение безопасности объектов»; Выпуск 2.

Ворона В. А., Тихонов В. А.

В83 Системы контроля и управления доступом. - М.: Горячая линия-Телеком, 2010. - 272 е.: ил.

ISBN 978-5-9912-0059-2.

В книге изложен широкий круг вопросов, связанных с организацией контрольно-пропускного режима на различных объектах и применением систем контроля и управления доступом (СКУД). Большое внимание уделено средствам идентификации и аутентификации. Описаны устройства идентификации (считыванием) различных типов; средства биометрической аутентификации личности и особенности их реализации; различные виды контроллеров и исполнительные устройства СКУД. Приведен обзор различных вариантов реализации СКУД. Даны основные рекомендации по выбору средств и систем контроля доступа. В приложении приведены ключевые выдержки из официальных нормативных материалов связанных с использованием СКУД .

Для специалистов в области создания и применения систем защиты объектов, руководителей и сотрудников служб безопасности, а также студентов учебных заведений и слушателей курсов повышения квалификации.

ББК 32.848

Адрес издательства в Интернет WWW.TECHBOOK.Ril

Справочное издание

Ворона Владимир Андреевич
Тихонов Виктор Алексеевич

Системы контроля и управления доступом

Редактор И. Н. Андреева
Обложка художника Ii. Г. Ситникова
Компьютерная верстка II. И. Дмитриевой

Подписано в печать **28.06.08.** Форма! **й0хУ0**/1(>.! 1cчaiь офсспми
Уч.-изд.л. **17.** Тираж **1000эт. (1-йзамвЗОО НО) lIii.V-sw к п М З**
ООО «Научно-техническое издательство -1 причли линия 1 ICKOM–

ISBN 978-5-9912-0059-2

ВВЕДЕНИЕ

Защита любого объекта включает несколько рубежей, число которых зависит от уровня режимности объекта. При этом во всех случаях важным рубежом будет система управления контроля доступом (СКУД) на объект.

Хорошо организованная с использованием современных технических средств СКУД позволит решать целый ряд задач. К числу наиболее важным можно отнести следующие:

- противодействие промышленному шпионажу;
- противодействие воровству;
- противодействие саботажу;
- противодействие умышленному повреждению материальных ценностей;
- учет рабочего времени;
- контроль своевременности прихода и ухода сотрудников;
- защита конфиденциальности информации;
- регулирование потока посетителей;
- контроль въезда и выезда транспорта.

Кроме этого, СКУД является барьером для «любопытных».

При реализации конкретных СКУД используют различные способы и реализующие их устройства для идентификации и аутентификации личности.

Следует отметить, что СКУД являются одним из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом. По данным ряда экспертов ежегодный прирост рынка СКУД составляет более 25 %. Число специалистов, работающих в сфере технических систем безопасности, превысило 500 тыс. человек.

В качестве наиболее часто используемых СКУД можно назвать такие:

- турникеты обычные и настенные;
- турникеты для прохода в коридорах;
- шлюзовые кабины;
- автоматические калитки;
- роторные турникеты;
- вращающиеся двери;
- дорожные блокираторы;
- шлагбаумы;
- парковочные системы;
- круглые раздвижные двери;
- трехштанговые турникеты;
- полноростовые турникеты;
- раздвижные турникеты.

Очень важным является вопрос о возможности интеграции СКУД с любой системой безопасности с использованием открытого протокола.

Важной особенностью рынка СКУД является то, что потребители стали покупать более дорогие исполнительные устройства, причем иностранного производства. Другой особенностью современных СКУД является внедрение технологии смарт-карты, вместо классических проксимити-карт, технологии дальней идентификации (частоты 800-900 МГц и 2,45 ГГц).

Следует отметить, что в настоящее время нормативная база в области СКУД разработана недостаточно полно. К числу основных документов можно отнести отечественные стандарты: ГОСТ 51241-98, ГОСТ 26342-89, ГОСТР 50009, ГОСТ 12.2.007.0, ГОСТ 12.2.004, а также международные стандарты серии ИСО 9000, DIN 14661, DIN 50050, IP 30, EN 50065, VDE 0833, VDSG 29023, VDSG 28523, BSI, VDS, UL, SEV и др.

По требованиям стандарта ISO 9000 Госстандарт России ряду СКУД выдал сертификат соответствия US 561839.

1. ОБЩАЯ ХАРАКТЕРИСТИКА СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Как уже говорилось выше, любая СКУД предназначена для того, чтобы автоматически пропускать тех, кому этот вход разрешен, и не пропускать тех, кому вход запрещен. Все ее остальные функции (сохранность материальных ценностей, контроль и учет рабочего времени и др.) вытекают из основного предназначения.

В общем случае под СКУД обычно понимают совокупность программно-технических и организационно-методических средств, с помощью которых решается задача контроля и управления помещением предприятия и отдельными помещениями, а также оперативный контроль за передвижением персонала и времени его нахождения на территории предприятия.

1.1. Организация контрольно-пропускного режима на предприятии

Для упорядочения допуска сотрудников и посетителей (клиентов), а также транспорта на территорию и в помещения охраняемого предприятия* организуется контрольно-пропускной режим (КПР) - комплекс организационно-правовых ограничений и правил, устанавливающих порядок пропуска через контрольно-пропускные пункты (КПП) в отдельные здания (помещения) людей, транспорта и материальных средств. КПР является одним из ключевых моментов в организации системы безопасности на предприятии. С этих позиций он представляет собой комплекс организационных мероприятий (административно-ограничительных), инженерно-технических решений и действий службы безопасности.

Механизм осуществления КПР основывается на применении «запретов» и «ограничений» в отношении субъектов, пересекающих границы охраняемых объектов, для обеспечения интересов предприятия. Такой механизм должен соответствовать требованиям действующего законодательства, уставу предприятия, а также иным нормативно-правовым актам, регулирующим деятельность предприятия. Основные направления создания КПР на предприятии: определение и оценка исходных данных, разработка мероприятий и нормативных документов, оборудование КПП. Система контроля и управления доступом является третьим рубежом защиты после системы видеонаблюдения и охранно-пожарной сигнализации.

** Здесь и далее под «предприятием» будем понимать ту или иную организацию независимо от формы собственности. Предприятие может состоять из объектов.*

1.1.1. Цели и задачи создания контрольно-пропускного режима

Основными целями создания КПР являются:

- защита законных интересов предприятия, поддержание порядка внутреннего управления;
- защита собственности предприятия, ее рациональное и эффективное использование;
- рост прибылей предприятия;
- внутренняя и внешняя стабильность предприятия;
- защита коммерческих секретов и прав на интеллектуальную собственность.

КПР как часть системы безопасности позволяет решить следующие задачи:

- обеспечение санкционированного прохода сотрудников и посетителей, ввоза/вывоза продукции и материальных ценностей, ритмичной работы предприятия;
- предотвращение бесконтрольного проникновения посторонних лиц и транспортных средств на охраняемые территории и в отдельные здания (помещения);
- своевременное выявление угроз интересам предприятия, а также потенциально опасных условий, способствующих нанесению предприятию материального и морального ущерба;
- создание надежных гарантий поддержания организационной стабильности внешних и внутренних связей предприятия, отработка механизма оперативного реагирования на угрозы и негативные тенденции;
- пресечение посягательств на законные интересы предприятия, использование юридических, экономических, организационных, социально-психологических, технических и иных средств для выявления и ослабления источников угроз безопасности предприятия.

КПР можно определить как систему обеспечения нормативных, организационных и материальных гарантий выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину, технологическое лидерство, научные достижения и охраняемую информацию и как совокупность организационно-правовых ограничений и правил, устанавливающих порядок пропуска через КПП сотрудников объекта, посетителей, транспорта ввоза/вывоза материальных ценностей.

Нормативные гарантии заключаются в толковании и реализации норм права, уяснении пределов их действия, в формировании необходимых правоотношений, определении и обеспечении правомерной деятельности подразделений и работников предприятия по поводу ее безопасности, использова-

ния ограничительных мер, применения санкций к физическим и юридическим лицам, посягающим на законные интересы предприятия.

Организационные гарантии формируются путем разработки, построения и поддержания высокой работоспособности общей организационной структуры управления процессом выявления и подавления угроз деятельности предприятия, использования эффективного механизма стимулирования его оптимального функционирования, а также соответствующей подготовки кадров.

Материальные гарантии формируются за счет выделения и использования финансовых, технических, кадровых, интеллектуальных, информационных и иных ресурсов предприятия, обеспечивающих своевременное выявление, ослабление и подавление источников угрозы, предотвращение и локализацию возможного ущерба, создание благоприятных условий для деятельности предприятия.

Основные мероприятия КПР разрабатываются службой безопасности предприятия, утверждаются его руководителем и оформляются инструкцией о КПР.

Ответственность за организацию КПР возлагается на начальника службы безопасности. Практическое осуществление КПР возлагается на охрану (дежурных по КПП, контролеров, охранников), работники которой должны знать установленные на объекте правила КПР, действующие документы по порядку пропуска на объект (с объекта) сотрудников и посетителей, ввоза/вывоза товарно-материальных ценностей.

КПР может быть установлен как в целом по предприятия, так и в отдельных корпусах, зданиях, отделах и других специальных помещениях.

1.1.2. Подготовка исходных данных для организации контрольно-пропускного режима

Разработка мероприятий и нормативных документов КПР начинается с определения исходных данных. Целесообразно предложить следующую последовательность определения и оценки исходных данных.

1. Организационная структура предприятия, расположение его отдельных элементов и характер производства (деятельности) на них. Выяснение этих вопросов позволяет решить следующие практические задачи:

- выделить объекты, площадки, здания и помещения, на которых необходимо организовать КПР;
- определить характер КПП для пропуска сотрудников и транспортных средств.

2. Оценка «суточного объема» потоков транспортных средств, грузов, материальных ценностей и людей (персонала фирмы и посетителей), проходящих через КПП и в отдельные здания (помещения). Только на основе оценки реального состояния мест пропуска можно оценить пропускную способность

действующих КПП и привести ее в соответствие с задачами объекта. Такая оценка позволит выбрать оптимальный вариант автоматизации и контроля прохода (проезда) на охраняемые территории.

3. Выделение (по степени важности) категории объектов, транспортных средств и грузов, а также категории лиц, пересекающих установленные границы. Для достижения четкости в определениях предлагается помещения и территорию объекта классифицировать в зависимости от условий доступа и степени защищенности.

Для организации пропускного режима также необходимо распределить объекты предприятия (здания, помещения) на следующие зоны: общедоступные, закрытые и ограниченного доступа. Определение категорий режима может дать четкий ответ на вопросы, которые нужно прояснить при организации КПР и разработке исходной документации по оборудованию объекта техническими средствами охраны. Закрепление за помещением конкретной категории помогает регламентировать и обосновать:

- условия доступа сотрудников предприятия и посетителей в ту или иную зону,
- предложения администрации предприятия по выработке оптимального варианта порядка пропуска лиц, транспортных средств и материальных ценностей на объекты предприятия;
- наличие и вид физической охраны;
- виды используемых технических средств для обеспечения безопасности.

1.1.3. Разработка инструкции о пропускном режиме

Оценивая исходные данные, разработчик определяет основные положения инструкции о КПР..

ППрактическое решение вопросов, связанных с организацией пропускного режима, оформляется в виде «Инструкции о пропускном режиме». Указанная инструкция должна определять систему организационно-правовых охранных мер, устанавливающих разрешительный порядок (режим) прохода (проезда) на предприятие (с предприятия), и может включать следующие шесть разделов:

1. Общие положения.
2. Порядок прохода через КПП предприятия.
3. Порядок въезда (выезда) транспортных средств и провоза материальных ценностей.
4. Виды пропусков и порядок их оформления.
5. Обязанности должностных лиц по поддержанию КПР.
6. Учет и отчетность, порядок хранения пропусков, печатей.

В разделе *общие положения* указываются:

- нормативные документы, на основании которых составлялась инструкция,

- определение КПР и цель его введения,
- должностные лица, на которых возлагается организация и практическое руководство контрольно-пропускной системой;
- санкции к нарушителям КПР;
- требования к оборудованию различных помещений.

Второй раздел определяет *порядок пропуска сотрудников предприятия, командированных лиц и посетителей через КПП.* В этом разделе рекомендуется:

- перечислить все КПП и их назначение, описание, расположение и единую нумерацию;
- изложить требования к оборудованию КПП;
- установить порядок прохода сотрудников и посетителей на территорию предприятия и в его категорированные помещения;
- определить права и основные обязанности контролеров КПП;
- установить помещения, где запрещается принимать посетителей и представителей сторонних организаций.

Третий раздел определяет *порядок допуска на предприятие транспортных средств, ввоза/вывоза продукции, документов и материальных ценностей.* В этом разделе указываются:

- порядок допуска на территорию объекта (с объекта) предприятия автотранспорта, принадлежащего данному предприятию;
- порядок въезда и стоянки на территории объектов транспорта, принадлежащего сотрудникам на правах личной собственности;
- порядок пропуска автомашин сторонних организаций, прибывших с грузом в адрес объекта в рабочее и нерабочее время;
- порядок ввоза/вывоза товарно-материальных ценностей;
- правила оформления документов на вывоз (вынос) материальных ценностей с территории объектов предприятия.

В четвертом разделе определяются:

- виды пропусков, их количество и статус;
- описание пропусков;
- порядок оформления и выдачи пропусков;
- порядок замены и перерегистрации пропусков;
- мероприятия, проводимые при утрате пропуска сотрудником.

В пятом разделе подробно описываются *обязанности должностных лиц по поддержанию КПР* как в нормальном режиме, так и при возникновении чрезвычайных ситуаций (ЧС).

Шестой раздел посвящается учету и отчетности документации, ведущейся на КПП, и порядку хранения пропусков и печатей.

При разработке инструкции о КПР определяются виды и группы пропусков, которые будут действовать на предприятии. На крупных предприятиях,

как правило, устанавливается несколько видов пропусков. Это могут быть постоянные, временные, разовые и материальные пропуска. Образцы бланков пропусков разрабатываются администрацией объекта (службой безопасности). По своему внешнему виду и содержанию пропуска должны отличаться друг от друга и обладать некоторыми степенями защиты. Все виды пропусков, за исключением материальных, оформляются и выдаются бюро пропусков (или иным подразделением) по письменным заявкам. Виды пропусков определяются в зависимости от специфики предприятия. Материальные пропуска для вывоза (выноса) товарно-материальных ценностей выдаются администрацией предприятия. Срок действия пропуска определяется инструкцией о КПР. Материальные пропуска должны изыматься на КПП и сдаваться в бюро пропусков. Образцы действующих пропусков должны находиться на КПП. Для обучения работников охраны выделяется необходимое число образцов пропусков.

Устанавливая и обеспечивая порядок перемещения персонала и посетителей по территории предприятия, система КПР решает не только вопросы безопасности предприятия, но и вопросы рациональной организации труда.

В контрольно-пропускном зале устраиваются проходы, которые оборудуются техническими средствами охраны и физическими барьерами. В комплект оборудования, как правило, входят:

- средства механизации, автоматизации системы контроля доступа;
- физические барьеры (ограждения, турникеты, калитки);
- основное и резервное освещение;
- средства связи и тревожной сигнализации;
- системы видеоконтроля.

Турникеты предназначены для управления потоками людей и регулирования входа (выхода). В качестве средств контроля доступа могут использоваться различные турникеты. В последнее время наиболее широкое распространение получили электромеханические турникеты, которые в отличие от громоздких и неудобных в управлении механических легко управляются с пульта охранника и могут работать в составе автоматизированной системы контроля доступа. Для осуществления надежного контроля чаще используются «нормально закрытые» турникеты: роторные турникеты-вертушки, турникеты-триподы и калитки.

Калитки применяются для управления потоками людей, организации свободного прохода в одну сторону (на вход или выход) и запрета прохода в другую. Калитки широко используются в магазинах, аэропортах, вокзалах. Применение калиток для контроля доступа неэффективно, это связано с тем, что калитки не разделяют поток людей по одному, так как после открытия калитки через нее могут пройти несколько человек. Калитки могут устанавливаться для организации свободного выхода, в то время как контроль входа доверяют триподам или вертушкам.

Турникеты-триподы с тремя преграждающими планками являются одним из наиболее оптимальных средств для осуществления контроля санкционированного прохода. Триподы имеют современный элегантный вид и легко монтируются. Триподы позволяют осуществлять эффективный контроль доступа, так как разделяют поток людей по одному, обеспечивая при этом высокую пропускную способность. Триподы могут применяться в системах электронных проходных, в том числе в условиях большого потока людей. Для предотвращения возможности подлезть под планки турникета или перепрыгнуть через них на турнике рекомендуется устанавливать специальные датчики, которые срабатывают при попытке несанкционированного прохода.

Роторные турникеты-вертушки применяются в тех случаях, когда необходимо полное перекрытие зоны прохода. Они могут быть различными по высоте - от поясных до турникетов в полный рост.

Для организации въезда (выезда) транспорта создаются **транспортные** КПП. В состав транспортного КПП входит досмотровая площадка и служебные помещения.

Контрольно-проездные пункты для пропуска авто- и железнодорожного транспорта оборудуются:

- раздвижными или распашными воротами и шлагбаумами с механическим, электромеханическим и гидравлическим приводами, а также устройствами для аварийной остановки ворот и открывания их вручную,
- контрольными площадками с помостами для просмотра автомобилей;
- светофорами, предупредительными знаками и световыми табло типа «Берегись автомобиля» и др.;
- телефонной и тревожной связью и освещением для осмотра транспорта.

Досмотровая площадка предназначена для размещения автомобилей при их досмотре. Досмотровые площадки могут располагаться как на территории предприятия, так и за ее пределами, на территории, непосредственно примыкающей к основным воротам КПП.

Досмотровая площадка должна отвечать следующим требованиям:

- иметь достаточную площадь для размещения досматриваемого транспорта и технических средств для обеспечения нормальных условий работы охраны;
- исключать возможность несанкционированного проникновения на объект (с объекта) людей и транспортных средств,
- обеспечивать при установленной интенсивности движения в любое время суток и года досмотр автомобильного транспорта и перевозимых грузов;
- быть изолированной от других сооружений, не имеющих отношения к охране объекта и оборудованию КПП;
- обеспечивать меры безопасности охраны при выполнении обязанностей.

Размеры досмотровой площадки могут составлять: 10-12 м в длину и 5-6 м в ширину. На проезжей части площадки выделяется место остановки транспорта для досмотра, ограниченное двумя линиями «СТОП», выполненными белой краской Транспортные КПП могут оборудоваться светофорами, весами для взвешивания автомобилей, досмотровой ямой или эстакадой для осмотра грузов, механизированными устройствами для автоматического открытия и закрытия ворот с фиксаторами.

Электромеханическое оборудование КПП для автомобильного транспорта обычно содержит: электродвигатели, привод ворот; концевые выключатели автоматического отключения электродвигателей при полностью закрытых и открытых створках ворот, магнитные пускатели электродвигателей, электрооборудование светофоров; кабельные, силовые линии.

Досмотровые площадки по периметру оборудуются физическими барьерами и рубежом сигнализации. Площадки, как правило, загораживаются просматриваемым забором из металлической сетки или декоративных решеток

высотой до 2,5 м. На площадке оборудуются основные и вспомогательные механизированные ворота. Основные ворота устанавливаются на линии основного ограждения объекта, а вспомогательные - на противоположной стороне досмотровой площадки. Вместо ворот могут применяться механизированные шлагбаумы. На автомобильных КПП используются ворота с ограничением и без ограничения габаритов по высоте. По конструкции они могут быть распашными или раздвижными (выдвижными). Распашные ворота должны оборудоваться фиксаторами Для регулирования движения транспорта, проходящего через проезды досмотровых площадок КПП, могут применяться двухсекционные светофоры с линзами красного и зеленого цвета.

1.2. Назначение, классификация и состав СКУД

Рассмотрим более подробно, что же представляет собой современная система контроля и управления доступом (СКУД). Будем понимать под СКУД объединенные в комплексы электронные, механические, электротехнические, аппаратно-программные и иные средства, обеспечивающие возможность доступа определенных лиц в определенные зоны (территория, здание, помещение) или к определенной аппаратуре, техническим средствам и предметам (персональный компьютер (ПК), автомобиль, сейф и т. д.) и ограничивающие доступ лицам, не имеющим такого права. Такие системы могут осуществлять контроль перемещения людей и транспорта по территории охраняемого объекта, обеспечивать безопасность персонала и посетителей, а также сохранность материальных и информационных ресурсов предприятия. Системы контроля и управления доступом используются на промышленных предприятиях, в офисах, магазинах, на автостоянках и автосервисах, в жилых помещениях.

Интерес к системам контроля и управления доступом растет еще и потому, что наличие такой системы важно для эффективной работы предприятия. Контроль не только существенно повышает уровень безопасности, но и позволяет оперативно реагировать на поведение персонала и посетителей. Также важной задачей для многих предприятий является необходимость контролировать график и вести учет рабочего времени. Особое внимание уделяется системам, позволяющим выстраивать необходимые конфигурации из стандартных блоков, учитывая все особенности предприятия.

Существующий *ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом» (прил. 1),* который устанавливает классификацию, общие технические требования и методы испытаний, подразделяет СКУД:

- по способу управления;
- числу контролируемых точек доступа;
- функциональным характеристикам;
- виду объектов контроля;
- уровню защищенности системы от несанкционированного доступа.

В соответствии с документом Р 78.36.005—99 [6] все СКУД делятся на четыре класса.

СКУД 1-го класса - малофункциональные системы малой емкости, работающие в автономном режиме и осуществляющие допуск всех лиц, имеющих соответствующий идентификатор. В такой системе используется ручное или автоматическое управление исполнительными устройствами, а также световая или/и звуковая сигнализация.

СКУД **2-го класса** - монофункциональные системы. Они могут быть одноуровневыми и многоуровневыми и обеспечивают работу как в автономном, так и в сетевом режимах. Допуск лиц (групп лиц) может осуществляться по дате, временным интервалам. Система способна обеспечить автоматическую регистрацию событий и автоматическое управление исполнительными устройства.

СКУД 3-го и 4-го классов, как правило, являются сетевыми. В них используются более сложные идентификаторы и различные уровни сетевого взаимодействия (клиент-сервер, интерфейсы считывателей карт Виганда или магнитных карт, специализированные интерфейсы и др.).

На сегодняшний день существует очень много разновидностей СКУД разных производителей, а также ее компонентов. Несмотря на уникальность каждой конкретной системы контроля доступа, она содержит 4 основных элемента: *идентификатор пользователя* (карта-пропуск, ключ), *устройство идентификации, управляющий контроллер* и *исполнительные устройства.* Общая схема СКУД показана на рис. 1.1. Основные понятия и определения, касающиеся терминологии, классификации и общих технических требований СКУД, приведены в прил. 1.

Рис. 1.1. Общая схема СКУД

Работу системы контроля и управления доступом можно в упрощенном виде описать следующим образом. Каждый сотрудник или постоянный посетитель организации получает идентификатор (электронный ключ) - пластиковую карточку или брелок с содержащимся в ней индивидуальным кодом. Электронные ключи выдаются в результате регистрации перечисленных лиц с помощью средств системы. Паспортные данные, фото (видеоизображение) и другие сведения о владельце электронного ключа заносятся в персональную электронную карточку. Персональная электронная карточка владельца и код его электронного ключа связываются друг с другом и заносятся в специально организованные компьютерные базы данных.

У входа в здание или в подлежащее контролю помещение устанавливаются считыватели, которые считывают с карточек их код и информацию о правах доступа владельца карты и передают эту информацию в контроллер системы.

В системе каждому коду поставлена в соответствие информация о правах владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует двери (замки, турникеты), переводит помещение в режим охраны, включает сигнал тревоги и т. д. Все факты предъявления карточек и связанные с ними действия (проходы, тревоги и т. д.) фиксируются в контроллере и сохраняются в компьютере. Информация о событиях, вызванных предъявлением карточек, может быть использована в дальнейшем для получения отчетов по учету рабочего времени, нарушениям трудовой дисциплины и др. На предприятиях можно выделить четыре характерные точки контроля доступа: проходные, офисные помещения, помещения особой важности, и въезд/выезд автотранспорта.

В зависимости от способа проверки принято различать несколько видов СКУД:

- ручные (определение подлинности личности осуществляется контролером на основе предъявляемого пропуска с фотографией владельца);
- механизированные (фактически та же ручная проверка с элементами автоматизации хранения и предъявления пропусков);
- автоматизированные (идентификация пользователя и проверка личностных атрибутов осуществляется электронным автоматом, а аутентификация и принятие решения о предоставлении доступа производится оператором КПП,
- автоматические (вся процедура проверки и принятия решения осуществляется компьютером).

Набор функций, выполняемых комплексными системами, дает возможность использовать систему контроля для выполнения различных контрольных задач на объекте. В зависимости от стоящей задачи можно выбрать соответствующую систему контроля и управления доступом. *Небольшая СКУД* позволит предотвратить доступ нежелательных лиц, а сотрудникам точно указать те помещения, в которые они имеют право доступа. *Более сложная система* позволит, помимо ограничения доступа, назначить каждому сотруднику индивидуальный временной график работы, сохранить и затем просмотреть информацию о событиях за день. *Комплексные СКУД* позволяют решить вопросы безопасности и дисциплины, автоматизировать кадровый и бухгалтерский учет, создать автоматизированное рабочее место охранника.

При выборе структуры системы и ее аппаратуры необходимо уделять особое внимание тщательному анализу ее характеристик.

К основным характеристикам СКУД относятся:

- стоимость;
- надежность функционирования;
- быстродействие;
- время регистрации пользователя;
- емкость памяти;
- устойчивость к злонамеренным действиям;
- вероятность ошибочного отклонения законного пользователя (ошибки 1-го рода);
- вероятность ошибочного предоставления доступа незаконному пользователю (ошибки 2-го рода).

1.2.1. Идентификатор пользователя

Идентификатор пользователя - это устройство или признак, по которому определяется пользователь. Для идентификации применяются *атрибутные* и *биометрические* идентификаторы. В качестве атрибутных идентификаторов используют автономные носители признаков допуска: магнитные карточки, бесконтактные проксимити-карты, брелки «тач-мемори», различные радиобрелки, изображение радужной оболочки глаза, отпечаток пальца, отпечаток ладони, черты лица и многие другие физические признаки. Каждый идентификатор характеризуется определенным уникальным двоичным кодом. В СКУД каждому коду ставится в соответствие информация о правах и привилегиях владельца идентификатора. В настоящее время применяются:

- ***бесконтактные радиочастотные проксимити-карты (proxmity) -*** наиболее перспективный в настоящее время тип карт. Бесконтактные карточки срабатывают на расстоянии и не требуют четкого позиционирования, что обеспечивает их устойчивую работу и удобство использования, высокую пропускную способность;
- ***магнитные карты -*** наиболее широко распространенный вариант. Существуют карты с низкокоэрцитивной и высококоэрцитивной магнитной полосой и с записью на разные дорожки;
- ***карты Виганда (Wiegand)*** - названные по имени ученого, открывшего магнитный сплав, обладающий прямоугольной петлей гистерезиса;
- ***штрих-кодовые карты -*** на карту наносится штриховой код. Существует более сложный вариант - штрих-код закрывается материалом, прозрачным только в инфракрасном свете, считывание происходит в ИК-области;
- ***ключ-брелок «тач-мемори» (touch-memory) -*** металлическая таблетка, внутри которой расположен чип ПЗУ.

Пропуска (идентификаторы) пользователей СКУД могут иметь различный статус. Для обеспечения большинства необходимых в реальной жизни требо-

ваний, как минимум, надо, чтобы контроллеры поддерживали следующие типы карт:

- постоянная: для сотрудников предприятия;
- временная: с ограничением срока действия;
- «-разовая: автоматически аннулируемая после исчерпания числа проходов;
- одноразовая - частный случай и-разовой карты

1.2.2. Контроллеры

Контроллеры - устройства, предназначенные для обработки информации от считывателей идентификаторов, принятия решения и управления исполнительными устройствами. Именно контроллеры разрешают проход через пропускные пункты. Контроллеры различаются емкостью базы данных и буфера событий, обслуживаемых устройств идентификации.

Любой контроллер СКУД состоит из четырех основных частей (рис. 1.2): считывателя, схем обработки сигнала, принятия решения и схемы буфера событий.

Рис. 1.2. Схема контроллера СКУД

Считыватель карт (устройство индификации) передает информацию на схему обработки сигналов контроллера. Далее информация в цифровом виде выдается на схему принятия решения, которая заносит факт попытки прохода в схему буфера событий, запрашивает схему базы данных на предмет правомочности прохода и в случае положительного ответа приводит в действие исполнительное устройство. Ограничение уже снято, но система контроля доступа ещё не завершила обработку информации: сам факт прохода именно этого человека заносится в схему буфера событий.

По способу управления (возможности объединения) контроллеры СКУД делятся на три класса: *автономные, сетевые* (централизованные) и *комбинированные.*

Независимо от типа применяемых считывателей контроллеры должны поддерживать следующие режимы доступа:

- по одной карте и/или ПИН-коду;
- доступ с подтверждением оператором;
- контроль количества людей в помещении (минимум и максимум).

Последнее важно в ситуациях когда, например, по условиям службы в заданном помещении не должно оставаться менее одного (двух, трех) человек.

Основу современных СКУД составляют автоматические и автоматизированные СКУД. В них процедура проверки может включать также сопоставление лица проверяемого с видеопортретом на мониторе контролера. Современные автоматические и автоматизированные СКУД в зависимости от способа управления подразделяются на ***автономные, сетевые*** (централизованные) и ***распределенные*** (комбинированные)

Автономные контроллеры - полностью законченные устройства, предназначенные для обслуживания, как правило, одной точки прохода. Возможность объединения с другими аналогичными контроллерами не предусмотрена. Существует много видов таких устройств: контроллеры, совмещенные со считывателем, контроллеры, встроенные в электромагнитный замок и т. д. В автономных контроллерах применяются считыватели самых разных типов. Как правило, автономные контроллеры рассчитаны на обслуживание небольшого числа пользователей, обычно не более 500 человек. Они работают с одним исполнительным устройством без передачи информации на центральный пункт охраны и без контроля со стороны оператора. Примером подобной системы контроля доступа может служить достаточно простая комбинация: «электромагнитный замок + считыватель карт идентификации». Если необходимо контролировать только одну дверь и в будущем расширение системы контроля доступа не планируется, это оптимальное и достаточно недорогое решение.

Сетевые контроллеры могут работать в сети под управлением компьютера. В этом случае решение принимает персональный компьютер с установленным специализированным программным обеспечением. Сетевые контроллеры применяются для создания СКУД любой степени сложности. Число сетевых контроллеров в системе может быть от двух до нескольких сотен с обменом информацией с центральным пунктом охраны и контролем, управлением системой со стороны дежурного оператора. В этом случае размеры системы контроля доступа опередяются по числу устройств дентификации, а не по числу контролируемых дверей, поскольку на каждую дверь может быть установлено одно-два устройства идентификации в зависимости от применяемой технологии прохода.

Используя сетевые контроллеры, администрация получает ряд дополнительных возможностей:

- получение отчета о присутствии или отсутствии сотрудников на работе;

- уточнение местонахождения конкретного сотрудника;
- ведение табеля учета рабочего времени;
- составление отчета о перемещении сотрудников практически за любой период времени;
- формирование временных графиков прохода сотрудников;
- ведение базы данных сотрудников (электронной картотеки).

Сетевые СКУД используются на крупных предприятиях и в тех случаях, если нужны ее специфические возможности, такие, как учет рабочего времени сотрудников. Сетевые контроллеры объединяются в сеть.

К базовым характеристикам сетевых контроллеров относят следующие количественные характеристики:

- число поддерживаемых точек прохода;
- объем базы данных пользователей,
- объем буфера событий.

Число поддерживаемых точек прохода. Оптимальное решение в этом случае следующее: один сетевой контроллер на две точки прохода, так как общие ресурсы (корпус, источник питания с аккумулятором) требуются в меньшем количестве. Контроллеры с большим числом обслуживаемых дверей существуют, но их немного по следующим причинам:

- высокая стоимость источника питания на 4-5 А с резервированием;
- увеличивается стоимость коммуникаций между контроллером и дверьми. Кроме того, если двери расположены далеко друг от друга, то становится проблемой и прокладка провода питания замка, так как при токах потребления около 1 А возникают большие потери.

Объем базы данных пользователей определяется исключительно количеством людей, которые будут ходить через максимально напряженную точку прохода (проходную).

Объем буфера событий определяет, сколько времени сетевая система сможет работать при выключенном (зависшем, сгоревшем) компьютере, не теряя информации о событиях. Например, для офиса с числом сотрудников порядка 20 человек объема буфера событий, равного 1000, может хватить на неделю. А для заводской проходной, через которую проходит 3 тыс. человек, и буфера на 10 тыс. событий с трудом хватит на сутки.

Практически все контроллеры поддерживают интерфейс Виганда, и практически все типы считывателей, в том числе и биометрические, поддерживают это формат.

Современный контроллер доступа должен поддерживать гибкую систему временных расписаний, на основе которых принимается решение о доступе того или иного человека. При этом стандартные недельные циклы с выходными днями - это самое простое решение. Реально еще требуется задавать праздники, рабочие дни в праздники, а самое главное различные «плавающие» графики по типу «сутки через трое» и т. п В профессиональном кон-

троллере временные расписания могут управлять не только доступом пользователей, но и автоматически открывать и закрывать двери в заданное время, ставить на охрану и снимать помещение с охраны (при наличии охранных функций), переключать дополнительные реле.

Комбинированные контроллеры совмещают функции сетевых и автономных контроллеров. При наличии связи с управляющим компьютером (онлайн) контроллеры работают как сетевые устройства при отсутствии связи - как автономные.

Смежные функции контроллеров. В первую очередь это функции поддержки охранно-пожарной сигнализации, интеграции с подсистемами телеНаблюдения и управления некоторыми функциями оповещения и пожаротушения. озможна также поддержк локальных компьютерных сетей с различными рабочими станциями и правами доступа, передачи информации через Интернет. В большинстве классических систем доступа эти функции отсутствуют. Однако в СКУД Apollo для этих целей имеются специализированные модули В других системах поддержка функций охранно-пожарной сигнализации может достигаться за счет интеграции с оборудованием третьих производителей.

1.2.3. Устройства идентификации личности (считыватели)

Для идентификации личности современные электронные системы контроля доступа используют устройства нескольких типов в зависимости от применяемого вида идентификатора пользователя. В литературных источниках, посвященных описанию различных СКУД, часто можно встретить подмену понятия аутентификация, понятием верификация. Это связано, по-видимому, со следующим:

1) в науке существует понятие «верификация» *(от лат.* verus - истинный и facio - делаю), которое означает проверку, эмпирическое подтверждение теоретических положений науки путем сопоставления их с наблюдаемыми объектами, тактильными данными, экспериментом;

2) в программировании и информатике существует понятие «аутентификация пользователя», которое означает проверку соответствия пользователя терминала в сети ЭВМ предъявленному идентификатору (применяется для защиты от несанкционированного доступа и выбора соответствующего режима обслуживания);

3) в программировании существует также понятие «верификация», которое означает формальное доказательство правильности программы, а также контроль, проверку вводимых оператором данных.

Таким образом, существует некоторое пересечение в определениях, связанное с использованием слов «проверка» и «подтверждение». Отсюда перенос названных терминов в другую предметную область (СКУД), очевидно,

носит достаточно условный характер. Они означают установление подлинности личности (объекта). Допуск осуществляется при непосредственном «физическом контакте» с пользователем в процессе идентификации и аутентификации его личности. *Идентификация* - это процедура опознания объекта (человека-пользователя) по предъявленному идентификатору, установление тождества объекта или личности по совокупности общих и частных признаков. В отличие от идентификации *аутентификация* подразумевает установление подлинности личности на основе сообщаемых проверяемым субъектом сведений о себе. Такие сведения называют идентификационными признаками.

Устройства идентификации (считыватели) расшифровывают информацию, записанную на карточках или ключах других типов, и передают ее в контроллер чаще в виде цифровой последовательности. Считыватели карточек доступа могут быть *контактные и бесконтактные.* Возможны следующие способы ввода признаков:

- ручной, осуществляемый путем нажатия клавиш, поворота переключателей и т. д.;
- контактный - в результате непосредственного контакта между считывателем и идентификатором;
- дистанционный (бесконтактный) при поднесении идентификатора к считывателю на определенное расстояние.

Для съема информации о биологических признаках человека используют специальные биометрические считыватели (терминалы), а ввод ПИН-кода осуществляется с клавиатур различных типов

Именно считыватели определяют внешний вид и основные эксплуатационные характеристики всей системы. Рассмотрим принципы их работы.

Кнопочные клавиатуры. Принцип действия достаточно ясен: если набранный на клавиатуре код доступа верен, то проход на защищаемую территорию разрешен. Кодонаборные устройства иногда совмещаются со считывателем карт, в этом случае код служит для подтверждения факта санкционированного использования карты.

Считывали штрих-кодов в настоящий момент практически не устанавливаются в системы контроля доступа, поскольку подделать пропуск чрезвычайно просто на принтере или на копировальном аппарате.

Считыватели магнитных карт. Основным элементом считывателя магнитных карт является магнитная головка, аналогичная магнитофонной. Код идентификации считывается при передвижении карты с магнитной полосой.

Основные достоинства таких идентификаторов:

- стоимость считывателей и магнитных карт достаточно низка;
- возможно изменение кода магнитной карты с помощью кодировщика.

Основные недостатки:

- защищенность от несанкционированного доступа невелика, поскольку нарушитель, завладев на весьма ограниченное время чужой картой, может подделать столько ее дубликатов, сколько ему нужно;
- считыватели магнитных карт достаточно ненадежны в эксплуатации: магнитные головки со временем засоряются и смещаются;
- низкая пропускная способность такой системы контроля доступа, поскольку зачастую приходится идентифицировать магнитную карту несколько раз;
- карты с магнитной полосой требуют весьма бережного хранения, необходимо избегать воздействия электромагнитных полей.

По указанным причинам сложные системы контроля доступа достаточно редко комплектуются подобными устройствами идентификации личности. Магнитные карты метро - исключение из правила, что объясняется дешевизной технологии.

Считыватели бесконтактных карт (интерфейс Виганда). Считыватель представляет собой индукционную катушку с двумя магнитами, которая находится в пластиковом или металлическом корпусе и для полной герметичности залита специальным изоляционным материалом. При проведении пластиковой карты через считыватель система контроля доступа получает бинарный код карты. Считывание ведется бесконтактным индукционным методом.

Основные достоинства:

- высокая надежность благодаря простоте устройства;
- невозможность подделки пластиковой карты, так как отсутствует информация о структуре;
- высокая устойчивость пластиковой карты к внешним воздействиям: чтобы испортить карту, ее необходимо сломать.

Считыватели проксимити-карт Такие карты позволяют производить дистанционную идентификацию личности. Внутри считывателя находится приемо-передающая антенна и электронная плата обработки сигналов.

Считыватели ключей «тач-мемори». Считыватель «тач-мемори» крайне прост и представляет из себя фактически контактную площадку, предназначенную для прикосновения специальных ключей. Ключ «тач-мемори» представляет собой специальную микросхему, размещенную в цилиндрическом корпусе из нержавеющей стали.

Сравнение различных технологий идентификации личности, наиболее распространенных в современных системах контроля доступа, производится по наиболее важным для потребителя параметрам. Достоинства и недостатки различных технологий идентификации приведены в табл. 1.1.

Таблица 1.1. Достоинства и недостатки различных технологий идентификации

Параметр	*Интерфейс Виганда*	*Проксимити-технология*	*Магнитные карты*
Затраты на эксплуатацию считывателя	-	Низкие	Высокие
Скрытность кода	Высокая	Средняя	Низкая
Время жизни карты	Большое	Большое	Малое
Время жизни считывателя	Большое	Среднее	Малое
Влияние электромагнитных полей	-	Высокое	Высокое
Стоимость инсталляции	Средняя	Высокая	Низкая
Стоимость эксплуатации	Низкая	Средняя	Высокая
Возможность изменения кода	-	-	Имеется
Пропускная способность	Средняя	Высокая	Низкая

Из сравнения различных технологий идентификации личности можно сделать следующие выводы:

- системы контроля доступа, использующие магнитные карты, не получили широкого распространения;
- наиболее практичной является технология, использующая интерфейс Виганда;
- в тех случаях, когда надо обеспечить высокую пропускную способность, скрытность места установки считывателя или необходимость дистанционного доступа наиболее целесообразно применять прокимити-технологию;
- в целях расширения области применения системы контроля доступа должны содержать в себе комплекс, совместно использующий интерфейс Виганда и проксимити-технологию.

Наименее защищенными от фальсификации считаются магнитные карточки, наиболее защищенными - карты Виганда и проксимити. Карты Виганда имеют высокие надежность и устойчивость к внешним воздействиям, невысокую стоимость считывателя и карт, которые практически невозможно подделать.

Биометрические считыватели. Проблема исключения подделки и кражи идентификаторов решается путем использования индивидуальных признаков человека - биометрических идентификаторов: отпечатков пальцев, геометрии кисти руки, рисунка радужной оболочки и кровеносных сосудов сетчатки глаза, теплового изображения лица, динамики подписи, спектральных характеристик речи.

Диапазон проблем, решение которых может быть найдено с использованием этих новых технологий, чрезвычайно широк:

- предотвратить проникновение злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;

- ограничить доступ к информации и обеспечить персональную ответственность за ее сохранность;
- обеспечить допуск к ответственным объектам только сертифицированных специалистов;
- избежать накладных расходов, связанных с эксплуатацией систем контроля доступа (карты, ключи);
- исключить неудобства, связанные с утерей, порчей или элементарным забыванием ключей, карт, паролей;
- организовать учет доступа и посещаемости сотрудников.

В настоящее время известен ряд технологий, которые могут быть задействованы в системах безопасности для идентификации личности по отпечаткам пальцев (как отдельных, так и руки в целом), чертам лица (на основе оптического и инфракрасного изображений), радужной оболочке глаз, голосу и другим характеристикам.

Все биометрические технологии имеют общие подходы к решению задачи идентификации, хотя все они различаются удобством применения и точностью результатов. Любая биометрическая технология применяется поэтапно:

- сканирование объекта;
- извлечение индивидуальной информации;
- формирование шаблона;
- сравнение текущего шаблона с базой данных.

Весьма важным является вопрос о пропускной способности биометрической системы контроля доступа. Поскольку объем данных, анализируемых считывателем, весьма велик, то даже простой перебор базы данных происходит достаточно долго. Чтобы уменьшить время анализа, биометрические считыватели имеют обычно дополнительно встроенную клавиатуру, на которой пользователь набирает свой личный код доступа и только после этого приступает к процессу биометрической идентификации. Преимущество биометрической системы контроля доступа заключается также в том, что идентифицируется не предмет (ключ «тач-мемори», проксимити-карта), а сам человек. Используемая характеристика неразрывно связана с ним - «биометрический паспорт» невозможно потерять, передать или забыть дома.

1.2.4. Исполнительные устройства

Среди исполнительных устройств контроля доступа наиболее распространены следующие запорные или управляемые преграждающие устройства: замки, защелки, турникеты (поясные, полноростные, «билетные», раздвижные, вращающиеся трех или четырехштанговые) и шлюзовые кабины (тамбурного типа, ротанты, шлагбаумы), автоматические ворота (распашные ворота, сдвигающиеся ворота, складывающиеся ворота, рулетные ворота), лифты.

В современных СКУД применяются в основном электромагнитные и электромеханические замки. Шлюзовые кабины тамбурного типа (2 поворотные двери) имеют пропускную способность от 8 до 12 человек в минуту. Гораздо выше пропускная способность шлюзов-ротантов, в которых используется только одна поворотная дверь.

Дверные замки и защелки. Принцип действия, который используется в электромеханических замках и защелках, весьма прост: при подаче на их специальные контактные клеммы напряжения (обычно в диапазоне 9-16 В) электромагнитное реле притягивает стопор механического устройства, предоставляя возможность открыть дверь.

Мощные штыревые электромеханические замки сейфового типа при подаче напряжения на специальный электромотор осуществляют вдвижение запорных штырей внутрь На строящихся объектах целесообразно использовать именно электромеханические замки, а при необходимости быстро установить систему контроля доступа на действующем объекте лучше применять электромеханические защелки, которые позволяют использовать уже существующие механические замки.

Электромагнитные замки состоят из электромагнита, прикрепляющегося к дверной коробке, и ответной металлической пластины, монтируемой на двери. В дежурном режиме на обмотку электромагнита подается постоянный ток удержания, вызывающий сильное магнитное поле, которое притягивает металлическую пластину двери, удерживая ее в закрытом состоянии. При подаче сигнала на специальный вход устройства магнитное поле исчезает, и дверь может быть открыта.

Все электромагнитные замки характеризуются максимальной механической нагрузкой удержания, которая измеряется в килограммах и может доходить до 1 ООО кг.

Вместе с дверными замками всегда должны использоваться и доводчики, возвращающие дверь в исходное положение.

Преимущество электромагнитных замков - небольшой, по сравнению с электромеханическими замками, потребляемый ток и отсутствие импульсных выбросов напряжения при открывании. Отрицательная сторона - большие размеры, унылый промышленный дизайн и полная зависимость от наличия электропитания.

Шлюзовые кабины. Шлюзовые кабины можно разделить на два основных типа, отличающихся устройством, пропускной способностью и ценой: шлюзовые кабины тамбурного типа и шлюзы-ротанты.

Шлюзовая кабина тамбурного типа представляет собой замкнутую систему двух зависимых дверей. Основным свойством любой шлюзовой кабины (шлюза) является то, что в любой момент времени открыта только одна из двух дверей. Принцип действия устройства следующий: человек свободно открывает дверь 1 и входит в шлюз, после чего предъявляет системе контроля доступа свой идентификатор. Если доступ разрешен, - открывается

дверь 2, а дверь 1 блокируется в закрытом состоянии. Таким образом, гарантируется, что на защищаемую территорию попадет только авторизованный сотрудник. Пропускная способность шлюзовой кабины тамбурного типа находится в пределах от 8 до 12 человек в минуту.

Для повышения пропускной способности применяются *шлюзы-ротанты.* Принцип их действия аналогичен шлюзам тамбурного типа, но вместо двух обычных дверей используется одна поворотная дверь турникетного типа. Пропускная способность шлюза-ротанта составляет от 18 до 22 человек в минуту.

Для более надежной защиты от злоумышленников шлюзы в большинстве случаев комплектуются системами взвешивания для дополнительного контроля количества людей внутри кабины и встроенными металлодетекторами для контроля проноса оружия. Стены кабины могут быть из стали или бронестекла.

Турникеты. Турникеты систем контроля доступа также можно разделить на два типа: поясные и полноростовые. Принцип работы турникета достаточно хорошо известен: если запрос на доступ правомерен, то механическая система, поворачиваясь, открывает проход на охраняемую территорию.

Турникеты поясные оставляют возможность для перепрыгивания, поскольку, как и следует из их названия, заградительный барьер доходит только до пояса человека, поэтому их целесообразно ставить только рядом с постом охраны.

Турникеты полноростовые можно устанавливать в удаленных от поста охраны местах и использовать в полностью автоматическом режиме работы.

Автоматические шлагбаумы и автоматика для ворот Ворота могут быть *распашными* (их сопротивление тарану не очень высокое и они требуют очистки проезжей части перед воротами от снега и льда), *раздвижные, подъемные и рулонные.* В качестве атрибутных идентификаторов на транспортное средство применяют путевой лист, в котором указывается государственный номер машины, фамилия водителя и лица, ответственного за перевозку груза (часто эти функции выполняет водитель), вид и количество груза. Идентификаторами водителя и пассажиров являются их пропуска.

Современные СКУД транспорта оснащаются также дистанционными атрибутными идентификаторами (типа проксимити), средствами досмотра транспорта (специальными зеркалами и техническими эндоскопами), а также на особо важных объектах - антитеррористическим средством для экстренной остановки автомобиля, пытающего протаранить ворота. Последнее средство представляет собой металлическую колонну (блокиратор) диаметром до 50 см, которая устанавливается перед воротами с внешней стороны в бетонированном или металлическом колодце. На дне колодца размещается баллон со сжатым воздухом и пиропатроном, который взрывается по электрическому сигналу с КПП, а сжатый воздух поднимает колонну за доли секунды пе-

ред движущимся автомобилем. Подобный блокиратор может остановить 20-тонный автомобиль, движущийся со скоростью 60 км/ч.

Контроллеры лифтов. Принцип их действия состоит в следующем. Система контроля доступа по персональному коду определяет доступные этажи и при попытке попасть на какой-либо этаж, выходящий из этого диапазона, блокирует движение лифта в запретный сектор.

Кроме СКУД на основе считывателя карточек доступа, находят применение СКУД на основе видеодомофона и СКУД на основе турникета, считывателя карточек доступа и видеодомофона.

СКУД на основе видеодомофона Принцип работы такой системы основан на передаче видеоизображения с телекамеры, установленной на входной двери или в ее зоне, на монитор поста охраны. Система также включает дистанционную систему открытия двери на основе электромеханического замка и переговорное устройство. Система может быть дополнена видеомагнитофоном, ведущим непрерывную запись сигнала телекамеры. Установка дополнительных камер для интеграции СКУД и системы видеонаблюдения требует установки «видеомультиплексора» - устройства, выводящего сигнал на монитор одновременно с нескольких камер.

СКУД на основе турникета, считывателя карточек доступа и видеодомофона. Данная СКУД является типовым проектом для бизнес-центра или любого другого комплекса помещений. Служащие проходят в комплекс помещений по индивидуальным карточкам доступа, считыватель которых управляет турникетом, расположенным у поста охраны. В нерабочее время (выходные дни, праздники, ночное время) проход через главную дверь блокируется электромеханическим замком. Переговорное устройство и система наружного видеонаблюдения входной двери позволяют охране дистанционно управлять входной дверью в нерабочее время, когда дверь находится в состоянии «всегда закрыто» в отличие от рабочего времени «всегда открыто». В нерабочее время такая система позволяет снизить численность охранников без ущерба для безопасности. За турникетом может располагаться рамочный металлодетектор.

1.3. Требования к системам контроля управления доступом

Как уже говорилось выше, системы контроля и управления доступом (СКУД) предназначены для обеспечения санкционированного входа в здание и в зоны ограниченного доступа и выхода из них путем идентификации личности по комбинации различных признаков, а также для предотвращения несанкционированного прохода в помещения и зоны ограниченного доступа объекта.

Согласно ГОСТ Р 51241-98 СКУД должна состоять из устройств преграждающих управляемых (УПУ) в составе преграждающих конструкций и ис-

нолнительных устройств; устройств ввода идентификационных признаков (УН1111) в составе считывателей и идентификаторов; устройств управления (УУ) н составе аппаратных и программных средств.

Считывателями и УПУ оборудуют: главный и служебные входы; КПП; помещения, в которых непосредственно сосредоточены материальные ценности; помещения руководства; другие помещения по решению руководства предприятия. Пропуск сотрудников и посетителей на объект предприятия через пункты контроля доступа следует осуществлять в здание и служебные помещения - по одному признаку; входы в зоны ограниченного доступа (хранилища ценностей, сейфовые комнаты, комнаты хранения оружия) - не менее чем по двум признакам идентификации.

СКУД должна обеспечивать выполнение следующих основных функций:

- открывание УПУ при считывании идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение) в заданный временной интервал или по команде оператора СКУД;
- запрет открывания УПУ при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;
- санкционированное изменение (добавление, удаление) идентификационных признаков в УУ и связь их с зонами доступа (помещениями) и временными интервалами доступа;
- защиту от несанкционированного доступа к программным средствам УУ для изменения (добавления, удаления) идентификационных признаков;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
- сохранение настроек и базы данных идентификационных признаков при отключении электропитания; ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;
- автоматическое закрытие УПУ при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;
- выдачу сигнала тревоги (или блокировку УПУ на определенное время) при попытках подбора идентификационных признаков (кода);
- регистрацию и протоколирование текущих и тревожных событий;
- автономную работу считывателя с УПУ в каждой точке доступа при отказе связи с УУ.

На объектах предприятия, где необходим контроль сохранности предметов, следует устанавливать СКУД, контролирующие несанкционированный

вынос данных предметов из охраняемых помещений или зданий по специальным идентификационным меткам.

УПУ с исполнительными устройствами должно обеспечивать:

- частичное или полное перекрытие проема прохода;
- автоматическое и ручное (в аварийных ситуациях) открывание;
- блокирование человека внутри УПУ (для шлюзов, проходных кабин);
- требуемую пропускную способность.

Считыватели УВИП должно обеспечивать:

- считывание идентификационного признака с идентификаторов;
- сравнение введенного идентификационного признака с хранящимся в памяти или базе данных УУ;
- формирование сигнала на открывание УПУ при идентификации пользователя;
- обмен информацией с УУ.

УВИП должны быть защищены от манипулирования путем перебора или подбора идентификационных признаков.

Идентификаторы УВИП должны обеспечить хранение идентификационного признака в течение всего срока эксплуатации для идентификаторов без встроенных элементов электропитания и не менее 3 лет - для идентификаторов со встроенными элементами электропитания.

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

УУ должно обеспечивать:

- прием информации от УВИП, ее обработку, отображение в заданном виде и выработку сигналов управления УПУ;
- ведение баз данных сотрудников и посетителей объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и другие);
- ведение электронного журнала регистрации проходов сотрудников и посетителей через точки доступа;
- приоритетный вывод информации о тревожных ситуациях в точках доступа;
- контроль исправности и состояния УПУ, УВИП и линий связи с ними.

Конструктивно СКУД должны строиться по модульному принципу и обеспечивать:

- взаимозаменяемость сменных однотипных технических средств;
- удобство технического обслуживания и эксплуатации, а также ремонтопригодность;
- исключение возможности несанкционированного доступа к элементам управления;

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

Выбор оборудования СКУД, места его установки на объекте следует проводить в соответствии с РД 78.36.005-99 (прил. 3) и РД 78.36.003-2002 (прил. 2).

1.4. Средства идентификации и аутентификации

Рассмотрим более подробно используемые средства идентификации и аутентификации.

Идентификационные карточки с магнитной дорожкой. Этот тип карточек был разработан еще в 60-е гг. XX в., но с тех пор был существенно усовершенствован: увеличена информационная емкость, износоустойчивость, повысилась защищенность от злоупотреблений. В ранних образцах запись информации велась магнитным полем напряженностью 300 эрстед. Это не обеспечивало надежной защиты от случайного или умышленного стирания. Кроме того, запись магнитным полем такой напряженности позволяла нарушителям достаточно просто подделывать такие карточки, не прибегая к помощи сложного оборудования. Устранить эти недостатки удалось путем применения специальных магнитных материалов, требующих для записи магнитного поля напряженностью 4000 эрстед. Такие магнитные материалы в конце 1970-х гг. впервые стала применять фирма 3М. В настоящее время достигнута плотность записи 75 бит/см. Высокая плотность записи дает возможность хранить на карточке достаточно большой объем информации.

Для повышения степени защищенности карточек, наряду с обычной информацией о владельце, может наноситься, например, специальный защитный код, описывающий структуру материала, из которого они изготавливаются. Этот способ был применен фирмой Copytex GmbH (ФРГ), где использовался тот факт, что каждая карточка имеет уникальную структуру материала, которая может быть зафиксирована с помощью соответствующих технических средств. При выпуске карточки в обращение структурные особенности ее основы в цифровом коде записываются на магнитную дорожку. При проверке специальное оптоэлектрическое устройство считывающего терминала сканирует карточку, просвечивая ее поверхность, после чего система автоматически определяет соответствие полученных данных записанному коду.

Идентификационные карточки с магнитной барий-ферритовой прослойкой. В таких карточках магнитный слой является серединой «сэндвича» из несущей основы (с фотографией и личными данными владельца) и пластикового покрытия. Расположение в нем и полярность зарядов барий-ферритовых частиц образуют код. Достоинством таких карточек является самая низкая стоимость по сравнению со всеми другими видами и повышенная защищен-

ность от копирования. Однако они не обеспечивают надежной защиты от случайного или умышленного стирания или изменения встроенного кода. Кроме того, они недостаточно износоустойчивы. Область их применения ограничена теми сферами, где не требуется сколько-нибудь высокий уровень безопасности при контроле доступа.

Идентификационные карточки, кодированные по принципу Виганда. В основу таких карточек встраиваются миниатюрные отрезки тонкой ферромагнитной проволоки специального вида (расположенные в строго определенной последовательности, различной для разных карт), которые и содержат информацию о персональном коде ее владельца (рис. 1.3). При вложении карточки в считыватель эти так называемые «проволочки Виганда» вызывают изменение магнитного потока, которое фиксируется соответствующим датчиком, преобразующим импульсы в двоичный код. Технология кодирования Виганда обеспечивает весьма высокую степень защиты идентификационной карточки от случайного и умышленного стирания, фальсификации зафиксированного кода и изготовления дубликата.

Рис. 1.3. Бесконтактная карта (интерфейс Виганда)]

Бесконтактные радиочастотные проксимити-карты. Считыватель генерирует электромагнитное излучение определенной частоты и при внесении карты в зону действия считывателя это излучение через встроенную в карте антенну запитывает чип карты. Получив необходимую энергию для работы, карта пересылает на считыватель свой идентификационный номер с помощью электромагнитного импульса определенной формы и частоты. Сама проксимити-карта состоит из приемопередающей антенны и электронного чипа (рис. 1.4).

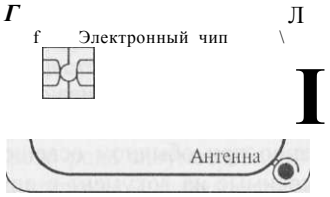


Рис. 1.4. Проксимити-карта

Идентификационные карточки со скрытым штриховым кодом (баркод). Невидимый штриховой код впечатывается в основу карточки и считы-

нас гея с помощью излучения в инфракрасном спектре. Код образуется за счет конфигурации теней при прохождении ИК-излучения через карточку и обладает высокой степенью защищенности от подделки. Однако эта технология ювольно дорого стоит, хотя стоимость таких карточек и ниже, чем стоимость карточек Виганда

Идентификационные карточки с оптической шшятыо. Кодирование информации на таких карточках осуществляется примерно так же, как при записи данных на оптических дисках - компьютерных носителях. Считывание производится лазером. Современная технология обеспечивает очень высокую плотность записи, поэтому емкость памяти таких карточек исчисляется мегабайтами. Это позволяет хранить не только буквенно-цифровые данные, но и изображения и звуковую информацию. Карточки этого типа имеют низкую стоимость и высокую степень защищенности от несанкционированного копирования. Однако высокая плотность хранения информации требует достаточно бережного отношения и сложных считывающих терминалов. Изготавливаются корпорацией Drexler Technology Corp., США (карточка LaserCard) и торонтской фирмой Optical Recording Corp.

Голографические идентификационные карточки. Используемые при изготовлении таких идентификационных документов трехмерные голограммы формируются на основе интерференции двух или нескольких когерентных волновых полей. Применение голограммы наряду с повышенной защитой документов от фальсификации обеспечивает высокую плотность записи информации (до 10 бит информации, содержащейся в изображении на 1 мм). Повышенная защищенность документов обусловлена тем, что техническая реализация методов голографии отличается достаточной сложностью и требует применения специальной аппаратуры.

Одним из видов голограмм, нанесение которых не сопряжено со значительными затратами, являются печатные голограммы. С помощью так называемой «радужной голограммы» формируется печатная основа, на которую затем может быть нанесено большое число голографическнх отличительных признаков подлинности идентификационного документа. Существенным достоинством печатных голограмм является то, что они могут наноситься на используемые в настоящее время документы. Это позволяет заметно повысить уровень защищенности удостоверений от фальсификаций при сравнительно низких затратах.

Более высокий уровень защиты обеспечивают голограммы, основанные на эффекте объемного отражения Информация, содержащаяся в них, может считываться непосредственно при обычном освещении (т. е. без вспомогательной аппаратуры). Наносимые на документ с помощью голограммы данные могут представлять собой как отдельные буквенно-цифровые знаки, так и сложную комбинацию буквенно-цифровых, графических и фотографических символов

Интерференционная диаграмма, содержащая информацию, распределяется квазислучайно по всей площади и на всю глубину эмульсионного слоя голограмм рассматриваемого вида, что обусловливает предельные трудности при попытке фальсифицировать идентификационный документ. Содержащаяся в голограмме информация становится видимой в лучах обычного света, источником которого может быть, например, настольная лампа. Информация представляется в виде реального или мнимого изображения.

Одним из новых перспективных видов голограмм являются так называемые «голограммы Даусманна». Разработанная технология нанесения информации обеспечивает возможность сочетания в одном фотоэмульсионном слое изображения буквенно-цифровых данных, черно-белого фотографического снимка, а также объемно-рефлексионной голограммы. Изготавливаемые с использованием этой технологии документы получили название «удостоверения в удостоверении», так как информация черно-белого изображения полностью совпадает с данными, содержащимися в голограмме. Какие-либо изменения в черно-белом фотоснимке обнаруживаются сразу путем его сличения с голограммой. Данная голографическая технология формирования признаков подлинности особенно эффективна для таких идентификационных документов, как удостоверение личности, загранпаспорт и т. д.

При необходимости голограммы могут применяться и для хранения биометрических данных (например, отпечатков пальцев). Подобная система разработана немецкой фирмой Siemens AG. Для обеспечения надежной защиты от попыток фальсификации или копирования идентификационных карточек фирма применила еще и шифрование данных.

Голографические методы защиты информации на документах, наряду с высокой надежностью, обладают и рядом недостатков. К ним относятся, например, высокая сложность аппаратуры автоматизации процесса контроля, достаточно жесткие требования к сохранности документа Наибольшую эффективность обеспечивает полуавтоматическая аппаратура, функционирующая с участием оператора-контролера, который анализирует результаты сравнения и принимает решение о пропуске на объект.

Идентификационные карточки с искусственным интеллектом (смарт-карты). Такие документы содержат вмонтированные в основу миниатюрные интегральные микросхемы - запоминающее устройство и микропроцессор. Одно из преимуществ карточек этого типа - возможность регистрации значительного объема идентификационных данных. Они обладают довольно высокой степенью защищенности записанной в них информации от фальсификации и различного рода злоупотреблений. В литературе встречаются другие названия этих карточек - «разумные» или «интеллектуальные».

Вычислительный микроблок этой карточки содержит три типа запоминающих устройств (ЗУ). Для хранения программного обеспечения предназначена память типа ПЗУ (постоянное ЗУ), в которую информация заносится

фирмой-изготовителем на этапе выпуска карточки в обращение и не допускает внесения каких-либо изменений в хранящиеся инструкции.

Для хранения промежуточных результатов вычислений и других данных временного характера применяется память типа ЗУПВ (запоминающее устройство произвольной выборки). Она управляется встроенным микропроцессором, который осуществляет контроль за процессом взаимодействия со считывателем. После отключения электрического питания информация здесь не сохраняется.

Память третьего типа - программируемое постоянное запоминающее устройство (ППЗУ) - предоставляется пользователю для записи персональной информации. Она также находится под управлением встроенного микропроцессора, т. е. только по его команде в эту память могут вноситься какие-либо изменения. Записанная информация не стирается и при отключении электрического питания. В памяти этого типа, как правило, выделены три зоны: *открытого доступа, рабочая и секретная.*

В *открытой зоне* может храниться, например, персональная информация пользователя (имя, адрес и т. п.), считывание которой допускается посторонним терминалом соответствующего типа. Однако какие-либо изменения в записях могут производиться только с разрешения пользователя и с помощью спецаппаратуры.

Рабочая зона предназначена для занесения специфической информации, изменение и считывание которой допускается только по команде пользователя и при наличии соответствующих технических средств.

В *секретной зоне* записывается идентифицирующая информация, например, личный номер или код-пароль. Кроме того, здесь же обычно хранятся временные и территориальные полномочия пользователя по доступу к охраняемым объектам и помещениям. Информация секретной зоны может быть считана только терминалом системы контроля доступа, для которого предназначена данная карточка. Изменения также вносятся только по команде этой системы.

Хранимые здесь данные не раскрываются никакой посторонней считывающей аппаратурой, в том числе фирмы-изготовителя. Секретная информация заносится в эту зону при регистрации пользователя контрольно-пропускной системой. До недавнего времени в качестве такой памяти применялись запоминающие устройства СППЗУ (стираемое программируемое постоянное ЗУ). Внесенная информация могла быть стерта только с помощью ультрафиолетового излучения и спецоборудования. Более современным типом памяти является ЭСППЗУ - электрически стираемое программируемое постоянное ЗУ, которое в отличие от предыдущего более долговечно (срок службы - до нескольких лет) и обладает большей гибкостью.

Некоторые интеллектуальные карточки позволяют хранить цифровые образы биометрических характеристик пользователя (динамику росписи, отпе-

чатка пальца, ладони, геометрических параметров кисти, рисунка глазного дна, портретного изображения). В целях защиты от несанкционированного использования идентификационных карточек, применяемых пользователями таких систем, электронный «портрет» хранится в памяти в цифровом зашифрованном виде, что значительно затрудняет восстановление записанной информации и ее подделку злоумышленниками.

Бесконтактные идентификационные карточки. Такие карточки по виду не отличаются от всех остальных, но наряду с обычной атрибутикой содержат встроенный миниатюрный приемопередатчик, который осуществляет дистанционное взаимодействие со считывателем системы контроля доступа.

В качестве коммуникационного средства при дистанционном считывании могут служить направленное электромагнитное поле (микроволновые радиосигналы), оптический луч (инфракрасное излучение) или акустические волны (ультразвук).

Особенность бесконтактных считывателей по сравнению с устройствами других типов состоит в том, что внешний элемент их конструкции (антенна) может быть вмонтирована, например, в стену рядом с охраняемой дверью Это обеспечивает скрытность и соответственно защиту от попыток физического разрушения

Расстояние, на котором взаимодействует бесконтактная идентификационная карточка с антенной считывающего устройства, в современных бесконтактных контрольно-пропускных автоматах может изменяться в зависимости от конкретной модели от нескольких сантиметров до 10 м и более.

Наибольшее распространение сейчас получили микроволновые считыватели и идентификационные карточки со встроенной электронной схемой или «электронные жетоны» (которые пользователь может носить во внутреннем кармане, портфеле или прикрепленными к связке ключей). Такие идентификаторы называют еще «электронными метками».

Различают следующие типы электронных меток.

Пассивные электронные метки Работают на основе переизлучения электронной энергии от микроволнового радиопередатчика терминала. Переизлучаемый сигнал улавливается радиоприемником терминала, после чего подаются соответствующие команды на механизм отпирания двери.

Полуактивные электронные метки. Содержат миниатюрную батарею, которая является источником электропитания для приемопередатчика. Сам приемопередатчик находится обычно в режиме ожидания, а при попадании в зону действия микроволнового излучателя поста выдает сигнал определенной частоты, принимаемый терминалом системы.

Активная электронная метка. Представляет собой микроволновый передатчик-радиомаяк, транслирующий сигнал определенной частоты (для некоторых моделей кодированный) непрерывно.

Наиболее простые модели бесконтактных контрольно-пропускных терминалов, развитие которых началось еще в начале 1970-х гг. в США, могли транслировать лишь групповой сигнал, не подразделяя пользователей по отдельности. В дальнейшем с развитием электронной технологии появились идентификационные карточки, которые кроме микросхемы приемопередатчика включали в свой состав запоминающее устройство. В этой памяти хранится многозначный код, который при обмене сигналами переносится в контрольный терминал и идентифицируется в соответствии с полномочиями конкретного пользователя.

Например, полуактивная электронная метка была разработана немецкой фирмой Burcka Systems в качестве пропуска бесконтактного типа. Ее встроенная память позволяет хранить сколько угодно большое число программируемых кодовых комбинаций, допускающих к тому же их дистанционное изменение. Максимальное расстояние считывания составляет 3 м. Пропуск можно носить под одеждой, так как микроволновый сигнал проникает даже через плотный (текстильный и кожаный) материал верхней одежды. В качестве источника питания используется миниатюрная литиевая батарея со сроком службы 10 лет.

Современные *проксимити-идентафикаторы* представляют собой электронные пропуска в виде пластиковых карточек или брелков и довольно широко используются в системах контроля доступа. Они обеспечивают бесконтактное дистанционное распознавание (идентификацию) персонального кода владельца электронными считывателями. В переводе на русский язык proximity (проксимити) означает «близость». Однако эта близость довольно условна, поскольку расстояние между проксимити-идентификатором и считывателем в зависимости от мощности считывателя и типа идентификатора может варьироваться от нескольких сантиметров до 2,5 м.

Специальные электронные считыватели проксимити-идентификаторов распознают личность его владельца по записанному на идентификаторе персональному коду. Механизм распознавания (считывания) базируется на дистанционной радиочастотной технологии. Проксимити-считыватель постоянно посылает радиосигнал. При попадании в зону действия считывания проксимити-идентификатор активизируется и посылает в ответ сигнал, содержащий уникальный код доступа, записанный в памяти его электронной схемы. Считывание кода с проксимити-идентификатора происходит на определенном расстоянии от считывателя, т. е. без непосредственного контакта. При этом позиционирование идентификатора относительно считывателя не имеет значения.

Все проксимити-идентификаторы делятся на две группы - пассивные и активные.

В настоящее время используются как активные, так и пассивные проксимити-идентификаторы. Пассивный проксимити-идентификатор не содержит встроенного источника энергии, он абсолютно герметичен и имеет практиче-

ски неограниченный срок службы. При этом расстояние, на котором он работает стабильно, составляет от 10 до 50 см от считывателя. Как правило, такие идентификаторы используются для быстрого и надежного обслуживания большого потока людей, например допуск их через проходную предприятия. Активный проксимити-идентификатор может работать на расстоянии от одного до трех метров, но требует постоянного контроля степени заряда встроенной батареи и ее своевременной замены (обычно не чаще чем через 5 лет). Так, например, автомобильные проксимити-идентификаторы HID ProxPass работают на расстоянии до 2,5 м. Большое расстояние считывания активного идентификатора позволяет использовать его в системах контроля въезда-выезда автомобилей, производить контроль перемещения крупногабаритных грузов, вагонов или контейнеров.

Все проксимити-идентификаторы HID отличаются высокой степенью защищенности от подделки. Благодаря отсутствию механического контакта между проксимити-идентификатором и считывателем, идентифткатор не изнашивается, и срок его службы практически не ограничен. Проксимити-идентификаторы обладают достаточной механической прочностью, устойчивы к изгибам, ударам, не боятся влаги и загрязнения.

На проксимити-идентификаторы можно наносить надписи, фотографии, логотипы. Для этого применяются специальные поливинилхлоридные наклейки, а фотоизображения и рисунки на поверхности тонких проксимити-идентификаторов печатаются на специальных принтерах.

Пластиковые ключи. Пластиковые ключи используются во всех рассмотренных выше способах кодирования. Их отличие заключается в конструктивном способе отпирания, внешне напоминающем способ отпирания обычного механического замка - вставление ключа в скважину, проверку доступа и индикацию владельцу ключа разрешения на открытие замка (поворот ключа).

Этот идентификатор отличается более высокой степенью износоустойчивости по сравнению с идентификационными карточками. В памяти такого ключа хранится личный номер его владельца Принцип проверки основан на сравнении вводимого пользователем номера с номером, хранящимся в памяти ключа, который счи гывается терминалом при его вставлении в прорезь.

В память ключа обычно заносится следующая информация:

- системный идентификационный номер (уникален для каждой установки и предоставляется фирмой-изготовителем при заказе системы; максимальное число различных системных номеров свыше 65 тыс.);
- пользовательский идентификационный номер (определяется покупателем при выпуске и программировании ключа; можно заказать до 9999 различных номеров);
- уровни доступа (для автономного считывателя до 256 уровней система предоставляет доступ от данного уровня и выше);

- дни недели (7 дней недели соотнесены с временными зонами; комбинация дня недели и временной зоны определяет право доступа через любой считыватель в любое данное время);
- временные зоны (каждая система располагает до 16 отдельными зонами, которые могут быть назначены пользователю);
- кодонаборная панель (для важных объектов в памяти ключа может храниться до 10 различных цифр).

Терминалы на базе комбинации считывателя и кодонаборного устройства. Комбинирование методов аутентификации личности позволяет повысить надежность защиты от несанкционированного доступа. Однако при этом увеличивается время выполнения процедуры проверки.

В настоящее время различными зарубежными фирмами освоен выпуск целого ряда моделей.

Наибольший интерес представляет комбинированный терминал фирмы Security Dynamics. Используемая идентификационная карточка (по размеру похожа на стандартную кредитную, но вдвое толще ее) содержит встроенный микропроцессор, миниатюрный источник питания, жидкокристаллический индикатор, электронные часы, а также запоминающие устройства двух типов - с произвольной выборкой (ЗУПВ) и постоянное (ПЗУ). Каждую минуту на индикаторе высвечивается число из псевдослучайной последовательности, алгоритм генерации которой известен микрокомпьютеру системы. Так что терминал «знает», какое конкретное число, на какой идентификационной карточке, в какой конкретный период времени будет записано. По существу этот псевдослучайный номер служит паролем в течение 60 с.

Процедура проверки выглядит следующим образом. Пользователь вводит с помощью клавиатуры свой личный идентификационный номер, а затем то число, которое отображено в данный момент на индикаторе его идентификационной карточки. Система определяет корректность этого числа для данной карты и отрезка времени.

Для противодействия угрозам перехвата личного кода законного пользователя может быть запрограммирована такая возможность, когда вместо раздельного ввода данных владельцем идентификационной карточки набирается на клавиатуре сумма идентификационного номера и числа, прочитанного на индикаторе.

1.5. Особенности СКУД для крупных распределенных объектов

В СКУД для крупного распределенного объекта с различной архитектурой используются мощные центральные контроллеры, осуществляющие процесс управления с использованием специализированных удаленных интерфейсных модулей. Особенности применения определяют требования, предъ-

являемые к программному обеспечению для таких систем Чаще всего используют СКУД с централизованной или распределенной архитектурой, но иногда применяется и архитектура смешанного типа.

1.5.1. Централизованная архитектура

В крупной распределенной системе контроля и управления доступом, особенно при больших расстояниях между отдельными зданиями охраняемого объекта, каждое здание должно иметь свой центральный контроллер. Это обеспечивает автономное функционирование системы безопасности каждого здания в случае нарушения связи между отдельными объектами. Число подключаемых считывателей на один контроллер, как правило, колеблется от 16 до 96, поэтому обычно мощности одного контроллера вполне хватает для создания СКУД отдельного объекта в крупной распределенной системе. Контроллеры централизованных СКУД являются чисто логическими устройствами и не управляют дверями, т. е не имеют релейных выходов управления замками, входов для подключения считывателей СКУД Функции управления дверями, другими внешними устройствами выполняют внешние интерфейсные модули и релейные блоки. Они, как правило, устанавливаются недалеко от объектов управления (двери, охранные шлейфы и др.) Для обмена информацией между контроллером и интерфейсными модулями наиболее часто используется интерфейс RS-485, однако уже появились системы, в которых возможно подключение интерфейсных модулей по стандарту LAN

Следует также отметить, что наиболее мощные центральные контроллеры насчитывают несколько коммуникационных интерфейсов RS-485, что обеспечивает широкий охват территории крупных зданий без применения усилителей интерфейса Фактически можно проложить свой интерфейс RS-485 в нескольких направлениях от центрального контроллера. Что касается сетевого интерфейса, то для крупных объектов возможность подключения интерфейсных модулей СКУД к центральному контроллеру по стандарту LAN весьма актуальна, поскольку в этом случае появляется перспектива использования существующей на объекте сетевой инфраструктуры и существенного снижения расходов на прокладку коммуникаций. Контроллер в системах с централизованной архитектурой хранит всю базу данных идентификаторов и событий, произошедших в системе. Располагается он обычно недалеко от управляющих компьютеров (серверов) в местах наивысшей защищенности (комнаты охраны, серверные и пр.). Разделение функций принятия решений и непосредственно управления повышает степень безопасности СКУД, так как сам контроллер хорошо защищен и установлен на большом расстоянии от управляемого им УПУ Кроме того, такой подход помогает снизить стоимость крупных систем, поскольку цена контроллера «растворяется» в общей стоимости системы. Следует отметить, что сами контроллеры можно объединять в сети, позволяя тем самым создавать СКУД значительного масштаба (рис. 1.5). При нарушении связи контроллера с компьютером система работа-

ет в автономном режиме. Другими словами, централизованная система - это жесткая властная вертикаль или пирамида, когда наверху руководящий контроллер («начальник»), а ниже - обычные интерфейсные модули («исполнители»), которые собственно и реализуют управляющие команды.

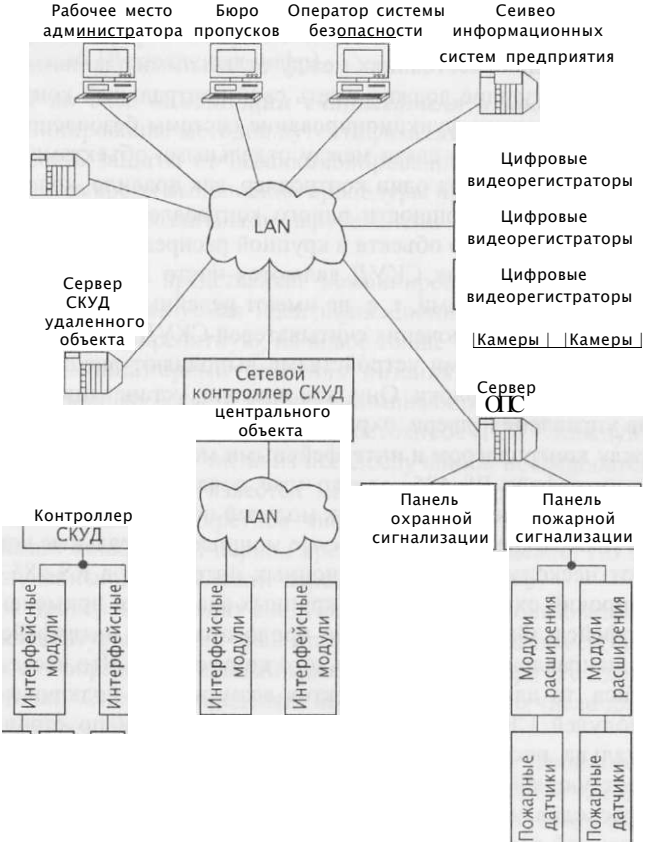


Рис. 1.5. Вариант построения СКУД с централизованной архитектурой

1.5.2. Распределенная архитектура СКУД

Отличительная особенность СКУД с распределенной архитектурой состоит в том, что база данных идентификаторов (и событий в системе) содержится не в одном, а в нескольких контроллерах. Они обычно выполняют функции управления внешними устройствами и охранными шлейфами через реле и входы охранной сигнализации, расположенные непосредственно на плате самого контроллера. Эти контроллеры, как правило, устанавливаются непо-

средственно внутри защищаемых ими помещений. Это не снижает вероятности несанкционированного манипулирования контроллером, но имеет свои плюсы - при таком подходе менее критично нарушение связи между контроллером и интерфейсным модулем (как в обычной централизованной системе). В случае обрыва линии связи между контроллерами и компьютером система продолжает выполнять основные функции управления процессом доступа в автономном режиме. Выведение из строя одного контроллера не повлияет на работу остальных. Наиболее часто в системах с распределенной архитектурой контроллер управляет проходом в 2-4 двери. При использовании таких СКУД на крупных распределенных объектах следует помнить, что каждое отдельное здание, скорее всего, будет оснащаться своей подсистемой, состоящей из группы контроллеров со своим управляющим компьютером. Такая особенность связана с ограничением длины наиболее часто используемых в таких системах интерфейсов - RS-485 и 20-мА токовая петля. Прокладка линий связи между удаленными зданиями потребует применения усилителей интерфейса, а это не всегда удобно и несколько снижает надежность, поэтому можно рассматривать систему в целом как совокупность подсистем нескольких зданий. Если перейти на строительную терминологию, то распределенная СКУД - это некоторое число контроллеров - «прорабов», которые отвечают только за свой участок работ и сами же их выполняют. Они самостоятельно анализируют и хранят часть информации о функционировании своей небольшой части системы.

1.5.3. Смешанная архитектура

Обычно такие системы получаются из СКУД с централизованной архитектурой путем добавления специализированных считывателей или интерфейсных модулей с собственным буфером памяти идентификаторов и событий - «интеллектуальных интерфейсных модулей». Можно сказать, что каждый такой модуль является небольшим контроллером СКУД, сравнимым с контроллером в распределенной системе. Благодаря использованию данного технического решения достигается избыточное резервирование функций, резко повышающее степень безопасности системы. Поскольку контроллер в СКУД с централизованной архитектурой управляет большим числом дверей, повреждение линии связи между ним и интерфейсными модулями управления оконечными устройствами может привести к блокированию значительной части или даже всей системы. Локальный считыватель или промежуточный интерфейсный блок, обладающий встроенным буфером памяти, в этом случае переходит в автономный режим управления доступом (на своем участке). Системы, построенные с использованием данных модулей, обладают наивысшей степенью безопасности и исключительной надежностью функционирования. Для крупных распределенных СКУД со смешанной аппаратной архитектурой важно, что некоторые производители имеют в номенклатуре интерфейсные модули с возможностью подключения к центральному кон-

троллеру по LAN-интерфейсу. При наличии развитых сетевых коммуникаций на территории объекта подобные модули устанавливаются в удаленных зданиях, что придает системе дополнительную гибкость и позволяет экономить значительные средства.

Таким образом, смешанная система - это властная вертикаль, или пирамида с возможностью передачи части функций управления на более низкий уровень в случае возникновения экстренной ситуации.

1.5.4. Программное обеспечение для крупных СКУД

Программные комплексы для крупных распределенных СКУД имеют свои особенности, которые необходимо иметь в виду при выборе ГІК для систем малого и среднего масштаба.

Одним из наиболее распространенных вариантов СКУД является ***небольшая изолированная система.*** Ее главная характеристика состоит в том, что все модули (управление базой данных, ядро, функциональные модули, драйверы оборудования и др.) устанавливаются и запускаются на одном компьютере. К этому же компьютеру подключается и все оборудование. Компьютер при этом должен обладать достаточной вычислительной мощностью и объемом памяти для выполнения всех программных модулей, а также адекватным исходной задаче дисковым пространством - для хранения базы данных системы Основные достоинства подобной системы - *простота инсталляции, обслуживания, контроля линий связи и низкая стоимость решения.* Из недостатков можно отметить, прежде всего, отключение некоторых функций при «зависании» или выключении компьютера, возможность администрирования только на одном компьютере, замедление реакций комплекса при большом количестве подключенного оборудования. Для крупной распределенной системы важнейшим негативным фактором окажется необходимость подключения всего управляемого оборудования к данному компьютеру, что часто просто невыполнимо.

При использовании ***централизованной системы с удаленным управлением*** все служебные модули комплекса (ядро, драйверы оборудования и логики) функционируют на одном компьютере - центральном сервере системы, а запуск управляющей консоли возможен не только на данном компьютере, но и на других машинах сети. В такой системе центральный компьютер должен обладать еще большими вычислительной мощностью, объемом памяти и дисковым пространством, чем в однопользовательской системе Однако в данной схеме появляется возможность задействовать не очень мощные компьютеры с небольшими дисками в качестве клиентских рабочих станций. *Достоинства* очевидны: простота установки, обслуживания и контроля линий связи, так как все оборудование подключено к одному компьютеру. В такой системе легко контролировать состояние функциональных модулей и драйверов оборудования, так как все они функционируют на одной машине. *Недостатки* в значительной степени такие же, как в предыдущем варианте.

Для централизованной системы главным отрицательным фактором будет тот же - необходимость подключения всего управляемого оборудования к одному компьютеру (серверу).

В крупных СКУД иногда используется вариант, при котором ***сервер управления базой данных системы и ядро работают па центральном сервере, а драйверы оборудования и логики распределены по всей сети.*** Запуск управляющих консолей возможен на любом компьютере сети, что делает управление более гибким. Необходимость распределения по сети драйверов оборудования и логики связана в основном с тем, что здания предприятия распределены по территории и часть оборудования может находиться достаточно далеко от центрального сервера. Поскольку часть модулей вынесена с центрального сервера системы на другие компьютеры, нагрузка на центральный сервер снижается. Применение такой архитектуры оправданно при наличии большой территории с распределенным по ней управляющим оборудованием. В этом случае нет необходимости прокладывать коммуникации из всех точек к центральному серверу. Достаточно подключить аппаратуру к ближайшему компьютеру сети и запустить на этом компьютере обслуживающий драйвер При этом требования к мощности данного компьютера остаются относительно скромными.

Надо отметить, что в случае распределенного запуска программных модулей встает задача контроля их состояния. Для упрощения работы в ПО системы должны быть встроены специальные средства, позволяющие администратору со своего рабочего места контролировать работу модулей на других компьютерах, запускать или останавливать их.

Выделим наиболее важные *достоинства* и недостатки такого ПО. К числу достоинств следует отнести:

- простоту подключения благодаря возможности присоединения оборудования к ближайшему компьютеру;
- возможность создания очень крупных СКУД высокой надежности для крупных распределенных объектов;
- повышение общей скорости работы системы за счет снижения нагрузки на центральный сервер,
- снижение стоимости монтажа системы благодаря экономии на прокладке линий связи.

Недостатками можно считать:

- требование контроля администратором состояния распределенных по системе модулей;
- необходимость наличия на объекте обученного персонала.

ПО с такой структурой подходит для построения СКУД и интегрированных систем безопасности (ИСБ) заводов, аэропортов, банков, офисов крупных компаний, институтов и других крупных объектов, имеющих значительные территории с большим числом отдельно стоящих зданий и сооружений.

Н общем случае программное обеспечение СКУД предоставляет пользован- по следующие стандартные возможности:

- программирование временных интервалов, в которые двери (ворота) открыты совсем, открываются при сканировании идентификационной карточки (или аутентификации пользователя на биометрических терминалах) или закрыты наглухо, а также включение/выключение по расписанию или по показаниям приборов, освещения, вентиляции, лифтов, датчиков охранной сигнализации;
- программирование выходных дней и праздников, когда допуск предоставляется только определенным лицам;
- создание нескольких иерархических групп пользователей в зависимости от уровня предоставляемого им допуска;
- исполнение функции «ни шагу назад», препятствующей тому, чтобы один сотрудник, пройдя через дверь передал свою карточку другому человеку (т. е. определяется временной интервал, в течение которого карточка не может открыть дверь еще раз, либо на выходе из помещения устанавливается еще один считыватель, и карточка может снова «зайти», только предварительно «выйдя»);
- если компьютер подключен к системе постоянно, на него может быть выведен план охраняемой территории со всеми точками контроля доступа, дверями, проходами, расположением датчиков и т. п., на котором в режиме реального времени отображаются все происходящие события;
- оператор системы постоянно контролирует обстановку и в случае необходимости может принять требуемые по обстановке решения

Обычно крупные СКУД работают в совокупности с системами охранной сигнализации и телевизионного наблюдения. В этом случае, например при попытке несанкционированного проникновения в помещение, оснащенное СКУД или датчиками охранной сигнализации, включаются телекамеры и блокируются выходы. Система может программироваться на разблокирование всех исполнительных устройств в экстренных случаях. Подобный набор функций заложен, например, в программном обеспечении систем безопасности «Multi Net 5100» (работающей в среде OS/2) фирмы «DIEBOLD».

Типовые возможности математического и программного обеспечения достаточно крупных СКУД позволяют решать задачи контроля за посетителями, контроля за выносом материальных ценностей, автоматизировать ряд функций службы патрулирования и т. д.

Каждому посетителю на входе выдается идентификационная карточка с разрешением на доступ в заданное время в определенные зоны. На выходе карточка должна сдаваться. При этом возможен оперативный контроль мест посещения, а в случае задержки на объекте вне пределов заданного временного интервала подается сигнал тревоги.

По аналогичной методике может быть организован контроль своевременного движения групп службы патрулирования.

Для выноса материальных ценностей на любой рабочей станции системы может быть сформирован список предметов, который скрепляется «электронной подписью» уполномоченного руководителя. При этом вводится личный идентификационный номер сотрудника, который выносит предметы. При подходе к проходной этот список автоматически (по предъявлению идентификационной карточки сотрудника) выводится на дисплей контролера, который сверяет список.

Гибкость ПО современных систем контроля доступа позволяет достаточно легко изменять их конфигурацию, менять заданные условия нахождения в помещениях и на территории для любого сотрудника.

В целях повышения надежности функционирования СКУД их программное обеспечение может предусматривать функционирование центральных рабочих станций в связке двух машин в режиме параллельной обработки данных.

2. УСТРОЙСТВА ИДЕНТИФИКАЦИИ (СЧИТЫВАТЕЛИ)

Для идентификации личности современные электронные СКУД используют устройства нескольких типов. Наиболее распространенными являются:

- кодонаборные устройства ПИН-кода (кнопочные клавиатуры);
- считыватели бесконтактных смарт-карт (интерфейс Виганда);
- считыватели проксимити-карт;
- считыватели ключа «тач-мемори»;
- считыватели штрих-кодов;
- биометрические считыватели.

В настоящее время самое широкое распространение получили всевозможные считыватели карт (проксимити, Виганда, с магнитной полосой и т. п). Они имеют свои неоспоримые преимущества и удобства в использовании, однако при этом в автоматизированном пункте доступа контролируется «проход карточки, а не человека». В то же время карточка может быть потеряна или украдена злоумышленниками. Все это снижает возможность использования СКУД, основанных исключительно на считывателях карт, в приложениях с высокими требованиями к уровню безопасности. Несравненно более высокий уровень безопасности обеспечивают всевозможные биометрические устройства контроля доступа, использующие в качестве идентифицирующего признака биометрические параметры человека (отпечаток пальца, геометрия руки, рисунок сетчатки глаза и т. п.), которые однозначно предоставляют доступ только определенному человеку - носителю кода (биометрических параметров). По на сегодняшний день подобные устройства все еще остаются достаточно дорогими и сложными, и поэтому находят свое применение только в особо важных пунктах доступа. Учитывая особую важность и перспективность биометрических считывателей, они будут рассмотрены в отдельном разделе.

Считыватели штрих-кодов в настоящее время практически не устанавливаются, поскольку подделать пропуск чрезвычайно просто на принтере или на копировальном аппарате.

Рассмотрим принципы работы и использования представленных устройств идентификации.

2.1. Кодонаборные устройства (клавиатуры)

Кодонаборные устройства (клавиатуры) являются достаточно простыми и недорогими устройствами с понятным и легко принимаемым различными категориями пользователей интерфейсом. Принцип действия кнопочных клавиатур достаточно ясен: если набранный на клавиатуре код доступа верен, то проход на защищаемую территорию разрешен.

Клавиатуры СКУД можно считать «псевдобиометрическими» устройствами СКУД, так как носителем ПИН-кода является память человека. Ответственность за его сохранность и использование неполномочным лицом возлагается на пользователя СКУД. Тем самым использование клавиатур контроля доступа делает пользователя СКУД активным участником программы безопасности. При этом, так как носителем кода является человек, необходимо рассмотреть возможность ввода ПИН-кода пользователем под угрозой ему или его близким (что, впрочем, относится и к использованию карт или биометрических считывателей). В случае с клавиатурами пользователь СКУД может быть снабжен так называемым «кодом под принуждением» (чаще всего это дополнительная цифра, вводимая после основного кода), при использовании которого доступ предоставляется, но при этом на посты (станции) охраны подается сигнал тревоги Однако, несмотря на все свои несомненные достоинства, подавляющее большинство клавиатур СКУД имеет один серьезный недостаток - ПИН-код, вводимый с них, может быть легко перехвачен как человеком, стоящим рядом, так и злоумышленником, находящимся на удалении и вооруженным устройствами визуального съема информации.

Для повышения уровня безопасности контроля доступа может использоваться двойная технология, подразумевающая совместное использование клавиатуры для ввода ПИН-кода и считывателя какого-либо типа (в зависимости от необходимого уровня обеспечения безопасности и финансовых или организационных ограничений). Однако подобное решение усложняет процедуры использования СКУД, является более дорогим в исполнении и сложным в обслуживании. В связи с этим рассмотрим возможности защиты вводимого ПИН-кода непосредственно на клавиатуре.

Первый вариант - предусмотреть такой способ установки клавиатуры, при котором возможность увидеть набираемый пользователем ПИН-код будет если не исключена полностью, то минимизирована. Этот результат также может быть достигнут использованием различных экранов, прикрывающих цифры на клавиатуре. При этом такое решение не может быть оптимальным, так как иногда нет возможности сильно варьировать местоположение клавиатуры или ее внешний вид. Существует еще одна угроза - только что введенный ПИН-код может быть снят с кнопок клавиатуры злоумышленником с помощью спецсредств.

Более широкие возможности предоставляют не кнопочные клавиатуры с нанесенными цифрами, а с электронным кодонаборным устройством, использующим для отображения информации светодиодные индикаторы. В этом случае для защиты от подсматривания вводимого ПИН-кода могут быть применены поляризационные фильтры, ограничивающие угол обзора, при котором можно различить отображаемые на клавиатуре цифры. Следующее преимущество подобных кодонаборных устройств заключается в том, что отображаемые на клавиатуре цифры не привязаны к определенному местоположению (кнопке). Используя эффект скремблирования (смешива-

ния), можно добиться того, что при каждом использовании клавиатуры цифры будут располагаться в новом, случайном порядке. А если цифры будут загораться только при активации клавиатуры пользователем и гаснуть сразу после ввода ПИН-кода, то снятие только что введенного ПИН-кода станет невозможным.

Все рассмотренные методики защиты ПИН-кода на этапе ввода нашли свое применение в современных кодонаборных устройствах высокозащищенных систем контроля и управления доступа.

Для защиты от перехвата информации, предаваемой по линиям связи между устройством контроля доступа и управляющим устройством СКУД, используются шифрование данных, циркулирующих в системе, другие безопасные способы передачи информации и контроль за несанкционированным подключением к линиям связи

2.2. Бесконтактные считыватели

2.2.1. Бесконтактные считыватели HID Corporation

Бесконтактные считыватели HID Corporation* предназначены для приема информации с проксимити-карты (пропуска) и передачи ее в контроллер СКУД. Как правило, считыватели устанавливают на входе в здание, офис или любое помещение. При поднесении на определенном расстоянии к считывателю HID электронного пропуска (проксимити-идентификатора), содержащего персональный код доступа, считыватель распознает код и передает его в контроллер СКУД. На основании этой информации контроллер принимает решение о запрете/разрешении прохода владельца пропуска в помещение, на входе которого установлен считыватель.

Работа считывателя СКУД, в которой используются проксимити-идентификаторы, основывается на технологии дистанционной радиочастотной передачи и приема информации. Конструктивно считыватели компании HID выполнены в виде небольшого корпуса, содержащего приемопередающую антенну, передатчик, приемник и устройство обработки сигналов. Проксимити-идентификатор, содержащий код доступа на охраняемый объект, также имеет антенну и приемно-обрабатывающее устройство. Во время работы считыватель постоянно посылает радиосигналы, поэтому при внесении, например, проксимити-брелка в зону действия считывателя радиочастотный сигнал считывателя принимается антенной идентификатора, детектируется и накапливается. За счет накопленной энергии устройство проксимити-брелка активизируется и излучает радиосигнал со своим кодом. Антенна считывате-

Корпорация HID Corporation вышла на рынок СКУД в 1991 г. Она входит в холдинг ASSA ABLOY Croup (г. Ирвин штат Калифорния, США). Производит проксимити-карты, брелки, автомобильные идентификаторы, смарт-карты, считыватели различных модификаций. Штат корпорации насчитывает более 400 человек.

ля принимает код проксимити-брелка, а устройство обработки сигнала посылает принятый код на контроллер, который принимает решение о праве его владельца на проход и дает команду на электромеханический замок, который разблокирует дверь. При этом весь процесс считывания информации с идентификатора занимает менее одной миллисекунды.

Простота монтажа, вандалозащищенность, надежность и долговечность, а также герметичность корпуса и работоспособность в широком температурном диапазоне позволяют устанавливать считыватели HID как в помещении, так и на улице. На лицевой панели считыватели имеют трехцветный светодиод индикации срабатывания и зуммер, информирующие входящего человека о действиях считывателя. Конструкция корпуса считывателя допускает различные варианты установки. Монтаж считывателя не требует специальных навыков.

В зависимости от конфигурации СКУД и условий ее применения HID Corporation предлагает различные считыватели. Так, помимо проксимити-считывателей, обеспечивающих дистанционное считывание идентификационного кода ряда проксимити-идентификаторов, производятся проксимити-считыватели с клавиатурой.

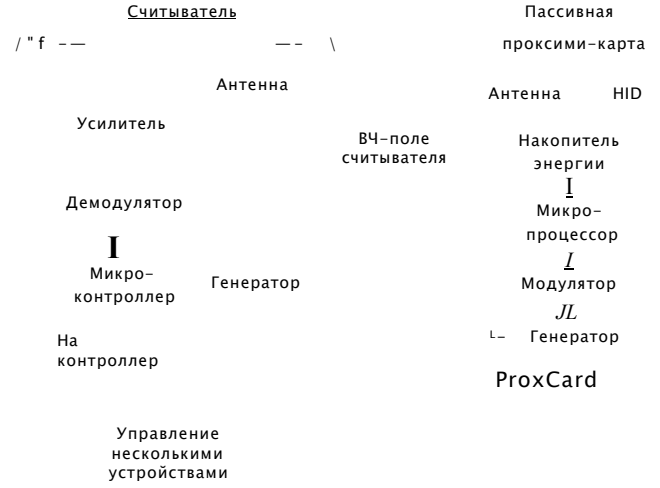


Рис. 2.1. Бесконтактный считыватель HID Corporation

Эти считыватели HID, помимо распознавания кодовой информации, например, Виганда-карты, требуют еще и ввода персонального номера с клавиатуры. На особо ответственных объектах используют бесконтактные считыватели iCLASS и считыватели MIFARE, отличающиеся возможностью их использования в нескольких приложениях и высокой криптозащитой данных. На рис. 2.1 приведена схема бесконтактного считывателя HID Corporation.

2.2.2. Бесконтактные считыватели iCLASS

Бесконтактные считыватели iCLASS компании HID Corporation предназначены для работы в СКУД и используют современные технологии чтения и записи данных на смарт-карты iCLASS.

Идентификаторы iCLASS различаются по объему доступной памяти и по внешнему виду. По объему памяти они могут быть либо 2 Кбит, либо 16 Кбит, последние могут иметь 2 или 16 независимых областей памяти. По внешнему виду они могут быть в виде карт, брелков и меток.

Конструктивно смарт-карта iCLASS представляет собой пластиковую карточку толщиной 0,79 мм, внутри которой находятся микросхема и приемопередающая антенна, работающая на частоте 13,56 МГц. Помимо приемопередатчика в микросхеме имеется шифратор, с объемом памяти 2 или 16 Кбит. Эта память разделена на 2 или 16 секторов. Каждый сектор состоит из 4 блоков, размер блока равен 16 или 32 байт.

Срок сохранности карты составляет около 10 лет, карта допускает около 100000 циклов записи/считывания. Смарт-карты iCLASS относятся к классу пассивных карт, так как не имеют своего источника питания.

Бесконтактные считыватели идентифицируют коды доступа, записанные на смарт-карты, и передают их на контроллер СКУД, который подает напряжение на **электромеханический замок** пли **турникет,** разблокируя их, если владельцу карты разрешен проход на охраняемый объект. Эти бесконтактные считыватели и бесконтактные смарт-карты являются компонентами новой технологии iCLASS компании HID и работают на частоте 13,56 МГц. Применяя это оборудование, можно обеспечить достаточно высокий уровень безопасности объекта, поскольку в iCLASS используются специальные алгоритмы обработки ключей кодирования и взаимной идентификации. При этом бесконтактные считыватели iCLASS просты в эксплуатации, стабильны в работе и легко монтируются на любые поверхности

Технология iCLASS обеспечивает чрезвычайно ***высокую степень безопасности СКУД*** за счет использования более длинных по сравнению с технологией M1FARE 64-битовых идентификационных ключей и более сложного алгоритма шифрования. По технологии iCLASS бесконтактный считыватель и смарт-карта содержат специальные программируемые ключи, только при совпадении которых смарт-карта передает бесконтактному считывателю свой код доступа. Такая система ключей с взаимной идентификацией бесконтактного считывателя и карты снижает также и риск дублирования карт.

В линейке новых бесконтактных считывателей iCLASS присутствуют как модели считывателей только для чтения, так и модели, позволяющие считывать/записывать данные на смарт-карты. Бесконтактные считыватели второй группы позволяют использовать смарт-карты iCLASS не только для СКУД, но и для других корпоративных приложений, например, доступа в информационную сеть. При этом считыватель может записывать на смарт-карту ин-

формацию, которая требуется для работы данного приложения, например о числе и времени проходов сотрудника через дверь или турникет для системы учета рабочего времени. Данные между считывателем и картой передаются в зашифрованном виде с применением алгоритмов повышенной безопасности. Это позволяет использовать бесконтактные считыватели и для особо ответственных задач, таких как вход в компьютерную сеть, электронные наличные деньги, хранение шаблонов биометрических данных, учет рабочего времени и пр.

В настоящее время выпускаются следующие виды смарт-карт, изготовляемые по технологии iCLASS:

iCIass Card - тонкая бесконтактная карта, работающая на частоте 13,56 МГц и имеющая возможность печати изображения на принтере карт. На карту можно наносить штрих-код.

iCIass 1'rox Card - тонкая бесконтактная карта, содержащая два чипа: Smart (f = 13,56 МГц) и Proximity (f = 125 кГц). Эта карта одновременно может использоваться в двух системах (на основе Proxmity и Smart-карт). Имеется возможность печати изображения.

iCIass Wiegand Card - карта с использованием возможностей считывателей карт Виганда. Имеется возможность печати изображения на принтере карт.

iCIass Key - миниатюрный бесконтактный брелок с интегрированным Smart-чипом (f = 13,56 МГц).

iCIass Tag - миниатюрная бесконтактная метка с интегрированным Smart-чипом (f = 13,56 МГц). Может наноситься на любые неметаллические поверхности и использоваться не только для идентификации людей. Метка выполнена в виде диска диаметром 32 мм и толщиной 1,78 мм.

Все карты имеют стандартные размеры 84 х 54 х 0,79 мм и изготавливаются из поливинирхлорида.

Так как смарт-карты iCLASS имют более длинные ключи доступа, а также более сложные алгоритмы шифрования, то они лучше защищены от подделки и несанкционированного доступа к информации. Расстояния, на которых считыватели распознают карту, составляют от 7 до 21 см.

В качестве идентификационного кода, как правило, используется порядковый номер карты, который записывается в один из ее секторов на заводе и не повторяется на других картах.

HID Corporation выпускает более 15 моделей смарт-карт iCLASS, отличающихся друг от друга числом секторов, а также типом второго чипа. Все модели отвечают стандартам CR80 ISO 7810 (по размеру и толщине).

Все бесконтактные считыватели iCLASS имеют интерфейс Виганда, который считается стандартным для систем контроля доступа, а считыватели, поддерживающие чтение/запись, имеют еще и порт RS-232. Кроме того, счи-

тыватели iCLASS могут считывать как данные с карт стандартного формата iCLASS, так и уникальные идентификационные номера смарт-карт MIFARE.

Различные тональные последовательности, создаваемые бесконтактным считывателем, служат для индикации таких состояний, как «доступ разрешен», «доступ запрещен», включение питания и диагностика. При этом звуковая индикация дублируется визуальной. Яркий световой индикатор обеспечивает четкую индикацию текущего режима, используя красный, зеленый или желтый цвета, хорошо различимые даже при ярком солнечном свете. Корпус бесконтактного считывателя, выполненный из поликарбоната, устойчив к любым погодным условиям и обеспечивает защиту считывателя от вандализма.

2.2.3. Проксимити-считыватели с клавиатурой PrоxPro

Проксимити-считыватели с клавиатурой PrоxPro компании HID Corporation устанавливаются в СКУД объектов, к которым предъявляются повышенные требования по безопасности. Внешний вид устройства показан на рис. 2.2.

Рис. 2.2. Проксимити-считыватели с клавиатурой PrоxPro

В отличие от обычных проксимити-считывателей, эти считыватели имеют еще и кодонаборную клавиатуру для ввода второго идентификационного кода. Так, для прохода в охраняемое помещение, у двери которого расположен считыватель с клавиатурой, сотрудник компании должен поднести к считывателю свой проксимити-идентификатор, содержащий персональный код доступа, а также набрать на клавиатуре считывателя второй, известный только ему идентификационный (ПИН) код. Обработав оба кода, считыватель с клавиатурой отправляет их на контроллер СКУД, который сравнивает эти коды с кодами, по которым доступ в данное помещение разрешен В случае если проход в охраняемое помещение разрешен, то контроллер подает напряжение на электромеханический замок, который разблокирует дверь, или напряжение на разблокировку турникета, который обслуживает данный считыватель. Такие считыватели с клавиатурой не допустят прохода на объект лиц по похищенным или чужим проксимити-картам или проксимити-брелкам.

Считыватели с клавиатурой ProxPro характеризуются простотой монтажа и надежностью клавиатуры. Их устанавливают как в помещении, так и на улице. Прочный герметичный корпус из специального пластика обеспечивает стабильную работу считывателя с клавиатурой в различных климатических условиях и защищает электронику от вандализма. Считыватель совместим со всеми протоколами Виганда и может работать в СКУД различных производителей. Считыватели с клавиатурой отличаются малым энергопотреблением, высокой надежностью работы и удобством монтажа.

Индикатор считывателя с клавиатурой ProxPro содержит трехцветный светодиод и зуммер для индикации действий считывателя. При считывании идентификатора, например Виганда-карты, светодиод переключается с красного цвета на зеленый, если доступ разрешен, при этом дополнительно звучит зуммер. Оба индикатора считывателя могут также управляться дистанционно с контроллера системы.

При несанкционированном вскрытии корпуса считывателя с клавиатурой срабатывает специальный встроенный датчик, включающий сигнализацию. Считыватели с клавиатурой поддерживают карты с форматом кода до 85 бит, что составляет 137 миллиардов уникальных комбинаций. Встроенная программа самодиагностики осуществляет проверку и подтверждение заданной конфигурации, устанавливает внутреннее или внешнее управление светодиодом и зуммером. При тестировании центральным контролером осуществляется проверка работы выходов и входов считывателя без использования дополнительного тестирующего оборудования.

2.2.4. Активные проксимити-идентификаторы ProxPass для установки на автомобили

Проксимити-идентификаторы ProxPass компании MID Corporation представляют собой пластиковые электронные пропуска или идентификаторы, которые устанавливаются на легковые или грузовые автомобили с целью контроля и учета въезда/выезда автомобилей на охраняемой территории. ProxPass относятся к классу активных проксимити-идентификаторов, которые считываются проксимити-считывателями на расстоянии до 2,5 м. Эти проксимити-идентификаторы применяются для контроля передвижения легкового, грузового транспорта, вагонов, контейнеров и пр.

При въезде или выезде с контролируемой территории проксимити-идентификатор, стоящий на автомобиле, излучает электромагнитный сигнал, который содержит персональный код данного автомобиля. Этот сигнал принимает считыватель, находящийся в зоне ворот или шлагбаума. После приема сигнала с проксимити-идентификатора считыватель направляет полученный код на контроллер СКУД, который сравнивает его с кодами допущенных на территорию автомобилей. Если код идентифицирован как «свой», СКУД фиксирует дату и время проезда и открывает ворота или шлагбаум.

Благодаря простоте монтажа и доступности проксимити-идентификаторы ProxPass получили наиболее широкое применение в СКУД автопарков, автобаз и служебных парковок как простое и надежное устройство системы ограничения доступа и учета движения автомобилей. В зависимости от модели различные считыватели HID распознают код идентификатора ProxPass на расстоянии от 1,9 до 2,5 м. Обычно проксимити-идентификатор крепится на внутренней стороне ветрового стекла автомобиля в верхнем или нижнем углу. При креплении на металлическую поверхность расстояние считывания незначительно уменьшается. Для надежного крепления проксимити-идентификатора к поверхности стекла на его обратную сторону нанесен специальный липкий слой.

Идентификаторы ProxPass имеют высокую степень защиты, поскольку на них можно записать индивидуальный код длинной 85 бит или один код из 137 млрд комбинаций. Продолжительность работы проксимити-идентификатора от встроенной батареи составляет от 2 до 5 лет и зависит от интенсивности его использования. Корпус идентификатора, сделанный из поликарбоната, прочен, водонепроницаем и устойчив к ультрафиолетовому излучению. Проксимити-идентификаторы могут работать в диапазоне температур от -30 до +80° С.

Для проксимити-идентификатора специалисты HID рекомендуют использовать проксимити-считыватель MaxiProx, разработанный специально для условий, где требуется большое расстояние считывания При использовании проксимити-идентификатора ProxPass дистанция считывания MaxiProx составляет до 240 см. Для идентификации грузового транспорта (установка считывателя на большой высоте) и легкового транспорта (установка считывателя на малой высоте) обычно используют два считывателя MaxiProx, которые монтируются на расстоянии более 1 м друг от друга. Заметим, что проксимити-идентификаторы работают как среднечастотном диапазон и должны соответствовать международным стандартам ISO 15693 и ISO 14443 (f= 33 -500 кГц), так и в высокочастотном диапазоне (f= 2,5 МГц - 10 ГГц).

2.3. Считыватели идентификационных карт Виганда

Карты Виганда представляют собой пластиковую карточку, в которую при изготовлении запрессованы хаотично расположенные отрезки проволочек из специального магнитного сплава. Считывание карты происходит с помощью электромагнитного поля, индуцируемого считывателем. При проведении карты через щель считывателя два ряда проволочек, запаянных в карту, вызывают разнополярные всплески индукционного тока, который преобразуется в двоичный код. Карты Виганда имеют хорошие эксплутационные характеристики.

Благодаря отсутствию движущихся частей и герметичности корпуса карта отличается высокой надежностью и долговечностью функционирования, высокой стойкостью по отношению к попыткам физического разрушения и неблагоприятным климатическим условиям, в частности, может работать в

диапазоне температур от -40 до + 70 °С. К недостаткам этой технологии можно отнести довольно высокую (по сравнению с магнитными) стоимость изготовления карточек при их коротком жизненном цикле. Кроме того, по сравнению с магнитной дорожкой плотность записи информации здесь меньше примерно на треть.

В настоящее время аппаратура на базе считывателей идентификационных карточек Виганда выпускается целым рядом зарубежных фирм. Это карточки SENSORCARD фирмы SENSOR Engineering Co., система Pass-4000 фирмы CardKey, система DODUCODE ID-Cardsystem немецкой фирмы Doduco KG.

Внешние считыватели карт Виганда похожи на считыватели магнитных карт, но их основное отличие - отсутствие магнитной головки

Корпорация HID Corporation предлагает интегрированный модуль считывания HID EntryProx, который позволяет считывать проксимити и карт Виганда. Память устройства может хранить до 2000 идентификационных кодов Считыватель связывается с котроллером проводом длиной до 3 м. Питание от источника 12 В, рабочий диапазон температур составляет от-35 до +60 °С.

Корпус устройства представляет собой кожух, внутри которого расположены: контроллер, микропроцессор, плата, порт. На переднюю панель выведена 12-кнопочная клавиатура. Считыватель имеет антенну для проксимити-карт и магнитный считыватель для карт Виганда.

На плате устройства расположены четыре разъема: 5-контактный Р1 позволяет подключать исполнительные устройства СКУД, разъем Р2 служит для подключения тревожного оборудования и/или кнопку выхода, через разъем Р4 подключаются считыватели проксимити-карт, а через Р3 - считыватель карт Виганда.

2.4. Считыватели карточек со скрытым штриховым кодом

Штриховой код представляет собой последовательность параллельных линий разной толщины, нанесенных на поверхность идентификатора. В ряде модификаций используется инфракрасное маскирование непрозрачной в оптическом диапазоне пленкой. Наиболее широко штрих-коды используются в торговых и складских системах.

В СКУД такая технология используется редко из-за низкой защищенности от подделки, невозможности перезаписи информации, низкой пропускной способности.

Но тем не менее СКУД на основе идентификационных карточек со скрытым штриховым кодом выпускаются многими фирмами Это, в частности, компании Intelligent Controls Inc. и Henderson Access Control Systems (США). Отдельно идентификационные карточки на базе скрытого штрихового кода, предназначенные для использования в различных СКУД, выпускаются, например, американской компанией Identification Systems Inc.

3. БИОМЕТРИЧЕСКИЕ СРЕДСТВА ИДЕИТФИКАЦИИ ЛИЧНОСТИ

3.1. Классификация и основные характеристики биометрических средств идентификации личности

Достоинства биометрических идентификаторов на основе уникальных биологических, физиологических особенностей человека, однозначно удостоверяющих личность, привели к интенсивному развитию соответствующих средств. В биометрических идентификаторах используются *статические методы,* основанные на физиологических характеристиках человека, т. е. на уникальных характеристиках, данных ему от рождения (рисунки папиллярных линий пальцев, радужной оболочки глаз, капилляров сетчатки глаз, тепловое изображение лица, геометрия руки, ДНК), и *динамические методы* (почерк и динамика подписи, голос и особенности речи, ритм работы на клавиатуре). Предполагается использовать такие уникальные статические методы, как идентификация по подноггевому слою кожи, по объему указанных для сканирования пальцев, форме уха, запаху тела, и динамические методы - идентификация по движению губ при воспроизведении кодового слова, по динамике поворота ключа в дверном замке и т. д. Классификация современных биометрических средств идентификации показана на рис. 3.1.

Биометрические идентификаторы хорошо работают только тогда, когда оператор может проверить две вещи: во-первых, что биометрические данные получены от конкретного лица именно во время проверки, а во-вторых, что эти данные совпадают с образцом, хранящимся в картотеке. Биометрические характеристики являются уникальными идентификаторами, но вопрос их надежного хранения и защиты от перехвата по-прежнему остается открытым

Биометрические идентификаторы обеспечивают очень высокие показатели: вероятность несанкционированного доступа - 0,1 - 0,0001 %, вероятность ложного задержания - доли процентов, время идентификации - единицы секунд, но имеют более высокую стоимость по сравнению со средствами атрибутной идентификации. Качественные результаты сравнения различных биометрических технологий по точности идентификации и затратам указаны на рис. 3.2. Известны разработки СКУД, основанные на считывании и сравнении конфигураций сетки вен на запястье, образцов запаха, преобразованных в цифровой вид, анализе носящего уникальный характер акустического отклика среднего уха человека при облучении его специфическими акустическими импульсами и т. д.

Тенденция значительного улучшения характеристик биометрических идентификаторов и снижения их стоимости приведет к широкому применению биометрических идентификаторов в различных системах контроля и управления доступом. В настоящее время структура этого рынка представля-

ется следующим образом: верификация голоса - 11 %, распознавание лица - 15 %, сканирование радужной оболочки глаза - 34 %, сканирование отпечатков пальцев - 34 %, геометрия руки - 25 %, верификация подписи - 3 %.

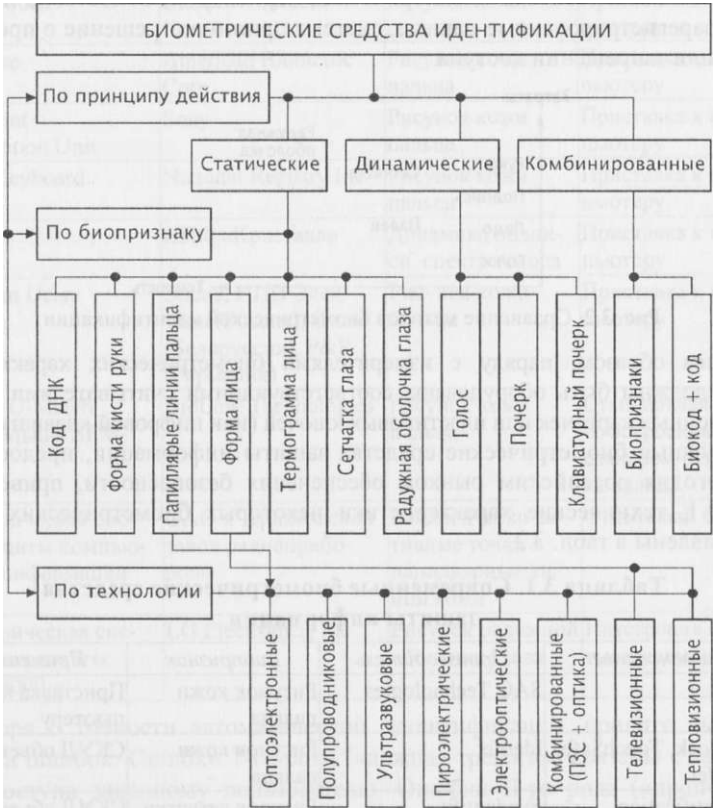


Рис. 3.1. Классификация современных биометрических средств идентификации

Любая биометрическая технология применяется поэтапно:

- сканирование объекта;
- извлечение индивидуальной информации;
- формирование шаблона;
- сравнение текущего шаблона с базой данных.

Методика биометрической аутентификации заключается в следующем. Пользователь, обращаясь с запросом к СКУД на доступ, прежде всего, идентифицирует себя с помощью идентификационной карточки, пластикового ключа или личного идентификационного номера. Система по предъявленному пользователем идентификатору находит в своей памяти личный файл

(эталон) пользователя, в котором вместе с номером хранятся данные его биометрии, предварительно зафиксированные во время процедуры регистрации пользователя. После этого пользователь предъявляет системе для считывания обусловленный носитель биометрических параметров. Сопоставив полученные и зарегистрированные данные, система принимает решение о предоставлении или запрещении доступа.

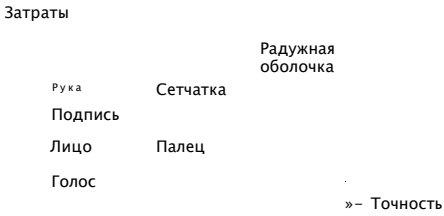


Рис. 3.2. Сравнение методов биометрической идентификации

Таким образом, наряду с измерителями биометрических характеристик СКУД должны быть оборудованы соответствующими считывателями идентификационных карточек или пластиковых ключей (или цифровой клавиатурой).

Основные биометрические средства защиты информации, предоставляемые сегодня российским рынком обеспечения безопасности, приведены в табл. 3.1, технические характеристики некоторых биометрических систем представлены в табл. 3.2.

Таблица 3.1. Современные биометрические средства защиты информации

Наименование	*Производитель*	*Биопризнак*	*Примечание*
SACcat	SAC Technologies	Рисунок кожи пальца	Приставка к компьютеру
TouchLock, TouchSafe, TouchNet	Identix	Рисунок кожи пальца	СКУД объекта
Eye Dentification System 7,5	Eyedentify	Рисунок сетчатки глаза	СКУД объекта (моноблок)
Ibex 10	Eyedentify	Рисунок сетчатки глаза	СКУД объекта (порт, камера)
eriprint 2000	Biometric Identification	Рисунок кожи пальца	СКУД универсал
ID3D-R Handkey	Recognition Systems	Рисунок ладони руки	СКУД универсал
HandKey	Escape	Рисунок ладони руки	СКУД универсал

Наименование	*Производитель*	*Биопризнак*	*Примечание*
ICAM 2001	Eyedentify	Рисунок сетчатки глаза	СКУД универсал
Secure Touch	Biometric Access Corp.	Рисунок кожи пальца	Приставка к компьютеру
BioMouse	American Biometric Corp	Рисунок кожи пальца	Приставка к компьютеру
Fingerprint Identification Unit	Sony	Рисунок кожи пальца	Приставка к компьютеру
Secure Keyboard Scanner	National Registry Inc.	Рисунок кожи пальца	Приставка к компьютеру
Рубеж	НПФ «Кристалл»	Динамика подписи, спектр голоса	Приставка к компьютеру
Дакточип Delsy	Элсис, НПП Электрон (Россия), Опак (Белоруссия), P&P (Германия)	Рисунок кожи пальца	Приставка к компьютеру
BioLink U-Match Mouse, Мышь SFM-2000A	BioLink Technologies	Рисунок кожи пальца	Стандартная мышь со встроенным сканером отпечатка пальца
Биометрическая система защиты компьютерной информации Дакто	ОАО «Черниговский завод радиоприборов»	Биологически активные точки и папиллярные линии кожи	Отдельный блок
Биометрическая система контроля Iris Access 3000	LG Electronics, Inc	Рисунок радужной оболочки глаза	Интеграция со считывателем карт

Говоря о точности автоматической аутентификации, принято выделять два типа ошибок Ошибки 1-го рода («ложная тревога») связаны с запрещением доступа законному пользователю. Ошибки И-го рода («пропуск цели»)- предоставление доступа незаконному пользователю. Причина возникновения ошибок состоит в том, что при измерениях биометрических характеристик существует определенный разброс значений. В биометрии совершенно невероятно, чтобы образцы и вновь полученные характеристики давали полное совпадение. Это справедливо для всех биометрических характеристик, включая отпечатки пальцев, сканирование сетчатки глаза или опознание подписи. Например, пальцы руки не всегда могут быть помещены в одно и то же положение, под тем же самым углом или с тем же самым давлением. И так каждый раз при проверке.

Таблица 3.2. Технические характеристики некоторых биометрических систем

Модель	*Принцип действия*	*Вероятность ложного задержания, %*	*Вероятность ложного допуска, %*	*Время идентификации, с*
Eye Dentify	Параметры глаза	0,001	0,4	1,5-4
Iriscan	Параметры зрачка	0,00078	0,00068	2
Identix	Отпечаток пальца	0,0001	1,0	0,5
Startek BioMet	Отпечаток пальца	0,0001	1,0	1
Partners Recognition	Геометрия руки	0,1	0,1	1
Systems	Геометрия руки	0,1	0,1	1
«Кордон»	Отпечаток пальца	0,0001	1,0	1
DS-100	Отпечаток пальца	0,001	-	1-3
TouchSafe Personal(8)	Отпечаток пальца	2	0,001	1
Eyedentify ICAM 2001 (Eyedentify)	Параметры сетчатки глаза	0,4	0,0001	1,5-4
Iriscan (Iriscan)	Параметры радужной оболочки глаза		0,00078	2
FingerScan (Identix)	Отпечаток пальца	1,0	0,0001	0,5
TouchSafe (Identix)	Отпечаток пальца	2,0	0,001	1
TouchNet (Identix)	Отпечаток пальца	1,0	0,001	3
Startek	Отпечаток пальца	1,0	0,0001	1
1D3D-R NDKEY (Recognition Systems)	Геометрия руки	0,1	0,1	1
U.areU. (Digital Persona)	Отпечаток пальца	3,0	0,01	1
Fill (Sony, I/O Software)	Отпечаток пальца	0,1	1,0	0,3
BioMause (ABC)	Отпечаток пальца	-	0,2	1
Кордон (Россия)	Отпечаток пальца	1,0	0,0001	1
DS-100 (Россия)	Отпечаток пальца	-	0,001	1…3
BioMet	Геометрия руки	0,1	0,1	1
Veriprint 2100 (Biometric ID)	Отпечаток пальца	0,001	0,01	1

Таким образом, биометрический процесс (под ним здесь понимается автоматизация оценки биометрических характеристик) констатирует уровень надежности, который гарантирует система в выявлении истинности проверяемого лица. Процесс не заявляет, что предъявленные характеристики являются точной копией образцов, а говорит о том, что вероятность того, что пользователь именно то лицо, за которое себя выдает, составляет величину X %. Всегда ожидается (предполагается), что автоматический процесс должен обеспечить вероятность правильного распознавания равную пли очень близкую к 100 %. Таким образом, намек на то, что здесь могут быть элементы

ошибки, заставляет некоторых думать, что биометрия не может играть существенной роли в организации входного контроля. Анализ показывает, что хотя ни одна система аутентификации не обеспечивает 100 %-ной надежности и что биометрический процесс не дает точного совпадения характеристик, все же он дает чрезвычайно высокий уровень точности. Некоторые зарубежные охранные структуры к разработчикам (производителям) СКУД применяют априори заданные требования, при выполнении которых последние могут рассчитывать на продажу своих систем.

Уровень надежности, дозволенный для системы контроля доступа, может быть совершенно различным, однако уровень ложных отказов истинным пользователям не вызывает какого-либо беспокойства, в то время как уровень фальшивых доступов фактически должен быть доведен до нуля.

Поскольку уровень надежности при сравнении может в конечном итоге регулироваться с тем, чтобы удовлетворить запросы конкретного потребителя, чрезвычайно важно этому пользователю реально представлять себе, чего данная система способна достигнуть. Наибольшую степень озабоченности вносит то, что фирмы-производители часто задают степени точности: скажем, 0,01% (т. е. 1 ошибка на 10 000 случаев аутентификации).

Можно получить статистические доказательства, позволяющие компьютеру сделать соответствующие расчеты, подтверждающие приведенные цифры, однако большинство пользователей не совсем доверяют этим результатам. Тем не менее реальная картина не столь мрачна, как кажется на первый взгляд. Большинство биометрических методов чрезвычайно точны. Так, результаты работы в г. Ньюхема в 1998 г. комплексной системы видеонаблюдения, дающей возможность идентификации преступников, впечатляют: уровень нападения на граждан снизился на 21%, нанесение ущерба имуществу граждан сократилось на 26 %, а уровень краж имел беспрецедентное снижение на целых 39 %.

Заметное оживление на рынке биометрических систем произошло после появления довольно мощных и в то же время недорогих 16-битовых микропроцессоров и создания эффективных алгоритмов обработки биометрической информации В настоящее время биометрические терминалы разрабатываются и предлагаются к продаже в основном фирмами США, небольшим количеством фирм в Англии, России, Украины, есть информация о работах в этом направлении в Японии и во Франции.

3.2. Особенности реализации статических методов биометрического контроля

3.2.1. Идентификация по рисунку папиллярных линий

Применение данной технологии получило широкое распространение в системах автоматической идентификации по отпечатку пальца (AFIS).

Весь *процесс идентификации* занимает не более нескольких секунд и не требует усилий от тех, кто использует данную систему доступа. В настоящее время уже производятся подобные системы размером меньше колоды карт. Определенным недостатком, сдерживающим развитие данного метода, является предубеждение части людей, которые не желают оставлять информацию о своих отпечатках пальцев. При этом контраргументом разработчиков аппаратуры является заверение в том, что информация о папиллярном узоре пальца не хранится - хранится лишь короткий идентификационный код, построенный на базе характерных особенностей отпечатка вашего пальца. По данному коду нельзя воссоздать узор и сравнить его с отпечатками пальцев, оставленными, допустим, на месте преступления. Преимущества доступа по отпечатку пальца - простота использования, удобство и надежность. Хотя процент ложных отказов при идентификации составляет около 3 %, ошибка ложного доступа - меньше 0,00001 % (1 на 1 000 000).

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.

Традиционно американские компании занимают лидирующие позиции в разработке биометрических систем безопасности, в этом направлении успешно работают такие фирмы, как Identix, T-Netix, American Biometric Company, National Registry, sagem, Morpho, Verditicom, Infenion. Из российских компаний-разработчиков идентификационных устройств по папиллярным узорам пальцев заслуживает внимания компания «Биолинк».

С целью идентификации личности по рисунку папиллярных линий пальца проверяемый набирает на клавиатуре свой идентификационный номер и помещает указательный палец на окошко сканирующего устройства. При совпадении получаемых признаков с эталонными, предварительно заложенными в память ЭВМ и активизированными при наборе идентификационного номера, подается команда исполнительному устройству. Хотя рисунок папиллярных линий пальцев индивидуален, использование полного набора их признаков чрезмерно усложняет устройство идентификации. Поэтому с целью его удешевления применяют признаки, наиболее легко измеряемые автоматом. Выпускают сравнительно недорогие устройства идентификации по отпечаткам пальцев, действие которых основано на измерении расстояния между основными дактилоскопическими признаками. На величину вероятности ошибки опознания влияют также различные факторы, в том числе температура пальцев (рис. 3.3). Кроме того, процедура аутентификации у некоторых пользователей ассоциируется с процедурой снятия отпечатков у преступников, что вызывает у них психологический дискомфорт.

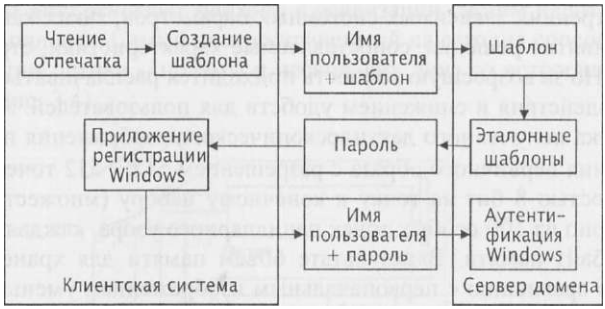


Рис. 3.3. Процесс аутентификации по отпечаткам пальцев

Дактилоскопия построена на двух основных качествах, присущих папиллярным узорам кожи пальцев и ладоней:

- стабильность рисунка узора на протяжении всей жизни человека;
- уникальность рисунка, что означает отсутствие двух индивидуумов с одинаковыми дактилоскопическими отпечатками.

Распознавание отпечатка пальца основано на анализе распределения особых точек (концевых точек и точек разветвления папиллярных линий), местоположение которых задается в декартовой системе координат.

Для снятия отпечатков в режиме реального времени применяются специальные контактные датчики различных типов. Системы идентификации по отпечаткам пальцев выпускаются в течение почти трех десятков лет Однако благодаря достигнутым успехам в области машинного распознавания отпечатков только в последние годы заметно увеличилось число фирм, выпускающих терминалы персональной аутентификации на базе дактилоскопии.

Американская фирма Fingermatrix предложила терминал Ridge Reader, который благодаря процедуре компенсации различных отклонений, возникающих при снятии отпечатка пальца в реальных условиях, а также применяемому способу «очищения» изображения и восстановления папилярного узора (который может быть «затуманен» из-за наличия на пальце грязи, масла или пота) допускает коэффициент ошибок 1-го рода не более 0,1 %, 2-го рода - не более 0,0001 %. Время обработки изображения составляет 5 с, регистрации пользователя составляет 2-3 мин. Для хранения одного цифрового образа отпечатка (эталона) расходуется 256 байт памяти.

Компания De La Rue Printrak Inc. производит систему PIV-100 на базе терминала аутентификации по отпечаткам пальцев. Кроме этих терминалов, в состав аппаратуры входят центральный процессор, контрольный пульт, дисплей, принтер, накопители на винчестерских дисках (для хранения базы данных), накопители на гибких дисках (для резервной памяти).

В этой системе требуемые коэффициенты ошибок могут выбираться в зависимости от необходимого уровня обеспечения безопасности путем под-

стройки внутренних зависимых системных параметров, таких как пороговые значения принятия решения, сопоставляемые характеристики, стратегия распознавания. Но за возросшую точность приходится расплачиваться уменьшением быстродействия и снижением удобств для пользователей. Автоматическая обработка полученного дактилоскопического изображения начинается с преобразования первичного образа с разрешением 512 х 512 точек изображения и плотностью 8 бит на точку к конечному набору (множеству), состоящему примерно из 100 особых точек папиллярного узора, каждая из которых занимает 3 байт памяти. В результате объем памяти для хранения одного отпечатка по сравнению с первоначальным изображением уменьшается примерно в 1000 раз. Сопоставление двух дактилоскопических образов - оригинального и эталонного, хранящегося в памяти системы, - производится с помощью некоторой корреляционной процедуры. Время регистрации пользователя в базе данных - меньше 2 мин; вся процедура проверки пользователя занимает около 10 с, из которых 2 с уходит на аутентификацию, т. е. на вычисления по сопоставлению отпечатков.

Говоря о надежности аутентификационной процедуры по отпечаткам пальцев, необходимо рассмотреть также вопрос о возможности их копирования и использования другими лицами для получения несанкционированного доступа. В качестве одной из возможностей по обману терминала специалисты называют изготовление искусственной кисти с требуемыми отпечатками пальцев (или изъятия «подлинника» у законного владельца). Но существует и способ борьбы с такой фальсификацией. Для этого в состав терминального оборудования должны быть включены инфракрасный детектор, который позволит зафиксировать тепловое излучение от руки (или пальца), и (или) фотоплетизмограф, который определяет наличие изменений отражения света от поверхности потока крови.

Другим способом подделки является непосредственное нанесение папиллярного узора пальцев законного пользователя на руки злоумышленника с помощью специальных пленок или пленкообразующих составов. Такой способ довольно успешно может быть использован для получения доступа через КПП. Однако в этом случае необходимо получить качественные отпечатки пальцев законного пользователя, причем именно тех пальцев, которые были зарегистрированы системой, и именно в определенной последовательности (например, если система настроена на проверку не одного, а двух и более пальцев по очереди), но эта информация неизвестна законному пользователю и, следовательно, он не может войти в сговор с нарушителем.

По оценкам западных экспертов до 80% рынка биометрии сегодня занимают устройства идентификации по отпечаткам пальцев. Это объясняется следующим: во-первых, это один самых доступных и недорогих методов, во-вторых, методика идентификации по отпечаткам пальцев проста в использовании, удобна и лишена психологических барьеров, которые имеются, например, у систем, требующих воздействия на глаз световым пучком.

Известны *три основных подхода* к реализации систем идентификации по отпечаткам пальцев. Самый распространенный на сегодня способ строится на использовании оптики - призмы и нескольких линз со встроенным источником света (рис. 3.4).

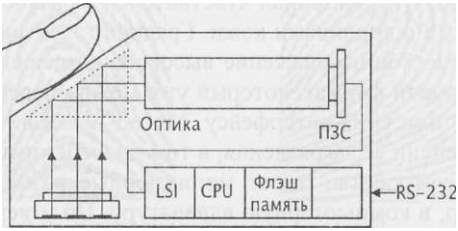


Рис. 3.4. Функциональная схема системы FIU фирмы SONY

Свет, падающий на призму, отражается от поверхности, соприкасаемой с пальцем пользователя, и выходит через другую сторону призмы, попадая на оптический сенсор (обычно, монохромная видеокамера на основе ПЗС-матрицы), где формируется изображение. Недостатки такой системы: отражение сильно зависит от параметров кожи - сухости, присутствия масла, бензина, других химических элементов. Например, у людей с сухой кожей наблюдается эффект размытия изображения и в результате - высокая доля ложных срабатываний.

Другой способ использует методику измерения электрического поля пальца с использованием полупроводниковой пластины. Когда пользователь устанавливает палец в сенсор, он выступает в качестве одной из пластин конденсатора (рис. 3.5). Другая пластина конденсатора - это поверхность сенсора, которая состоит из кремниевого чипа, содержащего 90 тыс. конденсаторных пластин с шагом считывания 500 точек на дюйм. В результате получается 8-битовое растровое изображение гребней и впадин пальца.

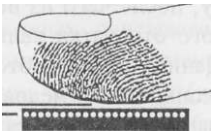


Рис. 3.5. Система идентификации
на основе полупроводниковой пластины

Естественно, в данном случае жировой баланс кожи и степень чистоты рук пользователя не играет никакой роли. Система идентификации в этом случае, получается гораздо более компактная. Недостатки метода - кремниевый чип требует эксплуатации в герметичной оболочке, а дополнительные покрытия уменьшают чувствительность системы. Кроме того, некоторое

влияние на изображение может оказать сильное внешнее электромагнитное излучение.

Существует еще один метод реализации таких систем. Его разработала компания «Who Vision Systems». В основе их системы TactileSense - электрооптический полимер. Этот материал чувствителен к разности электрического поля между гребнями и впадинами кожи. Градиент электрического поля конвертируется в оптическое изображение высокого разрешения, которое затем переводится в цифровой формат, который уже можно передавать в ПК по параллельному порту или USB-интерфейсу. Метод также нечувствителен к состоянию кожу и степени ее загрязнения, в том числе и химического. Вместе с тем считывающее устройство имеет миниатюрные размеры и может быть встроено, например, в компьютерную клавиатуру. По утверждению производителей, система имеет колоссально низкую себестоимость (на уровне нескольких десятков долларов).

Характеристики некоторых методов приведены в табл. 3.3.

Таблица 3.3. Характеристики типовых систем идентификации но отпечаткам пальцев

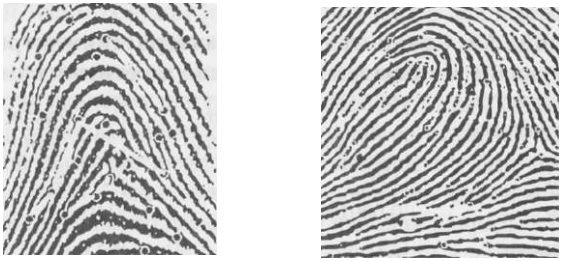
Свойства	*Оптическая система*	*Полупроводниковая технология*	*Электро-оптический полимер*
Небольшие размеры	Нет	Да	Да
Восприимчивость к сухой коже	Нет	Да	Да
Прочность поверхности	Средняя	Низкая	Высокая
Энергопотребление	Среднее	Низкое	Низкое
Цена	Средняя	Высокая	Низкая

Полученный одним из описанных методов аналоговый видеосигнал преобразуется в цифровую форму, после чего из него извлекается набор характеристик, уникальных для этого отпечатка пальца. Эти данные однозначно идентифицируют личность. Данные сохраняются и становятся уникальным шаблоном отпечатка пальца конкретного человека. При последующем считывании новые отпечатки пальцев сравниваются с хранимыми в базе.

В самом простом случае при обработке изображения на нем выделяются характерные точки (например, координаты конца или раздвоения папиллярных линий, места соединения витков). Можно выделить до 70 таких точек и каждую из них охарактеризовать двумя, тремя или даже большим числом параметров. В результате можно получить от отпечатка пальца до пятисот значений различных характеристик.

Более сложные алгоритмы обработки соединяют характерные точки изображения векторами и описывают их свойства и взаимоположение (рис. 3.6). Как правило, набор данных, получаемых с отпечатка, занимает до 1 Кбайт.

Алгоритм обработки позволяет хранить не само изображение, а его «образ» (набор характерных данных).



а *о*

Рис. 3.6. Изображение отпечатка пальца *(а)* и его «образ» (б)

Из соображений безопасности ряд производителей (SONY, Digital Persona и др.) используют при передаче данных средства шифрования. Например, в системе U are U фирмы «Digital Persona» применяется 128-битовый ключ, и, кроме этого, все пересылаемые пакеты имеют временную отметку, что исключает возможность их повторной передачи.

Хранение данных и сравнение при идентификации происходит в компьютере. Практически каждый производитель аппаратной части вместе с системой поставляет и уникальное программное обеспечение, адаптированное чаще всего под Windows NT.

Так как большинство систем предназначено для контроля доступа к компьютерной информации и ориентировано в первую очередь на рядового пользователя, ПО отличается простотой и не требует специальной настройки.

Следует отметить одну особенность СКУД, в которой используются отпечатки пальцев: такие устройства более громоздки, чем другие типы считывателей. Это связано с тем, что, во-первых, нет необходимости экономить место на рабочем столе, а во-вторых, считыватели должны быть автономны. Поэтому, кроме сканера, в один корпус помещают устройство принятия решения и хранения информации, клавиатуру (для увеличения степени защищенности) и жидкокристаллический дисплей (для удобства настройки и эксплуатации). При необходимости к системе может быть подключен считыватель карт (смарт, магнитных и т. д.). Существуют и более экзотические модели. Например, фирма SONY поместила в корпус прибора динамик, а фирма «Mytec» считает, что будущее за интеграцией биометрии и таблеток iButton.

Кроме того, такие устройства должны обеспечивать простое подключение электрозамков и датчиков сигнализации и легко объединяться в сеть (наличие интерфейсов RS-485).

В табл. 3.4 приведены сравнительные характеристики устройств, использующих методы идентификации по отпечаткам пальцев. Одно из них - устройство Veriprint 2100 фирмы «Biometric ID» - показано на рис. 3.7.

Таблица 3.4. Сравнительные характеристики устройств, использующих методы идентификации по отпечаткам пальцев

Характеристика	*Finger Scan фирмы «Identix»*	*Veriprint 2100 фирмы «Biometric Ю»*
Ошибка 1 рода	1%	0,01 %
Ошибка 2 рода	0,0001%	0,01 %
Время регистрации	25 с	<5 с
Время идентификации	1 с	1 с
Интерфейс	RS232, RS485, TTL, вх/вых сигнализации	RS232, RS485, TTL
Макс, число пользователей	50 000 (сетевая версия)	8 000
Флеш-память	512 кВ или 1,5 МВ	2 МВ или 8 МВ
Дополнение	ЖК-дисплей, клавиатура	ЖК-дисплей, клавиатура

Отметим, что все представленные устройства предназначены для работы только внутри помещения. Поверхность сканера должна быть чистой, поэтому априори исключаются запыленные склады, бензоколонки и т. д. Наиболее частое применение - банковские системы (доступ к сейфам, хранилищам ценностей), контроль доступа в различные клубы и загородные резиденции, системы электронной коммерции.

Рис. 3.7. Система Veriprint 2000 позволяет контролировать доступ в помещения

3.2.2. Идентификация по радужной оболочке глаз

Первооткрывателем в области идентификации личности по радужной оболочке глаза является доктор Джон Даугман. В 1994 г. он запатентовал в США метод распознавания радужной оболочки глаза (US Patent S, 291, 560). Разработанные им алгоритмы используются до сих пор.

С помощью этих алгоритмов необработанные видеоизображения глаза преобразуются в уникальный идентификационный двоичный поток Iris-код, полученный в результате определения позиции радужки, ее границы и вы-

полнения других математических операций для описания текстуры радужки в виде последовательности чередования фаз, похожей на штрих-код.

Полученный таким образом Iris-код используется для поиска совпадений в базах данных (скорость поиска - около 1 млн сравнения Iris-кодов в 1 с) и для подтверждения или неподтверждения заявленной личности

Преимущество сканеров для радужной оболочки глаза состоит в том, что они не требуют от пользователя сосредоточения на цели, так как образец пятен на радужной оболочке находится на поверхности глаза. Фактически видеоизображение глаза может быть отсканировано на расстоянии менее 1 м, что делает возможным использование сканеров для радужной оболочки глаза, допустим, в банкоматах. Разработкой технологии идентификации личности на основе принципа сканирования радужной оболочки глаза в настоящее время занимаются более 20 компаний, в том числе British Telecom, Sensar, японская компания Oki.

Различают *активные и пассивные системы* распознавания. В системах первого типа пользователь должен сам настроить камеру, передвигая ее для более точной наводки. Пассивные системы проще в использовании, поскольку камера в них настраивается автоматически. Высокая надежность этого оборудования позволяет применять его даже в исправительных учреждениях.

В качестве примера современной системы идентификации на основе анализа радужной оболочки глаза рассмотрим решение, предложенное компанией LG [8]

Система IrisAccess позволяет менее чем за 1 с отсканировать рисунок радужной оболочки глаза, обработать и сравнить с 4 тыс. других записей, которые она хранит в своей памяти, а затем послать соответствующий сигнал в охранную систему. Технология - полностью бесконтактная. На основе изображения радужной оболочки глаза строится компактный цифровой код размером 512 байт. Устройство имеет высокую надежность по сравнению с большинством известных систем биометрического контроля, поддерживает объемную базу данных, выдает звуковые инструкции на русском языке, позволяет интегрировать в систему карты доступа и ПИН-клавиатуры. Один контроллер поддерживает четыре считывателя Система может быть интегрирована с LAN Система IrisAccess 3000 состоит из оптического устройства внесения в реестр E01J3000, удаленного оптического устройства R01J3000, контрольного устройства опознавания ICLI3000, платы захвата изображения, дверной интерфейсной платы и PC-сервера. Если требуется осуществлять контроль за несколькими входами, то ряд удаленных устройств, включая ICU3000 и R01J3000, может быть подключен к PC-серверу через локальную сеть (LAN).

Представляет интерес камера для идентификации личности путем сканирования радужной оболочки глаза, используемая в системах защиты и безопасности для компьютеров типа десктоп/лэптоп. Разработки визуальных систем (Vision Systems) компании Panasonic и хорошо показавшие себя на прак-

тике разработки в области идентификации личности на основе рисунка радужной оболочки глаз компании Iridian Technologies позволили создать легкие в использовании и отличающиеся высокой точностью средства, которые можно использовать в широком диапазоне современных и будущих потребностей в области обеспечения безопасности.

Камера Authenticam™ компании Panasonic в сочетании с программным продуктом PrivatelD™ компании Indian Technologies представляет собой экономически выгодный и надежный путь обеспечения безопасности доступа. Для такой камеры характерны безопасность и простота использования. Достаточно взглянуть в объектив камеры с расстояния приблизительно 50 см, и менее чем через 2 с произойдет захват изображения.

Программный продукт PrivatelD™ обрабатывает рисунок радужной оболочки глаз и кодирует полученную информацию в виде 512-байтовой записи IrisCode. Эти записи вводятся для хранения в память и используются для сравнения с другими записями кодов IrisCodes - для идентификации личности при любых транзакциях и деловых операциях, когда для сравнения представляется радужная оболочка глаза живого человека.

Дифференциатор ключей для идентификации личности по рисунку радужной оболочки глаза осуществляет поиск в базе данных для нахождения соответствующего идентификационного кода. При этом база данных может состоять из неограниченного числа записей кодов IrisCode.

Технология допуска, основанная на сканировании радужной оболочки глаза, уже несколько лет успешно применяется в государственных организациях США и в учреждениях с высокой степенью секретности (в частности, на заводах по производству ядерного вооружения). Эффективность этого способа доказана, он безопасен для пользователя и надежен в работе. Он обеспечивает моментальную аутентификацию личности, предназначенную для замены символов ПИН-кодов и паролей.

Многие эксперты подчеркивают «незрелость» технологии, хотя потенциальные возможности метода достаточно высоки, так как характеристики рисунка радужной оболочки человеческого глаза достаточно стабильны и не изменяются практически в течение всей жизни человека, невосприимчивы к загрязнению и ранам [9, 10]. Отметим также, что радужки правого и левого глаза по рисунку существенно различаются. Этот метод идентификации отличается от других большей сложностью в использовании, более высокой стоимостью аппаратуры и жесткими условиями регистрации.

3.2.3. Идентификация по капиллярам сетчатки глаз

При идентификации по сетчатке глаза измеряется угловое распределение кровеносных сосудов на поверхности сетчатки относительно слепого пятна глаза и другие признаки. Капиллярный рисунок сетчатки глаз различается даже у близнецов и может быть с большим успехом использован для идентификации личности. Всего насчитывают около 250 признаков. Такие биомет-

рические терминалы обеспечивают высокую достоверность идентификации, сопоставимую с дактилоскопией, но требуют от проверяемого лица фиксации взгляда на объективе сканера.

Сканирование сетчатки происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Сканеры сетчатки глаза получили широкое распространение в СКУД особо секретных объектов, так как у них один из самых низких процентов отказа в доступе зарегистрированных пользователей и практически не бывает ошибочного разрешения доступа. Однако изображение радужной оболочки должно быть четким, поэтому катаракта может отрицательно воздействовать на качество идентификации личности.

Начало разработок этого направления идентификации относится к 1976 г., когда в США была образована компания Eye Dentify, которая до настоящего времени сохраняет монополию на производство коммерческих систем аутентификации по ретине.

Основным устройством для системы такого типа является бинокулярный объектив. При осуществлении процедуры аутентификации пользователь должен прильнуть глазами к окулярам и, глядя вовнутрь, сфокусировать взгляд на изображении красного цвета. Затем ему следует дождаться смены цвета на зеленый (что укажет на правильную фокусировку) и нажать на стартовую кнопку. Сканирование глазного дна выполняется источником инфракрасного излучения, безопасного для глаз. Достаточно смотреть в глазок камеры менее минуты. За это время система успевает подсветить сетчатку и получить отраженный сигнал. Для сканирования сетчатки используется инфракрасное излучение низкой интенсивности, направленное через зрачок к кровеносным сосудам на задней стенке глаза. Отраженное от ретины излучение фиксируется специальной чувствительной камерой.

Замеры ведутся по 320 точкам фотодатчиками и результирующий аналоговый сигнал с помощью микропроцессора преобразуется в цифровой вид. При этом используется алгоритм быстрого преобразования Фурье. Полученный цифровой вектор, состоящий из коэффициентов Фурье, сравнивается с зарегистрированным эталоном, хранящимся в памяти системы. Благодаря такому методу преобразования и представления изображения глазного дна для хранения каждого эталона расходуется по 40 байт. Память терминала Eye Dentification System 7.5, реализующего этот алгоритм, рассчитана на запоминание до 1200 эталонов. Время регистрации составляет примерно 30 с, время аутентификации - 1,5 с. Коэффициент ошибок 1-го рода - 0,01 %, 2-го рода - 0,0001 % (т. е. вероятность ошибок 1-го рода - 0,0001, 2-го рода - 0,000001) [2].

С точки зрения безопасности данная система выгодно отличается от всех других, использующих биометрические терминалы, не только малым значением коэффициентов ошибок как 1-го, так и 2-го рода, но и использованием

специфического аутентификацииоиного атрибута, который практически невозможно негласно подменить для обмана системы при проверке.

К недостаткам подобных систем следует отнести психологический фактор: не всякий человек отважится посмотреть в неведомое темное отверстие, где что-то светит в глаз. К тому же надо следить за положением глаза относительно отверстия, поскольку подобные системы, как правило, чувствительны к неправильной ориентации сетчатки. Сканеры для сетчатки глаза получат большое распространение при организации доступа к сверхсекретным системам, поскольку гарантируют один из самых низких процентов отказа в доступе зарегистрированных пользователей и почти нулевой процент ошибок.

3.2.4. Идентификация по геометрии и тепловому изображению лица

Идентификация человека но чертам (геометрии) лица - одно из самых динамично развивающихся направлений в биометрической индустрии. Привлекательность данного метода основана на том, что он наиболее близок к тому, как люди обычно идентифицируют друг друга. Рост мультимедийных технологий, благодаря которым можно увидеть все больше видеокамер, установленных на городских улицах и площадях, аэропортах, вокзалах и других местах скопления людей, определили развитие этого направления.

Техническая реализация метода - более сложная (с математической точки зрения) задача, чем распознавание отпечатков пальцев, и, кроме того, требует более дорогостоящей аппаратуры (нужна цифровая видео- или фотокамера и плата захвата видеоизображения). У этого метода есть один существенный плюс: для хранения данных об одном образце идентификационного шаблона требуется совсем немного памяти, так как человеческое лицо можно «разобрать» на относительно небольшое количество участков, неизменных у всех людей. Например, для вычисления уникального шаблона, соответствующего конкретному человеку, требуется всего от 12 до 40 характерных участков.

Обычно камера устанавливается на расстоянии нескольких десятков сантиметров от объекта. Получив изображение, система анализирует различные параметры лица (например, расстояние между глазами и носом). Большинство алгоритмов позволяет компенсировать наличие у исследуемого индивида очков, шляпы и бороды. Для этой цели обычно используется сканирование лица в инфракрасном диапазоне, но пока системы такого типа не дают устойчивых и очень точных результатов.

Распознавание человека по изображению лица выделяется среди биометрических систем тем, что, во-первых, не требует специального дорогостоящего оборудования. Для большинства приложений достаточно только персонального компьютера и обычной видеокамеры. Во-вторых, отсутствует физический контакт человека с устройствами. Не надо ни к чему прикасаться

или специально останавливаться и ждать срабатывания системы. В большинстве случаев достаточно просто пройти мимо или задержаться перед камерой на несколько секунд. Распознавание изображений аналогично распознаванию образов.

Такие задачи не имеют точного аналитического решения. При этом требуется выделение ключевых признаков, характеризующих зрительный образ, определение относительной важности признаков путем выбора их весовых коэффициентов и учет взаимосвязей между признаками.

Компания ISS разработала ряд алгоритмов, позволяющих обрабатывать видеоданные в режиме реального времени и производить локализацию, определять положение головы и отслеживать перемещение с целью дальнейшего распознавания.

В настоящее время существует 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. Комбинируя характеристики 100-120 «eigenface», можно восстановить большое число лиц. В момент регистрации «eigenface» каждого конкретного человека представляется в виде ряда коэффициентов. Для режима установления подлинности, в котором изображение используется для проверки идентичности, «живой» шаблон сравнивается с уже 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» -*** наиболее широко используемая технология идентификации. Она подобна методу «Eigenface», но в большей степени адаптирована 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, отпускать бороду и усы, надевать очки - все это увеличивает сложность процедуры идентификации. Например, при улыбке наблюдается некоторое смещение частей лица, расположенных около рта, что в свою оче-

редь 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 шаблона 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.

Задачу идентификации личности человека по видеоизображению можно разбить на несколько этапов.

1. *Локализация лица в кадре.* Для локализации лица в кадре разработан алгоритм на основе нейронной сети, который сканирует исходное изображение в разных масштабах, оценивая по ключевым признакам каждый участок изображения с определенной вероятностью, и классифицирует, является ли данный участок лицом или нет. Выделение ключевых признаков осуществляется путем автоматического анализа достаточно большой обучающей выборки, охватывающей большинство возможных ситуаций (например, изменение внешности, условий освещенности, ракурса и т. п.).

2. *Определение положения головы.* Определение положения головы человека является важным этапом и позволяет внести поправки при дальнейшем распознавании. На этом этапе созданная компанией трехмерная модель головы сопоставляется с изображением головы в кадре. При этом оцениваются такие параметры, как угол поворота головы по осям X, Y, Z, точный замер и смещение изображения в кадре.

3. *Отслеживание перемещения лица от кадра к кадру.* При идентификации движущегося в поле зрения камеры человека необходимо отслеживать перемещение лица от кадра к кадру. Имея несколько изображений одного и того же человека в разных ракурсах, программа выбирает наиболее удачный

с ее точки зрения кадр и сохраняет его в базе данных. Обрабатывая несколько изображений одного и того же человека в разных ракурсах, можно добиться очень высокой точности распознавания.

4. *Сравнение изображения с данными базы.* В настоящее время компания ISS ведет разработки алгоритма сравнения лица с имеющимся в базе данных. Этот этап является логическим завершением в цепочке алгоритма идентификации личности по видеоизображению.

Оценочные характеристики при проверке эффективности различных вариантов таких устройств приведены в табл. 3.5.

Таблица 3.5. Проверка эффективности распознавании черт лица

Условия оценки эффективности	*Уровень ошибочных подтверждений, %*	*Уровень ошибочных отказов, %*
Один и тот же день, одно и то же освещение	2	0,4
Один и тот же день, разное освещение	2	9
Разные дни	2	11
Разные дни в течение 1,5 лет	2	43

Основой любой системы распознавания лица является метод его кодирования. В ряде случаев используется анализ локальных характеристик для представления изображения лица в виде статистически обоснованных, стандартных блоков данных. Такой метод использует корпорация Viscionics в своей системе Facelt. Данный математический метод основывается на том, что все лица могут быть получены из репрезентативной выборки лиц с использованием современных статистических приемов. Они охватывают пиксели изображения лица и универсально представляют лицевые формы. Фактически в наличии имеется намного больше элементов построения лица, чем число самих частей лица. Идентичность лица определяется не только характерными элементами, но и способом их геометрического объединения (учитываются их относительные позиции). Полученный сложный математический код индивидуальной идентичности - шаблон Faceprint - содержит информацию, которая отличает лицо от миллионов других, и может быть составлен и сравнен с другими с феноменальной точностью. Шаблон не зависит от изменений в освещении, тона кожи, наличия/отсутствия очков, выражения лица, волос на лице и голове, устойчив к изменению в ракурсах до 35" в любых направлениях

В *качестве примера* действующей системы контроля доступа на базе распознавания лица можно привести систему распознавания посетителей мест для обналичивания чеков, установленных компанией Mr. Payroll в нескольких штатах США. По свидетельству представителей компании клиенты считают такую процедуру весьма удобной. При первом посещении производится цифровой снимок лица клиента, который передается в сервисный центр При

каждом следующем обращении система сверяет соответствующее изображение с лицом клиента и только после этого производит обналичивание чека. Выше уже упоминалась система распознавания лиц Facelt, разработанная корпорацией Visionics. Она успешно работает на улицах английского города Ньюхем, а также в аэропортах, на крупных стадионах и в торговых центрах США. Технология распознавания лица или множества лиц в сложных сценах Facelt позволяет автоматически обнаружить человеческое присутствие, определить месторасположение, выделить изображение, выполнить идентификацию.

Распознавание лица предусматривает выполнение любой из следующих функций: аутентификация - установление подлинности «один в один», идентификация - поиск соответствия «один из многих».

Система Facelt автоматически оценивает качество изображения для опознания лица и, если необходимо, способна его улучшить. Она также создает изображение лица из сегментов данных, генерирует цифровой код или внутренний шаблон, уникальный для каждого индивидуума. В системе заложен режим слежения за лицами во времени, а также «сжатия» лица до размера 84 байт для использования в смарт-картах, штриховых кодах и других устройствах с ограниченным размером хранения.

Среди признаков лица, используемых для идентификации человека, наиболее устойчивыми и трудно изменяемыми является также *признака изображения его кровеносных сосудов.* Путем сканирования изображения лица в инфракрасном свете создается уникальная температурная карта лица - *термограмма.* Идентификация по термограмме обеспечивает показатели, сравнимые с показателями идентификации по отпечаткам пальцев.

3.2.5. Идентификация но геометрии кисти руки

Метод идентификации пользователей по геометрии руки по своей технологической структуре и уровню надежности вполне сопоставим с методом идентификации личности по отпечатку пальца. Статистическая вероятность существования двух кистей рук с одинаковой геометрией чрезвычайно мала. Но признаки руки меняются с возрастом, а само устройство имеет сравнительно большие размеры.

Математическая модель идентификации по данному параметру требует немного информации - всего 9 байт, что позволяет хранить большой объем записей и быстро осуществлять поиск. Устройства идентификации личности по геометрии руки находят широкое применение Так, в США устройства для считывания отпечатков ладоней в настоящее время установлены более чем на 8 ООО объектах. Наиболее популярное устройство Handkey сканирует как внутреннюю, так и боковую сторону ладони, используя для этого встроенную видеокамеру и алгоритмы сжатия. При этом оценивается более 90 различных характеристик, включая размеры самой ладони (три измерения), длину и ши-

рину пальцев, очертания суставов и т. п. Устройства, которые могут сканировать и другие параметры руки, в настоящее время разрабатываются несколькими компаниями, в том числе BioMet Partners, Palmetrics и BTG.

Представителем этого направления разработок СКУД является американская компания Steller Systems, выпускающая терминал Identimat. Для считывания геометрических характеристик кисти ее кладут ладонью вниз на специальную панель. Через прорези в ее поверхности оптические сенсорные ячейки сканируют четыре кольца. Эти ячейки определяют стартовые точки по двум парам пальцев - указательному и среднему, безымянному и мизинцу. Каждый палец сканируется по всей длине, при этом замеряется длина, изгиб и расстояние до «соседа». Если каждое измерение укладывается в определенные допустимые рамки зарегистрированного эталонного набора данных, то результат аутентификации будет для пользователя положительным. Цифровой эталон хранится либо в базе данных, либо в памяти идентификационной карточки. При этом с целью обеспечения защиты данные шифруются.

Рассматриваемый терминал прост в обращении и надежен Время обработки - всего 1 с; время регистрации - 1,5 мин; вероятность ошибок 1-го рода - 0,01, 2-го рода - 0,015 (т.е. коэффициенты 1 и 1,5% соответственно). Для хранения эталона используется 17 байт памяти.

Отличительной особенностью алгоритма работы этого терминала является наличие так называемых битов качества, которые регулируют рамки допустимых отклонений в зависимости от качества изображения кисти. Однако настораживает тот факт, что у каждого сотого сотрудника могут появиться проблемы с проходом на рабочее место. И каждый стопятидесятый может оказаться чужим.

На базе подобной технологии биометрии японская фирма Mitsubishi Electric построила контрольно-пропускной терминал автономного типа Palm Recognition System. Его отличие от американского прототипа состоит в том, что производится считывание геометрических размеров силуэта кисти руки со сжатыми пальцами, в то время как у американцев пальцы для измерения должны представляться растопыренными. Благодаря такому подходу на результатах оценки биометрических характеристик в японской системе не сказывается появление на ладони ран или грязи. Однако вероятность ошибок 1-го рода также составляет 0,01, но ошибок 2-го рода - 0,000001. Время обработки занимает 2 с, время регистрации при оформлении допуска - 20 с. Память системы позволяет хранить до 220 эталонов.

В настоящее время идентификация пользователей по геометрии руки используется в законодательных органах, международных аэропортах, больницах, иммиграционных службах и т. д. Достоинства идентификации по геометрии ладони сравнимы с достоинствами идентификации по отпечатку пальца с точки зрения надежности, хотя устройство для считывания отпечатков ладоней занимает больше места.

3.3. Особенности реализации динамических методов биометрического контроля

3.3.1. Идентификация по почерку и динамике подписи

Основой аутентификации личности по почерку и динамике написания контрольных фраз (подписи) является уникальность и стабильность динамики этого процесса для каждого человека, характеристики которой могут быть измерены, переведены в цифровой вид и подвергнуты компьютерной обработке. Таким образом, при аутентификации для сравнения выбирается не продукт письма, а сам процесс.

Разработка аутентификационных автоматов на базе анализа почерка (подписи - как варианта объекта исследования), предназначенных для реализации контрольно-пропускной функции, была начата еще в начале 1970-х г. В настоящее время на рынке представлено несколько эффективных терминалов такого типа.

Подпись - такой же уникальный атрибут человека, как и его физиологические характеристики. Кроме того, это и более привычный для любого человека метод идентификации, поскольку он, в отличие от снятия отпечатков пальцев, не ассоциируется с криминальной сферой. Одна из перспективных технологий аутентификации основана на уникальности биометрических характеристик движения человеческой руки во время письма. Обычно выделяют два способа обработки данных о подписи: простое сравнение с образцом и динамическую верификацию. Первый весьма ненадежен, так как основан на обычном сравнении введенной подписи с хранящимися в базе данных графическими образцами. Из-за того, что подпись не может быть всегда одинаковой, этот метод дает большой процент ошибок. Способ динамической верификации требует намного более сложных вычислений и позволяет в реальном времени фиксировать параметры процесса подписи, такие, как скорость движения руки на разных участках, сила давления и длительность различных этапов подписи. Это дает гарантии того, что подпись не сможет подделать даже опытный графолог, поскольку никто не в состоянии в точности скопировать поведение руки владельца подписи. Пользователь, используя стандартный дигитайзер и ручку, имитирует свою обычную подпись, а система считывает параметры движения и сверяет их с теми, что были заранее введены в базу данных. При совпадении образа подписи с эталоном система прикрепляет к подписываемому документу информацию, включающую имя пользователя, адрес его электронной почты, должность, текущее время и дату, параметры подписи, содержащие несколько десятков характеристик динамики движения (направление, скорость, ускорение) и другие. Эти данные шифруются, затем для них вычисляется контрольная сумма, и далее все это шифруется еще раз, образуя так называемую биометрическую метку. Для настройки системы вновь зарегистрированный пользователь от пяти до десяти

раз выполняет процедуру подписания документа, что позволяет получить усредненные показатели и доверительный интервал. Впервые данную технологию использовала компания РепОр.

Идентификацию по подписи нельзя использовать повсюду, в частности, этот метод не подходит для ограничения доступа в помещения или для доступа в компьютерные сети. Однако в некоторых областях, например в банковской сфере, а также всюду, где происходит оформление важных документов, проверка правильности подписи может стать наиболее эффективным, а главное, необременительным и незаметным способом. До сих пор финансовое сообщество не спешило принимать автоматизированные методы идентификации подписи для кредитных карточек и проверки заявления, потому что подписи все еще слишком легко подделать. Это препятствует внедрению идентификации личности по подписи в высокотехнологичные системы безопасности.

Устройства идентификации по динамике подписи используют геометрические или динамические признаки рукописного воспроизведения подписи в реальном масштабе времени. Подпись выполняется пользователем на специальной сенсорной панели, с помощью которой осуществляется преобразование изменений приложенного усилия нажатия на перо (скорости, ускорения) в электрический аналоговый сигнал. Электронная схема преобразует этот сигнал в цифровой вид, приспособленный для машинной обработки. При формировании «эталона» необходимо учитывать, что для одного и того же человека характерен некоторый разброс характеристик почерка от одного акта к другому. Чтобы определить эти флуктуации и назначить рамки, пользователь при регистрации выписывает свою подпись несколько раз. В результате формируется некая «стандартная модель» (сигнатурный эталон) для каждого пользователя, которая записывается в память системы.

В качестве примера реализации такого метода идентификации можно рассматривать систему Automatic Personal Verification System, разработанную американской корпорацией NCR Corp. Эта система на испытаниях продемонстрировала следующие результаты: коэффициент ошибок 1-го рода - 0,015%, 2-го рода - 0,012% (в случае, если злоумышленник не наблюдал процесс исполнения подписи законным пользователем) и 0,25 % (если он наблюдал).

Системы аутентификации по почерку поставляются на рынок, например, фирмами Inforete и De La Rue Systems (США), Thompson T1TN (Франция) и рядом других. Английская фирма Quest Micropad Ltd выпустила устройство QSign, особенностью которого является то, что сигнатурный эталон может храниться как в памяти системы, так и в памяти идентификационной карточки пользователя. Пороговое значение коэффициентов ошибок может изменяться в зависимости от требуемой степени безопасности. Подпись выполняется обычной шариковой ручкой или карандашом на специальной сенсорной панели, входящей в состав терминала.

Основное достоинство подписи по сравнению с использованием, например, дактилоскопии в том, что это распространенный и общепризнанный способ подтверждения своей личности (например, при получении банковских вкладов). Этот способ не вызывает «технологического дискомфорта», как бывает в случае снятия отпечатков пальцев, что ассоциируется с деятельностью правоохранительных органов. В то же время подделка динамики подписи - дело очень трудновыполнимое (в отличие, скажем, от воспроизведения рисунка подписи). Причем благодаря росписи не на бумаге, а на сенсорной панели, значительно затрудняется копирование злоумышленником ее начертания.

Идентификация по *ритму работы на клавиатуре* основана на измерении временных интервалов между двумя последовательными ударами по клавишам при печатании знаков.

3.3.2. Идентификация но голосу и особенностям речи

Биометрический подход, связанный с идентификацией голоса, удобен в применении. Однако основным и определяющим недостатком этого подхода является низкая точность идентификации. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем. Причинами внедрения этих систем являются повсеместное распространение телефонных сетей и практика встраивания микрофонов в компьютеры и периферийные устройства. В качестве недостатков таких систем можно назвать факторы, влияющие на результаты распознавания: помехи в микрофонах, влияние окружающей обстановки на результаты распознавания (шум), ошибки при произнесении, различное эмоциональное состояние проверяемого в момент регистрации эталона и при каждой идентификации, использование разных устройств регистрации при записи эталонов и идентификации, помехи в низкокачественных каналах передачи данных и т. п.

При рассмотрении проблемы аутентификации по голосу важными вопросами с точки зрения безопасности являются следующие:

- Как бороться против использования магнитофонных записей парольных фраз, перехваченных во время установления контакта законного пользователя с аутентификационным терминалом?
- Как защитить систему от злоумышленников, обладающих способностью к имитации голоса, если им удастся узнать парольную фразу?

Ответом на первый вопрос является генерация системой псевдослучайных паролей, которые повторяются вслед за ней пользователем, а также применение комбинированных методов проверки (дополняя вводом идентификационной карточки или цифрового персонального кода).

Ответ на второй вопрос не так однозначен. Человек вырабатывает свое мнение о специфике воспринимаемого голоса путем оценки некоторых его характерных качеств, не обращая внимание при этом на количественную сто-

рону разнообразных мелких компонент речевого сигнала. Автомат же наоборот, не обладая способностью улавливать обобщенную характеристику голоса, свой вывод делает, основываясь на конкретных параметрах речевого сигнала и производя их точный количественный анализ.

Специфическое слуховое восприятие человека приводит к тому, что безупречное воспроизведение профессиональными имитаторами голосов возможно лишь тогда, когда подражаемый субъект характеризуется ярко выраженными особенностями произношения (интонационной картиной, акцентом, темпом речи и т. д.) или тембра (гнусавостью, шепелявостью, картавостью и т. д.). Именно этим следует объяснить тот факт, что даже профессиональные имитаторы оказываются не в состоянии подражать ординарным, не примечательным голосам.

В противоположность людям распознающие автоматы, свободные от субъективного отношения к воспринимаемым образам, производят аутентификацию (распознавание) голосов объективно, на основе строго детерминированных и априори заданных признаков. Обладая «нечеловеческим» критерием оценки схожести голосов, системы воспринимают голос человека через призму своих признаков. Вследствие этого, чем сложнее и «непонятнее» будет совокупность признаков, по которым автомат распознает голос, тем меньше будет вероятность его обмана. В гоже время, несмотря на то, что проблема имитации очень важна и актуальна с практической точки зрения, она все же далека от окончательного решения. Прежде всего до конца не ясен ответ на вопрос, какие именно параметры речевого сигнала наиболее доступны подражанию и какие из них наиболее трудно поддаются ему.

Выбор параметров речевого сигнала способных наилучшим образом описать индивидуальность голоса является, пожалуй, самым важным этапом при построении систем автоматической аутентификации по голосу. Такие параметры сигнала, называемые признаками индивидуальности, помимо эффективности представления информации об особенностях голоса диктора, должны обладать рядом других свойств. Во-первых, они должны быть легко измеряемы и мало зависеть от мешающих факторов окружающей среды (шумов и помех) Во-вторых, они должны быть стабильными во времени. В-третьих, не должны поддаваться имитации.

Постоянно ведутся работы по повышению эффективности систем идентификации по голосу. Известны системы аутентификации по голосу, где применяется метод совместного анализа голоса и мимики, ибо, как оказалось, мимика говорящего характерна только ему и будет отличаться от говорящего те же слова мимики другого человека.

Разрабатываются комбинированные системы, состоящие из блоков идентификации и верификации голоса. При решении задачи идентификации находится ближайший голос (или несколько голосов) из фонотеки, затем в результате решения задачи верификации подтверждается или опровергается принадлежность фонограммы конкретному лицу. Система практически ис-

пользуется при обеспечении безопасности некоторых особо важных объектов.

В последнее время ведутся активные разработки по усовершенствованию и модификации голосовых систем идентификации личности, поиск новых подходов для характеристики человеческой речи, комбинации физиологических и поведенческих факторов.

Задача повышения надежности распознавания может быть решена за счет привлечения грамматической и семантической информации в системах распознавания речи. Для решения этой задачи разработана (при участии экспертов: лингвистов, рядовых носителей языка) модель входного языка, учитывающая особенности их грамматического и семантического поведения (28 основных грамматических классов, около 300 грамматических разрядов слов), ее компьютерное воплощение - лингвистическая база знаний (ЛБЗ) и лингвистический процессор (ЛП). В состав ЛБЗ входят: обширный грамматический словарь - объемом около 100000 единиц; словари словосочетаний; словари униграмм и лексических биграмм; грамматические таблицы и словарь моделей управления. Программы синтактико-семантического анализа, входящие в состав ЛП, обеспечивают: быстрое отсеивание маловероятных вариантов распознавания (локальный анализ), учет обнаруженных при анализе грамматических событий, характеризующих регулярность грамматической структуры и степень грамматичности предложения в целом или отдельных групп (и тем самым возможность выбора в качестве окончательного результата распознавания неграмматичных, но допустимых в речи вариантов). Для решения многокритериальной задачи выбора окончательного варианта были разработаны специальные эвристики метауровня. Лингвистический модуль (ЛБЗ и ЛП) позволяет повысить надежность акустического и фонетического распознавания с 94-95 до 95-97 %.

Уделяется внимание проблемам автоматизированного формирования и сопровождения ЛБЗ систем распознавания речи (для английского и русского языков): построение тезауруса, коррекция словаря лексических n-грамм на основе синтактико-семантической информации и др. Новые методы, как показывают результаты экспериментов, позволяют повысить надежность распознавания еще на 1 %.

Сегодня идентификация по голосу используется для управления доступом в помещения средней степени секретности, например, лаборатории производственных компаний. Лидерами в разработке таких систем являются компании T-Netix, ITT Nuance, Veritel. В системе фирмы Texas Instruments (TI) парольные фразы состояли из 4-словного предложения, причем каждое слово было односложным. Каждая фраза являлась 84 байтами информации. Время аутентификации составляло 5,3 с. Для предотвращения использования заранее записанного на магнитофон пароля система генерировала слова в произвольной последовательности. Общее время проверки на КПП составляло 15 с

на одного человека. Для четырех парольных фраз ошибка 1-го рода составила 0,3 %, 2-го рода - 1 %.

3.3.3. Идентификация по ритму работы на клавиатуре

Современные исследования показывают, что клавиатурный почерк пользователя обладает некоторой стабильностью, что позволяет достаточно однозначно идентифицировать пользователя. Применяются статистические методы обработки исходных данных и формирования выходного вектора, являющегося идентификатором данного пользователя. В качестве исходных данных используют временные интервалы между нажатием клавиш на клавиатуре и время их удержания. При этом временные интервалы между нажатием клавиш характеризуют темп работы, а время удержания клавиш характеризует стиль работы с клавиатурой - резкий удар или плавное нажатие.

Идентификация пользователя по клавиатурному почерку возможна следующими способами:

- по набору ключевой фразы;
- по набору произвольного текста.

Принципиальное отличие этих двух способов заключается в том, что в первом случае используется ключевая фраза, задаваемая пользователем в момент регистрации его в системе (пароль), а во втором случае используются ключевые фразы, генерируемые системой каждый раз в момент идентификации пользователя. Подразумеваются 2 режима работы:

- обучение;
- идентификация.

На этапе обучения пользователь вводит некоторое число раз предлагаемые ему тестовые фразы При этом рассчитываются и запоминаются эталонные характеристики данного пользователя. На этапе идентификации рассчитанные оценки сравниваются с эталонными, на основании чего делается вывод о совпадении или несовпадении параметров клавиатурного почерка. Выбор текста, на котором выполняется обучение системы, - достаточно важный этап для нормального функционирования системы. Предлагаемые пользователю фразы необходимо подбирать таким образом, чтобы используемые в них символы полностью и равномерно покрывали рабочее поле клавиатуры. Более того, если в процессе обучения системы видно, что статистические характеристики отдельных клавиш имеют существенный разброс, необходимо формировать очередную тестовую фразу таким образом, чтобы уменьшить эту неопределенность. Возможна организация «неявного» процесса обучения системы, когда программа перехватывает весь ввод с клавиатуры и соответственно рассчитывает эталонные характеристики пользователя. Данная процедура достаточно легко организуется практически в любой операционной системе. В DOS для этого используется перехват прерываний от клавиатуры, в Windows - стандартный механизм ловушек (hooks).

Однако существует ряд ограничений по применению данного способа на практике. Применение способа идентификации по клавиатурному почерку целесообразно только по отношению к пользователям с достаточно длительным опытом работы с компьютером и сформировавшимся почерком работы на клавиатуре, т. е. к программистам, секретарям и т. д. В противном случае вероятность неправильного опознания «легального» пользователя существенно возрастает и делает непригодным данный способ идентификации на практике. Исходя из теории машинописи и делопроизводства можно определить время становления почерка работы с клавиатурой, при котором достигается необходимая вероятность идентификации пользователя: примерно 6 месяцев.

Эталонные характеристики пользователя, полученные на этапе обучения системы, позволяют сделать выводы о степени стабильности клавиатурного почерка пользователя и определить доверительный интервал разброса параметров для последующей идентификации пользователя. Чтобы не дискредитировать работу системы, можно отсеивать пользователей, клавиатурный почерк которых не обладает необходимой стабильностью Для этого можно пользоваться табл. 3.6.

Таблица 3.6. Оценка стабильности клавиатурного почерка пользователя

Ошибки,%	*Аритмичность, %*	*Скорость, знак/мин*	*Характеристика перекрытии*		*Оценка*
			Число перекрытий, %	*Используемое число пальцев*	
Менее 2	Менее 10	Более 200	Более 50	Все	Отлично
Менее 4	Менее 15	Более 150	Более 30	Большинство	Хорошо
Менее 8	Менее 20	Более 100	Более 10	Несколько	Удовл.
Более 8	Более 20	Менее 100	Менее 10	По одному	Неуд.

В задаче идентификации пользователя по клавиатурному почерку важным этапом является обработка первичных данных. В результате этой обработки входной поток данных разделяется на ряд признаков, характеризующих те или иные качества идентифицируемой личности. В дальнейшем эти признаки, подвергаясь статистической обработке, позволяют получить ряд эталонных характеристик пользователя.

Начальный этап обработки данных - фильтрация. На этом этапе из потока данных удаляется информация о «служебных» клавишах - клавишах управления курсором, функциональных клавишах и т. и.

Затем выделяется информация, относящаяся к следующим характеристикам пользователя:

- количество ошибок при наборе;
- интервалы между нажатиями клавиш;

- время удержания клавиш;
- число перекрытий между клавишами;
- степень аритмичности при наборе;
- скорость набора.

Увеличить число эталонных характеристик, а следовательно, увеличить надежность системы можно, выполнив разделение входного потока на данные, относящиеся к левой и правой руке соответственно. Работу данного алгоритма можно построить, опираясь на ряд достаточно простых правил, например: клавиша SHIFT нажимается, как правило, мизинцем левой руки; клавиша ENTER - пятым или вторым пальцем правой руки и т. п. Причем, анализируя относительное время между нажатием клавиши ENTER и предыдущей клавиши, можно с определенной вероятностью предсказать, каким пальцем была нажата клавиша ENTER, так как время нажатия этой клавиши мизинцем будет существенно меньше, чем для любого другого пальца. Несмотря на кажущуюся простоту алгоритма, процесс реализации его достаточно сложен, так как для этого необходимо использовать рекурсивные алгоритмы анализа входного потока данных.

В последние годы применяют ***нейросетевой подход к задаче идентификации*** Нейронные сети - это обобщенное название нескольких групп алгоритмов, обладающих одним ценным свойством: они умеют обучаться на примерах, извлекая скрытые закономерности из потока данных. Если между входными и выходными данными существует какая-то связь, пусть даже не обнаруживаемая традиционными корреляционными методами, нейронная сеть способна автоматически настроиться на нее с заданной степенью точности.

Применение нейросетевого подхода к задаче идентификации пользователя по клавиатурному почерку позволяет решить ряд проблем, возникающих при использовании стандартных методов статистической обработки входного потока данных.

В частности, применение статистических методов обработки данных базируется на утверждении, что входные величины подчинены нормальному закону распределения, хотя в ряде случаев это утверждение неверно. Например, проведенные исследования показывают, что время удержания клавиш - при малом шаге дискретизации - описывается пересечением двух нормальных распределений, что приводит к большим погрешностям при расчете эталонных характеристик пользователя.

Кроме того, нейронная сеть обладает свойством фильтрации случайных помех, присутствующих во входных данных, что позволяет отказаться от алгоритмов сглаживания экспериментальных зависимостей, необходимых при статистической обработке данных.

Наиболее перспективным методом решения задачи идентификации пользователя по клавиатурному почерку представляется использование трехслойного перцептрона Розенблатта следующей конфигурации:

- первичный слой — входной, состоит из *к* формальных нейронов с линейной активаторной функцией, где *к* - размерность входного вектора, содержащего параметры клавиатурного почерка пользователя;
- второй слой - скрытый, состоит из к формальных нейронов с сигмоидной активаторной функцией,
- третий слой - выходной, состоит из п формальных нейронов с сигмоидной активаторной функцией, где п - число зарегистрированных пользователей.

Предлагаемый подход к задаче идентификации пользователя по клавиатурному почерку позволяет увеличить размерность вектора, содержащего эталонные характеристики пользователя. Применение нейронных сетей позволяет упростить математический аппарат обработки данных и уменьшить вероятность возникновения ошибок второго рода - положительного результата идентификации для незарегистрированных пользователей. В результате возможно существенное повышение надежности и устойчивости работы систем идентификации пользователя по клавиатурному почерку.

3.4. Биометрические технологии будущего

Спектр технологий, которые могут использоваться в системах безопасности, постоянно расширяется. В настоящее время ряд биометрических технологий находится в стадии разработки, причем некоторые из них считаются весьма перспективными. К ним относятся технологии на основе:

1) термограммы лица в инфракрасном диапазоне излучения;
2) характеристик ДНК;
3) клавиатурного почерка;
4) анализ структуры кожи и эпителия на пальцах на основе цифровой ультразвуковой информации (спектроскопия кожи);
5) анализ отпечатков ладоней;
6) анализ формы ушной раковины;
7) анализ характеристик походки человека;
8) анализ индивидуальных запахов человека;
9) распознавание по уровню солености кожи;
10) распознавание по расположению вен.

Технология построения и анализа **термограммы** является одним из последних достижений в области биометрии. Как обнаружили ученые, использование инфракрасных камер дает уникальную картину объектов, находящихся под кожей лица. Разные плотности кости, жира и кровеносных сосудов строго индивидуальны и определяют термографическую картину лица

пользователя. Термограмма лица является уникальной, вследствие чего можно уверенно различать даже абсолютно похожих близнецов. Из дополнительных свойств этого подхода можно отметить его инвариантность по отношению к любым косметическим или косметологическим изменениям, включая пластическую хирургию, изменения макияжа и т. п., а также скрытность процедуры регистрации.

Технология, построенная на анализе **характеристик ДНК** (метод геномной идентификации) является, по всей видимости, хотя и самой продолжительной, но и наиболее перспективной из систем идентификации. Метод основан на том, что в ДНК человека имеются полиморфные локусы (локус - положение хромосомы (в гене или аллели), часто имеющие 8-10 аллелей. Определение набора этих аллелей для нескольких полиморфных локусов у конкретного индивида позволяет получить своего рода геномную карту, характерную только для этого человека. Точность данного метода .определяется характером и количеством анализируемых полиморфных локусов и на сегодняшний день позволяет достичь уровня 1 ошибки на 1 млн человек.

Динамику ударов по клавиатуре компьютера **(клавиатурный почерк)** при печатании текста анализирует способ (ритм) печатания пользователем той или иной фразы. Существуют два типа распознавания клавиатурного почерка. Первый предназначена для аутентификации пользователя при попытке получения доступа к вычислительным ресурсам. Второй осуществляет мониторинговый контроль уже после предоставления доступа и блокирует систему, если за компьютером начал работать не тот человек, которому доступ был предоставлен первоначально. Ритм работы на клавиатуре, как показали исследования ряда фирм и организаций, является достаточно индивидуальной характеристикой пользователя и вполне пригоден для его идентификации и аутентификации. Для измерения ритма оцениваются промежутки времени либо между ударами при печатании символов, расположенных в определенной последовательности, либо между моментом удара по клавише и моментом ее отпускания при печатании каждого символа в этой последовательности. Хотя второй способ считается более эффективным, наилучший результат достигается совместным использованием обоих способов. Отличительной особенностью этого метода является его дешевизна, так как для анализа информации не требуется никакого оборудования, кроме клавиатуры. В литературе описаны 4 математических подхода к решению задачи распознавания клавиатурного почерка пользователя ЭВМ: статистический, вероятностно-статистический (на базе теории распознавания образов) и нечеткой логики (на основе нейросетевых алгоритмов).

Следует отметить, что в настоящий момент данная технология находится в стадии разработки, и поэтому сложно оценить степень ее надежности, особенно с учетом высоких требований, предъявляемых к системам безопасности.

Для **идентификации** человека **по руке** используют несколько биометрических параметров - это геометрическая форма кисти руки или пальцев, рас-

положение подкожных кровеносных сосудов ладони, узор линий на ладони. Технология анализа **отпечатков ладоней** стала развиваться сравнительно недавно, но уже имеет определенные достижения. Причиной развития этой технологии послужил тот факт, что устройства для распознавания отпечатков пальцев имеют недостаток - им нужны только чистые руки, а отпечаток грязного пальца система может и не распознать. Поэтому ряд компаний-разработчиков (например, в Великобритании) сосредоточились на технологии, анализирующей не рисунок линий на коже, а очертание ладони, которое также имеет индивидуальный характер. Аналогичная система, работающая с отпечатками пальцев, успешно используется британскими полицейскими уже три года. Но одних лишь отпечатков пальцев, как утверждают криминалисты, часто оказывается недостаточно. До 20 % следов, оставляемых на месте преступления - это отпечатки ладоней. Однако их анализ традиционными средствами достаточно трудоемок. Компьютеризация этого процесса позволит использовать отпечатки ладоней более широко и приведет к существенному увеличению раскрываемости преступлений. Следует отметить, что устройства сканирования ладони, как правило, имеют высокую стоимость, и поэтому оснастить ими большое число рабочих мест не так уж и просто.

Технология анализа **формы ушной раковины** является одной из самых последних подходов в биометрической идентификации человека. С помощью даже недорогой Web-камеры можно получать довольно надежные образцы для сравнения и идентификации. Этот способ недостаточно изучен, в научно-технической литературе достоверная информация о текущем состоянии дел отсутствует.

В настоящее время ведутся разработки систем «электронного носа», реализующих процесс распознавания **по запаху.** Наличие генетического влияния на запах тела позволяют считать эту характеристику перспективной для использования в целях биометрической аутентификации личности. Как правило, «электронный нос» представляет собой комплексную систему, состоящую из трех функциональных узлов, работающих в режиме периодического восприятия пахучих веществ: системы пробоотбора и пробоподготовки, линейки или матрицы сенсоров с заданными свойствами и блока процессорной обработки сигналов матрицы сенсоров. Этой технологии, как и технологии анализа формы ушной раковины, еще предстоит пройти долгий путь развития, прежде чем она станет удовлетворять биометрическим требованиям.

В заключение хочется отметить, что обойтись без биометрической идентификации, если необходимо получить позитивные, надежные и неопровержимые результаты проверки, невозможно. Ожидается, что в самом ближайшем будущем пароли и ПИН-коды уступят место новым, более надежным средствам авторизации и аутентификации.

4. КОНТРОЛЛЕРЫ СКУД

Контроллеры - интеллектуальный элемент системы контроля управления доступом, подразделяют на автономные, сетевые и интегрированные. Контроллеров в системе может быть несколько, а в больших системах они еще и многоуровневые. Контроллеры низкого уровня устанавливаются обычно вблизи считывателя и с задачей справляются сами, если же встречают незнакомую карту, запрашивают контроллер более высокого уровня, который их координирует. В более сложных случаях запрос идет на центральный компьютер, хранящий всю базу данных. В минимальном варианте контроллер может быть встроен в корпус считывателя Иногда все проблемы ложатся на стандартный компьютер. Хорошие контроллеры обязательно поддерживают режим связи с удаленным компьютером по телефонной линии. Это позволяет централизованно координировать базу данных во всех филиалах одной организации, и, кроме того, иметь оперативные рапорты обо всех нештатных ситуациях.

4Л. Автономные контроллеры

Автономные (локальные) СКУД, управляемые микрокомпьютером, как правило, обслуживают один КПП (возможно, с несколькими линейками прохода и соответственно контрольными терминалами). Идентификационная информация о пользователях и их полномочиях хранится в локальной базе данных. СКУД такого типа наиболее просты по конфигурации, но и наименее надежны с точки зрения возможности вывода их из строя. Они могут применяться в основном на тех объектах, где не требуется высокий уровень безопасности. Часто в литературе такие системы носят название однодверных. На рис. 4.1 приведена типовая схема построения такой системы.

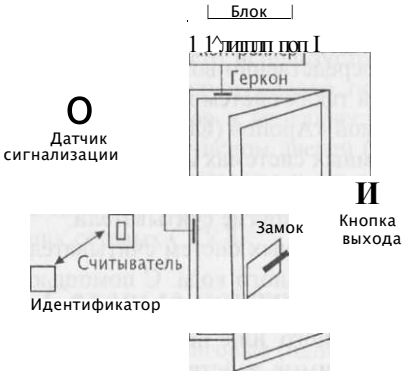


Рис. 4.1. Схема системы с разделенным контроллером и считывателями

Чаще всего к контроллеру можно подключить до двух считывателей, которые устанавливаются на две двери или на одну для контроля входа и выхода. Один из считывателей можно заменить на клавиатуру для набора кода. Кроме этого, система позволяет подключать электрозамки, кнопки выхода, герконы, ИК-датчики, сирену и др.

Существуют однодверные системы, аналогичные описанной выше, но в них считыватель и контроллер объединены в один корпус (рис. 4.2), т. е. блок, принимающий решение об открытии замка, находится в считывающем модуле. Это, с одной стороны, удешевляет систему, но с другой - уменьшает функциональные возможности, а главное - увеличивает вероятность взлома корпуса считывателя и замыкание контактов, к которым подключен замок.

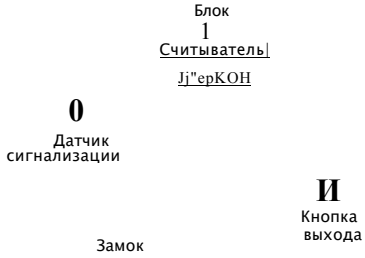


Рис. 4.2. Схема системы с совмещенным контроллером и считывателем

В еще более дешевых системах совмещаются в одном корпусе принимающий решение блок, клавиатура для набора кода, считыватель и замок. Наибольшее распространение такие системы получили в гостиницах.

На объектах с требованиями повышенной безопасности применяются контроллеры с цифровым управлением реле замка. Выносной модуль реле замка монтируется непосредственно возле замка и управляется особым цифровым кодом. Примером таких систем являются СКУД на основе контроллеров, предлагаемых фирмой «Apollo» (США).

Чаще всего в автономных системах используются считыватели магнитных карт «тач-мемори» и проксимити, гораздо реже - биометрические средства, индентификаторы Виганда или другие считыватели.

Но в большинстве автономных систем считыватели совмещены с клавиатурой для набора индивидуального кода. С помощью клавиатуры осуществляется программирование систем.

Системы на основе одного или нескольких автономных контроллеров осуществляют все необходимые действия, присущие СКУД, автономно (без использования управляющего компьютера).

Контроллеры в таких системах обязаны иметь собственный буфер памяти номеров карт (идентификаторов) и происходящих в системе событий. Обычно они имеют выход на локальный принтер для распечатки протокола событий. Программируются указанные контроллеры, как правило, с каких-либо кнопочных панелей или с помощью мастер-карт, позволяющих заносить в память контроллера новые карты и удалять старые. Один контроллер в таких системах обычно управляет доступом в одну (максимум - две) двери. В качестве идентификаторов (электронных пропусков) в таких системах могут применяться: магнитные карты, электронные «таблетки» - «i Button», радиочастотные PROX-карты и др. Все устройства управления дверями и охранными шлейфами (реле управления замком, входы для подключения датчика двери, кнопки выхода и охранных датчиков) располагаются в автономных системах обычно на плате самого контроллера. Часто сам контроллер конструктивно объединяется в одном корпусе со считывателем. Наиболее простые автономные системы (часто называемые - «гостиничными») вообще объединяют в одном корпусе контроллер принятия решений, считыватель/клавиатуру и электрозамок. Следует, однако, отметить, что данная мера, позволяющая снизить себестоимость системы, может привести к снижению безопасности, увеличивая вероятность взлома системы

В целях повышения безопасности в наиболее совершенных автономных системах применяется вынесенное цифровое реле управления замком. Данная мера позволяет предотвратить попытки проникновения в помещение путем прямого подключения электрозамка к проводам питания

В некоторых системах предусмотрена возможность расширения. Достигается это различными способами:

- за счет объединения отдельных контроллеров в сеть (использование добавочного сетевого модуля в дополнение к контроллеру);
- путем увеличения мощности и усложнения самого контроллера, что позволяет подключать к нему более двух считывателей.

В обоих случаях для связи контроллеров между собой или с периферийными исполнительными модулями часто используется какой-либо стандартный интерфейс, например RS-485. Следует, однако, помнить, что программировать приходится каждый контроллер в отдельности (несмотря на обмен данными между ними). Для систем с числом дверей более трех данный процесс может оказаться весьма утомительным и трудоемким (особенно при большом числе пользователей). В этом случае более предпочтительным является установка простейших сетевых СКУД.

4.2. Сетевые контроллеры

Сети контроллеров бывают одноранговые (одноуровневые) и многоранговые (многоуровневые), где число уровней редко превышает два.

В *одноранговой сети* имеется единственная шина (она может удлиняться за счет повторителей или разветвителей). В одноранговой сети все ее узлы (контроллеры доступа) имеют равные права (рис. 4.3). Среди представителей этого семейства - системы Northern Computers, Kantech, Parsec и большинство других систем, в том числе и российского производства.

Рис. 4.3. Одноранговая сеть

Недостатки одноранговой сети:

- необходимость иметь в каждом контроллере полную базу данных (список пользователей, их прав и т. д.);
- невозможность реализации некоторых глобальных функций, требующих взаимосвязанной работы нескольких контроллеров (например, глобальный «антипассбэк» - запрет повторного прохода). Этот недостаток имеет место только в сетях, где компьютер является ведущим, т. е. обмен информацией происходит только по его инициативе. Если сеть контроллеров работает на принципе произвольного доступа, недостаток отсутствует.

Достоинства, максимальная «живучесть» сети, поскольку каждый контроллер имеет все необходимое для автономной работы при выключенном («зависшем») компьютере или повреждении сети. Для систем безопасности это является существенным фактором

В многоранговой сети контроллеров имеется ведущий, или мастер-контроллер, который координирует работу «ведомых» контроллеров, реально управляющих одной или несколькими точками прохода (рис. 4.4). Самый известный в России представитель - система Apollo. Такие системы имеют как достоинства, так и недостатки.

Рис. 4.4. Многоранговая сеть

Недостатки многоранговой сети:

- нарушение работы системы при повреждении связи между мастер-котроллером и ведомыми контроллерами, поскольку значительная часть информации и алгоритмов являются, прерогативой мастер-контроллера;
- удорожание небольших систем за счет высокой стоимости мастер-контроллера (из-за его явной избыточности).

Достоинства многоранговой сети:

- централизованная память для баз данных, что сегодня не очень существенно;
- реализация всех функций даже при выключении компьютера;
- выигрыш в стоимости одной точки прохода при средних и больших размерах системы.

Оценивая общую топологию, необходимо отметить, что сегменты сети могут существовать в рамках системы в единственном экземпляре (см. рис. 4.3, 4.4), либо таких сегментов может быть много (рис. 4.5), т. е. оборудование СКУД может подключаться не к единственному ПК, а к любому из ПК, объединенных, в свою очередь, в компьютерную сеть. Вариант, показанный на рис. 4.5, позволяет строить сети любого масштаба (при наличии компьютерной сети между рабочими станциями). Далеко не все системы обеспечивают подключение оборудования к любому из ПК в сети.

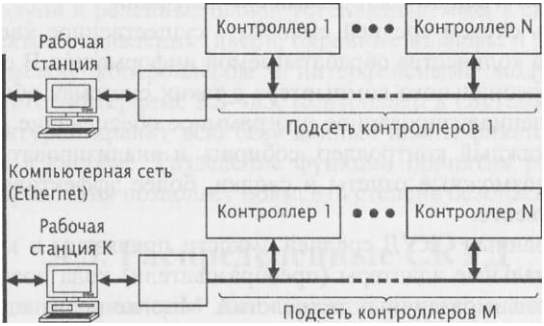


Рис. 4.5. Полная схема сети СКУД

Сетевые (централизованные) СКУД находятся под непосредственным и постоянным управлением центрального компьютера системы охраны объекта, обслуживающего все периферийные звенья КПП (рис. 4.6). База данных централизована. Применение таких систем экономически оправдано, лишь когда к центральному компьютеру подключено достаточно большое число терминалов - от нескольких десятков и более. Преимущество таких систем в том, что они в отличие от автономных позволяют вести централизованную регистрацию времени прохода служащих и осуществлять статистическую машинную обработку этих

сведений, а также оперативно вводить все необходимые изменения в режимы доступа тех или иных лиц или в целом на объект.

Сетевые СКУД способны обеспечить высокий уровень безопасности объекта. Для повышения надежности функционирования системы может быть применена параллельная обработка данных на двух ПЭВМ.

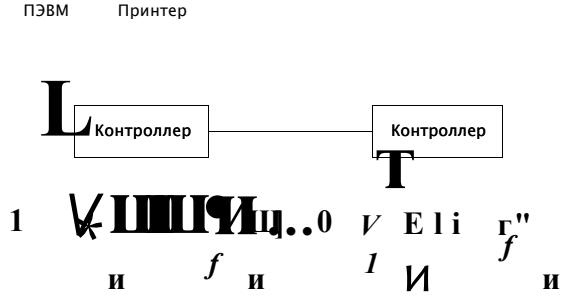


Рис. 4.6. Схема централизованной СКУД

Число контроллеров зависит от емкости системы и максимального числа считывателей, обслуживаемых одним контроллером.

Обычно для увеличения эффективности работы и уменьшения стоимости всей системы безопасности объекта централизованные СКУД позволяют осуществлять интеграцию с датчиками сигнализации.

Особенность систем средней емкости - существенное увеличение числа пользователей и количества обрабатываемой информации. В связи с этим использование персонального компьютера в таких системах обязательно. Компьютер и его специализированное программное обеспечение позволяют программировать каждый контроллер, собирать и анализировать информацию, составлять всевозможные отчеты и сводки, более эффективно отслеживать ситуацию на объекте.

Централизованные СКУД средней емкости привязаны к конкретной технологии. Специальные адаптеры (преобразователи) кода позволяют подсоединить считыватели различных технологий. Многие производители даже заявляют о том, что их система интегрируется с любым считывателем. Но, как правило, либо это утверждение недостаточно обосновано, либо требует серьезных дополнительных затрат на установку новых модулей.

Главная особенность таких СКУД в том, что они имеют возможность конфигурирования аппаратуры и управления процессом доступа с компьютерных терминалов (терминала). Различные СКУД имеют свои индивидуальные особенности и различаются по архитектуре, возможностям, масштабу (предельному числу считывателей/дверей), числу управляющих компьютеров, типу применяемых считывателей, степени устойчивости к взлому, степени устойчивости к электромагнитным воздействиям.

В соответствии с указанными параметрами производится разделение сетевых СКУД на 3 основных класса по ГОСТ Р 51241-98.

Большинство сетевых СКУД сохраняют многие достоинства автономных систем, основное из которых - работа без использования управляющего компьютера. Это означает, что при выключении управляющего компьютера система фактически превращается в автономную. Контроллеры данных систем так же, как и автономные контроллеры, имеют собственный буфер памяти номеров карт пользователей и событий, происходящих в системе. Наличие в системе компьютера позволяет службе безопасности оперативно вмешиваться в процесс доступа и осуществлять управление системой в режиме реального времени. Важнейшим элементом сетевых СКУД является программное обеспечение (ПО). Оно отличается большим разнообразием как по возможностям - от относительно простых программ для одного управляющего терминала, позволяющих добавлять в базу данных новых пользователей и убирать выбывших, до сложнейших программ с архитектурой клиент-сервер.

В системах данного класса используются мощные центральные контроллеры, осуществляющие процесс управления большим числом периферийных исполнительных устройств. Например, один контроллер AAN-100 компании Apollo может управлять процессом доступа в 96 дверей. Как правило, контроллеры в таких системах являются чисто электронными устройствами и не содержат релейных выходов. В таких системах функции управления внешними устройствами и охранными шлейфами обычно выполняют внешние интерфейсные модули и релейные блоки, устанавливаемые, в свою очередь, недалеко от объектов управления (двери, охранные шлейфы и др.). Для обмена информацией между контроллером и интерфейсными модулями наиболее часто используется интерфейс RS-485. Контроллер в системах с централизованной архитектурой хранит всю базу данных идентификаторов и событий, произошедших в системе. Разделение функции принятия решений и непосредственно управления позволяет повысить степень безопасности СКУД.

4.3. Распределенные СКУД

Возможности контроллеров наиболее полно раскрываются в распределенных СКУД.

Распределенные СКУД наиболее совершенны с точки зрения организации процесса обработки информации в системе, так как наилучшим образом противостоят сбойным и аварийным ситуациям, в частности, при сбоях в работе центрального ПК, нарушении целостности проводной линии, связывающей его с периферией и т. п.

Периферийные пункты оснащены локальными сетями на базе микрокомпьютеров (контроллеров), которые выполняют процедуру проверки самостоятельно, а центральный компьютер включается в работу лишь для актуа-

лизации локальных баз данных и статистической и логической обработки информации.

На рис. 4.7 показана схема разветвленной сети СКУД. Отличительная особенность СКУД с распределенной архитектурой состоит в том, что база данных идентификаторов (и событий в системе) содержится не в одном, а в нескольких контроллерах, которые, как правило, сами выполняют функции управления внешними устройствами и охранными шлейфами через реле и входы охранной сигнализации, расположенные непосредственно на плате самого контроллера.

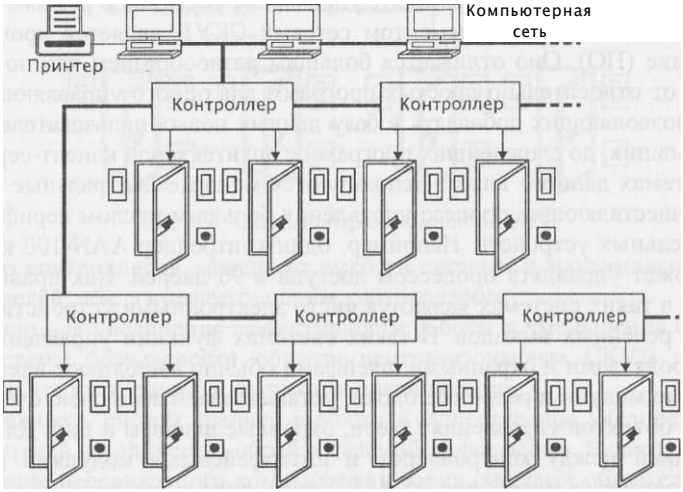


Рис. 4.7. Схема разветвленной сети СКУД

Еще одна отличительная особенность системы такого класса - возможность связи входных и выходных устройств разных контроллеров системы. Например, можно запрограммировать систему так, чтобы срабатывание датчика сигнализации у входа в офис, вызывало блокирование электрозамков, подключенных к нескольким контроллерам, контролирующим близлежащие помещения.

Кроме того, программное обеспечение больших систем позволяет использовать для управления сразу несколько компьютеров и осуществлять распределение исполнительных функций между ними. Например, можно на компьютер администратора возложить обязанности отслеживать местонахождение сотрудников и использование ими рабочего времени; оператору компьютера отдела кадров вменить в обязанность пополнять базу данных, печатать пропуска; на проходную установить компьютер с программами, помогающими идентифицировать личность, а на пост охраны - выводить тревожную графику и т. д.

Большие системы, как правило, работают в самом тесном взаимодействии с другими инженерными системами объекта: охранной сигнализацией, с системами телевизионного наблюдения и контроля, с системами жизнеобеспечения, оперативной связи и др.

Из-за невозможности удаленной установки от объекта управления данные контроллеры устанавливаются непосредственно внутри защищаемых ими помещений. Это не способствует снижению вероятности несанкционированного манипулирования контроллером, но имеет свои плюсы - при обрыве линии связи между контроллерами и компьютером система продолжает выполнять основные функции по управлению процессом доступа в автономном режиме. Наиболее часто в системах с распределенной архитектурой контроллер может управлять проходом в 1-2 двери.

Типичный пример таких систем:

- контроллер компании NORTHERN COMPUTERS (контроллер N-1000 II) - на 2 двери;
- контроллер компании KANTECH (КТ-200) - на 2 двери.

Распределенные системы обладают также тем преимуществом, что благодаря своей модульной конструкции позволяют наращивать мощность СКУД постепенно, переходя от локальных пунктов к распределенной сети; проще выполняется модернизация оборудования; авария на отдельном КПП не влияет на работу всей сети; для обработки проверяемых лиц требуется меньше времени.

Из систем с централизованной архитектурой обычно получаются системы со смешанной логикой путем добавления специализированных считывателей или интерфейсных модулей с собственным буфером памяти идентификаторов и событий. Благодаря использованию такого технического решения достигается избыточное резервирование функций, резко повышающее степень безопасности системы. Поскольку контроллер в СКУД с централизованной архитектурой управляет большим числом дверей, повреждение линии связи между ним и интерфейсными модулями управления оконечными устройствами может привести к блокированию значительной части или всей системы. Локальный считыватель с собственной базой данных в этом случае переходит в автономный режим управления доступом на своем участке. Пример такого решения - считыватель AP-500 компании Apollo или интерфейсный блок управления четырьмя дверями AIM-4SL. Системы, построенные с использованием данных модулей, обладают наивысшей степенью безопасности.

Приведем наиболее известные сетевые СКУД разной архитектуры с указанием числа считывателей, поддерживаемого одним контроллером.

Большинство контроллеров, на основе которых строятся системы с компьютерным управлением, поддерживают четное число считывателей: 2, 4, 8,16, 24, 32, 50, 64, 96 (на 1 контроллер). Наиболее известные на российском рынке компании: Apollo, ADVANTOR, CARDAX, COTAG, eff-eff HIRSCH,

lei, KANTECH, Keri Systems, NORTHERN COMPUTERS, PAC, TSS-201, Westinghous и др.

4.4. Контроллеры СКУД iSecure Pro

Реализацию контроллера рассмотрим на примере контроллеров iSecure Simplex СКУД iSecure Pro компании SimplexGrinnell, которые представляют собой самостоятельные микропроцессорные системы с распределенной обработкой данных. Они предназначены для управления устройствами контроля доступа и охранной сигнализации, такими, как считыватели, клавиатуры, дверные магнитоконтактные датчики, кнопки выхода, дверные замки, сирены и другие, а также для обеспечения взаимосвязи системы контроля доступа с системами и базами данных различных подразделений компании. При потере связи с управляющим компьютером встроенная в контроллер программа позволяет ему функционировать самостоятельно до восстановления связи.

Все контроллеры системы контроля доступа iSecure интегрируются с аппаратно-программной платформой комплексной системы безопасности iSecure PRO Simplex и обеспечивают стандартную организацию сетей Ethernet, TCP/IP, LAN/WAN и интеграцию с действующими в компании информационными системами. Для эффективного управления ресурсами контроллеры iSecure имеют распределенный уровень интеллекта, а для снижения эксплуатационных расходов - встроенную самодиагностику.

Основные характеристики контроллеров iSecure Simplex:

- iSecure имеет модульную, конфигурируемую и легко расширяемую схему;
- распределенная интеллектуальная архитектура контроллера позволяет выполнять непрерывную самодиагностику и регистрацию сбоев, обеспечивая его надежное функционирование и освобождая головной узел от рутинных операций;
- специальный пакет средств графической диагностики представляет оператору информацию на трех уровнях: общий вид всей сети, внутренняя конфигурация и статус каждого контроллера системы контроля доступа, а также статус всех устройств доступа и модулей контроллера;
- каждый контроллер iSecure Simplex может иметь индивидуальную конфигурацию в сети, которая позволяет объединять сотни контроллеров, поддерживающих тысячи считывателей магнитных карт, охранных датчиков, дверей доступа и других устройств;
- съемные модули конфигурации контроллера заменяются непосредственно на объекте, что ускоряет процесс их обслуживания и сокращает эксплуатационные расходы;
- через интерфейсные платы контроллеры поддерживают различные виды связи.

Используя Ethernet TCP/IP, можно значительно сократить расходы на монтаж и обслуживание системы, соединив контроллеры через уже существующие локальные или глобальные сети. В контроллерах удаленных объектов используется плата модемной связи:

- контроллеры совместимы с широким спектром оборудования систем безопасности компании Simplex, включая систему нового поколения iSecure Pro Simplex, а также с оборудованием других производителей;
- при применении отказоустойчивой архитектуры сети iSecure Path с автоматической реконфигурацией потоков данных контроллеры обеспечивают максимальную живучесть всей системы безопасности в случае повреждения линий связи.

Все контроллеры iSecure Simplex имеют российские сертификаты. Схема подключения контроллера в систему контроля доступа iSecure PRO Simplex показана на рис. 4.8.

Рис. 4.8. Схема подключения контроллера в систему контроля доступа iSecure PRO Simplex

Конструктивные и технические характеристики контроллеров iSecure системы контроля доступа Simplex рассмотрены ниже.

1 ***Внутренняя архитектура.*** На материнской плате контроллера располагаются: слот ЦПУ для карты ЦПУ с 32-разрядным встроенным процессором Intel, слот карты связи для проводной сетевой карты 4120, либо модульной сетевой карты 4120, шесть) слотов расширения для модулей входов/выходов и модулей подключения считывателей, а также источник питания с узлом зарядки батарей.

Контроллер имеет компактные размеры, позволяющие устанавливать его в небольших помещениях. Датчик вскрытия крышки корпуса обеспечивает защиту от несанкционированного доступа к узлам контроллера.

2. ***Технические характеристики контроллера:***

- встроенный 32-разрядный процессор компании Intel;
- внутренняя самодиагностика и встроенный индикатор состояния;
- поддерживает клавиатуры и считыватели проксимити-карт, магнитных карт, Виганда-карт, биометрических данных, радиочастотных приемников и карт со штрих-кодом;
- возможность программирования формата карты.

Рабочие возможности по поддержке:

- до 8 форматов карточек на контроллер;
- до 96 контролируемых входов;
- до 48 релейных выходов;
- до 5 ООО владельцев карточек и 3 ООО сообщений (стандартная конфигурация);
- до 50 ООО владельцев карточек и 25 ООО сообщений (расширяемая конфигурация) ;
- до 12 считывателей.

Модули-компоненты (рис. 4.9).

Карты линии связи (одна на контроллер): карта линии связи 4120 для проводного подключения, модульная карта линии связи 4120 или модем.

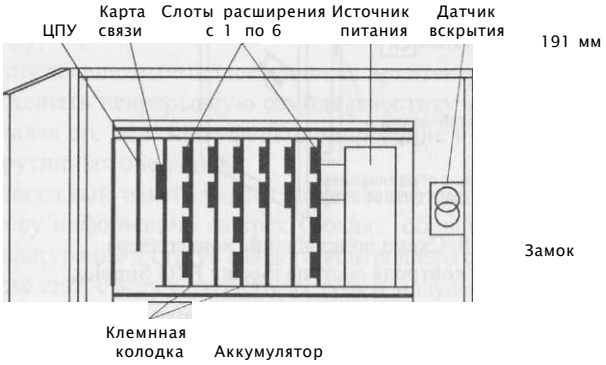


Рис. 4.9. Внешний вид, размеры контроллера СКУД iSecure Simplex и расположение модулей в стойке

Используются следующие модули расширения: модуль для подключения 2 считывателей, модуль с 16 контролируемыми входами, модуль с 8 релейными выходами, модуль с 8 контролируемыми входами/8 релейными выходами, модуль с 8 контролируемыми входами. Все входы могут быть сконфигурированы для мониторинга как двух, так и четырех состояний.

3. ***Модули для подключения к контроллеру считывателей.*** Каждый модуль имеет два порта, каждый из которых поддерживает считыватель карточек, клавиатуру или считыватель, совмещенный с клавиатурой. Каждый порт обеспечивает полный контроль и управление точкой доступа, используя следующие элементы: релейный выход ИЗ или НР (задается перемычкой) для управления дверными замками, контролируемый вход (2 или 4 состояния) дверного магнитоконтактного датчика, контролируемый или неконтролируемый вход кнопки выхода. Кроме этого модуль, содержит 4 многоцелевых контролируемых входа и 2 многоцелевых релейных выхода.

4. Бесперебойное питание. Встроенный источник питания имеет схему заряда аккумуляторов. При использовании аккумулятора емкостью 18 А. ч время стабильной работы контроллера составит около 4 ч. Тестирование аккумуляторов осуществляется контроллером каждые 5 мин. Время заряда батарей составляет менее 24 ч.

5. ИСПОЛНИТЕЛЬНЫЕ УСТРОЙСТВА СКУД

Для того чтобы пройти через вход, контролируемый СКУД, система на основании ограничений, заданных для владельца идентификатора, принимает решение о приведении в действие исполнительных механизмов и устройств, непосредственно регулирующих доступ. В настоящее время существуют различные способы защиты входа в охраняемое помещение: простые и укрепленные двери, калитки с электромагнитными и электромеханическими замками или защелками, трехштанговые турникеты (триподы), полуростовые и полноростовые турникеты, автоматизированные проходные, шлюзовые кабины (тамбур-шлюзы), ворота, шлагбаумы и другие. Все устройства, перечисленные выше, могут использоваться как автономно, так и в составе СКУД.

В СКУД предусматриваются меры по обеспечению устойчивости к вскрытию злоумышленниками замков и запорных механизмов, по предотвращению наблюдения за вводом идентификационных признаков и копирования эталонных признаков идентификаторов.

Так как преграждающие устройства могут подвергаться разрушающим и неразрушающим воздействиям злоумышленников, то их по механической устойчивости стандарт классифицирует следующим образом:

- повышенная устойчивость к взлому путем нанесения ударов и применения инструментов;
- высокая устойчивость, характеризуемая пуле- и взрывоустойчивостью сплошного перекрытия проходного проема.

5Л. Электрические замки и защелки

Электрические замки рекомендуется использовать в качестве основного запирающего устройства в дневное время. Эти замки в отличие от механических открываются дистанционно по электрическому сигналу и используются совместно с домофонами, кодовыми панелями, считывателями карточек различных типов. Электрозамки делятся на два класса: электромагнитные и электромеханические.

Электромагнитные замки представляют собой корпус с электромагнитом и ответную металлическую пластину. Пластина крепится на дверном полотне, а сам замок - на косяке. Электромагнитный замок удерживает дверь в закрытом состоянии за счет усилия мощного электромагнита. При обесточивании замка дверь остается открытой, поэтому для обеспечения работы в условиях отключения напряжения питания необходимо применять блоки гарантированного питания.

Электромеханический замок имеет механический ригель (засов), удерживающий дверь в закрытом состоянии, а управление этим ригелем осуществляется относительно маломощным соленоидом. При закрытии двери взводящий ригель замка взводит имеющуюся в замке пружину, при этом рабочий ригель входит в ответную часть замка и удерживает дверь в закрытом состоянии. При подаче напряжения соленоид отпускает фиксатор пружины, и рабочий ригель под действием пружины втягивается в замок - дверь может быть открыта. После того как дверь будет открыта, а затем закрыта, она вновь окажется в запертом состоянии. Предусматривается режим, исключающий автоматическое запирание замков и случайное закрывание двери.

В соленоидных электрозамках ригель приводится в движение усилием электромагнита. Оборудованная таким замком дверь может быть открыта только в период действия управляющего сигнала. После снятия этого сигнала закрытая дверь останется запертой независимо от того, открывалась ли она. Существуют также другие разновидности электромеханических замков: электромоторные (ригель приводится в движение электромотором с редуктором), с ручным приводом ригеля (ригель приводится в движение поворотом ручки, а электромагнит разблокирует механизм привода). Электромеханические замки могут быть накладного и врезного типа.

Электрозащелки представляют собой ответную часть замка и используются совместно с обычным механическим замком. При подаче управляющего напряжения разблокируется фиксатор электрозащелки, и дверь может быть открыта при выдвинутом положении ригеля механического замка. При этом используемый механический замок не должен открываться снаружи поворотом ручки. При наличии ручки с внутренней стороны двери она может быть открыта изнутри поворотом ручки без подачи управляющего напряжения на защелку. Специальные модели соленоидных замков и электрозащелок предназначены для оборудования аварийных выходов. Такие замки открываются при отключения напряжения питания.

При выборе модели замка необходимо учитывать, какие помещения и для каких целей предполагается оборудовать замком. При этом необходимо учитывать: массу, конструкцию, материал двери, требуемую интенсивность использования, различные функциональные особенности системы, включающей замок. Все это определяет надежность и долговечность работы электрозамка.

Доводчики двери (закрыватели) служат для принудительного закрывания двери и обеспечивают надежную работу электрозамков. Регулирующие клапаны позволяют выбрать требуемую скорость закрывания двери. Для дверей разного размера можно подобрать соответствующий доводчик. Модели также отличаются конструктивным исполнением, дизайном, рядом дополнительных функций: фиксация двери в положении «открыто», ускорение в завершающей фазе закрывания - «прихлоп» и др.

5.2. Турникеты

В соответствии с ГОСТ Р 51241-98 все турникеты отьносятся к разделу «Устройства преграждающие управляемые (УПУ)» и классифицируются по следующим двум признакам:

- вид перекрытия проема;
- способ управления УПУ.

По *виду перекрытия проема* различают следующие виды турникетов:

- с частичным перекрытием проема;
- с полным перекрытием проема;
- с блокирование объекта в проеме (шлюзы, кабины проходные).

По *способу управления УПУ* делят на устройства:

- с ручным управлением;
- с полуавтоматическим управлением;
- с автоматическим управлением.

А. Гинце [40] предлагает более упрощенную по сравнению с ГОСТ Р 51241-98 классификацию. В основу такой классификации положен принцип функциональности. В соответствии с этим признаком все турникеты можно разделить на УПУ, осуществляющие *полное* или *неполное* перекрытие проема, а также «*нормально закрытые*» или *анормально открытые».*

Принцип работы турникета СКУД прост: если запрос на доступ правомерен, то механическая система, поворачиваясь, открывает проход на охраняемую территорию.

К основным видам турникетов относятся:

- калитки;
- триподы;
- роторные поясные турникеты;
- турникеты с выдвижными створками;
- турникеты с откидными створками на электроприводы;
- роторные полнопрофильные или полноростовые турникеты.

Нормально открытые турникеты имеют более высокую пропускную способность, но не исключают возможность прохода нескольких прижавшихся друг к другу человек.

Наиболее распространены трехлопастные турникеты с вращающимся в одном направлении преграждающим устройством - *триподы* и *роторные* Они обеспечивают гарантированный единовременный проход одного человека. Преграждающее устройство трипода выполнено в виде вращающегося блока с тремя цилиндрическими брусьями (штангами), расположенными под углом 120°. Вращающийся блок крепится сбоку зоны прохода. При вращении каждый из брусьев фиксируется в горизонтальном положении, преграждая путь человеку. Роторные турникеты бывают высотой до пояса человека (по-

ясные) и в полный рост (полноростовые). Полноростовые обеспечивают полное перекрытие зоны прохода, а через заградительный барьер поясного турникета можно перелезть или перепрыгнуть, поэтому он размещается на посту охраны и управляется нажатием на его педаль ногой вахтера.

Турникеты обеспечивают высокую пропускную способность - до 60 человек в 1 мин., они дешевле шлюзовых кабин, но их конструкция не мешает задерживаемому применить против сотрудников охраны оружие. Кроме того, размеры пространства между заградительными барьерами устанавливаются исходя из размеров человека средней комплекции, что создает неудобства для толстяков и при проносе крупногабаритных носимых вещей. Для повышения эффективности защиты турникеты оснащаются датчиками, срабатывающими при нерегламентированном поведении человека, например, попытке перепрыгнуть через заграждающий барьер.

Электромеханические турникеты являются традиционными исполнительными механизмами систем контроля доступа. Они применяются для оборудования входов в помещения или ограничения входа в отдельные части помещений, а некоторые модели - для ограничения входа на территорию. В отличие от двери, оборудованной электрозамком, турникет является исполнительным устройством, обеспечивающим проход людей «по одному».

Для управления электромеханическими турникетами могут использоваться пульты ручного управления, а также любые устройства контроля доступа: считыватели карточек различного типа, электронные ключи, радиобрелки, клавиатуры, приемники жетонов и т. д. Это позволяет включать турникеты в состав сетевых компьютеризированных систем контроля доступа.

Разнообразие областей применения турникетов обусловливает разнообразие их типов: от миниатюрных турникетов, устанавливаемых в автобусах, до полнопрофильных моделей высокой степени секретности для оборудования входов на охраняемую территорию и скоростных моделей с очень высокой пропускной способностью для станций общественного транспорта. Наиболее популярные модели турникетов: *турникеты-триподы, турникеты-«вертушки» (роторные), турникеты-калитки.*

Турникеты-триподы с тремя преграждающими планками - оптимальный выбор, если необходимо оборудовать проходную предприятия, банка, административного учреждения или организации и осуществлять контроль с целью пресечения допуска посторонних лиц на предприятие (рис. 5.1).

Они разделяют поток людей по одному, обеспечивая при этом высокую пропускную способность. В режиме однократного прохода через турникет в разрешенном направлении может пройти один человек, после чего турникет автоматически возвращается в закрытое положение. При необходимости пропуска группы лиц устанавливается режим многократного прохода в нужном направлении, возможен режим свободного прохода. Направление прохода высвечивается на табло. В случае экстренных ситуаций возможна механическая разблокировка преграждающих планок с помощью ключа или их де-

монтаж. При отсутствии сетевого питания турникет переходит на работу от аккумулятора.

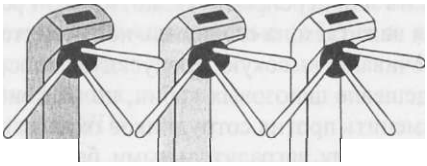


Рис. 5.1. Турникеты-триподы стремя преграждающими планками

Турникеты-триподы - наиболее популярный вид турникета. Это обусловлено их невысокой стоимостью и компактностью. Триподы имеют современный элегантный внешний вид, легко монтируются.

Степень защиты этих турникетов относительно невысока по сравнению с более сложными моделями, так как через преграждающую планку можно перелезть или проползти под ней. Однако такой турникет устанавливается, как правило, в местах постоянного присутствия сотрудника охраны. Кроме того, повысить безопасность можно установкой инфракрасных датчиков, срабатывающих при попытках перелезть через турникет или проникнуть под преграждающей планкой. В этом случае срабатывание датчика вызовет сигнал тревоги, который может быть подан на сирену, в помещение охраны или включить видеозапись действий злоумышленника.

Роторные турникеты, или так называемые «вертушки», предназначены для регулирования входа/выхода на проходных предприятий, военных и специальных объектов, где необходимо полное или почти полное перекрытие зоны прохода (рис. 5.2).

Рис. 5.2. Роторные турникеты
для регулирования входа/выхода
на проходных предприятий

Они могут быть различными по высоте: от поясных до турникетов в полный рост. Степень защиты весьма высока.

Установка двух роторных турникетов один за другим позволяет организовать шлюз-тамбур. Это удобно при необходимости жесткого контроля доступа, например, на таможне.

Роторные турникеты могут работать в автономном режиме с управлением от пульта охранника, а также в составе СКУД. В режиме однократного прохода через турникет в разрешенном направлении проходящий толкает преграждающие планки в разрешенном направлении, после чего происходит автоматический доворот «вертушки» в исходное закрытое положение. При необходимости пропуска группы лиц устанавливается режим многократного прохода в нужном направлении, возможен режим свободного прохода. В случае экстренных ситуаций возможна механическая разблокировка преграждающих лопастей с помощью ключа. При отсутствии сетевого питания турникет переходит на работу от аккумулятора.

Турникеты-калитки широко используются в магазинах, аэропортах, вокзалах для организации свободного прохода в одну сторону и запрета прохода в другую сторону, а также в банках, учреждениях, на предприятиях для организации свободного выхода (рис. 5.3).

Рис. 5.3. Турникет-калитка
для одностороннего прохода

Калитки можно использовать в системах контроля доступа, но для более полной защиты необходимо подключать к калиткам датчики прохода и организовать дополнительный контроль. Эти турникеты не разделяют поток людей по одному и после открытия калитки через нее могут пройти несколько человек.

Автоматическая электромеханическая калитка с приводом автоматически распахивается по команде с пульта охраны или при срабатывании ИК-датчика. Створку при необходимости можно придержать или толкнуть быстрее. Электромеханическая калитка без привода управляется от пульта, но при проходе створка отводится рукой. При отсутствии сетевого питания калитка работает от аккумулятора.

Механическая калитка не имеет дистанционного управления и просто механически обеспечивает свободный проход в одну сторону и запрет прохода в другую сторону.

После прохода человека створка калитки любой модели автоматически возвращается в исходное положение и блокируется. В экстренных случаях калитку можно открыть обычным ключом, а створку повернуть рукой, освободив проход.

Ограждения предназначены для формирования потоков людей, ограничения зон прохода (рис. 5.4).

Рис. 5 4. Ограждения
для формирования потоков людей

При оборудовании проходных турникетами различного типа часто оказывается, что зона прохода перекрыта не полностью и есть необходимость в ограждениях. Ограждения можно выполнить в едином дизайне с турникетами. В качестве заполнений можно использовать тонированные или зеркальные стекла с нанесением логотипа заказчика. Ограждения легко монтируются и могут быть любой высоты и формы.

Турникеты поясные (рис. 5.5) оставляют возможность для перепрыгивания, поскольку, как следует из их названия, заградительный барьер доходит только до пояса человека. При их использовании практически невозможно обеспечить защиту от перебрасывания предметов, поэтому такие турникеты обязательно должны быть установлены в зоне видимости охраны.

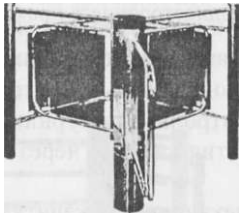


Рис. 5.5. Турникет поясной

Турникеты полноростовые (рис. 5.6) устанавливают в удаленных от поста охраны местах и используют в полностью автоматическом режиме работы.

Полноростовые роторные турникеты используются на режимных предприятиях, таких, как атомные станции, военные объекты, аэропорты, а также в банках, на стадионах, складских комплексах, в офисах. Они представляют собой металлоконструкцию из стальной рамы, вращающейся центральной колонны со штангами и дополнительной системы ограждений. Существует несколько модификаций полноростовых турникетов, отличающихся как конструктивно, так и функционально. Например, существуют турникеты с одним или двумя проходами, с двумя, тремя или четырьмя преграждающими лопастями, с прямыми или закругленными штангами, сделанные целиком

из полированной нержавейки, анодированные или крашеные. Есть модели с дополнительной крышей, имеющие освещение и дренаж, модели со стеклянными боковыми панелями и преграждающими элементами, выполненными из прочного пластика. Существуют также модели турникетов с интегрированной дверью. Интегрированная дверь может быть очень полезна, например, если нужно провезти через турникет тележку или организовать эвакуацию персонала. Кроме того, существуют специальные конструкции, имеющие 2 прохода для персонала и интегрированную двухстворчатую дверь между ними, что позволяет при необходимости даже проезжать через подобное устройство на автокарах и автомобилях.

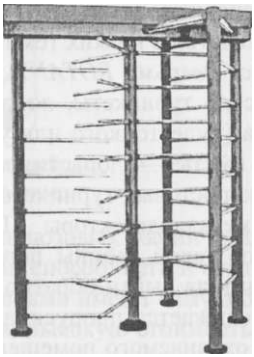


Рис. 5.6. Турникет полноростовой

Для организации максимально защищенных проходов в офисах, банках и на аналогичных объектах с повышенными требованиями к внешнему виду проходных предпочтительны более эстетичные полноростовые турникеты, выполненные из стекла. Подобные устройства с пулестойким стеклом, оборудованные считывателями, датчиками контроля положения человека и даже весовой системой, ограничивают доступ на объект, разделяют людской поток и при этом имеют все достоинства обычных дверей - защищают фойе от холода, а также позволяют создать необходимый дизайн интерьера и фасада здания.

По типу привода турникеты подразделяют на *механические, электромеханические и турникеты с серводвигателем.* Механические турникеты, как правило, устанавливаются на выходе с объекта и позволяют беспрепятственно выходить, но не допускают проникновения на охраняемую территорию (обеспечивают односторонний проход). Электромеханические турникеты и турникеты с серводвигателем могут работать в составе СКУД и управляться внешними контроллерами других систем.

Принцип действия всех турникетов примерно одинаков. Если карточка пользователя действительна, турникет разблокируется. Турникет проворачивается вручную (если нет встроенного двигателя), и пользователь, пройдя

между створок, оказывается на охраняемой территории. Одновременно можно пройти только одному человеку и только в одном направлении.

В режиме шлюзования турникет может быть остановлен в промежуточной позиции, блокируя перемещение пользователя с целью запросить дополнительное подтверждение личности - введения ПИН-кода, предъявления биометрических идентификаторов (отпечатка пальца, геометрии руки и т. п.). Существуют модели с интегрированной весовой платформой, где вес пользователя, предъявившего карточку и вошедшего в контролируемый сегмент, сравнивается с данными из базы данных.

Для того чтобы турникет мог работать в уличных условиях в российском климате, необходимо обеспечить влаго- и пылезащищенность системы, а также устойчивость к воздействию низких температур.

Кабины с вращающимися дверьми ROTANT представляют собой полноростовые электромеханические турникеты, лопасти и стены которых изготавливаются из бронестекла (пулестойкого или устойчивого к пробиванию). Вращающиеся двери могут иметь 3-4 лопасти, либо 2 сектора (рис. 5.7-5.9). В отличие от обычных полноростовых турникетов в кабины с вращающимися дверьми встраиваются металлодетекторы. При обнаружении оружия у проходящего человека ротор такой кабины переходит в реверсный режим вращения, вынуждая нарушителя выйти обратно из кабины. Однако при подобном алгоритме работы снижается пропускная способность шлюза и осложняется выход людей из охраняемого помещения. Эта проблема решается установкой дополнительных полукруглых раздвижных дверей на выходе из кабины. Такое решение применяется, например, в кабинах ROTOCOM производства фирмы SAIMA и PRIORA TONDA фирмы TONALI. (рис. 5.7).

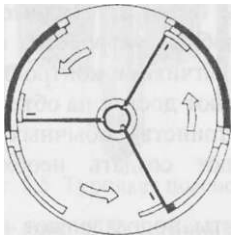


Рис. 5.7. Кабина с вращающейся дверью с тремя лопастями и дополнительной раздвижной дверью

При срабатывании металлодетектора направление вращения ротора этих кабин не меняется. Вместо этого проход нарушителя в охраняемое помещение блокируется с помощью дополнительной двери, закрывающейся только перед нарушителем. Выход из помещения при этом остается открытым и пропускная способность кабины не снижается. Дополнительные раздвижные двери могут устанавливаться как с одной, так и с двух сторон кабины. При

этом описанный алгоритм работы действует как при входе, так и при выходе из охраняемого помещения.

Кабины с вращающимися дверьми, как и тамбур-шлюзы, могут работать в ручном и автоматическом режимах, интегрируются с СКУД. Основным достоинством кабин с вращающимися дверьми является их очень высокая пропускная способность. К недостаткам этих кабин, в первую очередь, относится их большая стоимость.

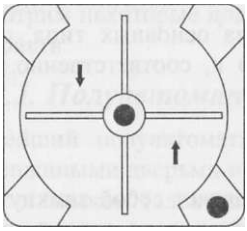


Рис. 5.8. Кабина с вращающейся дверью с четырьмя лопастями

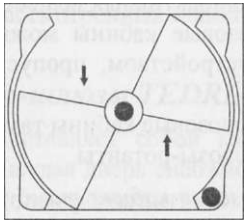


Рис. 5.9. Кабина с вращающейся дверью с двумя секторами

Области применения шлюзовых кабин различных типов определяются требованиями к пропускной способности и ограничениями по стоимости. Кабины с вращающимися дверьми имеют самую большую пропускную способность и вместе с тем самую высокую стоимость. Полуавтоматические тамбуры, наоборот, отличаются низкой стоимостью и невысокой пропускной способностью. Автоматические шлюзы имеют средние значения стоимости, пропускной способности и позволяют наиболее надежно контролировать доступ на охраняемый объект.

5.3. Шлюзовые кабины

Для систем управления доступом с высоким уровнем защиты применяют устройства закрытого типа — шлюзовые кабины. Шлюзовые кабины могут быть *полуавтоматические* и *автоматические*. В полуавтоматических шлюзовых кабинах применяются распашные двери, которые открываются вручную и закрываются доводчиком, но блокируются с помощью электромагнитных или электромеханических замков, управляемых вахтером или контролером. В автоматических шлюзовых кабинах двери открываются и закрываются с помощью электромеханических приводов, управляемых контролером СКУД или вахтером. В отличие от полуавтоматических шлюзов в автоматических шлюзах применяются двери различных конструкций: распашные одностворчатые и двустворчатые, раздвижные с плоскими или полукруглыми створками, складывающиеся, цилиндрические, одностворчатые и двустворчатые с плоскими поворачивающими створками.

В шлюзовые кабины устанавливаются считыватели и другие средства биометрической идентификации. Закрытая конструкция шлюза оказывает психологическое давление на человека, стремящегося проникнуть на территорию организации без надежных документов. Двери и стены шлюзов, как правило, выполняются из ударопрочного стекла (бронестекла) или пластика. Часто в шлюзы встраиваются датчики металлодетектора и других средств контроля вносимых или выносимых вещей, прежде всего, оружия, взрывчатых и радиоактивных веществ.

Шлюзовые кабины можно разделить на два основных типа, отличающихся устройством, пропускной способностью и, соответственно, стоимостью:

- шлюзовые кабины тамбурного типа;
- шлюзы-ротанты.

Шлюзовая кабина тамбурного типа представляет собой замкнутую систему двух зависимых дверей, которые одновременно не открываются. Основным свойством любой шлюзовой кабины (шлюза) является то, что в любой момент времени открыта только одна из двух дверей. Принцип действия подобного устройства следующий: человек свободно открывает дверь 1 и входит в шлюз, после чего предъявляет системе контроля доступа свой идентификатор. Если доступ разрешен, открывается дверь 2, а дверь 1 блокируется в закрытом состоянии. Таким образом, гарантируется, что на защищаемую территорию попадет только авторизованный сотрудник. В случае отказа на допуск обе двери блокируются для выяснения службой безопасности личности находящегося в шлюзе человека. Пропускная способность шлюзовой кабины тамбурного типа находится в пределах от 8 до 12 человек в минуту.

Шлюзы-ротанты. Принцип их действия аналогичен шлюзам тамбурного типа, но вместо двух обычных дверей используется одна поворотная дверь турникетного типа (рис. 5.10).

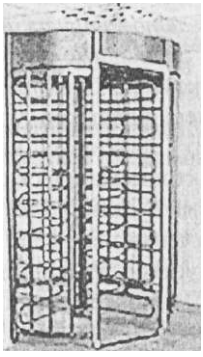


Рис. 5.10. Шлюз-ротант

Для повышения вероятности отсечения злоумышленников шлюзы в большинстве случаев комплектуются системами взвешивания (для дополнительного контроля количества людей внутри кабины) и встроенными металлодетекторами (для контроля проноса оружия). Различным может быть и материал стен кабины: от стали до бронестекла

Пропускная способность шлюза-ротанта составляет от 18 до 22 человек в минуту.

Рассмотрим некоторые *примеры реализации* рассмотренных исполнительных устройств.

5.3.1. Полуавтоматические тамбур-шлюзы TEDRIA

Простейший полуавтоматический шлюз представляет собой кабину с двумя распашными дверьми на входе и выходе. Каждая дверь снабжается доводчиком и замком (электромеханическим или электромагнитным). Замки обоих дверей управляются общей шлюзовой логикой, которая следит за тем, чтобы двери не были открыты одновременно. Для контроля за состоянием дверей (закрыта/открыта) в простейшем случае применяются герконы. Кроме того, в полуавтоматических кабинах часто применяются электромеханические замки со встроенным датчиком состояния замка (заперт/открыт). В этом случае шлюзовая логика считает дверь закрытой только при наличии одновременно двух сигналов: «закрыто» от геркона и «заперт» от датчика замка. Полуавтоматический шлюз может работать в ручном или в автоматическом режимах.

В *ручном режиме* команды на открытие дверей поступают в шлюзовую логику с пульта управления, устанавливаемого на посту охраны. Разрешение прохода в этом случае принимают сотрудники охраны. Для получения информации о посетителе тамбур-шлюз может быть оборудован переговорным устройством (интеркомом) и/или устройством телевизионного наблюдения. Для того чтобы сотрудники службы безопасности могли наблюдать за посетителем, находящимся внутри шлюзовой кабины, используется дополнительная видеокамера, размещаемая внутри шлюза. Кроме того, в большинстве случаев полуавтоматические кабины представляют собой металлоконструкцию с дверьми и боковыми стенками из непробиваемого или пулестойкого стекла. Двери и боковые стенки могут быть остеклены полностью или частично. Кроме поочередного открывания дверей, сотрудники охраны имеют возможность с помощью пульта управления разблокировать обе двери одновременно. Это необходимо для обеспечения беспрепятственного выхода людей из здания при экстренной эвакуации или при необходимости проноса через шлюз крупногабаритных предметов.

В *автоматическом режиме* разрешение прохода через шлюз принимается без участия сотрудников охраны. В простейшем случае разрешающий сигнал в шлюзовую логику может поступать от датчика присутствия человека перед кабиной. Однако в большинстве случаев для управления шлюзовой ло-

гикой в автоматическом режиме используется СКУД. В СКУД для принятия решения о разрешении прохода могут использоваться различные идентификаторы личности: считыватели магнитных карт, карт Виганда, бесконтактных радиочастотных (проксимити) карт, клавиатуры, различные биометрические идентификаторы и т. д.

Использование СКУД позволяет не только разрешать проход на охраняемый объект различным категориям сотрудников и посетителей только в определенные часы и дни, но и вести регистрацию событий и учет рабочего времени.

В автоматическом режиме шлюзовая логика, получив сигнал на разрешение доступа, проверяет, завершен ли предыдущий цикл прохода.

Только после этого отпирается замок первой двери. Затем шлюзовая логика контролирует закрытие первой двери и присутствие человека внутри кабины (например, с помощью пассивного инфракрасного датчика). Если в течение заданного интервала времени (обычно несколько десятков секунд) в шлюзовую логику не поступает сигнал о том, что человек зашел в кабину, цикл считается завершенным и вторая дверь не открывается, а шлюзовая логика переходит в режим ожидания следующего сигнала разрешения прохода. В случае если человек зашел в кабину и первая дверь закрылась, шлюзовая логика в зависимости от заданного алгоритма работы либо выдает команду на отпирание замка второй двери, либо ждет поступления дополнительного разрешающего сигнала от СКУД. Для формирования этого сигнала СКУД должна получить подтверждение от дополнительного идентификатора, устанавливаемого внутри кабины. Так, для входа в шлюз может использоваться считыватель магнитных или проксимити-карт, а в качестве дополнительного идентификатора внутри кабины обычно располагается клавиатура для ввода индивидуального кода владельца предъявленной карты или биометрический идентификатор. Такая организация работы шлюза в автоматическом режиме позволяет исключить проход по украденной или потерянной карте. При использовании дополнительного идентификатора, получив разрешающий сигнал от СКУД, шлюзовая логика дает команду на отпирание замка второй двери. Если же в течение заданного промежутка времени дополнительного разрешающего сигнала от СКУД не поступило, то шлюзовая логика, в зависимости от заданного алгоритма либо отпирает замок первой двери и выдает речевое сообщение с предложением нарушителю покинуть кабину, либо блокирует нарушителя внутри кабины и ждет дальнейших команд с пульта управления или от СКУД,

При работе шлюза в автоматическом режиме под управлением СКУД, вместе с человеком, имеющим право доступа на объект, могут пройти еще один или несколько человек. Кроме того, через шлюз может пройти террорист с заложником, имеющим право доступа. Для предотвращения этих ситуаций в шлюзовых кабинах используются различные системы контроля прохода «по одному». В полуавтоматических шлюзах в качестве датчиков

этих систем используются различные емкостные и контактные коврики, инфракрасные и микроволновые датчики, системы взвешивания. Однако все эти системы имеют свои недостатки и в ряде случаев не позволяют осуществлять контроль прохода «по одному».

Наилучшие результаты дает применение системы взвешивания в сочетании со СКУД. При этом вес человека, находящегося внутри кабины, сравнивается с соответствующим значением из базы данных СКУД. Этот метод, позволяющий полностью контролировать проход через шлюз «по-одному», чаще применяется не в полуавтоматических тамбурах, а в некоторых моделях автоматических шлюзовых кабин.

Иногда в полуавтоматических тамбурах применяются чисто механические решения, позволяющие проходить через шлюз только одному человеку. Например, в шлюзе UNIVERSAL 2000 швейцарской фирмы Scheebrli используются откидные дефлекторы, поднимающиеся в горизонтальное положение после того, как человек вошел в шлюз (рис. 5.11). Недостатком этих систем является неудобство прохода через кабину, особенно крупным людям.

I

Рис. 5.11. Шлюз UNIVERSAL 2000

Кроме проблемы контроля прохода «по одному», существуют трудности при установке металлодетекторов (МД) внутри полуавтоматических шлюзов. Существуют 2 основных типа металлодетекторов: динамические и статические.

Динамические МД реагируют только на движущиеся металлические предметы, а статические как на движущиеся, так и на неподвижные. Большинство выпускаемых в мире МД являются динамическими. Динамические МД, обладая хорошей устойчивостью к внешним электромагнитным помехам, обладают высокой чувствительностью к движущимся поблизости большим массам металла. Поэтому при установке динамического МД внутри полуавтоматической кабины с распашными дверьми, имеющими металлическое полотно или металлическую раму, МД будет давать ложные сигналы тревоги при движении двери. Если же МД на время закрывания входной двери заблокировать, то нарушитель с оружием за время закрывания двери пройдет через рамку МД и остановится, а на неподвижный металлический предмет динамический МД реагировать уже не будет.

Статические металлодетекторы позволяют дождаться закрытия входной двери, после чего осуществляют контроль на наличие оружия у человека, находящегося внутри кабины, даже если он стоит неподвижно. Для этого рамка МД делается на всю глубину шлюза. Такое решение применяется в шлюзовых кабинах, производимых некоторыми итальянскими фирмами (CESCU, MUZIO, PROGETECH). Недостатком этого решения является высокая чувствительность статических МД к внешним электромагнитным помехам, что затрудняет использование таких шлюзов на многих объектах. Другим решением, реализованным, например, в полуавтоматических шлюзах «TEDRIA» производства итальянской фирмы SECOD является изготовление входной двери шлюза практически без использования металлических деталей. Рама двери, в которой устанавливается бронестекло, изготавливается из специальных композитных материалов, электромеханический замок устанавливается не в раме двери, а в косяке, дверные ручки изготавливаются из пластика и т. д. Благодаря этим конструктивным решениям в непосредственной близости от входной двери устанавливается постоянно работающий динамический МД. В этом случае МД реагирует на наличие оружия у входящего в шлюз человека и не дает ложных срабатываний при движении двери.

Достоинством полуавтоматических шлюзов является их сравнительно небольшая стоимость, к недостаткам относятся низкая пропускная способность и необходимость прикладывания значительных усилий при открывании дверей, снабженных тяжелыми бронестеклами.

5.3.2. Автоматические тамбур-шлюзы SIRIO

Главной отличительной чертой автоматических тамбуров является то, что двери в них открываются и закрываются с помощью электромеханических приводов. Это существенно упрощает их использование и увеличивает пропускную способность шлюзов.

Шлюзовая логика в автоматических кабинах управляет не замками, а приводами дверей. Автоматический шлюз может иметь одностворчатые или двустворчатые распашные двери; складывающиеся двери; одностворчатые или двустворчатые раздвижные двери с плоскими или полукруглыми створками, цилиндрические двери; одностворчатые и двустворчатые двери с плоскими поворачивающимися створками.

Существуют автоматические шлюзы, имеющие две двери разного типа, а также комбинированные шлюзы, в которых только одна дверь имеет электромеханический привод.

Наиболее простыми с точки зрения инженерных решений являются автоматические шлюзы с распашными дверьми. Они отличаются от полуавтоматических шлюзов тем, что вместо доводчика на дверь устанавливается электромеханический привод. Однако автоматически открывающаяся распашная дверь может задеть стоящего перед ней человека, а применение специальных защитных датчиков позволяет только отчасти решить проблему, так как при

этом значительно снижается реальная пропускная способность шлюза - человек, находящийся в зоне движения двери, препятствует ее открытию и закрытию.

Этот недостаток устранен в автоматических тамбурах с плоскими раздвижными дверьми. В этих кабинах двери, имеющие одну или две створки, с помощью приводов сдвигаются в сторону (рис. 5.12).

Автоматические шлюзы с плоскими раздвижными дверьми имеют большую пропускную способность, чем шлюзы с распашными дверьми, однако их наружные габариты существенно превышают габариты шлюзов других моделей, имеющих ту же ширину прохода. Это объясняется тем, что в шлюзе с плоскими раздвижными дверьми должно быть предусмотрено место сбоку от прохода, в которое заходят створки при их открывании. Для обеспечения наилучшего соотношения «ширина прохода/ширина кабины» применяются двустворчатые двери, в которых обе створки двигаются в одну сторону (рис. 5.13).

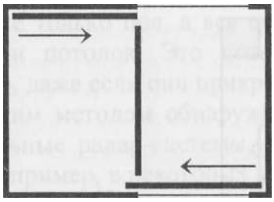


Рис. 5.12. Шлюз с одностворчатыми раздвижными дверьми

Рис. 5.13 Шлюз с двустворчатыми дверьми

Еще лучше это соотношение в кабинах типа TELESCOPICA DOPPIA фирмы SECOD и MULTITRANSITO фирмы SAIMA, представляющих собой объединенные в одну конструкцию два независимо работающих шлюза (рис. 5.14).

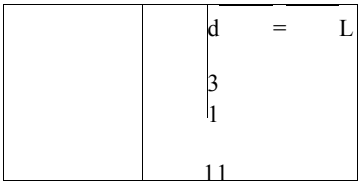


Рис. 5.14. Шлюз TELESCOPICA DOPPIA

Тамбур-шлюзы со складывающимися дверьми (рис. 5.15) и кабины с поворачивающимися створками имеют хорошие показатели пропускной способности и соотношения «ширина прохода/ширина кабины». Однако применение в этих шлюзах металлодетекторов динамического типа затруднено по тем же причинам, что и в полуавтоматических кабинах.

Рис. 5.15. Шлюз со складывающимися дверьми

Отдельные итальянские производители (MUZIO, CESCU, PROGETECH) выпускают шлюзовые кабины с двустворчатыми дверьми с плоскими поворачивающимися створками, в которых применяются металлодетекторы статического типа (рис. 5.16).

Достоинством этих кабин является очень хорошее соотношение «ширина прохода/ ширина кабины», а недостатком - сложность настройки статического металлодетектора при наличии внешних электромагнитных помех.

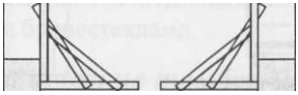


Рис. 5.16. Шлюз с двухстворчатыми дверьми
с плоскими поворачивающимися створками

Наибольшее распространение получили автоматические тамбур-шлюзы с раздвижными полукруглыми дверьми (рис. 5.17). Модели такого типа выпускаются практически всеми европейскими производителями шлюзовых кабин.

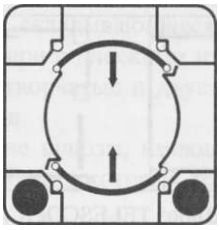


Рис. 5.17. Шлюз с полукруглыми
раздвижными дверьми

Автоматические шлюзы с полукруглыми раздвижными дверьми могут иметь как одностворчатые, так и двустворчатые двери. Большинство моделей итальянских производителей могут комплектоваться встроенным металлоде-

тектором динамического типа, так как все движущиеся металлические детали приводов располагаются выше зоны прохода.

Система контроля прохода «по одному» в автоматических шлюзах этого типа выполняется чаще всего на базе системы взвешивания. Шлюз, в котором система взвешивания контролирует только половину кабины, позволяет пройти через него нарушителю с оружием, несмотря на встроенный динамический металлодетектор. Это объясняется тем, что динамический металлодетектор выдает сигнал тревоги при проходе нарушителя через створ входной двери. В этом случае вторая дверь не открывается, и синтезатор речи выдает сообщение с требованием покинуть кабину. Нарушитель может прикрепить оружие к внутренним стенам или потолку кабины, выйти из шлюза и опять войти в него. При этом второй раз он проходит через металлодетектор уже без оружия, вторая дверь открывается, нарушитель забирает ранее оставленное оружие и входит с ним в охраняемое помещение.

В автоматических шлюзах с полукруглыми дверьми ряда производителей (SECOD, NUOVA VETRO) в некоторых моделях (SAIMA, TONALI) взвешивается не только пол, а вся центральная часть кабины, включая внутренние стенки и потолок. Это позволяет обнаруживать предметы, оставленные в шлюзе, даже если они прикреплены к стенам и потолку.

Другим методом обнаружения оставленного в шлюзе оружия являются специальные радар-системы, применяемые вместе с системой взвешивания пола, например, в некоторых моделях фирмы SAIMA.

Система взвешивания определяет, один или два человека зашли в кабину, сравнивая сигнал с датчика веса с пороговым значением. Величина этого порогового значения устанавливается фирмой-изготовителем или может настраиваться при пусконаладочных работах. В автоматических шлюзах некоторых производителей, например SECOD, информация с датчика веса может также выводиться на последовательный интерфейс внешнего компьютера. В этом случае при наличии в базе данных СКУД информации о весе каждого человека, имеющего право доступа на охраняемый объект, система взвешивания не только обеспечивает абсолютно надежный контроль прохода «по одному», но может использоваться как дополнительная идентифицирующая система, практически исключая несанкционированный проход по чужой магнитной или проксимити-карте.

Логика и алгоритмы работы автоматических тамбуров аналогичны применяемым в полуавтоматических шлюзах. Разница заключается в том, что шлюзовая логика автоматических кабин управляет не замками, а приводами дверей.

Автоматические шлюзы, как правило, комплектуются встроенным источником резервного питания (аккумуляторы с устройством их подзарядки). Кроме того, предусматривается возможность открывания дверей вручную в случае аварийной ситуации.

Автоматические кабины, как правило, комплектуются выносным пультом управления, с помощью которого сотрудники службы безопасности охраняемого объекта могут изменять режимы работы тамбура и управлять им в ручном режиме.

Минимальный набор функций, реализуемых выносным пультом управления:

- включение/выключение шлюза;
- включение автоматического или ручного режима;
- управление дверьми в ручном режиме;
- включение режима экстренной эвакуации (одновременное открытие двух дверей);
- включение/выключение металлодетектора;
- включение/выключение системы прохода «по одному».

Кроме того, на пульт обычно выводится информация о сбоях в основной сети питания и о состоянии аккумуляторов резервного питания.

Автоматические шлюзы интегрируются со СКУД так же, как и полуавтоматические кабины.

К достоинствам автоматических тамбуров относится большая по сравнению с полуавтоматическими шлюзами пропускная способность и удобство их использования.

Недостатком автоматических шлюзов является их более высокая стоимость по сравнению с полуавтоматическими шлюзовыми кабинами.

5.4. Ворота и шлагбаумы

Современные СКУД транспорта оснащаются также дистанционными атрибутными идентификаторами (типа проксимити), средствами досмотра транспорта (специальными зеркалами и техническими эндоскопами), а также на особо важных объектах - антитеррористическим средством для экстренной остановки автомобиля, пытающего протаранить ворота. Последнее средство представляет собой металлическую колонну (блокиратор) диаметром до 50 см, которая устанавливается перед воротами с внешней стороны в бетонированном или металлическом колодце. На дне колодца размещается баллон со сжатым воздухом и пиропатроном, который взрывается по электрическому сигналу с КПП, а сжатый воздух поднимает колонну за доли секунды перед движущимся автомобилем. Подобный блокиратор может остановить 20-тонный автомобиль, движущийся со скоростью 60 км/ч.

Обработку всей информации и управление преграждающими устройствами осуществляют средства вычислительной техники (микропроцессоры и компьютеры).

5.4.1. Автоматические итагбаумы

Автоматические шлагбаумы очень часто используются для оперативного управления потоками автотранспорта, регулирования въезда/выезда на авто-

мобильные парковки, территории предприятий и организаций, торговых центров и др. Автоматический шлагбаум состоит из стойки с силовым механизмом, стрелы и электронного блока управления (рис. 5.18).

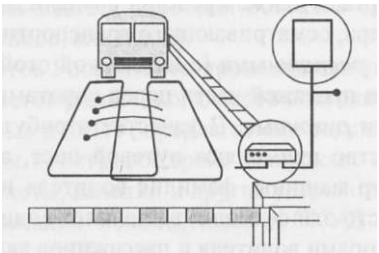


Рис. 5.18. Автоматический шлагбаум

По принципу действия шлагбаумы могут быть электромеханическими и гидравлическими. Длина стрелы шлагбаума может достигать нескольких метров, для перекрытия широких проездов можно использовать два шлагбаума, установленные навстречу друг другу и работающие синхронно.

Важным параметром шлагбаума является время открывания/закрывания. В некоторых моделях предусмотрена установка на стреле элементов световой сигнализации и бордюра безопасности - резинового профиля в нижней части стрелы, чувствительного к соприкосновению с препятствием. Управление шлагбаумом может осуществляться дистанционно от кнопки, подключенного считывателя карточек, кодовой клавиатуры, с помощью миниатюрного радиобрелка.

К блоку управления могут подключаться различные элементы обеспечения безопасности проезда: фотоэлементы, индукционные металлодетекторы для обнаружения автомобиля в заданной зоне проезжей части.

5.4.2. Ворота

Контрольно-проездные пункты для пропуска авто- и железнодорожного транспорта оборудуются:

- раздвижными или распашными воротами и шлагбаумами с механическим, электромеханическим и гидравлическим приводами, а также устройствами для аварийной остановки ворот и открывания их вручную;
- контрольными площадками с помостами для осмотра автомобилей;
- светофорами, предупредительными знаками и световыми табло типа «Берегись автомобиля» и др.;
- телефонной и тревожной связью и освещением для осмотра автотранспорта.

Традиционная (неавтоматическая или с автоматизированным приводом дверей) СКУД транспорта включает ворота или шлагбаумы для пропуска

и задержания транспорта, площадку с помостом для осмотра транспорта, которая часто представляет собой участок проезжей части дороги, светофор, предупредительные знаки, световые табло, оповещающие окружающих о выезде и въезде транспорта, а также средства сигнализации, освещения и тревожной связи контролера, осматривающего транспортное средство.

Ворота могут быть *распашными* (с невысокой стойкостью против тарана и требующими очистки проезжей части перед воротами от снега и льда), *раздвижные, подъемные* и *рулонные.* В качестве атрибутных идентификаторов на транспортное средство применяют путевой лист, в котором указывается государственный номер машины, фамилия водителя и лица, ответственного за перевозку груза (часто эти функции выполняет водитель), вид и количество груза. Идентификаторами водителя и пассажиров являются их пропуска.

Автоматика для ворот предназначена для обеспечения комфортного и безопасного управления воротами как бытового, так и промышленного назначения. Автоматизированы могут как уже существующие на объекте ворота, так и вновь устанавливаемые. Приводы подразделяются по типу ворот: распашные (рис. 5.19), откатные, подъемно-поворотные, секционные.

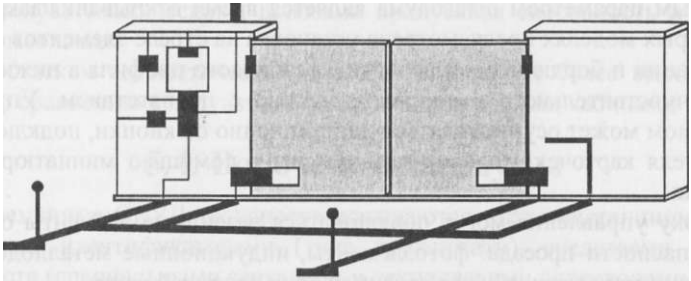


Рис. 5.19. Автоматизированные распашные ворота

Кроме того, при выборе привода необходимо учитывать размер и массу ворот, а также интенсивность нагрузки. Все приводы ворот оснащаются элементами безопасности (фотоэлементы, датчики и т. п.), исключающие возможность повреждения машины, находящейся в створе ворот. Кроме этого, все комплекты автоматизации ворот снабжаются удобными устройствами дистанционного управления воротами на основе инфракрасных или радиопередающих брелков-ключей.

5.5. Исполнительные устройства СКУД российского производства

В России имеется большое число компаний, производящих исполнительные устройства (УПУ) СКУД: калитки, турникеты, ворота, шлюзовые камеры и др. Среди наиболее известных можно отметить: «К-инженерант» (Санкт-

Петербург); «ОМАО» (Санкт-Петербург); «PERCo» (Санкт-Петербург); «РостЕвроСтрой» (Ростов-на-Дону) и др.

В последнее время чаще всего заказывают УПУ для решения конкретных узкоспециализированных задач и УПУ для объектов с повышенным трафиком носителей (сотрудников, клиентов).

Хотя рынок турникетов Российского производства еще уступает зарубежному, но выпуск турникетов различных классов постоянно растет.

Рассмотрим некоторые из УПУ, предлагаемых российскими компаниями.

Российская компания «РостЕвроСтрой» выпускает механические и электромеханические турникеты, калитки и другие устройства СКУД.

Турникеты этой компании используются в СКУД для объектов особой важности Минатепа, ФПС, ФСБ и др.

Наиболее распространенным турникетом является УПУ «Ростов-Дон Т-83L» (рис. 5.20).

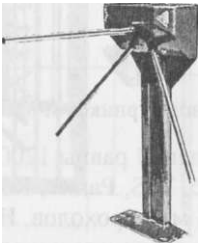


Рис. 5.20. «Ростов-Дон Т-83L»

В этом турникете пространство между боковыми стойками полое и закрывается съемной плитой, что позволяет использовать его для размещения дополнительных элементов и оборудования.

Турникет может работать в трех режимах:

1. «Закрыто» - турникет заблокирован.

2. «Открыто для прохода по одному» - после нажатия кнопки на ПУ турникет разблокируется и после прохода человека вновь блокируется.

3. «Открыто для прохода группы людей» - после прохода человека турникет не блокируется.

Все 3 режима независимо друг от друга работают как на вход, так и на выход.

Турникет «Ростов-Дон Т83» стыкуется с СКУД: Forsec, TSS, Parsec, Кодос, ШЭЛТ, Орион и др. Он обеспечивает пропускную способность до 30 человек в 1 мин в режиме однократного прохода.

Для стопора механизма используется электромеханический замок. Имеется также световая индикация. Питающее напряжение 12 В, потребляемый ток - 1,5 А. Режим эксплуатации: Т = от 0 до +50 °С. Наработка на отказ - 2 млн проходов.

Двойной турникет «Ростов-Дон Т283» является победителем национальной премии по безопасности «ЗУБР» в 2005 г. (рис. 5.21). Он представляет собой два абсолютно независимых полнофункциональных турникета, размещенных в одном корпусе. Все характеристики такие же, как и у турникета Т83, но пропускная способность составляет до 60 человек в 1 мин.

Полуростовые роторные электромеханические турникеты с гидромеханическими доводчиками «Ростов-Дон Р2М2/3» и «Ростов-Дон Р2М1/3» показаны на рис. 5.22 и 5.23.

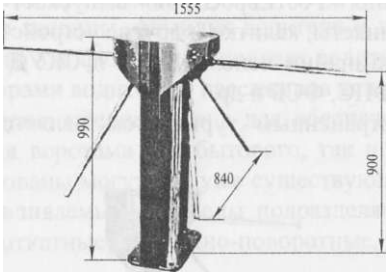


Рис. 5.21. Двойной турникет «Ростов-Дон Т283»

Габаритные размеры ограждений равны 1200 х 1260 х 1095 мм. Ограждения стыкуются со СКУД Forsec, TSS, Parsec, Кодос, ШЭЛТ, Орион и др. Наработка на отказ составляет 2,5 млн проходов Напряжение питания 12 В, потребляемый ток - 1,5 А. Режим эксплуатации от 0 до +50 °С при условии защиты от прямого воздействия атмосферных осадков.

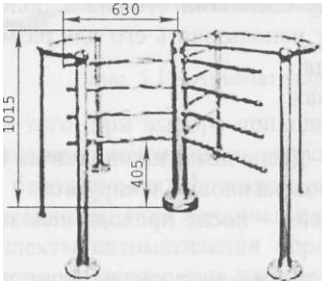


Рис. 5.22. «Ростов-Дон Р2М2/3»

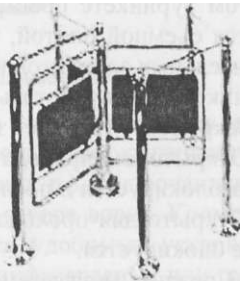


Рис. 5.23. «Ростов-Дон Р2М1/3»

Полноростовые роторные электромеханические турникеты с гидромеханическим доводчиком «Ростов-Дон ПР1/3» и «Ростов-Дон ПР1Л/3» обеспечивают надежный контроль доступа и полностью исключают возможность несанкционированного прохода через них (рис. 5.24 и 5.25).

Эти турникеты следует применять для организации прохода на объекты повышенной режимности, а также на объектах с большим количеством лю-

дей (спортивные сооружения, гаражи, платные пляжи, зрелищные учреждения и др.).

Турникеты имеют следующие размеры: высота - 2350 мм, ширина - 1500 мм. Турникеты стыкуются со СКУД, указанными выше для других турникетов. Режимы эксплуатации такие же, как и у других турникетов серии «Ростов-Дон». Напряжение питания 12 В, потребляемый ток - 3 А. Наработка на отказ составляет 3 млн проходов.

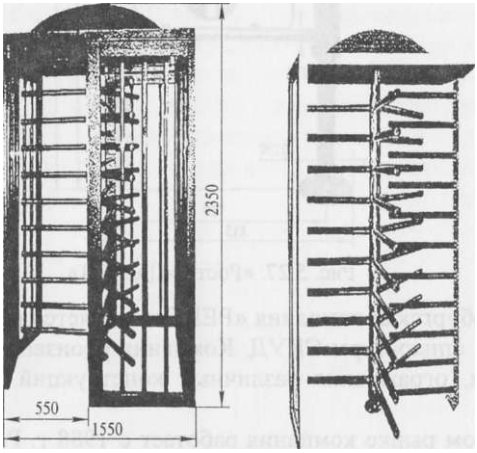


Рис. 5.24. «Ростов-Дон ПР1/3» Рис. 5.25. «Ростов-Дон ПР1Л/3»

Для экстренного выхода или для проноса крупногабаритных грузов предприятие выпускает ограждения стационарные открываемые антипаника «Ростов-Дон ОС2ар ХРОМ» и «Ростов-Дон ОС2апр ХРОМ» (рис. 5.26).

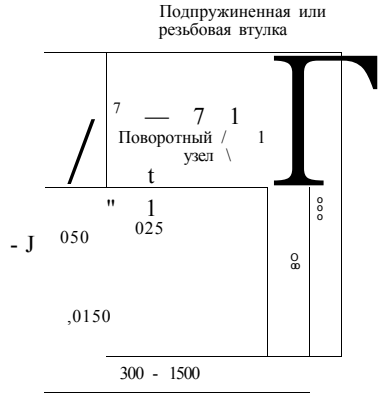


Рис. 5.26. «Ростов-Дон ОС2апр ХРОМ»

Кроме турникетов, предприятие выпускает калитки различных типов: «Ростов-Дон К32Д», «Ростов-Дон К32Д-Н», «Ростов-Дон К21» (рис. 5.27), «Ростов-Дон К11К».

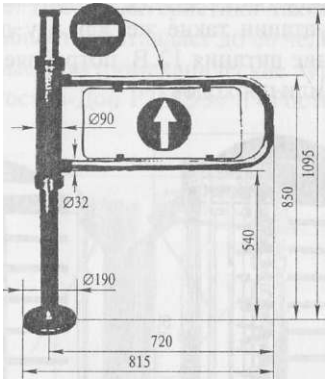


Рис. 5.27. «Ростов-Дон К21»

Санкт-Петербургская компания «PERCo» является одним из крупнейших производителей аппаратуры СКУД Компания производит электромеханические турникеты, ограждения различных конструкций и др. оборудование СКУД.

На российском рынке компания работает с 1988 г. Разрабатываемое оборудование кроме России поставляется еще в 48 стран мира.

Среди продукции компании отметим такие образцы:

Турникет RTD12 - полнопрофильный турникет высотой 2300 мм.

Турникет RTD03 - предназначен для управления потоками людей, когда необходим строгий контроль проходов (военные, специализированные и другие объекты).

Серия турникетов-триподов TTR04. Модели отличаются цветом покрытия, возможностью подключения к СКУД, наличием встроенного аккумулятора.

Тумбовые турникеты серии TTD03.

Группа компаний ООО «Аксэс Групп» реализует различные модели электромеханических турникетов-триподов, среди которых можно отметить турникет-трипод Т-02 и тумбовый турникет-трипод ТВ-01. Эти турникеты предназначены для ограничения доступа на проходных промышленных предприятий, в банках, бизнес-центрах, учебных заведениях и др.

Корпус турникетов выполнен из полированной нержавеющей стали. Турникеты позволяют подключаться к любым системам СКУД. В турникеты встроена сирена, управляемая СКУД.

Следует отметить также турникеты с торговой маркой ОМА (Оригинальная Механика и Автоматика). Эта серия турникетов выпускается как в на-

стенном (ОМА-26.461), так и напольном (ОМА-26.461/1 и ОМА-26.461/Ю) вариантах. Кроме того, предлагаются турникеты-триподы: скоростной усиленный ОМА-26.56, скоростной усиленный «ТВИКСЕР» ОМА-66.56, скоростной усиленный «Чупсер» ОМА-56.56.

Варианты исполнения предполагают использование корпусов турникетов из нержавеющей стали с любой окраской.

6. ВАРИАНТЫ РЕАЛИЗАЦИИ СКУД

6Л. Автономные и сетевые системы контроля и управления доступом

6.1.1. Автономные СКУД

1. СКУД **«Проход**-А» (рис 6.1) и СКУД **«Проход**-МА» (рис. 6.2). Обе системы являются автономными. Первая предназначена для контроля доступа на одну точку прохода (в данном случае дверь), вторая - на несколько точек прохода и состоит из отдельных автономных систем. В каждой автономной системе управление доступом осуществляется автономно работающим контроллером и служит для контроля входов людей в помещение (офис, комнату, кабинет, склад, зону и т. д.).

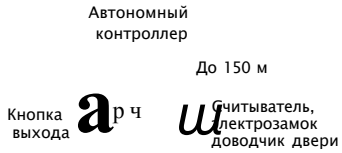


Рис. 6.1. Структурная схема СКУД «Проход-А»

Каждый сотрудник или посетитель предприятия получает идентификатор (электронный ключ) - пластиковую карточку или брелок с содержащимся в ней индивидуальным кодом. Загрузка кодов электронных ключей в контроллер и задание времени разблокировки пункта прохода осуществляется с помощью мастер-идентификатора (мастер-карты). Пользователь имеет возможность самостоятельно определить любую из используемых карт в качестве мастер-карты путем манипуляций с микропереключателем на плате контроллера. Удаление кодов электронных ключей, используемых для прохода, осуществляется с помощью повторной записи или перезаписи мастер-карты.

Рис. 6.2. Структурная схема СКУД «Проход-МА»

У входа в помещение устанавливается считыватель, который считывает с карточек их код и передает эту информацию в контроллер системы. Индикация считывания кода, разблокировки двери, отказа в доступе (например, при предъявлении «неизвестной карты»), а также текущего режима при программировании и загрузке кодов карт осуществляется с помощью управляемого светодиода или биппера (звукового индикатора) считывателя, подключенного к контроллеру.

В системе каждому коду поставлена в соответствие информация о разрешении доступа владельца карточки в помещение. На основе сопоставления этой информации контроллер открывает или блокирует проход через дверь, т. е. управляет исполнительным устройством (электрозамком или электрозащелкой), подключенным к контроллеру. Кроме считывателя и исполнительного устройства к контроллеру подключается кнопка выхода, после нажатия на которую можно выйти из помещения, а на дверь устанавливается доводчик.

Преимущества первой системы: энергонезависимая память, проксимити- и Виганда-считыватели, наличие индикатора падения напряжения, диапазон рабочих температур - (0...40) °С, питание - 12,6 В.

Типовой состав оборудования системы с одним пунктом прохода через дверь в варианте с проксимити-считывателями - контроллер TSS-201W/p, карточки HID, считыватель на вход ProxPoint, в варианте с «тач-мемори»-считывателями - контроллер TSS-201AT/p, считыватель на вход TM-05, ключ-брелок Dallas. Для обоих вариантов дополнительное оборудование включает кнопку выхода RTE, доводчик двери TS77, электрозамок CISA 15004.

Во второй системе, если сотруднику разрешен доступ в несколько помещений, то код его электронного ключа заносится в соответствующие контроллеры этих помещений. Таким образом, сотрудник пользуется только одним «ключом» для доступа в нужную ему комнату. Для системы на основе контроллера TSS-201W характерно: энергонезависимая память, наличие индикатора падения напряжения, использование проксимити-, Виганда-считывателей. Возможен вариант системы с «тач-мемори»-считывателями.

2. СКУД **«Проходная-1»** - система контроля и управления доступом с одной точкой прохода через турникет, выполненная на базе программного комплекса TSS-2000Profi. Система «Проходная-1» предназначена для решения задачи автоматизированного контроля и управления проходом на территорию предприятия и выходом с нее персонала и посетителей через одну точку прохода - турникет. Число контролируемых пунктов прохода может быть легко увеличено включением в систему дополнительных контроллеров и оборудования точек прохода. Система также позволяет организовать учет рабочего времени сотрудников и может быть использована на небольших предприятиях и организациях. Структурная схема СКУД «Проходная-1» приведена на рис. 6.3.

Каждый сотрудник или посетитель предприятия получает идентификатор (электронный ключ) - пластиковую карточку или брелок с содержащимся в ней индивидуальным кодом. Электронные ключи выдаются в результате регистрации перечисленных лиц с помощью средств системы. Паспортные данные, фото (видеоизображение) и другие сведения о владельце электронного ключа заносятся в персональную электронную карточку. Персональная электронная карточка владельца и код его электронного ключа объединяются и заносятся в специально организованные компьютерные базы данных.

Рис. 6.3. Структурная схема СКУД «Проходная-1»

У входа на предприятие на панели турникета или рядом с ним устанавливаются считыватели, которые считывают с карточек их код и передающие эту информацию в контроллер системы. Работник организации или посетитель, имеющий электронный ключ, подходит к турникету и предъявляет его считывателю.

Одновременно с этим на экране компьютера, установленного на проходной, появляется изображение и основная информация о владельце «ключа», занесенная в базу данных системы. В системе каждому коду поставлена в соответствие информация о правах доступа владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует проход через турникет.

Если в данное время для владельца предъявленного электронного ключа разрешен проход через данный турникет, система автоматически разблокирует его. Если же действует запрет на проход или предъявлен не зарегистрированный «ключ», то турникет останется в заблокированном состоянии, а на экране компьютера поста охраны появится надпись о запрете с указанием причины отказа в доступе. Одновременно с этим компьютер воспроизводит соответствующее речевое сообщение. Например: «Вход заблокирован. Истек срок действия ключа!» или «Запрет по времени!», «Внимание! Предъявлен неизвестный ключ!» и т. п.

Сотрудник службы безопасности, который дежурит на проходной, в любой момент времени может вмешаться в работу системы - сравнить фотографию на экране и входящего человека, а затем заблокировать или разблокиро-

вать турникет, нажав кнопку клавиатуры компьютера или выносного пульта управления турникетом.

Все факты предъявления «ключей» и связанные с ними действия (проходы, факты срабатывания датчика и нажатия кнопки турникета и т. д.) фиксируются в контроллере, автоматически заносятся в журнал событий («системный журнал»), связанных с проходом через турникет проходной и сохраняются в компьютере. Причем для каждого события указывается: его характер, дата, время, код предъявляемого «ключа» и Ф. И. О. его владельца или дежурного оператора, нажавшего кнопку.

Подобным же образом регулируется и выход с предприятия. Причем в том случае, если выходящий человек является посетителем организации, получившим разовый пропуск (ключ), система напомнит дежурному на проходной о необходимости изъятия у него временно выданного ключа звуковым или речевым сообщением типа: «Внимание, гость! Просьба забрать ключ».

Информация о событиях, вызванных предъявлением карточек, может быть использована в дальнейшем для получения отчетов по учету рабочего времени, нарушениям трудовой дисциплины и др. Момент первого входа через проходную, интерпретируется системой в процессе учета рабочего времени как начало, а момент последнего выхода - как конец рабочего дня владельца предъявленного электронного ключа.

Если в течение рабочего дня какому-либо сотруднику необходимо неоднократно входить и выходить через проходную, то при формировании отчетов о рабочем времени, система суммирует отдельные промежутки времени пребывания его на территории организации.

В системе «Проходная» применен контроллер TSS-Office, который предназначен для обработки информации от считывателей карточек («ключей»), принятия решения и управления исполнительным устройством (турникетом) в режиме реального времени.

Контроллер обеспечивает контроль прохода сотрудников и посетителей через турникет, формирует базу событий, хранит коды ключей (карточек), поддерживает связь с компьютером через интерфейсный модуль BIT - 4,3. В эту серию контроллеров входят двухпортовые контроллеры 2 типов - T и W, предназначенные, соответственно, для подключения двух считывателей «тач-мемори»-идентификаторов или двух считывателей с интерфейсом Виганда (26-48 бит).

Наличие встроенного календаря-часов и энергонезависимой памяти, в которой могут храниться коды идентификаторов, назначенные для них ограничения доступа, а также значительное число сообщений о событиях, позволяют контроллеру системы функционировать без подключения к компьютеру длительное время. В памяти контроллера сохраняется 504 кода, 7444 сообщения, 16 временных зон, 256 расписаний доступа по определенным датам.

Элементы оборудования пункта прохода через проходную включают: считыватели на вход и на выход (считывают код карточки-ключа пользователя и обеспечивают его ввод в контроллер при проходе через турникет), турникет, пульт (кнопка) управления турникетом.

Компьютер проходной является компьютером мониторинга системы и непосредственно компьютером проходной. Компьютер выводит данные из базы (электронная форма пропуска) непосредственно охраннику на пункт прохода при прохождении через турникет владельца пропуска. В составе системы используются обычные IBM-совместимые компьютеры со следующими параметрами: процессор типа Pentium, Celeron, оперативная память объемом не менее 64 Мбайт, SVGA-монитор и видеокарта, подцерживающиме разрешение не менее 800 х 600 точек и глубину цвета 24 бит (16,7 млн цветов).

Система может функционировать в автономном режиме работы через 3 с после отключении связи между контроллером и компьютером в результате повреждения линии связи, отключения сети питания в здании, при выходе из строя компьютера. В этом случае работает только режим контроля прохода через турникет, а режимы показа фотографий не работают.

3. СКУД «Нроходная-М» - система контроля и управления доступом с одной точкой прохода через турникет и организацией контроля доступа для четырех точек прохода внутри предприятия. Система выполнена на базе программного комплекса TSS-2000Profi и предназначена для решения задачи автоматизированного контроля и управления входом/выходом на территорию предприятия персонала и посетителей через проходную, а также для контроля доступа во внутренние помещения предприятия (в данном случае - четыре комнаты). Система также позволяет организовать учет рабочего времени сотрудников, получать разнообразные отчеты о событиях в системе. Структурная схема СКУД «Проходная-М» приведена на рис. 6.4.

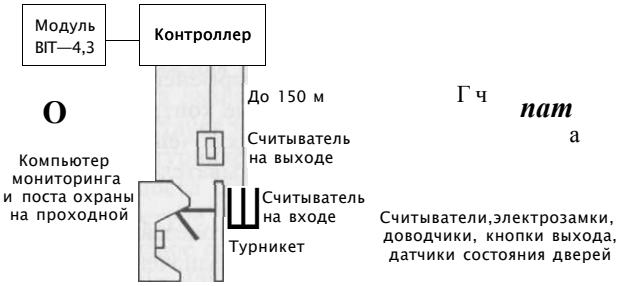


Рис. 6.4. Структурная схема СКУД «Проходная-М»

Сотрудники или посетители предприятия получают идентификатор (электронный ключ) - пластиковую карточку или брелок с содержащимся в ней индивидуальным кодом. Электронные ключи выдаются в результате регист-

рации перечисленных лиц с помощью средств системы. Паспортные данные и другие сведения о доступе владельца электронного ключа заносятся в персональную электронную карточку. Персональная электронная карточка владельца и код его электронного ключа объединяются и заносятся в специально организованные компьютерные базы данных. Имеется возможность поиска, сортировки и отбора в базе данных электронных карточек зарегистрированных владельцев ключей по самым различным критериям. Затем происходит загрузка кодов электронных ключей в контроллер и программирование контроллера с помощью программного обеспечения. Система позволяет:

- просто и наглядно загружать и выборочно удалять из памяти контроллера коды электронных ключей, предназначенных для прохода;
- задавать объектовые и временные ограничения доступа как для отдельных владельцев ключей, так и для групп владельцев, выделенных по какому-либо признаку;
- для каждого из зарегистрированных в системе ключей определить срок его действия;
- при установке ограничений доступа для владельца ключа можно задать номера зон доступа, представляющих собой списки дверей, через которые данный владелец может входить и выходить из помещений и здания.

СКУД «Г1роходная-М» функционирует аналогично СКУД «Проходная-1», описанной выше.

В системе также осуществляется контроль доступа во внутренние помещения предприятия (в рассматриваемой системе - 4 комнаты). Причем в особо важных помещениях (например, бухгалтерия, склад или др.) считыватели устанавливаются на входе и выходе, а в других комнатах - только на входе. Выход из этих помещений осуществляется при нажатии на кнопку выхода. На основе сопоставления информации о правах доступа и ситуации, при которой был предъявлен «ключ», система принимает решение: контроллер открывает или блокирует проход через двери, переводит помещение в режим охраны, включает сигнал тревоги и т. д.

Программное обеспечение системы позволяет вести учет рабочего времени сотрудников и посетителей, которым выданы «ключи», получать разнообразные *отчеты о событиях* в системе за выбранные промежутки времени. Например, все события (информация о всех или произвольно выбранных событиях), нарушения (информация о нарушениях рабочего графика), проходы (информация о проходах в помещения всех или выбранных лиц, рабочее время (учет рабочего времени всех или выбранных лиц).

Если в течение рабочего дня какому-либо сотруднику необходимо неоднократно входить и выходить через проходную, то при формировании отчетов о рабочем времени система суммирует отдельные промежутки времени пребывания его на территории организации. Важной особенностью системы

является то, что любой владелец ключа, проникший в здание, минуя проходную (код его ключа не был считан считывателем на входе проходной), не сможет войти ни в одну из контролируемых системой дверей.

При необходимости проводить визуальный мониторинг объектов можно также и в режиме отображения *поэтажных планов,* на которых наглядно отображается ситуация в здании. Контролируемые пункты прохода в помещения обозначаются на планах пиктограммами или значками, вид или цвет которых может меняться в зависимости от состояния соответствующего объекта. (Например, в случае блокировки оператором какой-либо двери, ее пиктограмма на поэтажном плане приобретает желтую подсветку, а при взломе двери периодически вспыхивает красным цветом.) В момент возникновения нештатного события на экране компьютера автоматически или по команде пользователя разворачивается план нужного этажа, на котором указывается место или объект, с которым связано тревожное событие. Это позволяет даже наиболее слабо подготовленному оператору быстро оценить ситуацию, подтвердить получение сигнала тревоги и принять правильное решение.

Система может круглосуточно функционировать в двух основных режимах: в комплексном, когда работой системы управляет компьютер мониторинга, и в автономном режиме работы контроллера.

В *автономный режим* система переходит:

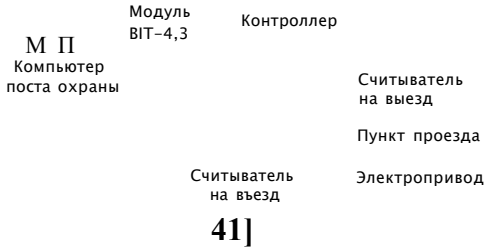
- по команде администратора системы (например, в случае необходимости замены или подключения какого-либо элемента, перед проведением профилактики и т. д.);
- автоматически через 3 с после отклячения связи между контроллером и компьютером в результате повреждения линии связи, отключения сети питания в здании, при выходе из строя компьютера.

В этом режиме контроллер управляет проходом через проходную и доступом в помещения владельцев тех электронных ключей, коды которых были занесены в память контроллера, а также фиксирует в памяти информацию о событиях, связанных с проходами через эти точки прохода. После запуска программного обеспечения и перехода системы в сетевой режим эта информация автоматически переписывается в «системный журнал» компьютера. Продолжительность автономной работы системы в случае отсутствия электропитания в сети может достигать 8 ч. Доступ к базе электронных карточек, содержащих информацию о зарегистрированных владельцах ключей, открыт только для уполномоченных сотрудников после ввода личного кода.

Контроллеры серии TSS-201-8W, TSS-201-8T имеют восемь портов, к каждому из которых можно подключить оборудование одной точки прохода. Каждый из портов контроллера имеет канал для подключения считывателя, датчика состояния пункта прохода (двери), кнопки открывания двери и релейный выход для управления исполнительным устройством.

Контроллер имеет энергонезависимую память, встроенный календарь-часы. Интерфейс подключаемых считывателей: T - для считывателей идентификаторов типа «тач-мемори», W - для считывателей с интерфейсом Виганда (26-48 бит).

4. СКУД «Проезд» - система контроля и управления въездом/выездом автотранспорта, выполненная на базе программного комплекса TSS-2000Profi. Исполнительные устройства: шлагбаум или управляемые ворота. Идентификаторы: магнитные и проксимти-карты, ключи «тач-мемори» или автомобильные: проксимити-метки (автотаги). Система может быть использована на предприятиях, автобазах, складских, товарных, продуктовых и др. базах для учета парка собственного автотранспорта, для автоматического учета времени въезда/выезда собственного транспорта, а также транспорта поставщиков и потребителей. Структурная схема СКУД «Проезд» приведена на рис. 6.5.



41]

Рис. 6.5. Структурная схема СКУД «Проезд»

Сотрудник или посетитель предприятия, въезжающий на объект получает идентификатор (электронный ключ) - пластиковую карточку с содержащимся в ней индивидуальным кодом. Паспортные данные, сведения об автотранспорте и другие сведения о владельце электронного ключа заносятся в персональную электронную карточку. Персональная электронная карточка владельца и код его электронного ключа объединяются и заносятся в специально организованные компьютерные базы данных.

У въезда на территорию устанавливаются считыватели, которые считывают с карточек их код и передают эту информацию в контроллер системы. Самый надежный и эффективный вариант - использование проксимити-карт, позволяющих проводить идентификацию на расстоянии. При въезде на территорию водителю не нужно выходить из машины или даже подъезжать вплотную к считывателю. Достаточно держать проксимити-карту сбоку у окна автомобиля на сравнительно большом расстоянии.

Среди предлагаемых систем есть системы, которые позволяют идентифицировать не только водителя, но и сам автомобиль. Например, разработаны специальные проксимти-метки (автотаги), которые крепятся на днище машины. Для считывания таких меток применяются считыватели с большой даль-

ностью действия. Например, считыватель Maxi Prox фирмы HID может прочитать на расстоянии до 2 м. Автомашина подъезжает к воротам или шлагбауму, останавливается перед соответствующей разметкой на асфальте, и метка автоматически считывается.

В системе каждому коду поставлена в соответствие информация о правах въезда на территорию владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует шлагбаум или автоматические ворота, включает сигнал тревоги и т. д.

Все факты предъявления карточек и связанные с ними действия (въезды, выезды, тревоги и т. д.) фиксируются в контроллере, автоматически заносятся в журнал событий, связанных с проездом через ворота или шлагбаум и сохраняются в компьютере.

Система может круглосуточно функционировать в двух основных режимах: в комплексном, при котором работой системы управляет компьютер мониторинга, и в автономном режиме работы контроллера. В ***автономный режим*** система переходит:

- по команде администратора системы (например, в случае необходимости замены или подключения какого-либо элемента, перед проведением профилактики и т. д.);
- автоматически через 3 с после отключения связи между контроллером и компьютером, между компьютерами удаленных объектов в результате повреждения линии связи, отключения сети питания в здании, при выходе из строя компьютера.

В этом режиме контроллер управляет проездом через ворота или шлагбаум владельцев тех электронных ключей, коды которых были занесены в память контроллера, а также фиксирует в памяти информацию о событиях, связанных с проездом через эти точки. После запуска программного обеспечения и перехода системы в сетевой режим эта информация автоматически переписывается в «системный журнал» компьютера.

Информация о событиях, вызванных предъявлением карточек, может быть использована в дальнейшем для получения различных отчетов по учету рабочего времени, нарушениям трудовой дисциплины и др.

В эту серию контроллеров входят двухпортовые контроллеры для подключения двух считывателей идентификаторов.

В памяти контроллера сохраняются 504 кода идентификаторов пользователей, 7444 сообщения о событиях, а также сведения о расписании доступа по определенным датам (16 временных зон, 256 праздников).

Наличие встроенного календаря-часов и энергонезависимой памяти, в которой могут храниться коды идентификаторов, назначенные для них ограничения доступа, а также значительное число сообщений о событиях, позволя-

ют контроллерам системы функционировать без подключения к компьютеру длительное время.

Для организации нескольких контролируемых пунктов проезда на территорию можно расширить систему, т. е. добавить в нее оборудование, аналогичное описанному (контроллер и элементы оборудования пункта проезда), в соответствии с необходимым числом контролируемых пунктов. Компьютер в данном случае - один на всю систему в целом.

5. **СКУД серии «PERCo-MS-400».** Обобщенная функциональная схема системы СКУД серии «PERCo-MS-400» приведена на рис. 6.6.

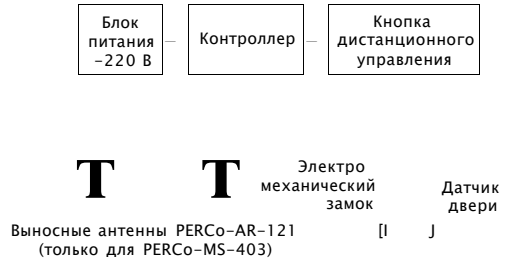


Рис. 6.6. Структурная схема СКУД серии «PERCo-MS-400»

Системы серии PERCo-MS-400 с открыванием замка по предъявлению бесконтактных карт доступа эффективны при установке на входные двери, на двери кабинетов и служебных (подсобных) помещений офисов, банков, складов, магазинов.

При установке системы на входные двери дополнительно могут быть подключены переговорные (аудио-) видеоустройства.

Системы серии PERCo-MS-400 могут использоваться в сочетании с более сложными системами контроля и управления доступом. При этом одни и те же карточки могут служить пропусками на все разрешенные к доступу объекты. Максимальное число пользователей для систем PERCo-MS-400 составляет примерно 500 человек. В настоящее время серия PERCo-MS-400 имеет несколько моделей. Для предприятия с большей численностью сотрудников целесообразно рассмотреть использование систем PERCo-S-600 или PERCo-SYSTEM-12000.

Система контроля доступа PERCo-MS-401 предназначена для работы с бесконтактными карточками фирмы Motorola. Имеет простую (для монтажа) компактную моноблочную конструкцию. Состоит из контроллера PERCo-СМ-401 со встроенным считывателем и блока питания. Дальность считывания карт составляет примерно 10 см. Система рассчитана на работу при температуре от -10 до +45 °С и влажности до 95 % при 25 °С.

Система контроля доступа PERCo-MS-402 предназначена для работы с бесконтактными карточками фирмы НЮ. Состоит из компактного контрол-

лера PERCo-CM-402 со встроенным считывателем и блока питания. Дальность считывания карт - до 10 см. Контроллер выпускается в варианте для наружного (уличного) применения и может работать при температуре от -25 до +50 °С и влажности до 95 % при 25 °С.

Система контроля доступа PERCo-MS-403 предназначена для работы с бесконтактными карточками HID. Состоит из компактного контроллера PERCo-RE-121, малогабаритной выносной антенны PERCo-AR-121 и блока питания. Контроллер устанавливается внутри охраняемого помещения. К одному контроллеру можно подключить одну или две выносных антенны. Антенна размещается в пластиковом корпусе, залитом компаундом, защищающим ее как от механических повреждений, так и от воздействий внешней среды. Она обеспечивает дальность считывания карт до 10 см. Система рассчитана на работу при температуре от -40 до +50 °С и влажности до 100 %. PERCo-MS-403 отличается от других систем серии повышенной вандалозащищенностыо и возможностью эксплуатации в неблагоприятных климатических условиях.

Система контроля доступа PERCo-MS-404 предназначена для работы с бесконтактными карточками HID. Состоит из компактного контроллера PERCo-CM-404, малогабаритной выносной антенны PERCo-AR-301 (позволяет не доставать карту из бумажника или сумки, чтобы открыть замок) и блока питания. Она обеспечивает дальность считывания карт до 30 см. Система рассчитана на работу при температуре от -25 до +50 °С и влажности до 98 %.

Система /шаткого доступа PERCo-S-700 предназначена для управления доступом и автоматизации расчетов. Внешний вид системы показан на рис. 6.7. В качестве билетов в системе используются бесконтактные смарт-карты или карты с магнитной полосой. Сфера применения системы: горнолыжные курорты, выставочные центры, аттракционы, спортивно-оздоровительные комплексы, аквапарки, пляжи, плавательные бассейны т. п.

Для системы PERCo-S-700 характерна *автономная работа* всех компонентов без объединения в сеть. Работа системы PERCo-S-700 основана на использовании пластиковых карт в качестве «электронных кошельков», в которые заносится вся необходимая информация о типе карты и произведенном платеже. Поскольку вся информация находится на самой карте, то отпадает необходимость передачи данных об оплаченных картах в контроллеры, управляющие турникетами в пунктах прохода. В качестве билетов в системе используются бесконтактные смарт-карты или контактные карты с магнитной полосой. Система обеспечивает решение следующих задач:

- организацию доступа владельца карты к месту предоставления оплаченных услуг;
- кодирование карт доступа (условия доступа, вид и объем предоплаченных услуг);
- регистрация действий оператора при выдаче карт доступа;

- регистрация всех событий при пользовании оплаченными услугами владельца карты;
- информирование владельца карты о текущем статусе карты;
- формирование отчетов: интенсивность пользования услугами, загрузка кассиров, число проданных билетов за определенный промежуток времени и т. п.

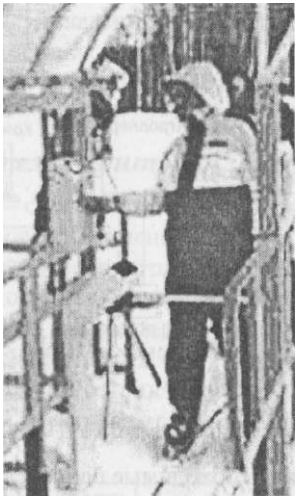


Рис. 6.7. Вид системы платного доступа PERCo-S-700

Программное обеспечение PERCo-S-700 предназначено для описания параметров функционирования системы, а также сбора и обработки информации, поступающей от них. ПО системы имеет удобный и понятный пользователям интерфейс и не требует специального обучения.

6. **Система ограничении доступа к банкомату PERCo-S-800** предназначена для обеспечения безопасности клиентов при совершении операций и предотвращения вандализма. Структурная схема СКУД «PERCo-S-800» приведена на рис. 6.8.

Система решает следующие задачи:

- организация доступа к банкомату владельцев пластиковой карты платежной системы из числа обслуживаемых данным банкоматом,
- ограничение доступа к банкомату лиц, у которых отсутствует пластиковая карта и лиц, имеющих карту с истекшим сроком действия;
- слежение за датчиком присутствия человека в зоне самообслуживания и датчиком охранной сигнализации;
- световая индикация присутствия человека в помещении;
- реакция на тревожную ситуацию - оповещение о тревоге на пульт охраны или оповещатель, включение видеозаписи.

Система управляет замком, установленным на дверь, закрывающую доступ к банкомату. Для того чтобы попасть в помещение, где расположен банкомат, клиент предъявляет считывателю любую банковскую карту, обслуживаемую данным банкоматом.

Рис. 6.8. Структурная схема СКУД «PERCo-S-800»

Пока клиент не завершит необходимые банковские операции и не покинет помещение, нажав кнопку «Выход», система не впустит в помещение других лиц. Этим обеспечивается безопасность клиента во время нахождения в зоне самообслуживания банкомата. Охрана помещения обеспечивается с помощью датчиков объема и охраны. Если было разбито стекло на двери или превышено допустимое время нахождения у банкомата, система подает сигнал тревоги и включает видеозапись. Объемный датчик позволяет отслеживать такие ситуации, когда человек предъявил карту, открыл дверь, но передумал входить и захлопнул дверь. В этом случае блокировка замка будет снята и доступ к банкомату следующего посетителя не будет запрещен.

Система распознает магнитные пластиковые карты 10 любых платежных систем.

В ее состав входят: контроллер управления доступом, контроллер конфигурации системы, считыватель магнитных карт, мастер-карта, электромеханический замок, датчик двери и датчики объема. Дополнительно в состав системы может входить информационное табло «Занято/Свободно» и устройство видеозаписи (видеомагнитофон с подключенной к нему видеокамерой). Контроллер управления доступом обеспечивает доступ клиента в зону самообслуживания банкомата, слежение за датчиками охраны и присутствия человека около банкомата, управление замком, информационным табло, сигнализатором тревоги и устройством включения видеомагнитофона. Один

контроллер конфигурации (и одно программное обеспечение) может обслуживать любое число банкоматов. Вместо контроллера конфигурации может использоваться переносной компьютер.

Программное обеспечение системы PERCo-S-800 предназначено для настройки параметров конфигурации системы, например, списка карт, обслуживаемых данным банкоматом, предельного времени нахождения клиента в зоне самообслуживания банкомата, необходимости контроля срока действия карты. Оно работает под управлением MS Windows 98/NT/2000 и имеет удобный современный интерфейс.

Доступ к управлению системой PERCo-S-800 защищается системой паролей.

6.1.2. Сетевые системы контроля и управления доступом

1. СКУД **«Проход**-С» - система контроля доступа на одну точку прохода с организацией учета рабочего времени Является сетевой (компьютерной) системой, выполненной на базе программного комплекса TSS-Office. Это программно-аппаратный комплекс, управляемый компьютером мониторинга. Система предназначена для контроля входа/выхода людей в помещение (офис, комнату, кабинет, склад, зону и т. д.). Система также позволяет организовать учет рабочего времени сотрудников, получать разнообразные отчеты о событиях в системе. Структурная схема СКУД «Проход-С» показана на рис. 6.9.

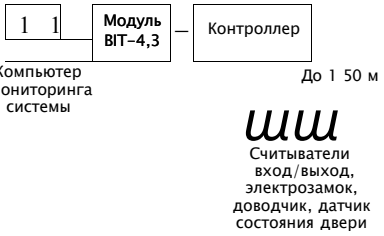


Рис. 6.9. Структурная схема СКУД «Проход-С»

При проходе сотрудник или посетитель предприятия получает идентификатор (электронный ключ) - пластиковую карточку или брелок с содержащимся в них индивидуальным кодом. Электронные ключи выдаются в результате регистрации перечисленных лиц с помощью средств системы. Паспортные данные и другие сведения о доступе владельца электронного ключа заносятся в персональную электронную карточку. Персональная электронная карточка владельца и код его электронного ключа объединяются и заносятся в специально организованные компьютерные базы данных. При загрузке кодов электронных ключей в контроллер задаются временные ограничения доступа для каждого ключа. На входе в помещение и на выходе из него устанавливаются считыватели, которые считывают с карточек их код и передаю-

щие эту информацию в контроллер системы. Для каждого из зарегистрированных в системе ключей можно определить срок его действия. На основе сопоставления информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует проход через дверь, переводит помещение в режим охраны, включает сигнал тревоги и т. д.

Все факты предъявления карточек и связанные с ними действия (проходы, тревоги и т. д.) фиксируются в контроллере, автоматически заносятся в специальную базу данных на жестком диске компьютера («системный журнал»). Доступ к базе электронных карточек, содержащих информацию о зарегистрированных владельцах ключей, открыт только для уполномоченных сотрудников после ввода личного кода.

Программное обеспечение системы позволяет вести учет рабочего времени сотрудников и посетителей, которым выданы «ключи», получать разнообразные отчеты о событиях в системе за выбранные промежутки времени.

Система может круглосуточно функционировать в двух основных режимах: в комплексном, при котором работой системы управляет компьютер мониторинга, и в автономном режиме работы контроллера.

В ***автономный режим*** система переходит:

- по команде администратора системы (например, в случае необходимости замены или подключения какого-либо элемента, перед проведением профилактики и т. д.);
- автоматически через 3 с после отключения связи между контроллером и компьютером в результате повреждения линии связи, отключения сети питания в здании, при выходе из строя компьютера.

В этом режиме контроллер управляет доступом в помещение владельцев тех электронных ключей, коды которых были занесены в память контроллера, а также фиксирует в памяти информацию о событиях, связанных с доступом в помещение. После запуска программного обеспечения и перехода системы в сетевой режим эта информация автоматически переписывается в «системный журнал» компьютера, продолжительность автономной работы системы в случае отсутствия электропитания в сети может достигать 8 ч.

Контроллер системы ограничения доступа одной точки прохода TSS-Office предназначен для обработки информации от считывателей карточек, принятия решения и управления исполнительными устройствами в режиме реального времени. Контроллер обеспечивает контроль прохода сотрудников и посетителей через дверь, формирует базу событий, хранит коды ключей (карточек), поддерживает связь с компьютером через интерфейсный модуль B1T-4,3. В используемую серию контроллеров входят двухпортовые контроллеры двух типов - T и W, предназначенные, соответственно, для подключения двух считывателей идентификаторов «тач-мемори» или двух считывателей с интерфейсом Виганда (26-48 бит). В памяти контроллера сохра-

няются 504 кода, 7444 сообщения, 16 временных зон, 256 расписаний доступа по определенным датам. Элементы оборудования пункта прохода через дверь - стандартные.

2. **СКУД «Проход-МС»** - сетевая система контроля доступа для нескольких точек прохода с организацией учета рабочего времени, выполненная на базе программного комплекса TSS-Office. Система предназначена для контроля входа/выхода людей в офис и доступ во внутренние помещения офиса (в данном случае - шесть комнат). Система также позволяет организовать учет рабочего времени сотрудников, получать разнообразные отчеты о событиях в системе. Структурная схема СКУД «Проход-МС» приведена на рис. 6.10. Функционирует аналогично СКУД «Проход-С».

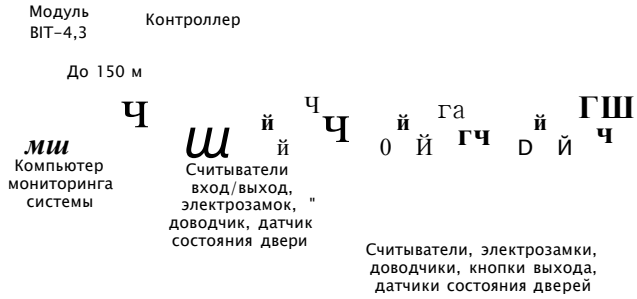


Рис. 6.10. Структурная схема СКУД «Проход-МС»

Допуск осуществляется с использованием идентификатора (электронного ключа) - пластиковой карточки или брелка с содержащимся в них индивидуальным кодом. Паспортные данные и другие сведения о доступе владельца электронного ключа заносятся в персональную электронную карточку. Персональная электронная карточка владельца и код его электронного ключа объединяются и заносятся в специально организованные компьютерные базы данных.

В системе каждому коду поставлена в соответствие информация о правах доступа владельца электронного ключа.

Считыватели также устанавливаются на входах дверей во внутренние помещения офиса. Причем в особо важных помещениях (например, бухгалтерия, склад и др.) считыватели устанавливаются на входе и выходе, а в других комнатах - только на входе. Выход из этих помещений осуществляется при нажатии на кнопку выхода.

Регулирование доступа осуществляется только с учетом полных запретов на доступ в то или иное помещение, а временные интервалы запрета доступа не учитываются.

Контроллеры серии TSS-201-8W, TSS-201-8T, TSS имеют восемь портов, к каждому из которых можно подключить оборудование одной точки прохода.

Каждый из портов контроллера имеет каналы для подключения считывателя, датчика состояния пункта прохода (двери), кнопки открывания двери и управления исполнительным устройством. Контроллер имеет энергонезависимую память и встроенный календарь-часы. В памяти контроллера сохраняются 2000 кодов и 2000 сообщений о событиях.

Интерфейс подключаемых считывателей: T - для считывателей идентификаторов типа «тач-мемори», W - для считывателей с интерфейсом Виганда (26-48 бит).

Элементы оборудования пункта прохода через дверь: считыватели на вход и на выход, датчик состояния двери, электрозамок, доводчик двери.

Компьютер (обычный IBM-совместимый) является компьютером мониторинга системы, хранит базу данных пользователей, формирует журналы событий и учета рабочего времени.

3. СКУД «Проходная - бюро нропусков» - система контроля и управления доступом с поддержкой всех функций бюро пропусков и проходной для трех точек прохода, оборудованных турникетами, а также автоматизированной выдачи электронных пропусков. Система позволяет вести протоколирование событий доступа, действий операторов и данных о работе оборудования в «системном журнале», а также вести учет рабочего времени, формировать отчеты на основе выбранных критериев с возможностью просмотра на экране и печати на принтере. Система выполнена на базе программного комплекса TSS-2000Profi. Структурная схема СКУД СКУД «Проходная - бюро пропусков» приведена на рис. 6.11.

Рис. 6.11. Структурная схема СКУД «Проходная - бюро пропусков»

В качестве идентификатора (электронного ключа) используется пластиковая карточка или брелок с содержащимся в них индивидуальным кодом. Перед выдачей электронного ключа его код и данные о его будущем владельце

заносятся в базу данных системы. Необходимые текстовые данные (Ф. И. О., должность, подразделение, паспортные данные и т. д.) вводятся в поля с помощью клавиатуры компьютера. В специальное окно «карточки» заносится изображение владельца электронного ключа. В процессе задания ограничений доступа можно указать начальную и конечную дату периода действия «ключа», а также доступные пункты прохода (турникеты) и интервалы времени по дням недели, в течение которых можно пройти через указанные турникеты с помощью данного электронного ключа. Причем ограничения доступа, заданные для какого-либо из сотрудников или посетителей, можно с помощью нажатия двух клавиш автоматически распространить на всех или на выбранных по какому-либо критерию владельцев «ключей» (например, на работников определенного отдела). Полная процедура регистрации занимает не более 2-3 мин.

У входа на предприятие на панели турникета или рядом с ним устанавливаются считыватели, которые считывают с карточек их код и передающие эту информацию в контроллер системы. В системе каждому коду поставлена в соответствие информация о правах доступа владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует проход через турникет.

Все факты предъявления «ключей» и связанные с ними действия (проходы, факты срабатывания датчика и нажатия кнопки турникета и т. д.) фиксируются в контроллере, автоматически заносятся в журнал событий, связанных с проходом через турникет проходной, и сохраняются в компьютере. Причем для каждого события указывается: его характер, дата, время, код предъявляемого «ключа» и Ф. И. О. его владельца или дежурного оператора, нажавшего кнопку. Подобным же образом регулируется и выход с предприятия. Информация о событиях, вызванных предъявлением карточек, может быть использована в дальнейшем для получения отчетов по учету рабочего времени, нарушениям трудовой дисциплины и др.

Контроллеры серии TSS-201-8W, TSS-201-8T имеют восемь портов, к каждому из которых можно подключить оборудование одной точки прохода. Контроллер имеет энергонезависимую память и встроенный календарь-часы. В памяти контроллера сохраняются 2000 кодов и 2000 сообщений о событиях.

Интерфейс подключаемых считывателей: T - для считывателей идентификаторов типа «тач-мемори», W - для считывателей с интерфейсом Виганда.

Компьютер бюро пропусков работает под управлением компьютера мониторинга, хранит базу данных пользователей, вносит в нее изменения, управляет вводом фотоизображений в базу данных, управляет печатью карточек-пропусков, автоматически формирует журналы событий и учета рабочего времени, формирует временные режимы доступа на объект для каждого пользователя. Электронный фотоаппарат обеспечивает ввод фотографии в

компьютер, принтер предназначен для печати пластиковых карт, служебный считыватель считывает коды ключей-карточек пользователей при внесении их в базу данных и заполнении личных карточек.

Система может круглосуточно функционировать в двух основных режимах: в комплексном, когда работой системы управляет компьютер мониторинга, и в автономном режиме работы контроллера.

4. СКУД «Центр» - система контроля доступа с контролем центральной проходной и пунктов прохода на удаленном объекте из головного офиса, выполненная на базе программного комплекса TSS-2000Profi. В данной системе на удаленном объекте контролируется проход через проходную и в два помещения внутри здания. Система также позволяет организовывать учет рабочего времени сотрудников, получать разнообразные отчеты о событиях в системе. Вся информация в реальном режиме отображается на экранах компьютеров системы, в том числе на планах этажей зданий или планах территории. Структурная схема СКУД «Центр» приведена на рис. 6.12.

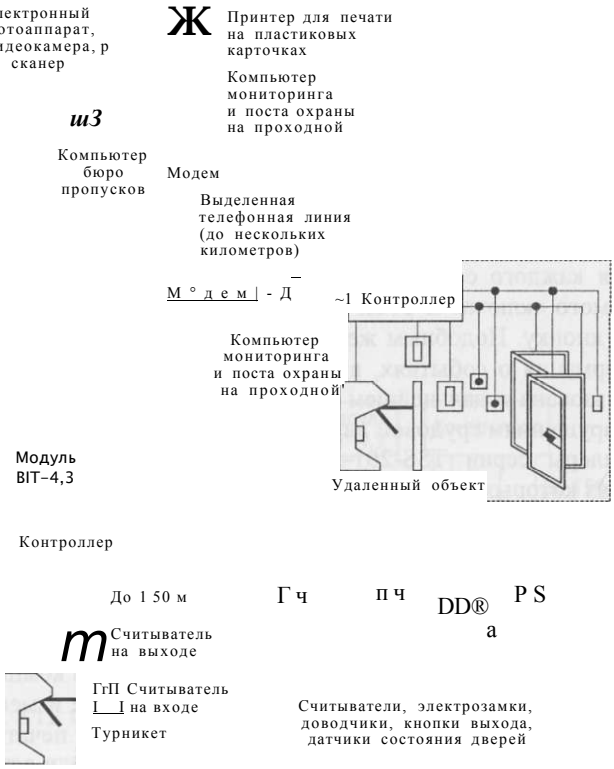


Рис. 6.12. Структурная схема СКУД «Центр»

Перед выдачей электронного ключа его код и данные о его будущем владельце заносятся в базу данных системы. Для занесения кода «ключа» оператору достаточно коснуться им контрольного считывателя, установленного на рабочем месте рядом с компьютером. Необходимые текстовые данные (Ф. И. О., должность, подразделение, паспортные данные и т. д.) вводятся в поля с помощью клавиатуры компьютера. В специальное окно «карточки» заносится изображение владельца электронного ключа. В процессе задания ограничений доступа можно указать начальную и конечную дату периода действия «ключа», а также доступные пункты прохода (турникеты) и интервалы времени по дням недели, в течение которых можно пройти через турникеты с помощью данного электронного ключа. Полная процедура регистрации занимает не более 2-3 мин.

При выходе посетителя в момент считывания кода система автоматически переводит выданный ему «ключ» в разряд свободных, а компьютер поста охраны на проходной выдает речевое сообщение типа: «Внимание! Гость организации, просьба забрать ключ!» После возвращения гостевого ключа в бюро пропусков он вновь может быть выдан очередному посетителю, а вся информация об ушедшем госте сохраняется в базе данных.

У входа на предприятие на панели турникета или рядом с ним устанавливаются считыватели, которые считывают с карточек их код и передающие эту информацию в контроллер системы. В системе каждому коду поставлена в соответствие информация о правах доступа владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует проход через турникет. Подобным образом регулируется и выход с предприятия. Информацию об этих событиях в любой момент можно просмотреть на экране компьютера.

В системе также осуществляется контроль доступа во внутренние помещения предприятия. Причем в особо важных помещениях (например, бухгалтерия, склад или др.) считыватели устанавливаются на входе и выходе. На основе сопоставления информации о правах доступа и ситуации, при которой был предъявлен «ключ», система принимает решение: контроллер открывает или блокирует проход через двери, переводит помещение в режим охраны, включает сигнал тревоги и т. д.

Все факты предъявления «ключей» и связанные с ними действия (проходы, факты срабатывания датчика и нажатия кнопки турникета и т. д.) фиксируются в контроллере, автоматически заносятся в журнал событий, связанных с проходом через турникет проходной и сохраняются в компьютере. Причем для каждого события указывается: его характер, дата, время, код предъявляемого «ключа» и Ф. И. О. его владельца или дежурного оператора, нажавшего кнопку. Программное обеспечение системы позволяет вести учет рабочего времени сотрудников и посетителей, которым выданы «ключи», получать разнообразные отчеты о событиях в системе за выбранные промежут-

ки времени. Если в течение рабочего дня какому-либо сотруднику необходимо неоднократно входить и выходить через проходную, то при формировании отчетов о рабочем времени система суммирует отдельные промежутки времени его пребывания на территории организации.

Важной особенностью системы является то, что любой владелец ключа, проникший в здание, минуя проходную (код его ключа не был считан считывателем на входе проходной), не сможет войти ни в одну из контролируемых системой дверей.

При значительных расстояниях между компьютерами, входящими в сеть системы, обмен данными может быть организован по оптоволокну, по телефонным линиям с помощью модемов, через Интернет. При необходимости проводить визуальный мониторинг объектов можно также и в режиме отображения поэтажных планов, на которых наглядно отображается ситуация в здании. В момент возникновения нештатного события на экране компьютера автоматически или по команде пользователя разворачивается план нужного этажа, на котором указывается место или объект, с которым связано тревожное событие. Это позволяет даже наиболее слабо подготовленному оператору быстро оценить ситуацию, подтвердить получение сигнала тревоги и принять правильное решение. Планы могут иметь иерархическую структуру типа «Общий - подробный». В этом случае ситуация в зданиях отображается на общем схематичном плане, а при возникновении экстренного события раскрывается подробный план соответствующего этажа или помещения.

Система может круглосуточно функционировать в двух основных режимах: в комплексном, когда работой системы управляет компьютер мониторинга, и в автономном режиме работы контроллера.

Продолжительность автономной работы системы в случае отсутствия электропитания в сети может достигать 24 ч.

При использовании универсального программируемого контроллера TSS-GlobalNet вместе с подключенными к нему контроллерами серии TSS-201 (рис. 6.13) в случае повреждения всей компьютерной сети и обесточивания здания будет обеспечен контроль доступа и управление оборудованием с учетом всех расписаний и ограничений по дате, времени, зонам, а также сохранность всей информации, связанной с работой системы.

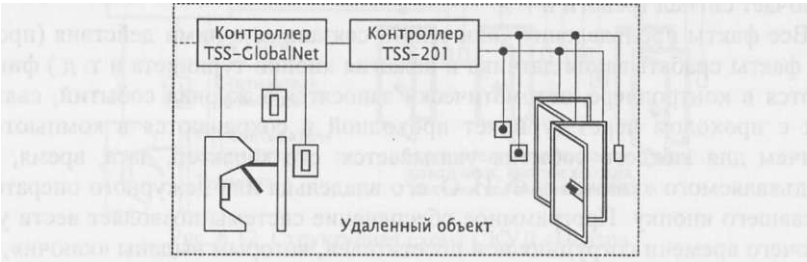


Рис. 6.13. Структурная схема СКУД с контроллерами TSS-GlobalNet и TSS-201

В случае обрыва линии связи система удаленного объекта функционирует самостоятельно и в полном объеме, а события, связанные с ее работой, сохраняются в локальном «системном журнале», хранящемся в контроллере TSS-GlobalNet объекта. После восстановления связи локальный «системный журнал» и база основного объекта автоматически синхронизируются без остановки нормального функционирования системы.

Контроллеры серии TSS-201-8W, TSS-201-8T имеют восемь портов, к каждому из которых можно подключить оборудование одной точки прохода. Интерфейс подключаемых считывателей: T - для считывателей идентификаторов типа «тач-мемори», W - для считывателей с интерфейсом Виганда (26-48 бит).

В составе системы используются обычные IBM-совместимые компьютеры со следующими параметрами: процессор типа Pentium, Celeron, оперативная память объемом не менее 64 Мбайт, SVGA-монитор и видеокарта, поддерживающие разрешение не менее 800 x 600 точек и глубину цвета 24 бит (16,7 млн цветов).

5. **СКУД «Офис-И»** - система контроля и управления доступом с организацией контроля прохода и контроля датчиков сигнализации и видеоконтроля, дистанционного управления видео- и телекамерами. Система позволяет получать изображение от камер на экране компьютера, а также вести запись изображения как по команде пользователя, так и в автоматическом режиме по факту срабатывания какого-либо из контролируемых датчиков. Система также обеспечивает учет рабочего времени сотрудников, получение разнообразных отчетов о событиях в системе. Вся информация в реальном режиме отображается на экранах компьютеров системы, в том числе на планах этажей зданий или планах территории. Рассматриваемая система выполнена на базе программного комплекса TSS-2000Profi. Структурная схема СКУД «Офис-И» приведена на рис. 6.14.

На входе в офис и на выходе из него устанавливаются считыватели информации идентификаторов. Считыватели также устанавливаются на входах дверей во внутренние помещения офиса. Причем в особо важных помещениях (например, бухгалтерия, склад и др.) считыватели устанавливаются на входе и выходе.

В системе каждому коду поставлена в соответствие информация о правах доступа владельца электронного ключа. На основе сопоставления этой информации и ситуации, при которой был предъявлен «ключ», система принимает решение: контроллер открывает или блокирует проход через дверь, переводит помещение в режим охраны, включает сигнал тревоги и т. д.

В процессе мониторинга контролируемых объектов информация о всех событиях, связанных с доступом в контролируемые помещения, датчиками сигнализации и работой системы, а также действия операторов фиксируется в специальной базе данных на жестком диске компьютера («системный жур-

нал»). Имеется возможность поиска, сортировки и отбора в базе данных электронных карточек зарегистрированных владельцев ключей по самым различным критериям.

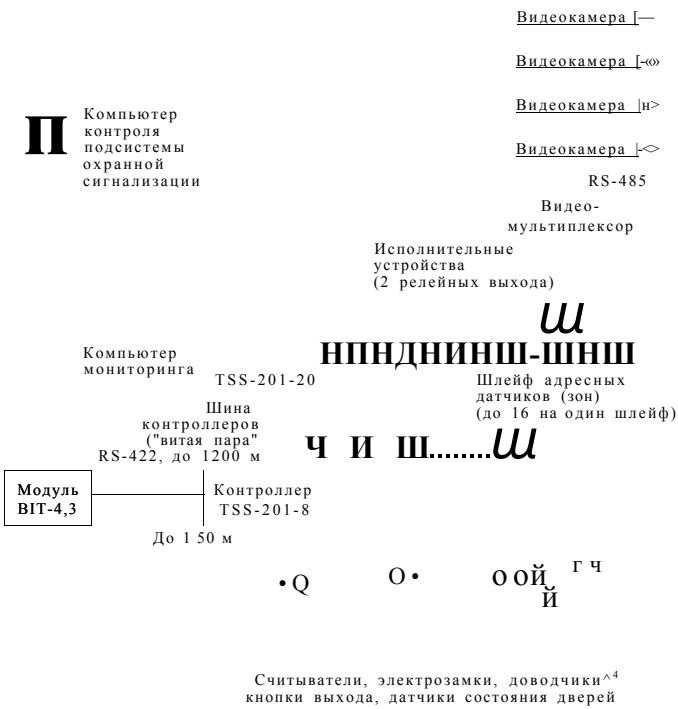


Рис. 6.14. Структурная схема СКУД «Офис -И»

Программное обеспечение системы позволяет вести учет рабочего времени сотрудников и посетителей, которым выданы «ключи», получать разнообразные отчеты о событиях в системе за выбранные промежутки времени. Помимо контроля и управления доступом в помещения система способна контролировать самые различные контрольные кнопки, пожарные извещатели и датчики сигнализации. Причем датчики, входящие в состав системы, могут быть как отдельными адресными сенсорами, так и датчиками, входящими в так называемые адресные группы датчиков (зоны). В момент срабатывания датчика система автоматически в соответствии с заранее заданной установкой может включить или выключить то или иное устройство (сирену, насосы пожаротушения), разблокировать двери и т. п. Событие фиксируется в «системном журнале».

Централизованная постановка и снятие с охраны осуществляется с рабочего места (компьютера) администратора системы или дежурного оператора.

Кроме этого, отдельные помещения или этажи могут ставиться и сниматься с охраны уполномоченным сотрудником организации. Информация о том, какие помещения и проходы находятся под охраной или сняты с охраны, отображается на поэтажных планах здания.

В состав системы может быть включено оборудование для видеонаблюдения (видеокамеры, видеомультиплексор) в необходимых зонах. Изображение от видеокамер передается на экраны компьютеров системы и/или записывается в базу данных после срабатывания определенного датчика или по таймеру. Число выходов видеомультиплексора и его параметры зависят от его типа.

При необходимости проводить визуальный мониторинг объектов можно также и в режиме отображения поэтажных планов, на которых наглядно отображается ситуация в здании. Если система имеет достаточно сложную структуру и контролирует объекты, расположенные в многоэтажном здании или в отдельных зданиях, планы могут иметь иерархическую структуру типа «Общий - подробный». В этом случае ситуация в зданиях отображается на общем схематичном плане, а при возникновении экстренного события раскрывается подробный план соответствующего этажа или помещения.

Система может круглосуточно функционировать в двух основных режимах: в комплексном, когда работой системы управляет компьютер мониторинга, и в автономном режиме работы контроллера. Продолжительность автономной работы системы в случае отсутствия электропитания в сети может достигать 24 часов. Двухрежимность работы системы особенно важна при контроле датчиков сигнализации. Все факты срабатывания датчиков в автономном режиме сохраняются в памяти контроллера с указанием времени, места (зоны) и типа датчика. При переходе в комплексный режим накопившиеся в автономном режиме сообщения о срабатывании датчиков выдаются на экран компьютера и автоматически переписываются в «системный журнал».

Контроллер TSS-GlobalNet обладает возможностью передачи на компьютеры системы, записи и сохранения видеоизображения от подключенных видеокамер в режиме «stand alone» по команде пользователя, по факту срабатывания датчика и/или по расписанию.

Контроллеры серии TSS-201-8W, TSS-201-8T имеют восемь портов, к каждому из которых можно подключить оборудование одной точки прохода. Интерфейс подключаемых считывателей: T - для считывателей идентификаторов типа «тач-мемори», W - для считывателей с интерфейсом Виганда (26-48 бит).

При необходимости может быть установлен компьютер контроля подсистемы охранной сигнализации. Он предназначен для:

- мониторинга датчиков сигнализации с отображением состояния на планах этажей, выдачей текстовых и речевых (звуковых) сообщений и ведения протокола событий;

- дистанционной постановки и снятия с охраны этажей, помещений и отдельных датчиков.

На экранах компьютеров может отображаться изображение от видеокамер.

6. **СКУД PERCo-S-600** - система контроля доступа, построенная на основе сети контроллеров, подключаемых к компьютеру. Связь с контроллерами осуществляется через конвертер интерфейса, который подключается к последовательному порту компьютера (скорость обмена данными 19200 бит/с). Максимальное число контроллеров в системе равно 64. Длина магистрали достигает 1200 м.

В качестве исполнительных устройств в системе могут использоваться электромагнитные и электромеханические замки, различные турникеты и калитки. Пропусками в системе PERCo-S-600 служат бесконтактные электронные карты форматов HID или EM-Marin. Максимальное число карт в системе составляет 64000. В состав системы могут входить 2 типа контроллеров: контроллеры замка и контроллеры турникета. Структурная схема СКУД «PERCo-S-бОО» приведена на рис. 6.15. В ряде случаев (например, при установке на наружную дверь) возможно использование модели, в которой имеется выносная антенна, что повышает вандалозащищенность системы. Контроллер замка с переговорным устройством (модель, не имеющая сегодня аналогов на рынке) совмещает в себе функции контроллера управления доступом (видео-) и аудиодомофона. В его вандалозащищенном корпусе одновременно находятся: считыватель бесконтактных карт, контроллер и переговорное (видео-) аудиоустройство. Это не только удобно, но и позволяет заметно снизить затраты на оборудование входа в офис.

На входе в офис и на выходе из него устанавливаются считыватели информации идентификаторов. Считыватели также устанавливаются на входах дверей во внутренние помещения офиса. Причем в особо важных помещениях (например, бухгалтерия, склад и др.) считыватели устанавливаются на входе и выходе.

Каждый контроллер замка управляет одним замком, поддерживает список из 1000 карт, и имеет энергонезависимый буфер на 3500 событий. Контроллеры турникета управляют широким спектром исполнительных устройств: турникетами-триподами, тумбовыми, роторными турникетами и калитками.

Каждый контроллер турникета управляет одним турникетом, поддерживает список из 2000 карт, а также имеет энергонезависимый буфер на 2000 событий. С помощью дополнительного модуля памяти М-600 число событий, хранимых в энергонезависимой памяти контроллера турникета или калитки, можно увеличить до 6000.

Сетевое программное обеспечение (ПО) системы позволяет организовать необходимое число автоматизированных рабочих мест (отдел кадров, бюро пропусков, администратор, охрана, бюро труда и заработной платы).

Рис. 6.15 Структурная схема СКУД «PERCo-S-6ОО» АРМ - автоматизированное рабочее место

ПО работает под управлением Windows 98 SE, Windows NT или Windows 2000 и имеет удобный русскоязычный интерфейс, напоминающий большинство современных Windows-приложений. В зависимости от решаемых задач можно использовать две версии ПО: базовое и с разграничением доступа по времени.

Система PERCo-S-600 обеспечивает эффективное решение следующих задач:

- контроль и управление доступом,
- контроль трудовой дисциплины и учет рабочего времени;
- защита материальных ценностей и информации;
- комфортные условия работы руководителя;
- автоматизированный кадровый учет, оформление и выдача пропусков;
- оперативное управление оборудованием.

7. **СКУД PERCo-SYSTEM-12000** - гибкая система контроля и управления доступом, которая дает возможность комплексно решать такие проблемы, как контроль доступа и перемещения персонала и посетителей, охрана территории, кадровый учет, трудовая дисциплина и учет рабочего времени. Система может применяться разных объектах: в банках, офисах, на промышленных предприятиях, в административных учреждениях, на военных и стратегических объектах, на автостоянках, атомных и гидроэлектростанциях, на вокзалах, в аэропортах. Структурная схема СКУД «PERCo-SYSTEM-12000» приведена на рис. 6.16.

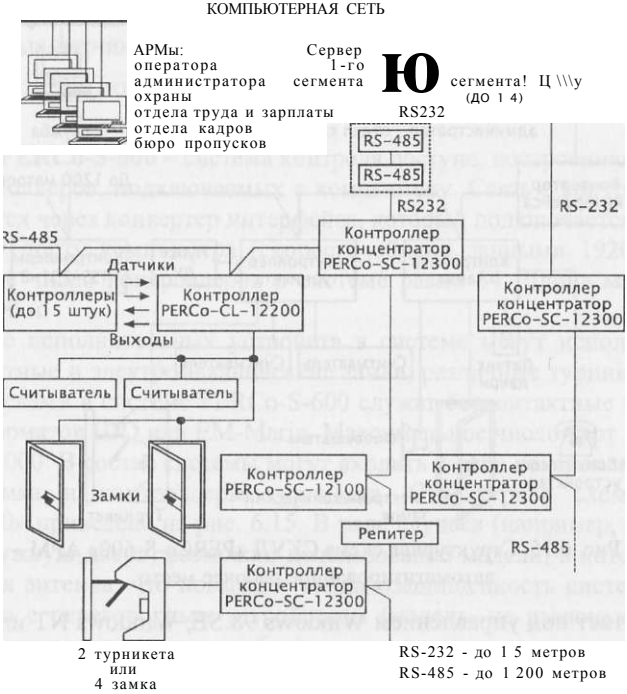


Рис. 6.16. Структурная схема СКУД «PERCo-SYSTEM-12000» АРМ - автоматизированное рабочее место

PERCo-SYSTEM-12000 представляет собой сеть контроллеров PERCo-SC-12100, PERCo-SC-12100P, PERCo-CL-12200 и концентраторов PERCo-SC-12200 (до 255). Каждый контроллер в системе обслуживает одно или два исполнительных устройства и один или два считывателя карт доступа. Для идентификации пользователей в системе используются бесконтактные или магнитные пластиковые карты доступа.

Программное обеспечение системы работает под управлением Windows 98 или Windows NT. Имеются несетевая версия ПО и сетевая версия для распределенных систем на неограниченное число рабочих мест операторов. Программное обеспечение организовано по модульному принципу: можно приобрести базовое ПО, а затем дополнительно к нему модуль учета рабочего времени, модуль удаленного контроля (с видеоидентификацией) модуль обхода территории охраной

В качестве исполнительных устройств могут применяться электромеханические замки, турникеты, шлагбаумы, ворота, светофоры. Контроллер имеет входы для подключения различных датчиков, например датчиков охранно-пожарной сигнализации. Возможна интеграция PERCo-SYSTEM-12000 с системой охран-

ио-пожарной сигнализации и организация на ее основе Центрального поста наблюдения.

Система PERCo-SYSTEM-12000 обеспечивает эффективное решение следующих задач:

- разграничение доступа на объекты контролируемой территории;
- контроль передвижения персонала по территории предприятия;
- охрана, т. е. получение в режиме реального времени информации о тревожных событиях на контролируемых объектах;
- учет присутствия и учет рабочего времени персонала предприятия;
- обход охраны;
- модуль оформления пропусков.

6.1.3. Семейство СКУД «Flex»

Семейство СКУД «P1ex»(производитель ЗАО «Контур безопасности» - Россия, Украина) относится к классу систем, позволяющих выстраивать необходимые конфигурации из стандартных блоков, учитывая все особенности предприятия. Управление системой осуществляется ключами lButton («тач-мемори») или проксимити-картами. Разработаны и производятся следующие версии системы «Flex»: автономные на одну дверь до 1000 ключей (серия 900), охранные на одну дверь (серия 1020), сетевые до 4000 ключей на одну точку прохода (серия 800), сетевые с функциями охраны (серия 1010).

Разнообразие версий СКУД «Flex» позволяет подобрать оптимальные варианты оснащения того или иного объекта именно тем оборудованием, которое для него требуется, не заставляя заказчика оплачивать большое число избыточных функций.

Процессорные блоки сетевых версий СКУД «Flex» используются для построения систем с рассредоточенной логикой, в которых каждый блок является полностью функционально законченным модулем. Данная архитектура имеет следующие преимущества:

- связь с блоками осуществляется через конвертер, который поставляется в отдельном корпусе и подключается к COM-порту или может быть встроен в компьютер;
- в режиме OFF LINE (оф-лайн) компьютер требуется в основном для формирования баз данных, управления графиком проходов и централизованного съема и обработки данных с подключенных процессорных блоков;
- режим ON LINE (он-лайн) позволяет управлять системой, аккумулировать данные, выводить их на монитор и обрабатывать в реальном времени. При отключении компьютера в режиме ON LINE система автоматически переходит в режим OFF LINE, полностью сохраняя свою работоспособность;
- все функции точки прохода сохраняются в полном объеме;
- позволяет объединять в сеть до 256 точек прохода на один компьютер;

- устойчива к неблагоприятным внешним воздействиям;
- линии связи в системе защищены от злоумышленников аппаратно и программно (применяется специальный протокол обмена);
- для управления замками и другими исполнительными устройствами на процессорной плате имеются транзистор и реле с НЗ/НО-контактами;
- на плате предусмотрен дополнительный источник стабилизированного питания 12 В, 3 А.

Процессорные блоки компьютерных версий СКУД «Flex» используются в качестве сетевых для построения систем с сосредоточенной логикой, в которых каждый блок является полностью функционально законченным модулем. Данная архитектура, позволяющая объединить в сеть до 32 считывателей, весьма удобна в проектировании и монтаже.

Программное обеспечение для всех основных сетевых версий СКУД «Flex» хорошо отлажено и защищено. Программы могут быть доработаны в соответствии с потребностями и запросами клиентов. Последняя разработка DigiFlex 5.10_Pro - расширенная версия DigiFlex 5.10_9600. Программное обеспечение состоит из программ «Клиент» и «Сервер».

Ниже перечислены особенности DigiFlex 5.10_Pro:

- модульная структура с возможностью работы по компьютерной сети.
- программа «Клиент» производит только обслуживание контроллеров, учитывает число посещений (данные поступают от контроллеров) и выполняет ряд простых функций. «Клиент» устанавливается на удаленных компьютерах, к которым подключаются отдельные ветки контроллеров;
- программа «Сервер» устанавливается на выделенном компьютере и выполняет функции комплексного управления всеми контроллерами сети, а также обработки данных, поступающих от программ «Клиентов». «Сервер» поддерживает в реальном времени мониторинг состояния и отображение событий от контроллеров;
- фотоидентификация - при касании ключом считывателя при выходе или входе на экране компьютера появляется фотография владельца ключа;
- поэтажные планы;
- программа может быть встроена в другие системы управления и контроля доступа;
- на основе программ «Клиент» (которые фактически накапливают только события от контроллеров - номер карты + время касания + вход/выход) можно строить интегрированные системы учета рабочего времени персонала на предприятии, учитывающие все индивидуальные особенности объекта. В этом случае в роли «Сервера» будет выступать программа, разработанная специально для конкретного заказчика.

Автономные версии «Flex» при умеренной стоимости обеспечивают все необходимые функции системы контроля доступа. По необходимости любой ключ можно сделать мастер-ключом, т. е. управляющим. В схеме предусмотрена защита от стирания ключей при аварийном отключении системы. Имеются два независимых канала управления с общей таблицей ключей на одной плате, что позволяет использовать ее для создания тамбура. Возможны варианты входа/выхода по устройству идентификации либо свободный выход (при выходе замок открывается простым нажатием кнопки или напряжением от домофона). Практически все перечисленные функции автономных версий имеются и в контроллерах магнитных замков серии 900, причем процессорная плата в данном случае устанавливается внутри замка и питается от внешнего источника постоянного или переменного тока.

Охранные версии являются специализированной разновидностью автономных систем СКУД «Flex», в которых предусмотрена охрана одной зоны. Охраняемая зона может включать датчики любого типа с нормально замкнутыми контактами, число которых ограничено лишь возможностями питания. Процессорная плата поддерживает два считывающих устройства (на входе для снятия с охраны и на выходе для постановки на охрану), замок, шлейф охранных датчиков (геркон, ИК и пр.) и сирену. Постановка системы на охрану и снятие с охраны производятся одним касанием ключа к считывателю при выходе и при входе.

При отключении питания 220 В система переключается на аккумулятор.

Охранные СКУД «Flex» могут работать автономно, предоставляя своему хозяину весь набор «вахтерских» услуг, которые комбинируются с надежной охранной сигнализацией. Также возможно включение системы «Flex» в любую стандартную систему охранной или охранно-пожарной сигнализации, с которой она будет согласованно работать в рамках интегрированной системы безопасности данного объекта.

Таким образом, очевидно, что СКУД «Flex» идеально подходят как для малых объектов с контролем от одной до двух дверей, так и для объектов, на которых необходимо ставить под полный контроль большое число дверей и требуется не только организация контроля доступа, но и учет рабочего времени персонала.

6.2. Биометрические СКУД

В качестве примера реализации систем биометрической идентификации рассмотрим биометрическое устройство идентификации по отпечатку пальца FingerScan V20 и его модификации V-Station.

В **FingerScan** V20 использована технология биометрического контроля доступа ID Safe (сканер). FingerScan V20 имеет простую процедуру инсталляции и разработан для применения как в сети, так и несетевых системах. Здесь обеспечена возможность эргономичной интеграции со счетчиком карт,

что позволяет производить чтение карты и параметров пальца одновременно и обеспечивает высокую скорость доступа.

Система просто интегрируется с другими приложениями и вписывается в любую уже существующую или только планируемую для установки систему контроля доступа, использующую протокол Виганда. Сканер также может функционировать без подключения к каким-либо другим устройствам, т. е. в одиночном режиме для управления и контроля за дверным проемом. В этом случае не требуется никаких дополнительный контроллеров.

Объединение в сеть нескольких устройств FingerScan V20 позволяет пользователям пройти регистрацию с помощью любого сканера, входящего в систему. Биометрические показатели нового пользователя посылаются остальным сканерам автоматически. Сетевое функционирование может осуществляться посредством стандартного интерфейса RS485 или благодаря модемному или Ethernet-соединениям.

FingerScan V20 обладает следующими возможностями:

- контроль состояния замка и мониторинг состояния двери,
- использование протокола Виганда для интеграции с уже существующими системами доступа по карточкам;
- работа с сетью или без нее;
- передача данных по сети с помощью протоколов RS485 или RS232, а также по модемному или Ethernet-соединениям;
- для регистрации достаточно одного касания;
- число пользователей может варьироваться от 512 до 32 ООО;
- полная обратная совместимость с устройствами TouchLockll и предыдущими моделями FingerScan производства компании Identix;
- эффективная Intel-архитектура, имеющая широкие возможности масштабирования.

Технические характеристики:

- среднее время подтверждения доступа: 1 с;
- среднее время чтения отпечатка при регистрации: 5 с;
- средний размер маски пальца: 300 байт;
- идентификационный номер: от 1 до 9 цифр или прочтение карточки;
- число хранимых транзакций: 8000;
- виды связи: RS485, Wiegand, RS232, TTL и опционально Ethernet и модем;
- скорость передачи информации в бодах: 300;
- число пользователей: стандартно - 512, максимум - 32 000 ;
- чтение карточек: Виганда, проксимити, с магнитной полосой, смарт, со штрих-кодом;
- число временных зон: 30;

- монитор: 2 линии, 16 символов;
- размеры (В(мм) х Ш(мм) х Г(мм)): 172 х 165 х 89, вес 0,9 кг.

V-Station — биометрическая СКУД по отпечатку пальца компании Bioscrypt (США). Представляет собой дальнейшее развитие считывателей серии «Very». Его основное отличие от других считывателей данной серии - наличие встроенной клавиатуры и ЖК-дисплея. Клавиатура, состоящая из 12 цифровых и 3 функциональных клавиш, позволяет программировать считыватель V-Station без использования компьютера. V-Station может работать в режиме ПИН-код + палец. Различные модификации V-Station повторяют весь остальной модельный ряд считывателей серии «Very», добавляя к ним клавиатуру. Особенности системы:

- программирование как с компьютера, так и со встроенной клавиатуры считывателя;
- встроенный 80-символьный ЖК-дисплей, упрощающий работу со считывателем;
- встроенный сетевой интерфейс Ethernet, существенно упрощающий процедуру ввода новых отпечатков пальцев, когда в системе используются несколько считывателей;
- простая интеграция в любые СКУД через встроенный интерфейс Виганда;
- считыватели V-Station (В, Р) имеют буфер памяти на 3000 отпечатков пальцев и позволяют автономно хранить до 7500 событий с привязкой к дате и времени возникновения,
- модификация V-Station S обеспечивает хранение 200 отпечатков пальцев и работу в режиме идентификации: 1 х 200;
- буфер памяти моделей V-Station (М и I) ограничен только мощностью контроллера СКУД, к которому они подключаются, поскольку хранение шаблона осуществляется на смарт-карте;
- диапазон входного напряжения - от 12 до 24 В.

Модификации V-Station

1. V-Station (В). Базовая модель: биометрический считыватель на 3 тыс. пользователей (клавиатура, ЖК-дисплей, RS-232, RS-485, Ethernet, Виганда, часы Real-time, размеры: 143 х 168 х 67 мм, 12В, 1,5А). Осуществляет верификацию в режиме ПИН-код + палец или Ключ + палец (в качестве ключа может выступать любой идентификатор, считываемый на внешнем считывателе, подключенном к V-Station по интерфейсу Виганда - по аналогии со считывателем V-Flex). ПО для программирования считывателя - VeriAdmin. Структурная схема биометрической СКУД «V-Station (В)» приведена на рис. 6.17.

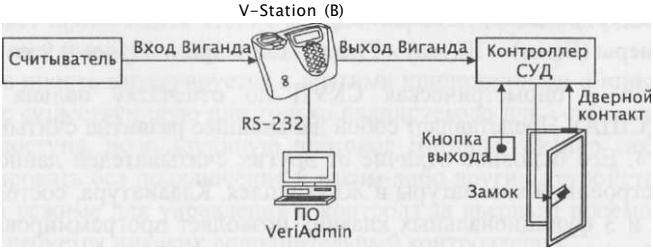


Рис. 6.17. Структурная схема биометрической СКУД «V-Station (B)»

2. V-Station (P). Биометрический считыватель, включающий все характеристики базовой модели со встроенным считывателем HID. Базовая модель + встроенный проксимити-считыватель HID (развитие идеи V-prox). ПО для программирования считывателя - VeriAdmin. Структурная схема биометрической СКУД «V-Station (P)» приведена на рис. 6.18.

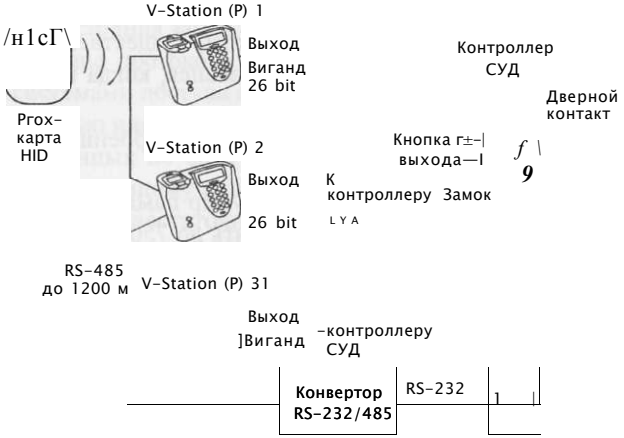


Рис. 6.18. Структурная схема биометрической СКУД «V-Station (P)»

3. V-Station (M). Биометрический считыватель, включающий все характеристики базовой модели со встроенным считывателем смарт-карт MIFARE. Базовая модель + встроенный считыватель бесконтактных смарт-карт Mifare (развитие идеи V-Smart - отпечаток пальца хранится на смарт-карте).

4. V-Station (I). Биометрический считыватель, включающий все характеристики базовой модели со встроенным считывателем смарт-карт iClass. Базовая модель + встроенный считыватель бесконтактных смарт-карт iCLASS (развитие идеи V-Smart iCLASS - отпечаток пальца хранится на смарт-карте).

ПО для программирования считывателя V-Station (M/I) - VeriAdmin. Структурная схема биометрической СКУД «V-Station (M/I)» приведена на рис. 6.19.

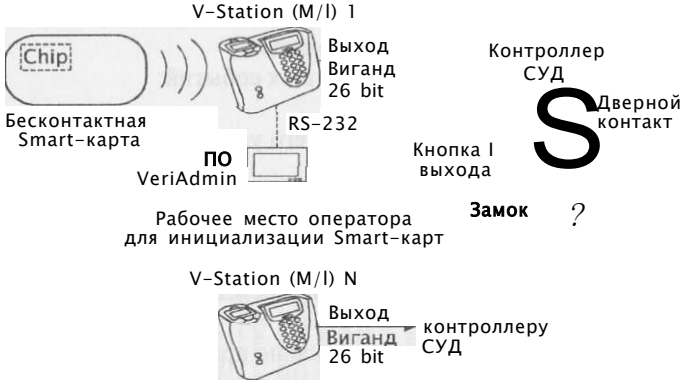


Рис. 6.19. Структурная схема биометрической СКУД «V-Station (M/I)»

5. V-Station (S). Биометрический считыватель, включающий все характеристики базовой модели с дополнительной возможностью идентификации до 200 пользователей (аналогично считывателю V-Pass).

Базовая модель + проведение идентификации 1:200 (развитие идеи V-Pass). ПО для программирования считывателя - VeriAdmin. Структурная схема биометрической СКУД «V-Station (S)» приведена на рис. 6.20.

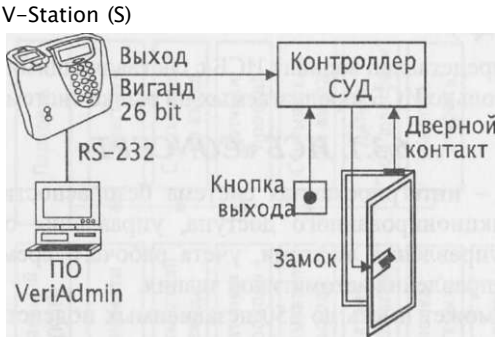


Рис. 6.20. Структурная схема биометрической СКУД «V-Station (S)»

6.3. Интегрированные СКУД

Интегрированные системы безопасности (ИСБ), системы комплексного обеспечения безопасности (СКОБ), интеллектуальное здание - все эти термины в последнее время все чаще встречаются на страницах научных и популярных изданий.

Специалисты отмечают целый ряд преимуществ ИСБ от других систем обеспечения безопасности.

Среди основных преимуществ ИСБ отметим следующие:

- более быстрая реакция на происходящее;
- точный и развернутый анализ текущих событий;
- упрощение проектирования;
- снижение затрат на оборудование, его установку, монтаж и эксплуатацию;
- экономия проводной и кабельной продукции;
- удобство в управлении подсистем.

ИСБ необходимо монтировать из совместимых модулей, лучше всего одной фирмы. Модульная структура ИСБ и, прежде всего, СКУД позволит решать следующие задачи:

1. Разделять сотрудников и посетителей по правам доступа.

2. Получать информацию обо всех лицах, чьи данные занесены в базу данных.

3. Создавать уровни доступа (например, проход по генеральному ключу - везде и всегда), последовательность двух и более идентификаторов (ключей, карт ПИН-кодов и биометрических отличий).

4. Осуществлять блокировку дверей на определенное время, открывать их надолго, например для прохождения группы людей.

5. Выполнять ряд специфических функций (невозможность передачи ключа другому лицу и проходу по одному и тому же пропуску двоим и больше людям и др.).

На рис. 6.21 представлен вариант ИСБ с составляющими СКУД.
Рассмотрим несколько ИСБ, предлагаемых на рынке систем безопасности.

6.3.1. ИСБ «CONCEPT»

«CONCEPT» - интегрированная система безопасности и контроля для обеспечения санкционированного доступа, управления охранно-пожарной сигнализацией, управления лифтами, учета рабочего времени, контроля за автостоянками, управления автоматикой здания.

«CONCEPT» может иметь до 250 независимых подсистем, каждая из которых работает как независимая контрольная панель. Охранно-пожарная сигнализация, система санкционированного доступа и система управления автоматикой здания в каждой из подсистем работают автономно. Выдача сигналов тревоги по различным каналам (передача сигнала на пульт централизованного наблюдения, на телефон или на пейджер, передача информации на удаленный ПК) для каждой подсистемы также может осуществляться независимо.

Рис. 2.3. Основные подсистемы СКУД

Подсистема охранно-пожарной сигнализации «CONCEPT» поддерживает до 2000 зон обнаружения. Каждая такая зона защищена от несанкционированного вмешательства извне, и ее состояние регулярно проверяется. Информация о состоянии подсистемы может быть передана на центральный пункт наблюдения. Это обеспечивается встроенным цифровым коммуникатором, который поддерживает различные протоколы (Contact ID, 4+2 Ir Fast и др.). Кроме того, сигналы тревоги могут передаваться на телефон (в т.ч. на мобильный), на пейджер или через модем на удаленный компьютер. Все события в подсистеме регистрируются в энергонезависимой памяти и в дальнейшем могут быть просмотрены или распечатаны на принтере пользователем, а также переданы или прочитаны дистанционно с помощью ПК.

Подсистема санкционированного доступа «CONCEPT» поддерживает управление и контроль более чем 250 точек прохода. Это могут быть контроллеры дверей, ворот или турникетов. Предлагаемое программное обеспечение позволяет организовать гибкую систему санкционированного доступа с заданием прав доступа в то или иное помещение, с разграничением доступа по времени и дням недели. Кроме того, существует возможность формирования различных отчетов по каждой точке прохода и по каждому пользователю, что может быть полезно при рассмотрении различных спорных ситуаций и для учета рабочего времени при начислении зарплаты.

Управление и контроль состояния системы «CONCEPT» предусматривает разграничение прав по доступу к возможностям системы. Они задаются при программировании администратором ИСБ. Оператор системы имеет возможность полностью управлять пользователями, правами доступа по каждому контроллеру и по каждому пользователю, а также режимами работы системы в целом. Можно задать графический план объекта и вести базу данных фотографий пользователей. Это позволяет оператору снизить до минимума ошибки при допуске пользователя в то или иное помещение. После того как пользователь ввел код доступа или приложил карту доступа, на экран оператора выводится фотография данного человека и после сравнения фотографии с внешностью пользователя на мониторе принимается окончательное решение о допуске в помещение.

Подсистема управления лифтами организована на базе тех же карт, которые используются в подсистемах санкционированного доступа. После ввода кода или предъявления карточки доступа пользователю предоставляется возможность прохода на те этажи, которые разрешены для посещения данному пользователю. Другие этажи для него будут недоступны. Эта функция особенно необходима для многоэтажных зданий, в которых находится большое число организаций и они расположены в здании поэтажно.

В той части здания, к которой предъявляются повышенные требования безопасности, необходимо устанавливать дополнительные средства защиты, такие, как шлюзы. Система «CONCEPT» имеет возможность управления данными устройствами. Логика работы шлюзов заключается в том, что вто-

рая дверь не будет разблокирована до тех пор, пока не будет закрыта первая дверь.

Подсистема управления автоматикой здания позволяет оптимизировать потребление тепловой и электрической энергии, а также минимизировать потери от их неэкономного использования. Например, система автоматически включит освещение при обнаружении движения в помещении и выключит при отсутствии движения в контролируемом объеме в течение заданного промежутка времени. Можно задавать логику включения (или выключения) освещения только при недостатке естественного света (в этом случае к расширителям входов аналогового сигнала подключаются фотосенсоры). К расширителям входов аналогового сигнала могут также подключаться датчики температуры, влажности и др. По сигналам этих датчиков можно контролировать состояние вентиляции и отопительных приборов.

В системе «CONCEPT» каждому пользователю - как временному, так и постоянному - может быть выдана карта доступа, разрешающая доступ только в определенный оператором период времени, и только в определенные помещения (этажи здания). Для временных пропусков может быть задан режим, позволяющий аннулировать пропуск сразу же после его первого использования.

Кроме управления освещением и отоплением здания, система «CONCEPT» позволяет управлять любым другим оборудованием и автоматикой. Например, с ее помощью можно управлять фонтанами и поливом газонов. Систему можно запрограммировать таким образом, чтобы данные устройства работали только в определенные часы суток и дни недели. Кроме работы по часам и по календарю, может быть задана любая другая логика, например, включение полива только в том случае, когда датчики влажности фиксируют отсутствие влаги. Отметим, что всеми системами можно управлять вручную, с ПК или с помощью SMS-сообщений.

Используя систему доступа, также можно контролировать въезд/выезд автомобилей со стоянки. Чтобы въехать/выехать, пользователи должны предоставить карточку, прописанную в системе. Система ведет автоматический подсчет въезжающих/выезжающих автомобилей и может выдавать число занятых и свободных мест на стоянке. Если стоянка полностью заполнена, система проинформирует об этом оператора и пользователя. При этом ворота будут для въезжающих автомобилей заблокированы до тех пор, пока какой-нибудь автомобиль не покинет стоянку и не освободит место.

Для больших объектов или нескольких зданий можно использовать несколько контрольных панелей «CONCEPT». Эти панели объединяются в сеть на базе TCP/IP-протокола. Панели могут контролироваться с нескольких рабочих мест с помощью программного обеспечения ACCEPT NET. Отметим, что отдельные здания могут находиться в разных городах и даже в разных странах.

ИСБ «CONCEPT» имеет следующие технические характеристики:

- длина магистрали (RS 485) - 1,2 км (при использовании изоляторов магистраль удлиняется до 6,5 км);
- скорость передачи данных в магистрали - 19,2 Кбит/с;
- число модулей в магистрали - 250 (до 99 одинаковых);
- число независимых групп - 250;
- число шлейфов - 2000;
- число программных выходов (PGM) - 2000;
- число пользователей - 4000;
- число типов пользователей - 250;
- число считывателей - 250;
- цифровой телефонный коммуникатор - Contact ID, 4+2 Ir Fast;
- число команд DTMF - 16.

6.3.2. ИСБ «Advisor Master»

ИСБ «Advisor Master» объединяет в себе функции СКУД, охранной подсистемы, управления автоматикой здания и другими функциями. ИСБ и ее подсистемы построены по модульному принципу. Обладая модульной структурой, система «Advisor MASTER» может быть построена оптимальным образом в зависимости от объекта: от небольшого офиса до универмагов, банков или промышленных предприятий. Модульная структура ИСБ реализована с помощью системной шины данных (RS485), что позволяет расширять систему.

Ядром подсистемы СКУД служит контрольная панель ATS4000 (рис. 6.22). Максимальное число охранных зон в системе контроля доступа составлет 256 На плате контрольной панели есть 16 зон для подключения охранных датчиков и дополнительный разъем для подключения двух 8-зонных расширителей. Базовым расширением охранных зон в системе контроля доступа является шина RS485, на которую подключаются адресные модули расширения. Максимальное расстояние между самыми удаленными модулями в системе контроля доступа составляет 1,5 км и может быть дополнительно расширено до 6 км с помощью изоляторов/повторителей. Линейка адресных модулей расширения включает модули на 4, 8 или от 8 до 32 охранных зон. В корпус адресного модуля ATS1201 системы контроля доступа устанавливаются до 3 зонных расширителей ATS1202, что дает расширение до 32 охранных зон. Дополнительно к адресному модулю системы контроля доступа расширения подключаются модули выходов на 16 выходов типа «Открытый коллектор», 4 или 8 реле. Таким образом, адресный модуль расширения представляет собой базовый элемент для построения охранной системы контроля доступа.

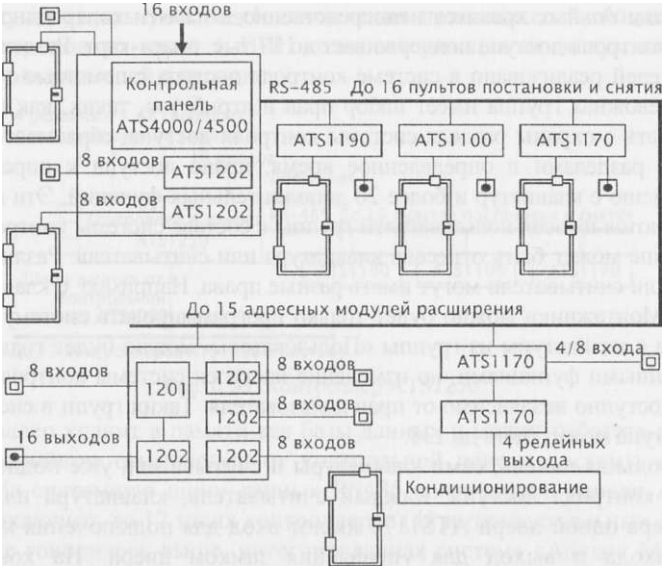


Рис. 6.22. Структурная схема ИСБ «Advisor MASTER»

Каждая контрольная панель системы контроля доступа поддерживает при помощи расширителей до 256 охранных зон. К каждой зоне можно подключить один охранный шлейф. У каждой зоны система контроля доступа идентифицирует 3 состояния: активное, пассивное и тампер. Система контроля доступа поддерживает до 67 типов охранных зон, например, «Кнопка с фиксацией». Активацию/деактивацию такой зоны выполняет подсистема охраны. Может использоваться на посту дежурного охранника. Система также включает 16 независимых подсистем (разделов). Каждая охранная зона может быть приписана к любому разделу или нескольким разделам. Система контроля доступа Advisor MASTER позволяет легко организовать постановку на охрану зон, относящихся к общим помещениям (коридор, холл, лестница). Для этого общие зоны приписываются одновременно к нескольким разделам. При постановке всех этих разделов такие зоны автоматически встанут на охрану.

В системе Advisor MASTER все управление разделами можно осуществлять как с клавиатуры, так и со считывателя. Когда пользователь подносит к считывателю смарт-карту, система контроля доступа открывает дверь и снимает раздел с охраны. Следующие пользователи только открывают картой дверь. Это упрощает пользование системой контроля доступа и уменьшает число ложных тревог. Пользователь может поставить раздел на охрану, если поднесет карту к считывателю системы контроля доступа 3 раза в течение 10 с.

Все *базы данных* хранятся непосредственно в памяти контрольной панели. Система контроля доступа поддерживает до 17 тыс. смарт-карт. Разделение прав пользователей реализовано в системе контроля доступа с помощью тревожных групп. Тревожная группа имеет набор прав и атрибутов, таких, как право ставить/снимать с охраны раздела системы контроля доступа, сбрасывать тревоги, управлять разделами в определенное время, право доступа к определенным пунктам меню с клавиатур и более 20 дополнительных функций. Эти права распространяются на всех пользователей группы в составе системы контроля доступа. К группе может быть отнесена клавиатура или считыватель. Различные клавиатуры или считыватели могут иметь разные права. Например, с клавиатуры из группы «Монтажник» можно будет только программировать систему контроля доступа, а с клавиатуры из группы «Пользователь» можно будет только управлять охранными функциями, но изменение настроек системы контроля доступа будет недоступно независимо от прав пользователя. Таких групп в системе контроля доступа может быть до 138.

Контрольная панель, сами клавиатуры и считыватели уже поддерживают функции контроля доступа. Каждый считыватель, клавиатура или модуль контроллера одной двери ATS1170 имеют вход для подключения кнопки запроса выхода и выход для управления замком двери. На контроллере ATS1170 этот выход релейный, на считывателях и клавиатурах - типа «открытый коллектор». При поднесении смарт-карты или наборе ПИН-кода система контроля доступа «Advisor MASTER» производит авторизацию пользователя и проверку прав.

В состав системы «Advisor MASTER» также входит интеллектуальный контроллер четырех дверей ATS1250, поддерживающий расширенные функции контроля доступа.

Контроллер ATS1250 предназначен для управления и контроля доступа через 4 двери (рис. 6.23). На плате контроллера есть 4 входа для подключения любых считывателей, поддерживающих формат Виганда. Это могут быть считыватели Aritech, считыватели других производителей или биометрические считыватели. На контроллере системы контроля доступа размещены 4 реле для управления замками дверей и 16 входов, к которым подключаются магнитные контакты от дверей, кнопки запроса выхода, зоны контроля состояния «Дверь открыта слишком долго». Магнитные контакты, используемые для функций контроля доступа, можно одновременно использовать в охранной системе.

С помощью локальной шины, к которой можно подключить еще 16 считывателей, клавиатур или модулей ATS1170, контроллер ATS1250 поддерживает до 20 считывателей. Проход через все 48 интеллектуальных дверей в системе «Advisor MASTER» контролируется функцией «Елобапьный Anti-passack». Кроме этого система контроля доступа позволяет использовать «программный Anti-pass-back», и тогда проход не запрещается, но делается соответствующее оповещение и запись в журнале событий. Контроллер по-

зволяет осуществлять учет местонахождения пользователей, поддерживает функции «проход по карте + ПИН-код», авторизация по «двум картам» и «счетчик пользователей в регионе».

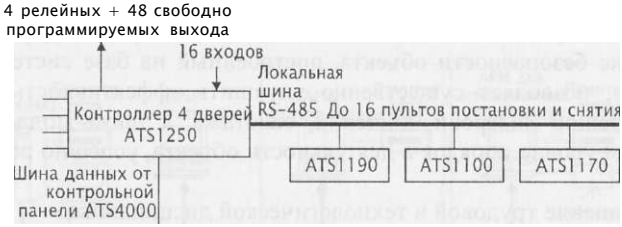


Рис. 6.23. Контроллер ATS1250

Контроллер хранит в памяти все базы данных и может работать автономно при аварийном отключении от контрольной панели системы контроля доступа. На системную шину данных RS485 контрольной панели ATS4000 можно подключить до 12 таких контроллеров (48 интеллектуальных дверей).

Как уже говорилось выше, интегрированная система «Advisor MASTER» предназначена не только для выполнения охранных функций и функций СКУД, но и для управления автоматикой в здании: кондиционированием, светом, вентиляцией на релейном уровне. Для этого в системе предусмотрен механизм флагов событий и макрологики.

Абсолютно все настройки системы контроля доступа можно сделать с клавиатуры, но удобнее использовать русифицированное ПО TITAN. С помощью ПО TITAN можно не только произвести все настройки системы контроля доступа, загрузить настройки удаленно в панель, но также вести мониторинг, осуществлять управление системой контроля доступа, проводить диагностику, программировать смарт-карты, управлять журналом событий и поддерживать графические планы помещений. С помощью средств диагностики можно не только проверить целостность системы «Advisor MASTER», журнала событий и баз данных, но также измерить сопротивление на охранных входах и оценить падение напряжения и ток в системной шине.

При необходимости панели системы Advisor MASTER могут быть объединены в *сеть.* В один сегмент сети можно объединить 16 панелей и 4 таких сегмента подключить к одному компьютеру с ПО TITAN.

Система «Advisor MASTER» была сертифицирована в России в 2003 г.

6.2.3. ИСБ «Цирконий-С 2000»

«Цирконий-С 2000» - многоуровневая интегрированная система управления доступом и охранной сигнализацией. Система предназначена для использования в качестве системной основы для создания централизованных комплексов безопасности средних и крупных объектов, в том

числе расположенных на пространственно разнесенных территориях. Она обеспечивает разграничение и контроль доступа персонала внутри объекта, охрану периметров, расположенных на территории объекта зданий, сооружений, зон (помещений). Система «Цирконий-С2000» имеет сертификат № РОСС RU.ОС02.000268.

Комплекс безопасности объекта, построенный на базе системы «Цирконий-С2000», позволяет существенно улучшить эффективность охраны по предупреждению диверсий, хищений, саботажа, а также поддерживать на надлежащем уровне порядок в деятельности объекта, успешно решая важные задачи:

- повышение трудовой и технологической дисциплины;
- оперативное управление действиями персонала;
- учет использования рабочего времени;
- снижение вероятности появления чрезвычайных и аварийных ситуаций, повышение достоверности анализа причин их возникновения и эффективности работ по ликвидации последствий.

При создании централизованного комплекса безопасности на базе системы «Цирконий-С2000» охраняемый объект делится на участки по периметру и зоны по территории, зданиям, сооружениям. На каждом участке, в каждой зоне устанавливаются средства обнаружения (СО) на входе в зону и выходе из зоны - средства контроля и управления доступом. Станционная часть системы, реализованная на основе локальной вычислительной сети, обеспечивает подачу команд управления на СО, средства управления и контроля доступом.

Для управления доступом каждому абоненту выдается карта-пропуск, которая используется как один из идентификаторов личности при проходе через точки доступа. Дополнительным идентификатором может служить набираемый сотрудником личный код, при необходимости может использоваться один из биометрических признаков (изображения кисти руки или отпечаток пальца) при подключении соответствующих устройств.

Система «Цирконий-С2000» является гибкой, архитектурно открытой системой с иерархическим распределением функций по компонентам нескольких уровней (рис. 6.24).

Каждое автоматизированное рабочее место (АРМ) специализировано на выполнение определенных функций за счет установки соответствующего ПО и настройки связей между составными частями системы. Число АРМ любого вида в системе не ограничено. Основой периферийной аппаратуры системы являются контроллеры, к которым подключаются считыватели пропусков, СО, кнопки экстренного вызова, отметки наряда, ЭМЗУ, турникеты, внешние устройства, управляемые релейными выходами контроллеров и т. д. Подключение контроллеров к станционной части системы осуществляется с помощью коммуникационных комплектов КР-1, каждый из которых обеспечивает

обмен информацией по четырем независимым магистралям длиной до 5 км каждая. Магистраль представляет собой одну витую пару кабеля ТПП или кабеля с аналогичными характеристиками. К каждой магистрали подключается до 25 контроллеров. Программное обеспечение АРМ оператора поддерживает работу до четырех комплектов КР-1, т. е. до 400 контроллеров.

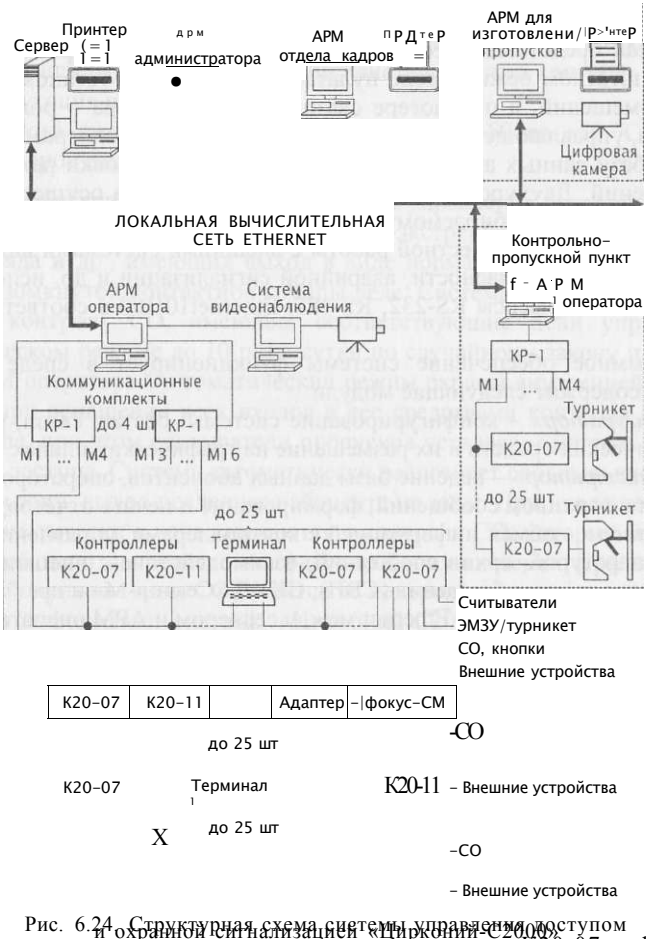


Рис. 6.24. Структурная схема системы управления доступом и охранной сигнализацией «Цирконий-С2000»

В системе используются контроллеры двух видов: К20-07 с функциями контроля доступа и охранной сигнализации; К20-11 с функциями охранной сигнализации.

При потере связи с АРМ оператора контроллеры работают автономно, накапливая сообщения в собственном внутреннем архиве. Контроллер К20-7

имеет внутреннюю базу данных на 10000 пропусков, используемую в автономном режиме для принятия решения о доступе абонентов.

Система обеспечивает возможность подключения ранее выпускаемых контроллеров К, К-01, К-02 системы «Цирконий-С». Вместо любого контроллера к магистрали можно подключать терминал или устройство отображения информации «Фокус-СМ», к которому, в свою очередь, подключаются до 16 СО.

Терминал представляет собой многофункциональное устройство, выполняющее в штатном режиме роль пульта управления для установки режимов охраны помещений, а при потере связи с АРМ оператора - роль ведущего устройства, управляющего подключенными к нему контроллерами. Терминал содержит базу данных абонентов, имеющих право установки режимов охраны помещений. Двухуровневая идентификация абонента осуществляется по пропуску и паролю, набираемому на клавиатуре.

Для обеспечения совместной работы с внешними системами видеонаблюдения, пожарной безопасности, аварийной сигнализации и др. используются стандартные интерфейсы RS-232, RS-485, Ethernet 10/100 и соответствующие драйверы.

Программное обеспечение системы функционирует в среде Windows NT/2000 и содержит следующие модули:

«Конфигуратор» - конфигурирование системы: состав, связи, режим работы технических средств и их размещение на графических планах.

«Администратор» - ведение базы данных абонентов, операторов рабочих мест, работа с архивом сообщений, формирование и печать отчетов.

«Оператор» - обмен информацией с контроллерами, управление периферийной аппаратурой, архив сообщений, взаимодействие с внешними системами: система видеонаблюдения (СВН), СКУД «Сектор-М» и др.

«Сеть» - обмен по сети Ethernet между сервером и АРМ операторов.

«РМИП» - изготовление пропусков на основе проксимити-карт, печать учетных карточек о пропусках.

«Табельный учет» - формирование отчетов о состоянии трудовой дисциплины и табелей учета использования рабочего времени.

В качестве системы управления базами данных (СУБД) используется SQL-сервер (InterBase, MicrosoftSQL, Oracle и др.). Модульный принцип построения программного обеспечения позволяет создавать АРМ с заданной функциональностью за счет инсталляции соответствующих модулей. Для повышения уровня защиты от несанкционированных действий на каждом АРМ может устанавливаться соответствующий аппаратно-программный комплекс типа «SecretNet».

При обеспечении контроля и управления доступом обеспечивается:

- индивидуальные перечни разрешенных зон и графика работы по каждому абоненту;
- поддержка временных и скользящих графиков работы;
- функция antipassback по всей территории объекта, включая нештатные и аварийные ситуации при наличии неконтролируемых связей между

зонами объекта (открыта аварийная дверь, точка доступа снята с контроля и т. п.);
- высокая интеграция функций охраны и доступа;
- использование любого сочетания режимов управления охраной помещений (автоматического, централизованного);
- реализация принципа работы по правилу «2... 6» лиц;
- создание комплексов с малопроводными линиями связи,
- удаление контроллеров от станционной части до 5 км с обеспечением грозозащищенности магистралей; -дистанционный контроль СО;
- коммутация питания СО;
- широкий диапазон рабочих температур (от -50 до +50 "С) для контроллеров с охранными функциями.

Система обеспечивает различные режимы управления охраной зон объекта при подключении СО, датчиков, кнопок экстренного вызова, кнопок отметки наряда и др., имеющих выход в виде нормально-замкнутой или нормально-разомкнутой контактной группы реле. Система обеспечивает дистанционный контроль СО, имеющих соответствующие цепи управления в автоматическом режиме до 10 раз в сутки по случайному закону и по командам с АРМ оператора Автоматический режим охраны внутренней зоны реализуется при оснащении всех входов в нее средствами контроля и управления доступа, при этом считыватели пропусков устанавливаются с обеих сторон точки доступа. Система автоматически распознает события: вход первого абонента в зону, выход последнего абонента из зоны. При входе первого абонента автоматически в зоне снимаются с контроля СО, которые были указаны для этой цели в процессе конфигурирования системы. При выходе последнего абонента из зоны СО ставятся на контроль.

Защита информации системы «Цирконий-С2000» от несанкционированного доступа обеспечивается реализацией развитых механизмов контроля и управления, имеющих трехуровневую архитектуру. Первый уровень защиты, основанный на объединении операторов в различные по своим полномочиям группы, обеспечивается конфигурированием операционной системы АРМ. Большинству операторов предоставляется возможность работы только с модулями системы «Цирконий-С2000». Второй уровень защиты обеспечивается системой управления базой данных (СУБД), реализованной на SQL сервере. Механизм защиты информации строится на возможности разграничения доступа к информации, хранящейся в таблицах базы данных. При подключении к СУБД проводится обязательная проверка подлинности клиента, после которой ему предоставляются полномочия по просмотру или редактированию данных. Третий уровень защиты обеспечивается ПО системы. Работа любого оператора в системе «Цирконий-С2000» начинается с идентификации по коду пропуска и личному коду, после чего предоставляются полномочия по управлению системой.

6.3.4. ИСБ «TSS-2000Profi» и «TSS-20000ffice»

«TSS-2000Profi» и «TSS-20000ffice» - полнофункциональные, универсальные системы контроля и управления доступом для малых, средних и крупных предприятий. Структурная схема «TSS-2000Profi» приведена на рис. 6.25, а «TSS-20000ffice» - на рис. 6.26.

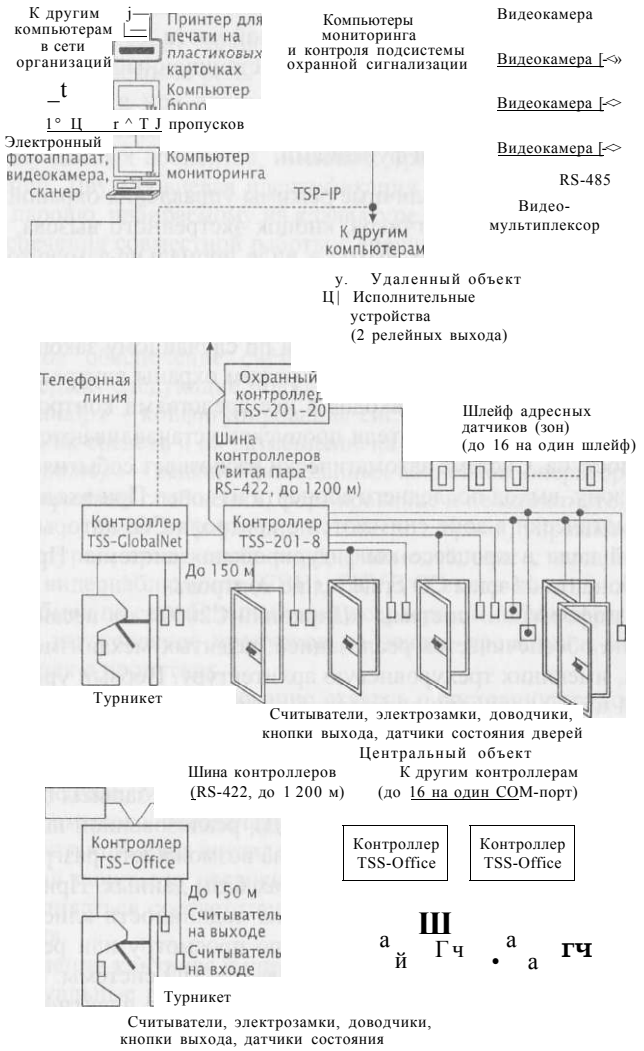


Рис. 6.25. Структурная схема СКУД «TSS-2000Profb>

Системы представляют собой программно-аппаратные комплексы на базе контроллеров серии TSS и одного или нескольких персональных компьютеров, объединенных в локальную компьютерную сеть.

Рис. 6.26. Структурная схема СКУД «TSS-20000ffice»

В общем случае в состав оборудования систем входят:

- универсальные контроллеры серий TSS-201 и TSS-WA48 (TSS-Office), а также универсальные программируемые контроллеры TSS-Global Net, предназначенные для обработки информации от считывателей идентификаторов, принятия решения и управления исполнительными устройствами;
- элементы оборудования пунктов прохода (дверей) в контролируемые помещения: электрозащелки, электромеханические или электромагнитные замки, датчики состояния дверей, кнопки открывания дверей, считыватели идентификаторов (ключей) пользователей и т. п.;
- компьютеры в системе «TSS-2000Profi», объединенные в локальную сеть и осуществляющие мониторинг и управление доступом в комплексном режиме работы;
- компьютер в системе «TSS-20000ffice», осуществляющий мониторинг и управление доступом в комплексном режиме работы.

Контроллеры системы «TSS-2000Profi» способны регулировать доступ как под управлением компьютера мониторинга (сетевая система, комплексный режим), так и автономно (автономная система). В автономных системах управление доступом осуществляет автономно работающий контроллер. Система может круглосуточно функционировать в двух основных режимах - в комплексном (штатном) режиме и в автономном. Продолжительность автономной работы системы в случае отсутствия электропитания в сети может достигать 8 ч. Двухрежимность работы системы особенно важна при контроле датчиков сигнализации. Все факты срабатывания датчиков в автономном

режиме сохраняются в памяти контроллера с указанием времени, места (зоны) и типа датчика.

Контроллеры системы «TSS-20000ffice» способны регулировать доступ как под управлением компьютера мониторинга (сетевая система, комплексный режим), так и автономно (автономная система). В автономных системах управление доступом осуществляет автономно работающий контроллер. Компьютер в таких системах либо полностью отсутствует, либо подключается только на время программирования и загрузки кодов идентификаторов в память контроллера, а также с целью переписывания из нее сообщений о событиях, накопленных за время автономной работы, в «системный журнал».

К контроллерам серии TSS-201 относятся контроллеры шести типов - TSS-201-8W, TSS-201-8T, TSS-201-4W,TSS-201-4T, TSS-201-2W, TSS-201-2T. Последняя цифра в маркировке типа контроллера указывает на число портов, служащих для подключения оборудования пунктов прохода и интерфейс подключаемых считывателей (T - для считывателей идентификаторов типа «тач-мемори», W - для считывателей с интерфейсом Виганда (26-48 бит).

В памяти контроллера сохраняются до 2000 кодов идентификаторов пользователей и до 2000 сообщений о событиях. Используются двухпортовые контроллеры двух типов - T и W, предназначенные соответственно для подключения двух считывателей идентификаторов «тач-мемори» или двух считывателей с интерфейсом Виганда (26-48 бит). В памяти контроллера сохраняются 504 кода идентификаторов пользователей, 7444 сообщения о событиях, а также сведения о расписании доступа по определенным датам (16 временных зон, 256 праздников).

В качестве программного обеспечения системы «TSS-2000Profi» используется программный комплекс TSS-2000Profi. Он предназначен для работы в ОС Windows 2000 или Windows NT и состоит из нескольких независимых программных модулей, каждый из которых поддерживает определенные функции системы:

- «Двери-объекты» (описание контроллеров, считывателей ключей, кнопок, датчиков и их привязки к поэтажным планам);
- «Персонал» (ввод и редактирование информации о персонале, контроль за работой системы, работа с системным журналом базы данных);
- «Мониторинг» (управление работой контроллеров, контроль за работой системы, экстренное вмешательство, выдача визуальных и речевых сообщений на русском языке об экстренных событиях);
- программы отчетов (формирование, просмотр и печать отчетов. «Все события», «Нарушения», «Проходы», «Рабочее время»);
- «Дистанционный монитор» (просмотр текущего системного журнала и списка владельцев ключей);

- «Проходная» (наблюдение за пересечением проходной: фото владельца ключа сопоставляется с его изображением с видеокамеры, управление дверями объекта);
- План - Browser (отображает состояние системы на поэтажных планах).

Упрощенная версия программного обеспечения TSS-2000Profi - система TSS-Office. Она предназначена для работы на одном компьютере и используется в качестве программного обеспечения системы «TSS-20000ffice».

Этот программный комплекс предназначен для работы в ОС Windows 2000 или Windows NT и состоит из нескольких независимых программных модулей, каждый из которых поддерживает определенные функции системы, аналогично как для системы «TSS-2000Profi».

6.3.5. ИСБ «Фокус ОПД»

«Фокус-ОПД» - система управления доступом и охранной сигнализацией. Она предназначена для организации комплексов управления доступом и охранной сигнализацией малой и средней ёмкости с отображением информации на ПК (табл. 6.1).

Таблица 6.1. Технические характеристики системы управлении доступом и охранной сигнализацией «Фокус-ОПД»

Буквенно-цифровое отображение информации на ЖК-дисплее (реальное время)	
Организация протяженности линий связи, км	до 14
Адресное управление шлейфами сигнализации и внешними устройствами	
Автоматический контроль работоспособности средств сигнализации и линий связи	
Энергонезависимое архивирование текущей информации	
Встроенные программируемые реле управления	
Напряжение питания, В	12/24
Ток потребления, мА	не более 70
Максимальная длина линий связи со средствами обнаружения, м	до 2000
Число шлейфов сигнализации	от 8 до 48
Управление: ЭМЗУ, турникетами; считывателями	 до 4 до 8
Контролируемое сопротивление, кОм	6,2

Возможность подключения различных шлейфов сигнализации и внешних устройств, а также модульный принцип построения и простота в эксплуатации позволяют создавать системы управления и контроля доступом, охран-

ной сигнализацией малой и средней ёмкости любой конфигурации и легко адаптировать их к требованиям различных объектов.

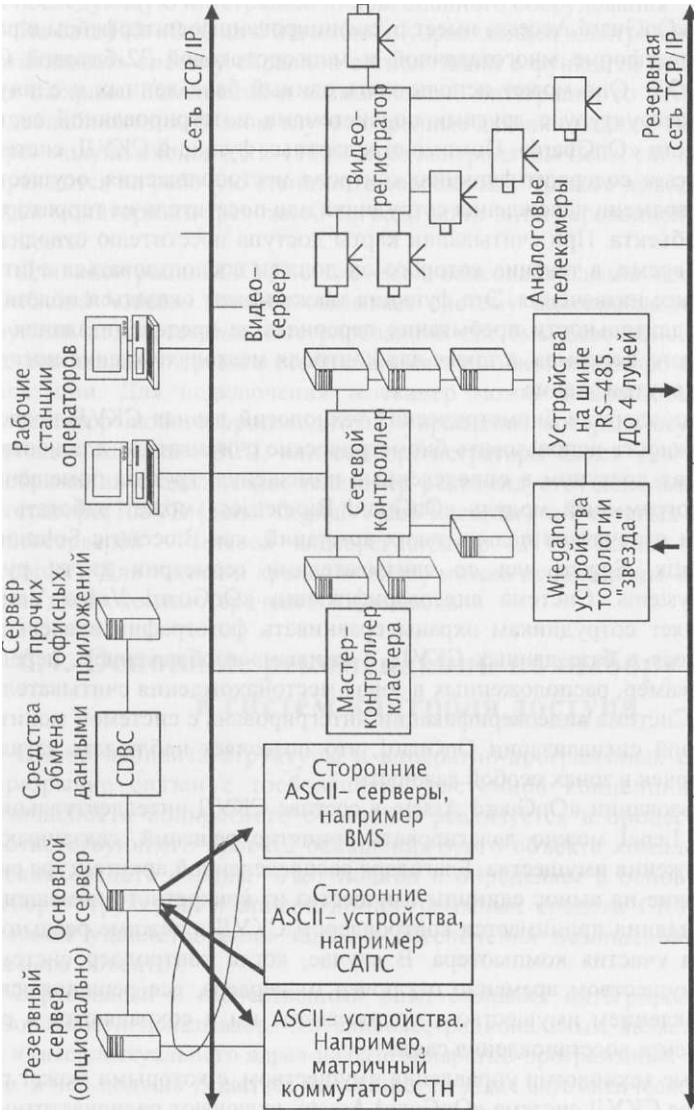
6.3.6. ИСБ «OnGuard Access»

«OnGuard Access» - интегрированная система контроля и управления доступом компании Lenel Systems. Система позволяет организовать контроль доступа в помещения здания или группы зданий через неограниченное число дверей для неограниченной численности персонала. Данная система является частью решения «OnGuard» компании Lenel для создания комплексной системы безопасности как одного здания, так и территориально распределенной группы зданий компании. «OnGuard Access» представляет собой аппаратно-программный комплекс и позволяет осуществлять интеграцию оборудования Lenel и сторонних производителей как на аппаратном, так и на программном уровне. Это единственное на сегодняшний день многосерверное решение с уникальной технологией синхронизации баз данных, обеспечивающее создание реально интегрированной системы безопасности корпорации с территориально удаленными объектами. Структурная схема системы управления доступом и охранной сигнализации «OnGuard Access» приведена на рис. 6.27

На базе СКУД Lenel и ПО OnGuard можно объединить в глобальный комплекс безопасности предприятия: системы контроля и управления доступом, видеонаблюдения, охранной и пожарной сигнализации, изготовления карт доступа, видеоидентификации, мониторинга тревожной сигнализации, управления учетом и движением имущества, управления персоналом и посетителями. Данная система имеет открытую архитектуру, которую можно наращивать и модифицировать, подключая неограниченное число устройств сторонних производителей.

Автономная или входящая в состав интегрированной системы безопасности система контроля и управления доступом «OnGuard» создается на базе контроллеров, модулей входов, модулей выходов, модулей управления считывателями и ПО «OnGuard Access» компании Lenel Systems. В зависимости от размеров и конфигурации СКУД специалисты Lenel предлагают использовать следующие устройства:

- интеллектуальные контроллеры LNL-500, LNL-1000 и LNL-2000, представляющие собой мастер-контроллеры, которые предназначены для осуществления обмена данными с сервером со скоростью до 115,2 кбит/с через порт RS-232/RS-485, через модем или по сети Ethernet, сохраняя в СКУД информацию о 350 ООО владельцах карт и 1 ООО ООО событий;
- модули входов LNL-1100 и модули выходов LNL-1200, которые имеют разъемы для подключения соответственно до 16 охранных датчиков и до 16 исполнительных устройств;


Сеть TCP/IP
Резервная сеть TCP/IP
Видео-регистратор
Аналоговые телекамеры
Видео-сервер
Рабочие станции операторов
Устройства на шине RS-485. До 4 лучей
Сетевой контроллер
Wiegand устройства топологии "звезда"
Сервер прочих офисных приложений
Мастер-контроллер кластера
Средства обмена данными
CDBC
Сторонние ASCII- серверы, например BMS
Основной сервер
Сторонние ASCII- устройства, например САПС
Резервный сервер (опционально)
ASCII- устройства. Например, матричный коммутатор СТН

- модули управления считывателями LNL-1300 и LNL-1320, предназначенные для подключения одного или двух считывателей карт доступа соответственно.

ПО СКУД «OnGuard Access» имеет русифицированные интерфейсы и разработано на платформе многозадачной и многопотоковой 32-битовой ОС Windows 2000/XP. Оно может использовать единый банк данных и единую сетевую инфраструктуру с другими подсистемами интегрированной системой безопасности «OnGuard». Помимо стандартных функций СКУД, система «OnGuard Access» содержит функцию контроля местоположения, осуществляющую учет времени нахождения сотрудника или посетителя на территории охраняемого объекта При считывании карты доступа посетителю отводится определенное время, в течение которого он должен воспользоваться считывателем в пункте назначения. Эта функция также может оказаться полезной для контроля длительности пребывания персонала за пределами здания во время обеденного перерыва, а также для контроля местонахождения посетителей (гостей) внутри здания.

Благодаря поддержке биометрических технологий данная СКУД предоставляет возможность использовать биометрические считыватели для контроля и управления доступом в определенные помещения, группы помещений или зоны. Программный модуль «OnGuard Biometrics» может работать со считывателями отпечатков пальца таких компаний, как Biocentric Solutions, Bioscript, Identix, Sagem или со считывателями геометрии кисти руки Recognition Systems. Система видеоверификации «OnGuard Video Verification» позволяет сотрудникам охраны сравнивать фотографии владельцев карт, хранящиеся в базе данных СКУД, с «живым» изображением, передаваемым с телекамер, расположенных в зонах местонахождения считывателей карт доступа. Система видеоверификации интегрирована с системой мониторинга тревожной сигнализации OnGuard, что позволяет наблюдать за владельцами карточек в зонах особой важности.

При использовании «OnGuard Asset» в составе СКУД интеллектуальным контроллерам Lenel можно делегировать принятие решений, связанных с контролем движения имущества. Благодаря распределенной архитектуре системы, разрешение на вынос единицы имущества из конкретного помещения офиса или из здания принимается контроллером СКУД в режиме реального времени и без участия компьютера. В случае, когда контроллер системы управления имуществом временно отключен от сервера, все решения, связанные с управлением имуществом, принимаются им и сохраняются в его памяти до момента восстановления связи.

Современные технологии управления имуществом, с которыми может работать в составе СКУД система «OnGuard Asset», включают радиочастотную идентификацию (RFID), штрих-код, локальные системы навигации и определения положения (LPS), любые стандартные считыватели с интерфейсом Ви-

ганда, считыватели HID RFID RS-485, ручные считыватели и регистраторы серии Symbol PDT 6100. Более того, «OnGuard Asset» разработана с расчетом на последующую интеграцию инновационного оборудования.

На базе ПО «OnGuard Intrusion» и управляющей электроники Lenel можно организовать систему охранной сигнализации с функцией постановки и снятия с охраны помещений и возможностью интеграции со СКУД и системой видеонаблюдения. В этом случае охранные датчики подключаются к системе через модули входов LNL-1100. Через контроллеры Lenel сигналы с датчиков передаются на рабочую станцию, а сообщения о тревоге выводятся на общий экран мониторинга тревожной сигнализации интегрированной системы безопасности.

Для интеграции СКУД с системой видеонаблюдения используется ПО «OnGuard Video», которое связывает систему видеонаблюдения со всеми другими подсистемами интегрированной системы безопасности OnGuard, а все сообщения о тревоге отображаются на общем мониторе тревожной сигнализации. Для подключения телекамер можно использовать матричный коммутатор любого производителя, управление которым осуществляется с помощью команд ASCII, или видеорегистраторы Lenel. Для записи видеоизображений с аналоговых телекамер рекомендуется использовать видеорегистраторы LDVR (Lenel Digital Video Recorder), а с сетевых телекамер или видеосерверов - сетевой видеорегистратор LNVR (Lenel Network Video Recorder). Для записи и хранения видео можно использовать внутренние жесткие диски компьютера или RAID-массив.

6.4. Основные рекомендации по выбору средств и систем контроля доступа

Выбор варианта структуры и аппаратно-программных средств СКУД неразрывно связан с требованиями системной концепции обеспечения безопасности конкретного объекта и реализуется в процессе разработки соответствующего проекта оснащения этого объекта комплексами технических средств охраны Этот подход и определяет в основном методику выбора структуры и аппаратно-программных средств СКУД (исходя из условий удовлетворения задачам обеспечения безопасности рассматриваемого объекта).

Зарубежный и отечественный опыт создания интегрированных систем безопасности показывает, что наиболее рациональным является реализация их «интеллектуального ядра» на базе аппаратно-программных средств СКУД, т. е. в ней должно решаться большинство задач автоматического управления контроля доступом, перемещения персонала, анализа попыток нарушения (несанкционированного проникновения), создания интегрированных баз данных, обслуживающих службу безопасности и т. д. Такой подход, в частности, позволяет сэкономить на аппаратуре СКУД и ТСОС (например, одни и те же

дверные датчики положения могут применяться и в аппаратуре контроля доступа, и в охранной сигнализации).

Отечественные разработки СКУД более предпочтительны, даже если обладают худшими параметрами относительно зарубежных аналогов. Это объясняется многими причинами, например, невозможностью проанализировать математическое и программное обеспечение импортных СКУД. В условиях, когда на СКУД «замыкается» управление потоками людей и ресурсов и управление системой безопасности, «цена» каждого отказа и даже простого сбоя в работе аппаратуры слишком велика.

6.4.1. Общие вопросы выбора СКУД

При разработке структуры и затем технического проекта СКУД для конкретного предприятия следует учитывать, что наиболее современные из них обладают высокой гибкостью и могут быть адаптированы к структурно-планировочным особенностям практически любого объекта. Существенным условием эффективного решения поставленной задачи является создание комплексной группы из специалистов по аппаратно-программным средствам СКУД, ответственных сотрудников службы обеспечения безопасности и специалистов по эксплуатации технических средств охраны. В функции группы входят составление, согласование и утверждение основных требований к аппаратуре системы контроля доступа, включающей:

- поименное формирование временных и зональных профилей для каждого сотрудника, лиц вышестоящих организаций и приходящих посетителей (понятие «профиль» применительно к аппаратуре СКУД означает совокупность «точек» (мест) прохода, например: проходная, входы в режимные помещения и т. п., и совокупность допустимых графиков проходов через эти «точки»);
- группирование временных и зональных профилей с целью их минимизации;
- уточнение отчетной статистики системы для возможного круга потребителей (служба безопасности - отдел режима, отдел кадров, службы организации труда, иные потребители);
- унификацию отчетной статистики;
- уточнение порядка взаимодействия с аппаратурой других подсистем безопасности объекта;
- подготовку нормативной базы для пользователей системы и сотрудников объекта;
- организацию разъяснительной работы среди сотрудников на этапе внедрения аппаратуры СКУД и т. д.

При составлении описания объекта, определении его характеристик и разработке основных требований необходимо учитывать два принципиально

важных момента: с какой целью внедряется система контроля доступа и какой ожидается эффект от ее внедрения.

Условный экономический эффект от внедрения СКУД может оцениваться как снижение затрат на содержание персонала охраны за вычетом стоимости аппаратуры, отнесенной на срок ее эксплуатации и затрат по обслуживанию. Косвенный (оперативный) эффект заключается в повышении надежности пропускного режима, усложнении для злоумышленников проникновения на объект и в закрытые для посетителей зоны, в возможности оперативно отслеживать и предотвращать нештатные ситуации. В случае «поголовного» внедрения среди сотрудников объекта идентификационных карточек косвенный эффект может быть достигнут и за счет возможности более четкой организации труда и контроля за ходом трудового процесса. В случае наличия большого количества средств вычислительной техники и при необходимости разграничения доступа к различным вычислительным ресурсам может потребоваться создание сети «контрольно-пропускных пунктов» для операторов автоматизированных рабочих мест, что также может быть реализовано в СКУД.

Особенностью отдельных объектов может быть их представительский характер (в отличие от режимных объектов), требующий достаточно «гуманного» пропускного режима. Это должно выражаться во внешней простоте процесса контроля и его малозаметности. Но требования надежности контроля должны соблюдаться неукоснительно.

Обычно зоны особого внимания (складские помещения, комнаты и залы с важнейшей аппаратурой) не требуют высокой скорости осуществления процесса контроля, основной фактор - это, прежде всего, надежность, а не время контроля.

С учетом возможностей существующих СКУД и особенностей объектов основной целью внедрения аппаратуры СКУД является разграничение доступа для сотрудников различных подразделений, надежный запрет доступа посторонних лиц в особо охраняемые помещения и контроль доступа лиц, не относящихся к персоналу. При этом следует помнить, что аналогичные задачи должны решаться и в АСОИ, обслуживающей проектируемую (внедряемую, модернизируемую) СКУД.

Более предпочтительно, чтобы структура СКУД для особо важных объектов была распределенной, это обеспечивает максимальную живучесть аппаратно-программных средств системы в целом.

В качестве аппаратуры контроля за доступом лиц к особо охраняемым зонам целесообразно применять терминалы для проведения аутентификации по отпечаткам пальцев или по узору сетчатки глаза.

К подзадачам контроля доступа, требующим реализации эффективных мер безопасности, следует отнести задачи, решаемые системой доступа к вычислительным ресурсам (рабочие места операторов и пользователей ПК).

Здесь целесообразно применение идентификационных карточек с искусственным интеллектом (смарт-карты). При высокой плотности размещения рабочих мест возможно применение контактных карточек или бесконтактных с ограниченным радиусом действия (опрос/ответ).

К более низкому уровню контроля доступа можно отнести остальных пользователей. Если не стоит задача поголовного охвата сотрудников системой контроля доступа, то входные двери в помещения могут быть оборудованы терминалами для считывания карт. Помещения для хранения материальных ценностей целесообразно оборудовать подобными терминалами с кодонаборными устройствами.

Если же предполагается полный охват персонала системой контроля доступа, то целесообразно ориентироваться на интеллектуальные бесконтактные идентификационные карточки или пластиковые ключи.

Поскольку взаимодействие считывающих терминалов с контроллерами системы осуществляется по стандартному интерфейсу, в общем случае тип считывающего терминала большой роли не играет. Эта особенность должна учитываться при выборе типа аппаратуры

В качестве центральной ПЭВМ системы и ее ПО целесообразно выбирать то, которое позволяло бы осуществлять формирование на экране дисплея поэтажных планов, а систему общения ПК - оператор построить максимально комфортной (например, с помощью пиктограмм). Это создает предпосылки для уменьшения времени реакции оператора на информацию (что особенно важно в экстренных случаях).

В процессе выбора СКУД (и ИСБ) для крупных распределенных предприятий необходимо обращать внимание на следующие важные моменты и дополнительные требования к программному комплексу:

- требуемый функционал должен быть заранее определен (прописан заказчиком или инсталлятором). Необходимо проверить выбранный продукт на соответствие данному функционалу;
- мультиплатформенный ПК снимет ограничения на выбор оборудования и ПО, он будет функционировать на различных аппаратно-программных платформах, т. е. не придется «подгонять» их под узкоспециализированные требования конкретного ПК;
- разработчик должен быть доступен, поскольку сложные и крупные системы часто требуют доработки программной части с учетом потребностей конкретного заказчика;
- если ПК построен по модульному принципу, создание новых драйверов, скорее всего, не вызовет больших сложностей у разработчика. Некоторые из них предоставляют пользователям возможность самим разрабатывать драйверы. В этом случае важно понять, отделен ли пользовательский интерфейс от драйверов оборудования и есть ли

развитая система контроля прав пользователей. Этот фактор в значительной степени влияет на безопасность;

- следует убедиться, возможна ли интеграция ПК с информационными системами организации. Конечно, это лишь малая часть того, что необходимо знать при выборе ПК для крупных распределенных СКУД и ИСБ.

6.4.2. Выбор СКУД по техническим показателям

Эффективность использования любых технических средств СКУД зависит от применяемой технологии контроля доступа и квалификации оперативно-технического персонала. При выборе систем необходимо учитывать, что возможность проведения аналитической работы с применением современных программно-аппаратных комплексов СКУД является необходимой качественной характеристикой системы

Должны выполняться следующие требования к структуре и возможностям СКУД:

- сложность СКУД должна соответствовать размерам предприятия (предполагаемым потокам служащих);
- число точек прохода СКУД должно соответствовать требуемому (с учетом перспектив развития);
- автономные контроллеры должны быть рассчитаны на применение различных типов считывателей;
- сетевые контроллеры используют для создания СКУД любой степени сложности;
- реализация дополнительных возможностей: получение отчета о наличии или отсутствии сотрудников, информация о местонахождении сотрудников, ведение табеля учета рабочего времени, формирование временного графика прохода сотрудников; ведение базы данных сотрудников и т. д.;
- комплектность оборудования и возможность работы (совместимость) системы контроля и управления доступом со всеми типами физических исполнительных устройств (ограждения, турникеты, калитки);
- совместимость с техническими системами обнаружения и пожарной сигнализации, управления основным и резервным освещением, средствами связи и тревожной сигнализации, системами видеоконтроля;
- возможность простого расширения системы и перехода к сетевой системе, например, установленные ранее автономные контроллеры должны работать в сетевом режиме.

Большинство особенностей функционирования СКУД определяются их сложностью (табл. 6.2):

Таблица 6.2. Сравнительные характеристики некоторых систем СКУД

*Модель **	*Максимальное число пропусков в СКУД*	*Исполнительные механизмы*	*Основные функции*	*Дополнительные функции*
PERCo-MS-400 (для офисов)	500	Электрозамки и защелки	Контроль доступа в помещение	Дистанционное открытие замка двери
PERCo-MS-600 (для средних предприятий)	1000*	Электрозамки, защелки, турникеты всех типов	Ограничение доступа, разделение полномочий по доступу,отчет о событиях, поддержка многосменных графиков работы	Автоматизированный учет рабочего времени (табель), графическое оформление пропусков
PERCo-SYS-1200 (для крупных предприятий)	12000**	Электрозамки, защелки, турникеты всех типов, шлагбаумы, ворота	Контроль доступа, разделение полномочий по доступу, автоматизированный учет рабочего времени, отчет о событиях on-line, поддержка многосменных графиков работы, графическое отображение объекта, графическое оформление пропусков	Поддержка датчиков ОПС, задание маршрута обхода охраны, видеоидентификация, выдача тревожных сообщений, определение местоположения сотрудников

** Указано число на каждый контроллер, всего в системе до 32000 карт.*
*** С расширением до 32000 карт на каждый контроллер.*

- простая СКУД позволит предотвратить доступ нежелательных лиц, а сотрудникам точно указать те помещения, в которые они имеют право доступа;
- более сложная система позволит, помимо ограничения доступа, назначить каждому сотруднику индивидуальный временной график работы, сохранить и затем просмотреть информацию о событиях за день. Системы могут работать в автономном режиме и под управлением компьютера;
- комплексные СКУД позволяют решить вопросы безопасности и дисциплины, автоматизировать кадровый и бухгалтерский учет, создать

автоматизированное рабочее место охранника Набор функций, выполняемых комплексными системами, дает возможность использовать систему контроля для выполнения конкретных задач именно на вашем предприятии или объекте.

Все большее число производителей СКУД рекламируют контроллеры, которые могут непосредственно подключаться к компьютерной сети - контроллеры с шиной Ethernet. Такие контроллеры обычно дороже контроллеров со стандартным для систем интерфейсом RS485, их применение потребует существенного увеличения количества сетевого (компьютерного) оборудования, что приводит к удорожанию стоимости системы Но контроллеры с таким интерфейсом имеют и очевидное преимущество: если между удаленными территориями объекта нельзя проложить сеть RS-485, но имеется компьютерная сеть (например, между удаленными проходными и главным зданием), то такую проходную можно включить в состав СКУД без дополнительного компьютера.

Кроме того, сеть контроллеров на базе Ethernet избыточна как по стоимости, так и по производительности. Редко находит применение сеть со скоростью передачи 10 Мбит, а тем более 100 Мбит в системе, где в лучшем случае один раз в секунду происходит событие, описание которого занимает пару десятков байт. Но если база данных контроллера составляет несколько десятков тысяч человек и его надо полностью перезагрузить, то Ethernet оказывается предпочтительным.

6.4.3. Выбор СКУД по экономическим показателям

В настоящее время на российском рынке имеется большой выбор систем контроля доступа как иностранного, так и российского производства. Попытка сравнивать системы СКУД разных производителей между собой, анализируя набор технических характеристик (число точек прохода, возможность работы в сети, полноту и удобство опций программного обеспечения и т. п.), ни к чему не приводит. Действительно, любая техническая задача (из области СКУД), решаемая одной из систем, точно также может быть решена с применением оборудования другого производителя.

Представляется целесообразным для сравнения между собой различных систем СКУД использовать более содержательную характеристику - стоимость системы конкретного производителя для реализации типовых или одинаковых функциональных характеристик. Ниже приводятся таблицы стоимости основного оборудования и программного обеспечения СКУД шести наиболее известных в России фирм-производителей (по состоянию на 2006-2007 гг.). Для каждого вида оборудования производился расчет стоимости системы со следующими типовыми характеристиками: число точек прохода- 16, тип считывателей - проксимити-карт, число рабочих мест (компьютеров) - 3, программное обеспечение - сетевое.

При этом использовались следующие условия:

- в стоимость оборудования не включалась стоимость считывателей, исполнительных устройств СКУД и другого вспомогательного оборудования пунктов прохода (дверей, проходных и т. п.);
- при расчетах итоговая стоимость каждой системы делилась на число точек прохода (16);
- исходные данные были взяты из прайс-листов с выставки «Технологии безопасности»;
- все цены приводились в долларах США с учетом НДС (20 %).

Данные, использованные для расчетов, приведены в табл. 6.3. Результаты расчетов показаны на рис. 6.28.

Таблица 6.3. Исходные данные для расчета стоимости систем контроля

Наименование	*Цена*	*Кол-во*	*Сумма*
СКУД «TSS-2000» фирмы «Семь печатей -TSS»			
Контроллер TSS-201-8W в корпусе с блоком питания и аккумулятором 7А-ч	1000	*2*	2400
Модуль BIT-4.3 (согласование интерфейсов RS-422/RS-232)	80	1	80
ПО TSS-2000Profi (сетевое, 3 рабочих места)	670	1	670
Программный модуль TSS-ImageCard (создание печати пропусков)	350	1	350
Итого:			3500
Итого в расчете на одну дверь:			218,75
СКУД «КОДОС»			
Сетевой контроллер КОДОС-СК-ЕС	230	1	230
Контроллер КОДОС-ЕС-202	249	8	1992
Адаптер КОДОС-АД-07 (для подключения считывателей с интерфейсом Виганда)	55	16	880
Блок питания контроллеров (КОДОС Р-01)	98	2	196
ПО базовое	280	1	280
Программный модуль контроля доступа	480	1	480
Программный модуль учета рабочего времени	40	1	40
Программный модуль графических планов	75	1	75
Программный модуль конфигурирования системы	95	1	95
Программный модуль персонализации карт доступа	95	1	95
Программный модуль удаленного администрирования	330	1	330
Итого:			4693
Итого в расчете на одну дверь			293
СКУД «APOLLO»			
Контроллер AAM-16	900	1	900

Наименование	*Цена*	*Кол-во*	*Сумма*
Модуль AIM-4 для 4 считывателей	960	4	3840
Внешний конвертер APC-10P1 (конвертер RS-485/RS-232)	220	1	220
Короб СБГ1-1 2-1.0 (с блоком питания, для установки контроллера AAM-16 или модуля AIM-4)	160	5	800
Терминатор ATM-48 (для линии RS-485)	12	2	24
НО APACS-Mini-Std-Mu 2.3 (стандартное многопользовательское, 1 рабочее место)	308	1	308
Стоимость ПО за дополнительное раб. место	420	2	840
Итого:			6932
Итого в расчете на одну дверь:			433
СКУД «PERCo-SYSTEM-12000»			
Контроллер PERCo-SC-12100	465	8	3720
Драйвер замка PERCo-DL-12001	80	8	640
Драйвер входов/выходов DI-12001	95	8	760
Блок питания контроллера (12В, 1,2А)	18	8	144
Аккумулятор (7А-ч)	8	15	120
ПО PERCo-SN-12100.01 (сетевое с модулем оформления пропусков)	1650	1	1650
Программный модуль «Учет рабочего времени»	550	1	550
Итого:			7584
Итого в расчете на одну дверь:			474
СКУД «NORTHERN»			
Контроллер N-1000-1V (в корпусе с аккумулятором)	1009	4	4036
Интерфейсный модуль N-485-PC1	186	1	186
Трансформатор к контроллеру N-1000-1V	39	4	156
Демпфирующая перемычка к замку	21,25	16	340
ПО W1N-PAK 1.16	418	3	1254
Итого:			5972
Итого в расчете на одну дверь:			373
СКУД «KANTECH SYSTEMS»			
Контроллер KT-200 (в корпусе без трансформатора)	699	8	5592
ПЗУ контроллера KT-200 для ПО KL-8000	20	8	160
Коммуникационный интерфейс VC-485 (RS-232/RS-485)	170	1	170
Трансформатор в корпусе ИЭП-26313/26	18	8	200
ПО KL-8000, 5 рабочих станций, 1 ветвь х 32 считывателя	1875	1	1875
Итого:			7997
Итого в расчете на одну дверь:			500

Наименование	*Цена*	*Кол-во*	*Сумма*
СКУД «FORSEC»			
Сетевой контроллер FS-4W	810	*4*	3240
Контроллер сети FS-CT	180	1	180
Профессионально многопользовательское ПО ForSec	980	1	980
Итого:			4400
Итого в расчете на одну дверь:			275

Рис. 6 28. Стоимость основного оборудования и программного обеспечения СКУД различных фирм в расчете на один пункт прохода (дверь)

Таблица 6.4. Стоимость СКУД различных фирм в расчете на один пункт прохода

Тип	*Приведенная стоимость*	*Ранг*	*Выбор*
«TSS-2000» фирмы «Семь Печатей -TSS»	218.75	1	
КОДОС	293	3	
APOLLO	433	5	
PERCo-SYSTEM-12000	474	6	
NORTHERN	373	4	
KANTECH SYSTEMS	500	7	
FORSEC	275	2	

Путем простого сравнения определяем, что при прочих равных условиях приведенная стоимость СКУД минимальна у системы TSS-2000 фирмы «Семь Печатей -TSS».

6.4.4. Выбор биометрических СКУД

Методы биометрической идентификаций различны; каждый их них имеет свои достоинства и недостатки и востребован в своей области применения. Тем не менее, после анализа различных устройств можно суммировать основные преимущества и недостатки наиболее популярных типов биометрических идентификаторов. Результат этого анализа представлен в табл. 6.5.

Таблица 6.5. Преимущества и недостатки биометрических идентификаторов

Свойство	*Отпечатки пальцев*	*Кисть руки*	*Радужная оболочка глаза*	*Лицо*
Точность верификации и идентификации	Высокая для верификации, средняя для идентификации	Высокая для верификации, низкая для идентификации	Высокая для верификации и идентификации	Средняя для верификации, низкая для идентификации
Число отказов в доступе	Среднее, зависит от пользователя и среды	Среднее, зависит от пользователя и среды	Низкое, слабо зависит от пользователя и среды	Среднее, зависит от пользователя и среды
Скорость прохода	Высокая	Высокая	Высокая	Средняя
Удобство сканирования	Контактный	Контактный	Бесконтактный, требования к позиционированию головы и взгляда	Бесконтактный, требования к позиционированию головы
Требования к производительности	Средние	Низкие	Высокие	Высокие
Возможность построения шаблона	Средняя	100%	Высокая	100%
Факторы, влияющие на распознавание	Влажность воздуха, загрязнения, сухость и повреждения кожи	Повреждения, артрит, опухоль руки	Плохое зрение, освещение, очки, контактные линзы	Очки, тип прически, освещение, возрастные изменения

Самыми *надежными* являются сканеры радужной оболочки или сетчатки глаза. Незначительно отстают от них сканеры отпечатков пальцев, лица или отпечатков ладони. Надежность этих устройств выше, чем у сканеров голоса или подписи, но ниже, чем у защиты с помощью паролей или аутентификационных жетонов.

На биометрические устройства аутентификации могут *влиять условия окружающей* среды. Оптические сканеры имеют небольшие размеры, и их лучше использовать в офисах. Однако они, вероятно, не подойдут для применения в помещениях, где много пыли, высокая влажность или присутствуют другие загрязнения. Грязные, жирные или неправильно позиционируемые по отношению к объективу пальцы, руки или лица могут привести к некорректному считыванию устройством информации. Очки, контактные линзы, специфическое освещение и неправильное расположение видеокамеры способны отрицательно повлиять на надежность работы

сканеров радужной оболочки или сетчатки глаза. Фоновые шумы и изменение голоса человека из-за болезни или стресса приводят к ошибкам в системах распознавания голоса.

Проведя выбор типа биопризнака, можно провести ранжирование биометрических СКУД различных производителей. Так, создатели всех биометрических устройств предъявляют *специфические требования к программным и аппаратным средствам.* Необходимо уточнить, есть ли у предприятия необходимые ресурсы для поддержки избранного устройства и сможет ли это устройство работать с имеющимся сетевым ПО, кроме того, выяснить, требуется и имеется ли в наличии внешний источник питания или порт USB

Всевозможные страхи и *культурные* и *религиозные предрассудки* тоже могут работать против выбора биометрических СКУД. Необходимо знать мнение служащих о том, как они воспринимают идею использовать для аутентификации биометрические устройства, и провести испытания устройства, чтобы узнать, способны ли они (служащие) аккуратно использовать его.

Одновременно с введением биометрических СКУД злоумышленники уже нашли способы обманывать биометрические устройства Отпечатки пальцев можно снять с любой гладкой поверхности, даже прямо со сканера отпечатков пальцев, с помощью графитового порошка и куска клейкой ленты или желатина. Сканеры радужной оболочки несложно обмануть, используя фотографию глаза пользователя, сделанную с высоким разрешением. Чтобы обнаружить обман, новейшие устройства регистрируют «признаки жизни», в частности пульсацию кровеносных сосудов.

Для биометрических устройств приемлемый порог неудач в распознавании устанавливается на основе процента ложных разрешений на допуск (False Acceptance Rate - FAR) и процента ложных отказов в допуске (False Rejection Rate - FRR). FAR соответствует вероятности того, что биометрическое устройство ошибочно признает пользователя, а FRR - что оно ошибочно отвергнет его. Если администратор занижает порог отказа в допуске, то система будет более «снисходительно» оценивать совпадение хранимого в устройстве биометрического образца с данными пользователя, и, естественно, увеличится вероятность, что она по ошибке разрешит вход постороннему. Устанавливая порог слишком высоко, мы увеличиваем вероятность того, что система будет отвергать вполне легитимных пользователей. Чтобы упростить эксплуатацию системы необходимо убедиться, что пороги устанавливаются и корректируются на месте.

В любой системе аутентификации пользователи сначала должны быть зарегистрированы, т. е. внесены в список допуска. Многие биометрические системы позволяют самостоятельно делать это пользователям. Последние проходят аутентификацию на локальной машине или сервере справочника и затем регистрируются с помощью биометрического устройства. К сожалению, если вы применяете биометрические устройства для повышения надежности аутентификации, но при первоначальной идентификации и аутентифи-

кации целиком полагаетесь на имена и пароли пользователей, то вы не получаете никаких преимуществ в плане защиты. Регистрация пользователей, выполняемая под контролем администратора, эту проблему решает, но она занимает больше времени.

Решив проблемы регистрации, определите, где будете хранить биометрические данные аутентификации. Системы, сохраняющие биометрические данные на локальной машине, могут аутентифицировать пользователя только для работы с этой машиной. Для крупномасштабных инсталляций и для улучшения управляемости решений выбирайте системы с централизованным хранением. Если биометрическое ПО развернуто на всех входящих в систему компьютерах, то пользователи, зарегистрировавшись однажды, смогут иметь доступ ко всем ресурсам.

Для большей надежности следует ввести регистрацию каждого пользователя по нескольким биометрическим харакгеристикам. Некоторые устройства позволяют регистрировать, например, отпечатки всех пальцев на правой руке пользователя. Если что-нибудь случилось с одним пальцем - порез или ожог, то пользователь вправе предложить для аутентификации другой палец, причем ему не придется заново проходить регистрацию.

В любом случае придется использовать аппаратные и программные средства от одного поставщика - интероперабельности в биометрической аутентификации до сих пор не существует, несмотря на старания консорциума BioAPI Consortium выработать стандартные интерфейсы для интеграции биометрических систем. Зато имеются приложения управления аутентификацией, подобные NMAS фирмы Novell и SafeWord PremierAccess фирмы Secure Computing, интегрирующие биометрические и небиометрические методы аутентификации для доступа к справочникам.

Интеграция приложений все еще определяется взаимоотношениями поставщиков, поэтому очень важно убедиться, что выбранное устройство поддерживает ваши приложения или что поставщик не против того, чтобы заняться интеграцией специально для вас. Интеграция с настольными компьютерами или серверами обычно осуществляется с помощью модулей PAM (Plugable Authentication Module) для ОС Unix, G1NA (Graphical Identification and Authentication) для ОС Windows или модулей Novell eDirectory LCM (Login Client Module) Все время, пока имя и пароль пользователя хранятся в кэш-памяти компьютера, они могут использоваться для доступа к приложениям. Однако если приложение требует отдельной регистрации, то необходимой может оказаться разработка дополнительного ПО.

Для контроля доступа к критически важным данным не следует применять одни лишь биометрические устройства, пока вы тщательно не протестируете эту технологию. Если цель состоит в том, чтобы обеспечить строгую аутентификацию, то необходимо задействовать более проверенные методы - аппаратные и программные жетоны и пароли.

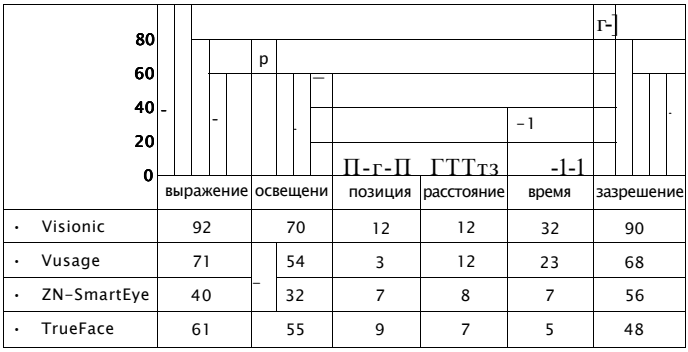
На сегодняшний день разработан ряд коммерческих продуктов, предназначенных для распознавания лиц. Алгоритмы, используемые в этих продуктах, различны и пока еще сложно дать оценку, какая из технологий имеет преимущества. Лидерами в настоящий момент являются системы Visionic, Viisage и Miros. В основе приложения Facelt компании Visionic лежит алгоритм анализа локальных признаков, разработанный в Университете Рокфеллера. Одна коммерческая компания в Великобритании интегрировала Facelt в телевизионную антикриминальную систему под названием Mandrake. Эта система ищет преступников по видеоданным, которые поступают с 144 камер, объединенных в замкнутую сеть. Когда устанавливается идентичность, система сообщает об этом офицеру безопасности. В России представителем компании Visionic является компания «ДанКом».

Другой лидер в этой области - компания Viisage - использует алгоритм, разработанный в Массачусетском технологическом институте. Коммерческие компании и государственные структуры во многих американских штатах и в ряде других стран используют систему компании Viisage вместе с идентификационными удостоверениями, например водительскими правами.

ZN Vision Technologies AG (Германия) предлагает на рынке ряд продуктов, в которых применяется технология распознавания лиц. Эти системы представляются на российском рынке компанией «Солинг».

В системе распознавания лиц TrueFace компании Miros используется технология нейронных сетей, а сама система применяется в комплексе выдачи наличных денег корпорации Mr.Payroll и установлена в казино и других увеселительных заведениях многих штатов США.

В США независимыми экспертами было проведено сравнительное тестирование различных технологий распознавания лиц. Результаты тестирования представлены на рис. 6.29.



	выражение	освещени	позиция	расстояние	время	зазрешение
· Visionic	92	70	12	12	32	90
· Vusage	71	54	3	12	23	68
· ZN-SmartEye	40	32	7	8	7	56
· TrueFace	61	55	9	7	5	48

Рис. 6.29. Сравнительный анализ эффективности распознавания лиц в разных системах

На практике, при использовании систем распознавания лиц в составе стандартных электронных охранных систем предполагается, что человек, которого следует идентифицировать, смотрит прямо в камеру. Таким образом, система работает с относительно простым двумерным изображением, что заметно упрощает алгоритмы и снижает интенсивность вычислений. Но даже в этом случае задача распознавания все же не тривиальна, поскольку алгоритмы должны учитывать возможность изменения уровня освещения, изменение выражения лица, наличие или отсутствие макияжа или очков.

Надежность работы системы распознавания лиц очень сильно зависит от нескольких факторов:

- качество изображения. Заметно снижается вероятность безошибочной работы системы, если человек, которого нужно идентифицировать, смотрит не прямо в камеру или снят при плохом освещении;
- актуальность фотографии, занесенной в базу данных;
- величина базы данных.

Технологии распознавания лица хорошо работают со стандартными видеокамерами, которые передают данные и управляются персональным компьютером, и требуют разрешения 320 х 240 пикселов на дюйм при скорости видеопотока, по крайней мере, 3-5 кадр/с. Для сравнения - приемлемое качество для видеоконференции требует скорости видеопотока уже от 15 кадр/с. Более высокая скорость видеопотока при более высоком разрешении ведет к улучшению качества идентификации. При распознавании лиц с большого расстояния существует сильная зависимость между качеством видеокамеры и результатом идентификации. Объем баз данных при использовании стандартных персональных компьютеров не превышает 10000 изображений.

ПРИЛОЖЕНИЕ 1

УДК 621.398:006.354 Группа П77

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Средства и системы контроля и управления доступом

ГОСТ Р 51241-98

КЛАССИФИКАЦИЯ. ОБЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ. МЕТОДЫ ИСПЫТАНИЙ

Access control systems and units. Classification. General technical requirements. Methods of tests.

ОКС 13.320
ОКП 43 7200

Дата введения 2000-01-01

1. Область применения

Настоящий стандарт распространяется на технические системы и средства контроля и управления доступом, предназначенные для контроля и санкционирования доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

Стандарт устанавливает классификацию, общие технические требования и методы испытаний средств и систем контроля и управления доступом

Настоящий стандарт распространяется на вновь разрабатываемые и модернизируемые средства и системы контроля и управления доступом.

Требования, изложенные в 5.3; 5.4; 5.8, являются обязательными

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ Р 8.568-97 ГСП. Аттестация испытательного оборудования. Основные положения.

ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность. Общие требования.

ГОСТ 12.1.006-84 ССБТ. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля.

ГОСТ 12.1.010-76 ССБТ Взрывоопасность. Общие требования.

ГОСТ 12 1.019—79 ССБТ Электробезопасность. Общие требования и номенклатура видов защиты.

ГОСТ 12.2.003—91 ССБТ. Оборудование производственное. Общие требования безопасности.

ГОСТ 12.2.006-87 (МЭК 65-85). Безопасность аппаратуры электронной сетевой и сходных с ней устройств, предназначенных для бытового и аналогичного общего применения. Общие требования и методы испытаний.

ГОСТ 12.2.007.0-75 ССБТ. Изделия электротехнические. Общие требования безопасности.

ГОСТ 20.57.406-81. Комплексная система контроля качества. Изделия электронной техники, квантовой электроники и электротехнические. Методы испытаний

ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения.

ГОСТ 27.003-90. Надежность в технике. Состав и правила задания требований по надежности.

ГОСТ 12997-84. Изделия ГСП. Общие технические условия.

ГОСТ 14254-96 (МЭК 529-86). Степени защиты, обеспечиваемые оболочками.

ГОСТ 15150-69. Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды.

ГОСТ 16962-71. Изделия электронной техники и электротехники. Механические и климатические воздействия. Требования и методы испытаний.

ГОСТ 16962.1-89. Изделия электротехнические. Методы испытаний на устойчивость к климатическим внешним воздействующим факторам.

ГОСТ 16962.2-90. Изделия электротехнические. Методы испытаний на стойкость к механическим внешним воздействующим факторам.

ГОСТ 17516-72. Изделия электротехнические. Условия эксплуатации в части воздействия механических факторов внешней среды.

ГОСТ 17516.1—90. Изделия электротехнические. Общие требования в части стойкости к механическим внешним воздействующим факторам.

ГОСТ 21552-84. Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение.

ГОСТ 23511-79. Радиопомехи индустриальные от электротехнических устройств, эксплуатируемых в жилых домах или подключаемых к их электрическим сетям. Нормы и методы измерений.

ГОСТ 23773-88. Машины вычислительные электронные цифровые общего назначения. Методы испытаний.

ГОСТ 24686-81. Оборудование для производства изделий электронной техники и электротехники. Общие технические требования. Маркировка, упаковка, транспортирование и хранение.

ГОСТ 26139-84 Интерфейс для автоматизированных систем управления рассредоточенными объектами. Общие требования.

ГОСТ 27570.0—87 (МЭК 335-1-76). Безопасность бытовых и аналогичных электрических приборов. Общие требования и методы испытаний.

ГОСТ 28195-89. Оценка качества программных средств. Общие положения.

ГОСТ 29156-91 (МЭК 801-4-88). Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Технические требования и методы испытаний.

ГОСТ 29191-91 (МЭК 801-2-91). Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Технические требования и методы испытаний.

ГОСТ 30109-94. Двери деревянные. Методы испытаний на сопротивление взлому.

ГОСТ Р 50007-92. Совместимость технических средств электромагнитная. Устойчивость к микросекундным импульсным помехам большой энергии. Технические требования и методы испытаний.

ГОСТ Р 50008-92. Совместимость технических средств электромагнитная. Устойчивость к радиочастотным электромагнитным полям в полосе 26-1000 МГц. Технические требования и методы испытаний.

ГОСТ Р 50009-92 Совместимость технических средств охранной, пожарной и охранно-пожарной сигнализации электромагнитная. Требования, нормы и методы испытаний на помехоустойчивость и индустриальные радиопомехи.

ГОСТ Р 50627-93. Совместимость технических средств электромагнитная. Устойчивость к динамическим изменениям напряжения сети электропитания. Технические требования и методы испытаний.

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

ГОСТ Р 50775-95 (МЭК 839-1-1-88). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения.

ГОСТ Р 50776-95 (МЭК 839-1^1-89). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.

ГОСТ Р 50862-96. Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость.

ГОСТ Р 50941-96. Кабина защитная. Общие технические требования и методы испытаний.

ГОСТ Р 51072-97. Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому и пулестойкость.

ГОСТ Р 51112-97 Средства защитные банковские. Требования по пулестойкости и метод испытаний.

3. Определения, обозначения и сокращения

В настоящем стандарте применяют следующие термины с соответствующими определениями

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

Несанкционированный доступ - доступ людей или объектов, не имеющих права доступа.

Санкционированный доступ - доступ людей или объектов, имеющих права доступа.

Контроль и управление доступом (КУД) - комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

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

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

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

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

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 т. д.).

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

Запоминаемый код - код, вводимый вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.

Устройства преграждающие управляемые (УПУ) - устройства, обеспечивающие физическое препятствие доступу людей, транспорта и других объектов и оборудованные исполнительными устройствами для управления их состоянием (двери, ворота, турникеты, шлюзы, проходные кабины и т. п. конструкции).

Устройства исполнительные - устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические и электромагнитные замки, защелки, механизмы привода шлюзов, ворог, турникетов и т. д.).

Устройства ввода идентификационных признаков (УВИП) - электронные устройства, предназначенные для ввода запоминаемого кода, биометрической информации и считывания кодовой информации с идентификаторов. **В** состав **УВИП** входят считыватели и идентификаторы.

Считыватель - устройство в составе УВИП, предназначенное для считывания (ввода) идентификационных признаков.

Устройства управления (УУ) - устройства и программные средства, устанавливающие режим доступа и обеспечивающие прием и обработку информации с **УВИП,** управление **УПУ,** отображение и регистрацию информации.

Точка доступа - место, где непосредственно осуществляется контроль доступа (например дверь, турникет, кабина прохода, оборудованные считывателем, исполнительным механизмом, электромеханическим замком и другими необходимыми средствами).

Зона доступа - совокупность точек доступа, связанных общим местоположением или другими характеристиками (например, точки доступа, расположенные на одном этаже).

Временной интервал доступа (окно времени) - интервал времени, в течение которого разрешается перемещение в данной точке доступа.

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

Правило двух (и более) лиц - правило доступа, при котором доступ разрешен только при одновременном присутствии двух пли более людей.

Пропускная способность - способность средства или системы КУД пропускать определенное количество людей, транспортных средств и т. п. в единицу времени.

Несанкционированные действия (НСД) - действия, целью которых является несанкционированное проникновение через УПУ.

Взлом - действия, направленные на несанкционированное разрушение конструкции.

Вскрытие - действия, направленные на несанкционированное проникновение через УПУ без его разрушения.

Манипулирование - действия, производимые с устройствами контроля доступа без их разрушения, целью которых является получение действующего кода или приведение в открытое состояние заграждающего устройства. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него; следы такого действия

не будут заметны. Манипулирование включает в себя также действия над программным обеспечением.

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

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

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

Саботаж (состояние саботажа по ГОСТ Р 50776) - преднамеренно созданное состояние системы, при котором происходит повреждение части системы.

Устойчивость к взлому - способность конструкции противостоять разрушающему воздействию без использования инструментов, а также с помощью ручных и других типов инструментов.

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

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

4. Классификация

4.1. Классификация средств КУД.

4.1.1. Средства КУД классифицируют по:

- функциональному назначению устройств;
- устойчивости к НСД.

4.1.2. Средства КУД по функциональному назначению устройств подразделяют на:

- устройства преграждающие управляемые (УПУ) в составе преграждающих конструкций и исполнительных устройств;
- устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;
- устройства управления (УУ) в составе аппаратных и программных средств.

4.1.3. УПУ классифицируют по виду перекрытия проема прохода и по способу управления.

По виду перекрытия проема прохода УПУ могут быть:

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

По способу управления УПУ могут быть:

- с ручным управлением;
- с полуавтоматическим управлением,
- с автоматическим управлением.

4.1.4. УВИП классифицируют по следующим признакам:

- по виду используемых идентификационных признаков;
- по способу считывания идентификационных признаков.

По виду используемых идентификационных признаков УВИП могут быть:

- *механические* - идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т. д.);
- *магнитные* - идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т. д.);
- *оптические* - идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т. д.);
- *электронные* - идентификационные признаки представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т. д.);
- *акустические* - идентификационные признаки представляют собой кодированный акустический сигнал;
- *биометрические* - идентификационные признаки представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т. д.);
- комбинированные - для идентификации используются одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков УВИП могут быть:

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

4.1.5. Классификацию УУ, включающих аппаратные, программные и программно-аппаратные средства, проводят в составе систем КУД.

4.1.6. Средства КУД к информации представляют собой программные, технические и программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации.

К этим средствам относятся также специальные защитные знаки (СЗЗ). СЗЗ представляют собой продукты, созданные на основе физико-химических технологий и предназначенные для контроля доступа к объектам защиты, а также для защиты документов, идентифицирующих личность, от подделки.

4.2. Классификация систем КУД.

4.2.1. Системы КУД классифицируют по:

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

4.2.2. По способу управления системы КУД могут быть:

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

4.2.3. По количеству контролируемых точек доступа системы КУД могут быть:

- малой емкости (менее 16 точек);
- средней емкости (не менее 16 и не более 64 точек);
- большой емкости (64 точки и более).

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

1 - системы с ограниченными функциями;

2 - системы с расширенными функциями;

3 - многофункциональные системы.

В системы любого класса могут быть введены специальные функции, которые определяются дополнительными требованиями заказчика.

4.2.5. По виду объектов контроля системы КУД могут быть:

- для контроля доступа физических объектов;
- для контроля доступа к информации.

4.3. Классификация средств и систем КУД по устойчивости к НСД.

4.3.1. Средства КУД классифицируют по устойчивости к НСД, которая определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости:

- нормальной;
- повышенной;
- высокой.

4.3.2. УПУ и УВИП классифицируют по устойчивости к разрушающим воздействиям. Устойчивость УПУ устанавливают по:

- устойчивости к взлому;
- пулестойкости;
- устойчивости к взрыву.

Устойчивость УВИП устанавливают по устойчивости считывателя к взлому. Для УПУ повышенной и высокой устойчивости устанавливают дополнительно 5 классов по показателям устойчивости (1-й класс - низший).

4.3.3. По устойчивости к неразрушающим воздействиям средства и системы КУД в зависимости от их функционального назначения классифицируют по следующим показателям:

- устойчивости к вскрытию - для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивости к манипулированию;
- устойчивости к наблюдению - для УВИП с запоминаемым кодом (клавиатуры, кодовые переключатели и т. п.);
- устойчивости к копированию (для идентификаторов);
- устойчивости защиты средств вычислительной техники УУ от несанкционированного доступа к информации.

4.3.4. Классификация по устойчивости к вскрытию, манипулированию, наблюдению, копированию должна быть указана в стандартах и других нормативных документах на средства КУД конкретного типа.

4.3.5. Класс защищенности от несанкционированного доступа к информации должен быть указан в нормативных документах на средства или системы КУД конкретного типа.

4.3.6. Классификацию систем КУД по защищенности от несанкционированного доступа к информации проводят по таблице А.1 приложения А.

4.3.7. Классификацию средств КУД по устойчивости от несанкционированного доступа к информации проводят по таблице Б. 1 приложения Б.

4.4. Условные обозначения средств и систем КУД.

4.4.1. Условные обозначения средств и систем КУД указывают в стандартах и (или) нормативных документах на средства и системы КУД конкретного типа.

Размещение символа условного обозначения должно быть частью технической информации и не должно быть совмещено с обозначением торговой марки.

4.4.2. Условное обозначение систем КУД в документации и при заказе должно содержать:

а) название «Система»;

б) название класса системы по количеству контролируемых точек доступа и по способу управления;

в) обозначение КУД;

г) три символа (первый и второй с точкой), обозначающие:

- класс системы по функциональным возможностям;
- степень жесткости по устойчивости к электромагнитным помехам;
- класс защищенности системы от несанкционированного доступа к информации для систем повышенной и высокой устойчивости к НСД или буква «Н» для систем нормальной устойчивости;

д) обозначение настоящего стандарта;

е) условное обозначение по нормативной документации изготовителя или поставщика.

Пример условного обозначения системы сетевой малой емкости второго класса по функциональным возможностям, первой категории по устойчивости к электромагнитным помехам и класса ЗА по защищенности системы от несанкционированного доступа к информации:

Система малой емкости сетевая КУД-2.1.Н ГОСТ Р ХКХХХ АБВГ.ХХХХХ ТУ.

5. Общие технические требования

5.1. Общие положения.

5.1.1. Средства и системы КУД должны изготовляться в соответствии с требованиями настоящего стандарта, ГОСТ Р 50775, а также стандартов и других нормативных документов на средства и системы КУД конкретного типа.

5.1.2. Средства и системы КУД должны обеспечивать возможность как круглосуточной, так и сменной работы, с учетом проведения регламентного технического обслуживания.

5.1.3. Средства КУД, предназначенные для построения систем, должны обладать конструктивной, информационной, надежностной и эксплуатационной совместимостью.

Параметры и требования, определяющие совместимость средств, должны быть установлены в зависимости от назначения и условий применения в нормативных документах на средства и системы КУД конкретного типа.

5.1.4. Требования к средствам контроля доступа вида «специальные защитные знаки» (СЗЗ) устанавливают по документу [2].

5.2. Требования назначения.

5.2.1. Требования к функциональным характеристикам систем КУД.

5.2.1.1 Автономные системы КУД должны обеспечивать:

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

5.2.1.2. Дополнительные характеристики автономных систем в зависимости от класса по функциональным характеристикам приведены в табл. П1.

Таблица П1. Функциональные характеристики автономных систем

Функциональные характеристики автономной системы	*Класс систем*		
	1	*2*	*3*
1 Установка уровней доступа	-	+ / -	+
2. Установка временных интервалов доступа	-	+ / -	+
3. Возможность установления времени открывания УПУ	-	+ / -	+
4. Защита от повторного использования идентификатора для прохода в одном направлении	-	+ / -	+
5. Ввод специального идентификационного признака для открывания под принуждением	-	+ / -	+
6. Подключение УВИП различных типов	-	+ / -	+ / -
7. Доступ по «правилу двух (и более) лиц»	-	+ / -	+ / -
8 Световая индикация о состоянии доступа	+ / -	+	+
9. Контроль состояния УПУ	+ / -	+	+
10. Световое и (или) звуковое оповещение о попытках НСД	+ / -	+ / -	+

Функциональные характеристики автономной системы	*Класс систем*		
	1	*2*	*3*
11. Регистрация и хранение информации о событиях в энергонезависимой памяти	-	+	+
12. Количество событий, хранимых в энергонезависимой памяти, не менее	-	16	64
13 Ведение даты и времени возникновения событий	-	+ / -	+
14. Возможность подключения принтера для вывода информации	-	+ / -	+
15. Возможность передачи информации на устройства сбора информации или ЭВМ	-	+ / -	+
16. Возможность объединения в сеть и обмена информацией с устройствами сбора информации и управления (ЭВМ)	-	+ / -	+
17. Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	-	+ / -	+
18. Возможность интегрирования с системой видеоконтроля на релейном уровне	-	+ / -	+
19. Возможность подключения дополнительных средств специального контроля, средств досмотра	-	-	+ / -
Примечание. Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «-» - отсутствие функции, а знак «+/-» - наличие или отсутствие функции.			

5.2.1.3. Системы КУД с централизованным управлением и универсальные должны соответствовать требованиям 5.2.1 и дополнительно обеспечивать:

- регистрацию и протоколирование тревожных и текущих событий;
- приоритетное отображение тревожных событий;
- управление работой УПУ в точках доступа по командам оператора;
- задание временных режимов действия идентификаторов в точках доступа «окна времени» и уровней доступа;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
- установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т. п.);

- блокировку прохода по точкам доступа командой с пункта управления в случае нападения;
- возможность подключения дополнительных средств специального контроля, средств досмотра.

5.2.1.4. Дополнительные характеристики систем с централизованным управлением в зависимости от класса по функциональным характеристикам, приведены в табл. П2.

Таблица 112. Функциональные характеристики систем с централизованным управлением и универсальных

Функциональные характеристики систем с централизованным управлением (сетевых) и универсальных	*Класс системы*		
	1	*2*	*3*
1. Количество уровней доступа	*2*	8	16
2. Количество временных интервалов доступа	*2*	8	16
3. Защита от повторного использования идентификатора для прохода в одном направлении	+ / -	+	+
4 Ввод специального идентификационного признака для открывания под принуждением	+ / -	+	+
5 Подключение УВИП различных типов	+ / -	+	+
6. Доступ по «правилу двух (и более) лиц»	+ / -	+ / -	+
7. Количество событий, сохраняемых в энергонезависимой памяти контроллеров,не менее	50	250	1000
8. Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	+	+ / -	+ / -
9. Возможность интегрирования с системой видеоконтроля на релейном уровне	+	+ / -	+ / -
10. Возможность интегрирования с системой охраной, пожарной сигнализации и системами видеоконтроля на системном уровне	+ / -	+ / -	+
11. Возможность управления работой дополнительных устройств в точках доступа (освещение, вентиляция, лифты, технологическое оборудование и т. п.)	-	+ / -	+ / -
12. Возможность подключения переговорных устройств и (или) средств связи в точках доступа	-	+ / -	+ / -
13. Обеспечение изображения на экране ЭВМ плана объекта и (или) помещений объекта с указанием мест расположения средств контроля доступа, охранной и пожарной сигнализации, средств видеоконтроля и графическим отображением тревожных состояний в контрольных точках на плане	+ / -	+ / -	+

Фунциональные характеристики систем с централизованным управлением (сетевых) и универсальных	*Класс системы*		
	1	*2*	*3*
14. Интерактивное управление средствами по изображению плана объекта на экране ЭВМ	-	-	+ / -
15. Ведение баз данных на сотрудников (пользователей)	+ / -	+	+
16. Поддержание фотографических данных пользователей в базе данных	-	+ / -	+
17. Контроль за перемещением и поиск сотрудников	+ / -	+ / -	+
18. Контроль времени нахождения на объекте посетителей	+ / -		+
Примечание. Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «-» - отсутствие функции, а знак «+/-» - наличие или отсутствие функции.			

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

5.2.1.6. Значения характеристик и требования, приведенные в пп. 5.2.1.1-5.2.1.5, должны быть установлены в стандартах и (или) технических условиях на системы КУД конкретного типа.

Системы КУД должны также иметь следующие характеристики, значения которых должны быть установлены в стандартах и (или) технических условиях на системы конкретного типа:

- максимальное количество точек доступа, зон доступа, пользователей, обслуживаемых системой;
- максимальное количество точек доступа, обслуживаемых одним УУ;
- количество и вид временных интервалов доступа (окон времени), уровней доступа;
- количество видов УВИП, используемых в системе,
- время реакции системы на заявку на проход;
- максимальное расстояние от наиболее удаленной точки доступа до пункта управления;
- максимальное расстояние действия считывателя (для бесконтактных считывателей);
- максимальное время хранения информации о событиях в памяти системы;
- максимальная пропускная способность системы в точках доступа;

- вероятность несанкционированного доступа, вероятность ложного задержания (требования обязательны для СКУД с биометрической идентификацией, для остальных допускается не указывать);
- показатели по уровням устойчивости к НСД.

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

5.2.2. Требования к функциональным характеристикам УПУ.

5.2.2.1. УПУ должны обеспечивать:

- полное или частичное перекрытие проема прохода;
- ручное, полуавтоматическое или автоматическое управление;
- блокирование человека или объекта для УПУ блокирующего тина.

5.2.2.2. УПУ в дежурном режиме могут быть в нормально открытом или нормально закрытом состоянии.

УПУ с частичным перекрытием проема прохода могут быть, при необходимости, обеспечены средствами сигнализации, срабатывающими при попытке обхода заграждающего устройства.

Для УПУ, используемых на проходных или в других местах с большими потоками людей, в стандартах или технических условиях на УПУ конкретного типа должны быть установлены показатели пропускной способности.

5.2.2.3. УПУ в закрытом состоянии должны обеспечивать физическое препятствие перемещению людей, транспорта и других объектов в (из) помещение, здание, зону или на территорию и открывание запирающего механизма при подаче управляющего сигнала от устройства управления.

Параметры управляющего сигнала (напряжение, ток и длительность) должны быть указаны в стандартах и (или) нормативных документах на УПУ конкретного типа.

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

5.2.2.4 УПУ при необходимости могут иметь защиту от прохода через них одновременно двух или более человек.

5.2.2.5. УПУ должны иметь возможность механического аварийного открывания в случае пропадания электропитания, возникновения пожара или других стихийных бедствий. Аварийная система открывания должна быть защищена от возможности использования ее для несанкционированного проникновения.

5.2.2.6. Умышленное повреждение внешних электрических соединительных цепей и элементов блокировки не должно приводить к открыванию УПУ.

Должны быть предусмотрены меры по защите внешних электрических соединительных цепей от возможности подачи по ним напряжений, приводящих к нарушению работы или к открыванию УПУ.

5.2.2.7. УПУ могут иметь дополнительно средства специального контроля, встроенные или совместно функционирующие. Требования к УГ1У, в состав которых входят средства специального контроля, устанавливаются в нормативных документах на устройства конкретного типа.

5.2.3. Требования к функциональным характеристикам УВИП.

5.2.3.1. Считыватели УВИП должны обеспечивать:

- возможность считывания идентификационного признака с идентификаторов;
- введение биометрической информации (для считывателей биометрической информации);
- преобразование введенной информации в электрический сигнал;
- передачу информации на УУ.

5.2.3.2. УВИП должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды защиты должны быть указаны в стандартах и (или) нормативных документах на УВИП конкретного типа.

5.2.3.3. Идентификаторы УВИП должны обеспечивать хранение идентификационного признака в течение срока службы и при эксплуатации.

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

5 2.3.5. Производитель идентификаторов должен гарантировать, что код данного идентификатора не повторится, или указать условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами.

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

5.2.3.7. В стандартах и нормативных документах на конкретные виды идентификаторов должен быть определен минимум кодовых комбинаций. Значение кодовых комбинаций приведено в табл. ПЗ.

Таблица ПЗ. Значение кодовых комбинаций

Уровень устойчивости к НСД	*Количество кодовых комбинаций*
Нормальный	10^2— 10^5
Повышенный	10^5-1 о^7
Высокий	Не менее 10^7

Пользователь автономных систем должен иметь возможность сменить или переустановить открывающий код не менее 100 раз. Смена кода должна происходить только после ввода действующего кода.

5.2.4. Требования к функциональным характеристикам УУ.

5.2.4.1. Аппаратные средства УУ должны обеспечивать прием информации от УВИП, обработку информации и выработку сигналов управления на исполнительные устройства УПУ.

5.2.4.2. Аппаратные средства УУ в системах с централизованным управлением и универсальных должны обеспечивать.

- обмен информацией по линии связи между контроллерами и средствами управления;
- сохранность данных в памяти при обрыве линий связи со средствами централизованного управления, отключении питания и при переходе на резервное питание;
- контроль линий связи между контроллерами и средствами централизованного управления. Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также, при необходимости, защиту информации.

Виды и параметры протоколов и интерфейсов должны быть установлены в стандартах и других нормативных документах на УУ конкретного типа с учетом требований ГОСТ 26139.

5.2.4.3. Программное обеспечение УУ должно обеспечивать:

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

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

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

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

5.2.4.5. Общие показатели качества программного обеспечения следует устанавливать по ГОСТ 28195.

5.3. Требования к электромагнитной совместимости.

5.3.1. Средства и системы КУД в зависимости от устойчивости к воздействию электромагнитных помех должны иметь следующие степени жесткости по ГОСТ Р 50009:

- первая или вторая степень - при нормальной устойчивости;
- третья степень - при повышенной устойчивости;
- четвертая или пятая степень - при высокой устойчивости.

Требования по устойчивости к искусственно создаваемым электромагнитным помехам пред являют к устройствам, имеющим степень жесткости не ниже второй, и должны быть установлены в технических условиях на средства и системы КУД конкретного типа.

5.3.2 Уровень допустимых радиопомех при работе средств и систем КУД должен соответствовать ГОСТ 23511 и ГОСТ Р 50009.

5.4. Требования по устойчивости средств и систем КУД в НСД.

5.4.1. Требования по устойчивости к НСД устанавливают в настоящем пункте и нормативны документах на средства и системы КУД конкретного типа.

5.4.2. Требования по устойчивости к НСД разрушающего действия распространяются на УГП и считыватели УВИП. Требования включают:

- устойчивость к взлому;
- пулестойкость;
- устойчивость к взрыву.

5.4.3. Устойчивость к разрушающим воздействиям устанавливают для средств с повышенным и высоким уровнями устойчивости.

Нормальная устойчивость обеспечивается механической прочностью конструкции без оценки по показателям устойчивости.

Повышенную устойчивость определяют по показателям устойчивости к взлому одиночными ударами и (или) набором инструментов

Высокую устойчивость определяют по показателям устойчивости к взлому, пулестойкости и (или) взрыву.

Требования по пулестойкости применяют только к УПУ с полным (сплошным) перекрытием проема прохода.

Показатели устойчивости по классам приведены в табл. П4.

Таблица П4. Классы УПУ по показателям устойчивости

Показатель устойчивости	*Класс УПУ*				
	1	*2*	*3*	*4*	*5*
1. Защищенность от взлома одиночными ударами	+	+	+	+	+
2. Защищенность от взлома набором инструментов	-	-	-	+	+
3. Пулестойкость	-	-	+	+	+
4. Устойчивость к взрыву	-	-	-	+	+
Примечание. Условный знак «+» означает наличие требования и обязательность его проверки, знак «-» - отсутствие требования, а знак «+» - возможность исполнения УПУ как устойчивыми, так и неустойчивыми к данному виду воздействия.					

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

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

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

5.4.5. Автономные СКУД должны быть защищены от манипулирования с целью изменения или подбора кода защиты должен быть указан в технических условиях на системы конкретного типа.

5.4.6. Системы КУД повышенной и высокой устойчивости к НСД должны иметь защиту от принуждения и саботажных действий Конкретный метод защиты и показатели защиты должны быть приведены в технических условиях на системы КУД конкретного типа.

5.4.7. Программное обеспечение УУ должно быть защищено от несанкционированного доступа. Требования по защите программного обеспечения УУ от несанкционированного доступа устанавливают по ГОСТ Р 50739.

5.4.8. Программное обеспечение УУ должно быть также защищено от:

- преднамеренных воздействий с целью изменения опций в системе;
- несанкционированного копирования;
- несанкционированного доступа с помощью паролей.
- Рекомендуемые уровни доступа по типу пользователей:
- первый («администратор») - доступ ко всем функциям;
- второй («дежурный оператор») - доступ только к функциям текущего контроля;

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

Количество знаков в пароле должно быть не менее шести.

При вводе пароля в систему вводимые знаки не должны отображаться на средствах отображения информации.

После ввода в систему пароли должны быть защищены от просмотра средствами операционных систем ЭВМ.

5.4.9. Требования по защите систем КУД с централизованным управлением и универсальных от несанкционированного доступа к информации должны соответствовать для систем нормальной устойчивости к НСД требованиям 5.4.8 данного стандарта, для систем повышенной и высокой устойчивости требования устанавливают по классам в соответствии с документом [3], и они должны соответствовать приложению А.

При этом класс защиты системы от несанкционированного доступа к информации должен соответствовать:

- 3А, 3Б, 2Б - для систем повышенной устойчивости;
- 1Г и 1В - для систем высокой устойчивости.

5.4.10. Требования по защите средств от несанкционированного доступа к информации устанавливают для средств КУД нормальной устойчивости в соответствии с требованиями настоящего стандарта, для средств КУД повышенной и высокой устойчивости требования устанавливают по классам в соответствии с документом [1], и они должны соответствовать данным приложения Б.

При этом класс защиты средств КУД от несанкционированного доступа к информации должен соответствовать:

- повышенной устойчивости - классу 5 или 6;
- высокой устойчивости - классу 4.

5.4.11. Системы и средства КУД высокой устойчивости подлежат обязательной сертификации по требованиям защиты от несанкционированного доступа к информации.

5.5. Требования надежности.

5.5.1. В стандартах и (или) технических условиях на средства и системы КУД конкретного типа должны быть установлены следующие показатели надежности в соответствии с ГОСТ 27.002 и ГОСТ 27.003:

- 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 устанавливают исходя из необходимости обеспечения надежности системы в целом.

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

5.5.2. Средняя наработка на отказ систем КУД с одной точкой доступа (без учета УПУ) - не менее 10000 ч.

5.5.3. Средний срок службы систем КУД не менее 8 лет с учетом проведения восстановительных работ.

5.6. Требования по устойчивости к внешним воздействующим факторам.

5.6.1 Требования по устойчивости в части воздействия климатических факторов устанавливают в стандартах и нормативных документах на средства и системы КУД конкретного типа в соответствии с климатическим исполнением и категорией изделий по ГОСТ 15150.

5.6.2. Оболочки средств КУД при необходимости защиты от внешних воздействий должны иметь степени защиты по ГОСТ 14254.

5.6.3. Требования по устойчивости в части воздействия механических факторов должны быть установлены в стандартах и (или) нормативных документах на средства и системы КУД конкретного типа в соответствии с требуемой группой условий эксплуатации по ГОСТ 17516 и степенью жесткости изделий по ГОСТ 16962.

5.7. Требования к электропитанию.

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

Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения сети от -15 до +10 % от номинального значения и частоты (50±1) Гц.

Электропитание отдельных средств контроля и управления доступом допускается осуществлять от источников с иными параметрами выходных напряжений, требования к которым устанавливают в нормативных документах на средства КУД конкретного типа.

5.7.2. Средства и системы КУД должны иметь резервное электропитание при пропадании напряжения основного источника питания. В качестве резервного источника питания допускается использовать резервную сеть переменного тока или источник питания постоянного тока.

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

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

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

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

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

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

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

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

5.8. Требования безопасности

5.8.1. Средства и системы КУД должны соответствовать требованиям безопасности ГОСТ 12.2.007.0, ГОСТ 12.2.006 и ГОСТ 27570.0.

5.8.2. Материалы, комплектующие изделия, используемые для изготовления средств и систем КУД, должны иметь токсико-гигиенический паспорт, гигиенический паспорт и гигиенический сертификат.

5.8 3. Монтаж и эксплуатация средств и систем КУД должны соответствовать требованиям безопасности ГОСТ 12.2.003.

5.8.4. Средства и системы КУД должны соответствовать требованиям пожарной безопасности ГОСТ 12.1.004

5.8 5. Электрическое сопротивление изоляции средств и систем КУД между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должно быть не менее значений, указанных в табл. П5.

Таблица 115. Требуемые значения сопротивления изоляции

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

5.8.6. Электрическая прочность изоляции средств и систем КУД между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должна соответствовать требованиям ГОСТ 12997.

5.8.7. Сопротивление изоляции и электрическая прочность средств и систем КУД, предназначенных для бытового и аналогичного общего применения, должны соответствовать требованиям ГОСТ 12.2.006 и ГОСТ 27570.0.

5.8 8. Для средств КУД, работающих при напряжениях не выше 12 В переменного тока и 36 В постоянного тока, допускается не приводить значение электрической прочности изоляции и ее сопротивления в нормативных документах на конкретные средства.

5.8.9. Конкретные значения сопротивления изоляции и электрическая прочность изоляции должны быть указаны в технических условиях на средства и системы КУД конкретного типа.

5.8.10. Уровни излучений средств и систем КУД должны соответствовать требованиям безопасности, установленным в ГОСТ 12.1.006.

5.8.11. Средства и системы КУД, предназначенные для эксплуатации в зонах с взрывоопасной средой, должны соответствовать требованиям ГОСТ 12.1.010, других стандартов и нормативных документов, регламентирующих требования к изделиям, предназначенным для работы во взрывоопасных средах.

5.9. Требования к конструкции.

5.9.1. Габаритные размеры средств КУД и их отдельных функционально и конструктивно оформленных устройств, блоков должны обеспечивать транспортирование через типовые проемы зданий, сборку, установку и монтаж - на месте эксплуатации.

5.9.2. Конструкции средств КУД должны быть построены по модульному и блочно-агрегатному принципу и обеспечивать:

- взаимозаменяемость сменных однотипных составных частей;
- удобство технического обслуживания, эксплуатации и ремонтопригодность;

- исключение возможности несанкционированного доступа к элементам управления параметрами;
- доступ ко всем элементам, узлам и блокам, требующим регулирование или замену в процессе эксплуатации.

5.9.3. Конструкционные и электроизоляционные материалы, покрытия и комплектующие изделия должны обеспечивать:

- механическую прочность;
- требуемую надежность;
- устойчивость к несанкционированным действиям по категориям и классам устойчивости;
- безопасную работу в заданных условиях эксплуатации.

5.10. Требования к маркировке.

5.10.1. Маркировка средств и систем КУД должна быть выполнена по ГОСТ Р 50775 и содержать:

- товарный знак и (или) другие реквизиты предприятия-изготовителя,
- условное обозначение средств и систем КУД;
- серийный номер;
- дату изготовления,
- знак сертификата соответствия (при его наличии).

5.10.2. Номер сертификата или реквизиты заключения (при их наличии), фирменный знак и (или) другие реквизиты организаций, проводивших сертификационные или экспертные испытания, должны быть указаны в сопроводительной документации.

6. Методы испытаний

6.1. Общие положения.

6.1.1. Испытания средств и систем КУД проводят по настоящему стандарту, а также по методикам действующих нормативных документов на отдельные виды испытаний и по техническим условиям на средства и системы КУД конкретного типа.

Объем и последовательность испытаний устанавливают в программе испытаний на средства и системы КУД конкретного типа.

6.1.2. Приборы и оборудование, применяемые при проведении испытании, должны быть поверены и аттестованы по ГОСТ Р 8.568 и обеспечивать требуемую точность измерений.

Оборудование для контроля электрических параметров, радиотехнических измерений должно соответствовать требованиям ГОСТ 24686.

6.1.3. При проведении испытаний должны соблюдаться требования техники безопасности, а также требования ГОСТ 12.2.006, ГОСТ 27570.0 и используемых нормативных документов.

Безопасность проведения работ, использования приборов, инструментов и оборудования должна соответствовать требованиям ГОСТ 12.1.006, ГОСТ 12.1.019, правил [4,5,6].

Помещения для проведения испытаний должны соответствовать необходимому уровню безопасности работ, а приборы и оборудование должны использоваться в соответствии с инструкциями по их эксплуатации.

6.1.4. Образцы, предназначенные для проведения испытаний, должны иметь техническую документацию в объеме, необходимом для проведения испытаний, и быть полностью укомплектованы в соответствии с технической документацией.

6.1.5. Все испытания, кроме климатических, проводят в нормальных климатических условиях по ГОСТ 15150.

6.1.6. Условия испытаний средств КУД по ГОСТ 12997, для УУ и систем КУД дополнительно необходимо учитывать требования ГОСТ 21552.

6.2. Испытания средств и систем КУД на соответствие общим техническим требованиям.

6.2.1. Испытания средств и систем КУД на соответствие функциональным характеристикам (5.2) проводят по методикам, приведенным в стандартах и технических условиях на средства и системы КУД конкретного типа.

6.2.2. Испытания средств и систем КУД на устойчивость к электромагнитным помехам (5.3.1) проводят по ГОСТ Р 50009, ГОСТ 29156, ГОСТ 29191, ГОСТ Р 50007, ГОСТ Р 50008, ГОСТ Р 50627.

6.2.3. Испытания средств и систем КУД на соответствие электромагнитной совместимости и нормам радиопомех (5.3.2) проводят по ГОСТ Р 50009 и ГОСТ 2351 1.

6.2.4. Испытания УПУ и считывателей УВИП на устойчивость к НСД разрушающего воздействия (5.4.2 и 5.4.3) проводят по ГОСТ 30109, ГОСТ Р 50862, ГОСТ Р 50941, ГОСТ Р 51072, ГОСТ Р 51112.

6.2.5. Испытания средств и систем КУД на устойчивость к НСД неразрушающего воздействия (5.4.4-5.4 6) проводят по стандартам и (или) другим нормативным документам на средства и системы КУД конкретного типа.

6.2.6. Испытания УУ по защите программного обеспечения от несанкционированного доступа (5.4.7 и 5.4.8) проводят по ГОСТ Р 50739.

6.2.7. Испытания средств и систем КУД на устойчивость от несанкционированного доступа к информации (5.4.9, 5.4.10) проводят по действующим методикам испытаний организациями, имеющими лицензию на право проведения работ в области защиты информации.

6.2.8. Испытания средств и систем КУД на соответствие требованиям надежности (5.5) проводят по методикам, разработанным с учетом требований ГОСТ 27.003, ГОСТ 23773.

6.2.9. Испытания средств и систем КУД на устойчивость к внешним воздействующим факторам (5.6) проводят по ГОСТ 12997 и/или ГОСТ 21552, ГОСТ 23773 с применением соответствующих методов испытаний по ГОСТ 20.57.406, ГОСТ 16962, ГОСТ 16962.1, ГОСТ 16962.2, ГОСТ 17516, ГОСТ 17516.1.

6.2.10. Испытания средств и систем КУД на соответствие требованиям к электропитанию (5.7) проводят по ГОСТ 12.2.006, ГОСТ 12997, ГОСТ 21552 и ГОСТ 27570.0.

6.2.11. Испытания средств и систем КУД на соответствие требованиям безопасности (5.8) проводят по ГОСТ 12.1.004, ГОСТ 12 2.006, ГОСТ 12997, ГОСТ 27570.0 и техническим условиям на средства и системы КУД конкретного типа.

6.2.12. Проверку конструкции (5.9) и маркировки (5.10) проводят по ГОСТ 23773, а также по стандартам и (или) техническим условиям на средства и системы КУД конкретного типа.

ПРИЛОЖЕНИЕ 2

РД 78.36.003-2002 Руководящий документ «Инженерно-техническая укрепленность. Технические системы охраны. Требования и нормативы проектирования по защите объектов от преступных посягательств» М.: МВД России, НИЦ «Охрана» ГУВО. 06 ноября 2002 г.

7. *Системы контроля и управления доступом*

7.1. Система контроля и управления доступом (СКУД) предназначена для:

- обеспечения санкционированного входа в здание и в зоны ограниченного доступа и выход из них путем идентификации личности по комбинации различных признаков: вещественный код (Виганда-карточки, ключи touch-memory и другие устройства), запоминаемый код (клавиатуры, кодонаборные панели и другие устройства), биометрические признаки (отпечатки пальцев, сетчатка глаз и другие признаки);
- предотвращения несанкционированного прохода в помещения и зоны ограниченного доступа объекта.

7.2. Согласно ГОСТ Р 51241-98 СКУД должна состоять из:

- устройств преграждающих управляемых (УПУ) в составе преграждающих конструкций и исполнительных устройств;
- устройств ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;
- устройств управления (УУ), в составе аппаратных и программных средств.

7.3. Считывателями и УПУ следует оборудовать:

- главный и служебные входы;
- КПП;
- помещения, в которых непосредственно сосредоточены материальные ценности;
- помещения руководства;
- другие помещения по решению руководства объекта.

7.4. Пропуск сотрудников и посетителей на объект через пункты контроля доступа следует осуществлять:

- в здание и в служебные помещения - по одному признаку;
- входы в зоны ограниченного доступа (хранилища ценностей, сейфовые комнаты, комнаты хранения оружия) - не менее чем по двум признакам идентификации.

7.5. СКУД должна обеспечивать выполнение следующих основных функций:

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

- запрет открывания УПУ при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;
- санкционированное изменение (добавление, удаление) идентификационных признаков в УУ и связь их с зонами доступа (помещениями) и временными интервалами доступа;
- защиту от несанкционированного доступа к программным средствам УУ для изменения (добавления, удаления) идентификационных признаков;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
- сохранение настроек и базы данных идентификационных признаков при отключении электропитания;
- ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;
- автоматическое закрытие УПУ при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;
- выдачу сигнала тревоги (или блокировку УПУ на определенное время) при попытках подбора идентификационных признаков (кода);
- регистрацию и протоколирование текущих и тревожных событий;
- автономную работу считывателя с УПУ в каждой точке доступа при отказе связи с УУ.

7.6. На объектах, где необходим контроль сохранности предметов, следует устанавливать СКУД, контролирующих несанкционированный вынос данных предметов из охраняемых помещений или зданий по специальным идентификационным меткам.

7.7. УПУ с устройствами исполнительными должно обеспечивать:

- частичное или полное перекрытие проема прохода;
- автоматическое и ручное (в аварийных ситуациях) открывание;
- блокирование человека внутри УПУ (для шлюзов, проходных кабин),
- требуемую пропускную способность.

7.8 Считыватели УВИП должно обеспечивать:

- считывание идентификационного признака с идентификаторов;
- сравнение введенного идентификационного признака с хранящимся в памяти или базе данных УУ;
- формирование сигнала на открывание УПУ при идентификации пользователя;
- обмен информацией с УУ.

УВИП должны быть защищены от манипулирования путем перебора или подбора идентификационных признаков.

Идентификаторы УВИП должны обеспечить хранение идентификационного признака в течение:

- всего срока эксплуатации - для идентификаторов без встроенных элементов электропитания;
- не менее 3 лет - для идентификаторов со встроенными элементами электропитания.

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

7.9. УУ должно обеспечивать:

- прием информации от УВИП, ее обработку, отображение в заданном виде и выработку сигналов управления УПУ;
- ведение баз данных сотрудников и посетителей объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и другие);
- ведение электронного журнала регистрации проходов сотрудников и посетителей через точки доступа;
- приоритетный вывод информации о тревожных ситуациях в точках доступа;
- контроль исправности и состояния УПУ, УВИП и линий связи с ними.

7.10. Конструктивно СКУД должны строиться по модульному принципу и обеспечивать:

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

7-11- Выбор оборудования СКУД, места его установки на объекте следует проводить в соответствии с Р 78.36.005-99.

ПРИЛОЖЕНИЕ 3

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЛАВНОЕ УПРАВЛЕНИЕ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ

Выбор и применение систем контроля и управления доступом

Рекомендации

Р 78.36.005-99

Данные Рекомендации разработаны сотрудниками НИЦ «Охрана» ГУВО МВД России Н. И. Котовым, Л. И Савчук, Е. П. Тюриным под руководством В. Г. Синилова и утверждены ГУВО МВД России 31 марта 1998 г.

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

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

Введение

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

компании, стараясь заполнить пока еще свободную нишу российского рынка, порой проявляют недобросовестность в рекламе, в предоставлении полной информации о технических и функциональных возможностях систем, об особенностях их эксплуатации в сравнительно сложных климатических условиях и т. п. Зачастую поставщики и продавцы ради прибыли предлагают заказчику аппаратуру низкого качества и неквалифицированные услуги. Повсеместно и сами покупатели не имеют достаточного опыта в этой сфере. В результате на важных объектах можно встретить непрофессионально спроектированные системы СКУД, у которых даже технические характеристики не соответствуют условиям эксплуатации в России. Помимо всего этого среди отечественных пользователей систем не хватает высококвалифицированных специалистов, способных на высоком уровне осуществлять техническое обслуживание и в сжатые сроки устранять дефекты оборудования.

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

1. Основные компоненты СКУД

Системы контроля и управления доступом позволяют осуществлять:

- ограничение доступа сотрудников и посетителей объекта в охраняемые помещения;
- временной контроль перемещений сотрудников и посетителей по объекту;
- контроль за действиями охраны во время дежурства;
- табельный учет рабочего времени каждого сотрудника;
- фиксацию времени прихода и ухода посетителей;
- временной и персональный контроль открытия внутренних помещений (когда и кем открыты);
- совместную работу с системами охранно-пожарной сигнализации и телевизионного видеоконтроля (при срабатывании извещателей блокируются или, наоборот, например при пожаре, разблокируются двери охраняемого помещения или включается видеокамера);
- регистрацию и выдачу информации о попытках несанкционированного проникновения в охраняемое помещение.
- СКУД обычно состоит из следующих основных компонентов:
- устройства идентификации (идентификаторы и считыватели);
- устройства контроля и управления доступом (контроллеры),
- устройства центрального управления (компьютеры).
- устройства исполнительного (замки, приводы дверей, шлагбаумов, турникетов и т.п.).

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

1.1. Устройства идентификации доступа

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

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

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

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

В СКУД существует порядка десяти видов индентификаторов и считывателей, использующих различные способы записи, хранения и считывания кодовой информации, обеспечивающие разный уровень секретности и имеющие существенно отличающиеся цены.

Наиболее широкое распространение получили следующие виды идентификаторов и считывателей.

Карточка перфорированная - карточка из двухслойной недеформируемой пластмассы. Информация записывается на ней с помощью пробивки специальных отверстий один раз при изготовлении. Считывание информации осуществляется оптическим или механическим считывателями. Данная карточка самый простой и дешевый тип идентификатора, но который практически не обеспечивает секретность кода и легко подделывается. Срок службы карточки 1-2 года. Стоимость карточек и механического считывателя достаточно низка: карточка стоит приблизительно 0,5 долл. США, считыватель - приблизительно 100 долл. США. Механический считыватель очень капризен в эксплуатации.

Карточка со штриховым кодом - карточка с нанесенными на поверхность полосами иного цвета, чем остальная поверхность, ширина и расстояние между которыми представляют собой кодовую последовательность. Кодовая последовательность наносится на карточку при ее изготовлении (обычно она определяется генератором случайных чисел), и в дальнейшем не может быть изменена. Код считывается оптическим считывателем (инфракрасным или лазерным). Самые распространенные системы штрихового кодирования, код 39 (3 из 9) и код 25 (2 из 5).

Оптический считыватель не содержит движущихся частей, и при сканировании карточки она не контактирует со считывателем физически. Поэтому считыватель надежен в работе и с успехом может применяться вне помещений. Карточка со штриховым кодом может быть пропущена через считыватель в любом направлении. Вероятность подделки карточки такая же, как и магнитных. Стоимость карточки и считывателя достаточно низка: карточка стоит приблизительно 0,5 долл. США, считыватель - приблизительно 100 долл. США.

Карточка магнитная - карточка с магнитной полосой, на которой записан код. Данный тип носителя является самоочищающимся и не оставляет окислов на считывателе. При желании код, записанный на дорожках магнитной полосы может быть легко перепрограммирован, а при утере карточки можно быстро, дешево и без проблем закодировать новую карточку. Код с карточки считывается магнитным считывателем, принцип работы которого аналогичен считывателю обычного магнитофона: информация считывается при перемещении карточки между магнитными головками считывателя. Карточки с магнитной полосой являются дешевыми, но не очень надежными, так как существует вероятность их подделки. К их недостаткам можно также отнести наличие механического контакта при считывании с головками считывателя, который сокращает срок службы (средний срок службы 1 год) и необходимость очень аккуратного обращения, связанного с возможностью искажения или уничтожения записанной информации в относительно слабых магнитных полях и температур окружающего воздуха свыше 80 °С.

Размер карточки совпадает с кредитными и банковскими карточками, что позволяет использовать уже имеющуюся у пользователя карточку (например, кредитную) для СКУД. При этом из трех магнитных дорожек одна используется для банковской информации, вторая - для СКУД и третья для любой другой информации Стоимость карточек и считывателя достаточно низка: карточка стоит 1-8 долл. США, считыватель в зависимости от типа 100—300 долл. США.

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

тывателя достаточно низка: карточка стоит 3-8 долл. США, считыватель в зависимости от типа стоит 250-460 долл. США. В настоящее время один из самых перспективных типов индентификаторов.

Карточка бесконтактная (Proximity) - карточка, внутри которой расположена микросхема (чип) с записанной в ней информацией. Информация с таких карточек считывается радиочастотным способом на расстоянии от 5 до 90 см (для автомобильных идентификаторов данного типа расстояние считывания достигает 2 м). Карточки делятся на активные и пассивные. В пассивных карточках информация записывается один раз на все время действия карточки, а в активных существует возможность изменения информации в микросхеме. Пассивные карточки питаются энергией, получаемой от считывателя, срок службы их неограничен, и они не могут быть подделаны. Активные - имеют встроенные, незаменяемые батарейки, срок работы которой обычно достаточно велик - до 10 лет. В надежности эти карточки уступают карточкам Виганда, но они более удобны в применении. Считыватель может быть скрытно размещен за не металлической стенкой. Эта технология идеально сочетает эффективный контроль со свободой перемещения. Информация с карточки может быть считана, даже если она находится в кошельке или кармане. Недостатком является невозможность работы при воздействии сильных электромагнитных полей. Стоимость пассивных карточек составляет 2-10 долл. США', считывателя в зависимости от типа 800-3400 долл. США. Стоимость активных карточек приблизительно в 5-10 раз дороже пассивных. Эта карточка незаменима для случаев, когда необходимо обеспечить высокую пропускную способность, скрытность места установки считывателя или дистанционный контроль доступа.

Электронные ключа «тач-мемори» выполнены в виде брелков. Все необходимые данные записываются на заключенную в них микросхему. Запись, добавление или стирание ключа осуществляется мастер-ключом из контроллера. Считывается информация при касании ключом считывателя. Микросхема, как правило, питается от вмонтированной в ключ батарейки. Срок ее работы достаточно велик - несколько лет, но рано или поздно ключ подлежит замене. Ключ очень надежен в работе, устойчив к механическим, электромагнитным воздействиям. Стоимость ключа и считывателя достаточно низка, ключ стоит 5-25 долл. США, считыватель в зависимости от типа стоит 400-1500 долл. США. Широко применяются в небольших СКУД, когда необходимо контролировать большое количество дверей при малом количестве пользователей.

Кроме перечисленных выше могут использоваться идентификаторы следующих типов:

- С использованием цифровой клавиатуры (ПИН-код). Носителем информации является пользователь, набирающий на клавиатуре замка личный код (условное число) и, если он верен, то получает право доступа. Это наиболее простое и дешевое средство контроля доступа. Хо-

тя в последнее время появились клавиатуры, у которых после каждого нажатия, изменяется порядок цифр на клавиатуре по случайному закону, что исключает возможность «подсмотреть» порядок нажатия кнопок или определить наиболее часто используемые кнопки.

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

Стоимость считывателя в зависимости от типа 2000-7000 долл. США.

1.2 Устройства контроля и управления доступом

Контроллеры — электронные устройства, контролирующие работу считывателей и управляющие исполнительными устройствами.

Контроллеры бывают однофункциональными и многофункциональными.

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

Наиболее существенными дополнительными функциями контроллеров являются:

- защита от повторного использования карточки, т. е. повторный вход по данной карточке возможен только после «ее выхода»;
- наличие и возможности программирования временных зон;
- наличие релейных выходов для подключения средств оповещения, телевизионного оборудования и т. д.;
- возможность подключения охранной сигнализации;
- возможность установки двух и более считывателей на одну дверь для организации двухстороннего прохода или многоуровневого контроля.

На практике применяются контроллеры рассчитанные на управление 1—8 считывателями. Все контроллеры, используемые на объекте могут быть объединены в единую систему и подключаться либо к ведущему контроллеру (мастер-контроллеру), либо к компьютеру, управляющему работой всех контроллеров. Обычно ведущий контроллер отличается от остальных только заложенной программой. К нему же может подключаться управляющий компьютер, принтер и другие периферийные устройства. Однофункционапьные

контроллеры являются интеллектуальным аналогом кодового замка и работают только в автономном режиме. Многофункциональные контроллеры не только управляют доступом, но и обладают функциями мониторинга состояния исполнительных устройств и вывода данных на компьютер и печать. С помощью многофункциональных контроллеров можно создавать сложные комплексы, интегрированные с другими подсистемами безопасности, например, с охранно-пожарной сигнализацией и телевизионными системами видеоконтроля. Связь контроллеров между собой в единую сеть осуществляется через стандартный интерфейс RS 485. Для связи ведущего контроллера с компьютером используется стандартный интерфейс RS 232. Многофункциональные контроллеры работают в основном в сетевом режиме (централизованный контроль и управление доступом).

Стоимость контроллеров в зависимости от фирмы изготовителя, номенклатуры и комплекта поставки может колебаться в широких пределах 800—3000 долл. США.

1.3. Устройства центрального управления

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

Для работы в СКУД может использоваться любой персональный IBM- совместимый компьютер. Наряду с работой в составе СКУД он может выполнять и другие функция, так как компьютер нужен в основном лишь для программирования системы и получения отчетов о работе системы. Персональный компьютер, используя специально разработанное для охраняемого объекта программное обеспечение (желательно русифицированное), осуществляет общее управление и программирование СКУД, собирает информацию с контроллеров, создает общий банк данных, формирует различные отчеты и сводки. Русифицированное программное обеспечение под MS DOS и Windows позволяет осуществлять автоматическую запись данных по всем операциям входа/выхода. В любой момент можно запросить разнообразные сведения, например, о местонахождении сотрудников и посетителей. Текущее состояние СКУД отображается в удобной графической форме. В компьютер вводится план охраняемого объекта, на котором стандартными значками указываются считыватели, замки, технические средства охранно-пожарной сигнализации, видеоконтроля и т. п. На плане система автоматически в реальном масштабе времени показывает состояние всех нанесенных объектов контроля - открыта или закрыта дверь, какой именно извещатель сработал в случае тревоги. Таким образом, в любой момент времени можно быстро оценить ситуацию и в случае внештатной ситуации оперативно и эффективно принять меры предосторожности.

1.4. Устройства исполнительные

Принимают команды управления с контроллеров и обеспечивают блокировку возможных путей несанкционированного проникновения через устройства заграждения (двери, ворота, турникеты, кабины прохода и т. п.) людей, имущества, транспорта в помещения, здания и на территорию.

В устройствах исполнительных применяются исполнительные механизмы электромеханического и электромагнитного принципа действия.

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

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

Часто в устройствах исполнительных применяется электромагнитная блокировка (магнитные защелки, задвижки и т. п.) закрывающих элементов с возможностью перемещения их вручную при открывании или закрывании в экстремальных условиях.

Для возвращения устройств заграждения в закрытое состояние, они дооборудуются специальными устройствами - доводчиками, без которых СКУД теряют свою основную функцию - ограничения доступа, так как без них устройство заграждения может находиться в любом состоянии. По виду исполнительного механизма доводчики подразделяются на пружинные, пневматические, гидравлические и электромеханические.

Функция доводчика - не только гарантировать закрытие устройства заграждения (например, двери), но и оберегать замок от механических ударов, а при пожаре - автоматически раскрывать двери и помогать эвакуации. В некоторых типах доводчиков используется, так называемая «система торможения с подтягом»: вначале доводчик дает разогнаться, потом тормозит движение и уже в конце, у самой дверной коробки, резко подтягивает дверь, обеспечивая гарантированное ее закрытие. Кроме этого, некоторые доводчики могут иметь встроенный режим безопасности, исключающий случайное придавливание человека в момент прохождения через устройство заграждения.

2. Классификация СКУД

2.1. Критерии оценки системы

Критериями оценки СКУД являются основные технические характеристики и функциональные возможности.

К основным техническим характеристикам относятся:

- уровень идентификации;
- количество контролируемых мест;
- пропускная способность;

- количество пользователей;
- условия эксплуатации.

По уровню идентификации доступа СКУД могут быть:

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

Но количеству контролируемых мест СКУД может быть:

- малой емкости (до 16);
- средней емкости (от 16 до 64);
- большой емкости (более 64).

По условиям эксплуатации различают системы (части систем) для работы:

- в закрытых отапливаемых помещениях;
- в закрытых неотапливаемых помещениях;
- под навесом на улице в условиях умеренно-холодного климата;
- на улице в условиях умеренно-холодного климата;
- в особых условиях (повышенная влажность, запыленность, вибрации и т. п.).

К основным функциональным возможностям относятся:

- возможность оперативного перепрограммирования;
- схемно-техническая и программная защита от вандализма и саботажа;
- высокий уровень секретности;
- автоматическая идентификация;
- разграничения полномочий сотрудников и посетителей по доступу в помещения и на объект в целом;
- надежное механическое запирание контролируемых мест с возможностью аварийного ручного открытия;
- автоматический сбор и анализ данных;
- выборочная распечатка данных.

По техническим характеристикам и функциональным возможностям СКУД условно подразделяются на четыре класса (таблица 1), В зависимости от особенностей объекта, конфигурации СКУД, фирмы изготовителя набор функций в каждом классе может изменяться и дополняться функциями из других классов.

2.2. Классы СКУД

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

СКУД не контролируется. Обычно администратор (или лицо, ответственное за пропускной режим) имеет мастер-карту (мини-компьютер), при помощи которой он может вносить в список системы коды идентификаторов сотрудников и посетителей или исключать их из списка, а также считывать информацию из буфера системы.

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

СКУД 2-го класса также монофункциональные системы, но у них уже имеется возможность расширения и включения их или их составных частей в общую линию связи (сетевой режим). Данные системы имеют ряд дополнительных функций (табл. 1). На объектах, оборудованных средствами и системами ОПС, СКУД 2-го класса применяются как самостоятельные системы, и они часто рассматриваются только как средства усиления режима обеспечения безопасности объекта.

Таблица 1. Классы СКУД

Класс системы	*Степень защиты от несанкционированного доступа*	*Выполняемые функция*	*Применение*
I	Недостаточная	Одноуровневые СКУД малой емкости, работающие в автономном режиме и обеспечивающие: - допуск в охраняемую зону всех лиц, имеющих соответствующий идентификатор; - встроенную световую/звуковую индикацию режимов работы; - управление (автоматическое или ручное) открытием/закрытием устройства заграждения (например, двери)	На объектах, где требуется только ограничение доступа посторонних лиц(функция замка)
2	Средняя	Одноуровневые и многоуровневые СКУД малой и средней емкости, работающие в автономном или сетевых режимах и обеспечивающие: - ограничение допуска в охраняемую зону конкретного лица, группы лиц по дате и временным интервалам в соот-	То же, что для СКУД 1-го класса. На объектах, где требуется учет и контроль присутствия сотрудников в разрешенной зо-

Класс системы	*Степень защиты от несанкционированного доступа*	*Выполняемые функция*	*Применение*
		ветствии с имеющимся идентификатором; - автоматическую регистрацию событий в собственном буфере памяти, выдачу тревожных извещений (при несанкционированном проникновении, неправильном наборе кода или взломе заграждающего устройства или его элементов) на внешние оповещатели или внутренний пост охраны; - автоматическое управление открытием/закрытием устройства заграждения	не. В качестве дополнения к имеющимся на объекте системам охраны и защиты
3	Высокая	Одноуровневые и многоуровневые СКУД средней емкости, работающие в сетевом режиме и обеспечивающие: - функции СКУД 2-го класса; - контроль перемещений лиц и имущества по охраняемым зонам (объекту); - ведение табельного учета и баз данных по каждому служащему, непрерывный автоматический контроль исправности составных частей системы; - интеграцию с системами и средствами ОПС и ГСВ на релейном уровне	То же, что для СКУД 2-го класса. На объектах, где требуется табельный учет и контроль перемещений сотрудников по объекту Для совместной работы с системами ОПС и ТСВ
4	Очень высокая	Многоуровневые СКУД средней и большой емкости, работающие в сетевом режиме и обеспечивающие: - функции СКУД 3-го класса; - интеграцию с системами и средствами ОПС, ТСВ и другими системами безопасности и управления на программном уровне; - автоматическое управление устройствами заграждения в случае пожара и других чрезвычайных ситуациях	То же, что для СКУД 3-го класса. В интегрированных системах охраны (ИСО) и интегрированных системах безопасности (ИСБ) и управления системами жизнеобеспечивания

СКУД 3-го и 4-го классов обычно называются сетевыми, так как контроллеры объединены в локальную сеть, работают в реальном времени и ведут непрерывный диалог с периферийными устройствами, с ведущим контроллером или управляющим компьютером, расположенным в пункте охраны. Сис-

темы этих классов - это крупные и многоуровневые системы, рассчитанные на большое число пользователей (1500 человек и более)

Подобные системы применяются в случае, когда необходимо контролировав время прохода сотрудников и посетителей на объект и в помещения. При этом применяются более сложные электронные идентификаторы (Proxmity, карточка Виганда, биометрический контроль или их сочетания). Время прохода на каждый день недели и для каждого владельца электронной карточки задается администратором системы.

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

Системы 4-го класса - это многоуровневые системы большой емкости. Отличительные особенности больших систем - наличие развитого программного обеспечения, позволяющего реапизовывать большое число функциональных возможностей и высокую степень интеграции на программном (системном) уровне с другими системами охраны и безопасности.

Программный уровень предполагает объединение различных систем на основе единой программно-аппаратной платформы с единым коммуникационным протоколом и общей базой данных.

Обычно при построении сетевых СКУД используются четыре уровня сетевого взаимодействия.

Первый (высший) уровень представляет собой компьютерную сеть типа клиент/сервер на основе сети ETHERNET, с протоколом обмена TCP/IP и с использованием сетевых операционных систем Windows NT или Unix. Этот уровень обеспечивает связь между сервером и рабочими компьютерами подсистем.

Второй уровень - связь между контроллерами и компьютерами подсистем. На этом уровне используется интерфейс RS 232.

Третий уровень - связь между контроллерами и считывающими устройствами. Здесь применяется интерфейс RS 485 или, ставшие уже стандартом, интерфейсы считывателей Виганда или магнитных карт.

Четвертый уровень - уровень извещателей ОПС и цепей управления (сбалансированные и несбалансированные радиальные и адресные шлейфы, релейные выходные цепи управления). Здесь, как правило, применяются нестандартные специализированные интерфейсы и протоколы обмена информацией.

3. Выбор СКУД для оборудования объекта

3.1. Обследование объекта

Выбор варианта оборудования объекта средствами СКУД следует начинать с его обследования. При обследовании определяются характеристики значимости помещений объекта, его строительные и архитектурно-планировочные решения, условия эксплуатации, режимы работы, ограничения или, наоборот, расширения права доступа отдельных сотрудников, параметры установленных (или предполагаемых к установке на данном объекте) устройств, входящих в СКУД По результатам обследования определяются тактические характеристики и структура СКУД, технические характеристики ее компонентов, а также составляется техническое задание на оборудование объекта СКУД.

В техническом задании указывается:

- назначение системы, техническое обоснование и описание системы;
- размещение составных частей системы;
- условия эксплуатации составных частей системы;
- основные технические характеристики, такие, как:
  - пропускная способность в охраняемые зоны особенно в час пик;
  - " максимально возможное число пользователей на один считыватель;
  - " максимальное число и виды карточек-пропусков;
  - требования к маскировке и защите составных частей СКУД от вандализма;
  - оповещение о тревожных и аварийных ситуациях и принятие соответствующих мер по их пресечению или предупреждению;
  - * возможность работы и сохранения данных без компьютера или при его отказе;
- программное обеспечение системы;
- требования к безопасности;
- требования к электропитанию;
- обслуживание и ремонт системы;
- требования к возможности включения системы СКУД в интегрированную систему безопасности.

3.1.1. Архитектурно-планировочные и строительные решения

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

- количество входов/выходов и их геометрические размеры (площадь, линейные размеры, пропускная способность и т. п.);
- материал строительных конструкций;
- количество отдельно стоящих зданий, их этажность;
- количество открытых площадок;

- количество отапливаемых и неотапливаемых помещений и их расположение.

3.1.2. Условия эксплуатации

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

3.1.3. Интегрированные системы охраны (ИСО)

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

- минимизировать капитальные затраты на оснащение объекта. Аппаратная часть значительно сокращается как за счет исключения дублирующей аппаратуры в разных системах, так и из-за увеличения эффективности работы каждой системы;
- на основе полной и объективной информации, поступающей оператору, значительно сокращается время, необходимое на принятие соответствующих решений по пресечению несанкционированного проникновения, проходу и других чрезвычайных ситуаций на объекте;
- оптимизировать необходимое число постов охраны и существенно снизить расходы на их содержание, а также уменьшить влияние субъективного человеческого фактора;
- четко разграничить права доступа как своих сотрудников, так и посторонних в охраняемые помещения и к получению информации;
- автоматизировать процессы взятия, снятия охраняемых помещений, включения телевизионных камер, контроля шлейфов охранно-пожарной сигнализации и т. п.

При создании ИСО следует учитывать:

- возможность совместной синхронизации всех составляющих ИСО устройств;
- возможность интеграции на программном, аппаратном и релейных уровнях;

- возможность организации линий связи стандартных интерфейсов RS 485 и RS 232 (при значительной удаленности панелей систем сигнализации и управления доступом);
- состояние выходов тревоги средств сигнализации и управления доступом в различных режимах, так как отечественные и большинство зарубежных средств охранной сигнализации имеют в дежурном режиме на выходе замкнутые контакты, которые размыкаются при тревоге.

3.2. Требования к основным компонентам СКУД

3.2.1. Требования к устройствам исполнительным

Устройства исполнительные должны обеспечивать открытие/закрытие запорного механизма или устройства заграждения при подаче управляющего сигнала от контроллера, а также необходимую пропускную способность для данного объекта.

Параметры управляющего сигнала (напряжение, ток и длительность) должны быть указаны в стандартах и/или ТУ на конкретные виды устройств заграждения.

Рекомендуемая величина напряжения питания 12 или 24 В, однако для некоторых видов приводов исполнительных устройств (ворота, массивные двери, шлагбаумы) допускается использовать электропитание от сети 220/380 В

Умышленное повреждение наружных электрических соединительных цепей не должно приводить к открыванию устройства заграждения.

В случае пропадания электропитания в устройствах исполнительных должна предусматриваться возможность питания от резервного источника тока, а также механическое аварийное открытие устройств заграждения. Аварийная система открытия должна быть защищена от возможности использования ее для несанкционированного проникновения.

Устройства исполнительные должны быть защищены от влияния вредных внешних факторов (электромагнитных полей, статического электричества, нестабильного напряжения питания, пыли, влажности, температуры и т. п.) и вандализма.

При выборе доводчиков необходимо учитывать нагрузку (вес) устройства заграждения, а также количество циклов открытия/закрытия. Данные параметры указываются в паспорте на изделие.

3.2.2. Требования к устройствам идентификации доступа

Считыватели должны обеспечивать надежное считывание кода с идентификаторов, преобразование его в электрический сигнал и передачу на контроллер.

Считыватели должны быть защищены от манипулирования путем перебора, подбора кода и радиочастотного сканирования.

При вводе неверного кода должен блокироваться ввод на время, величина которого задается в паспортах на конкретные виды считывателей Время блокировки должно быть выбрано таким образом, чтобы обеспечить задан-

ную пропускную способность при ограничении числа попыток подбора. При трех попытках ввода неправильного кода должно выдаваться тревожное извещение. Для систем, работающих в автономном режиме, тревожное извещение передается на звуковой/световой оповещатель, а для систем, работающих в сетевом режиме, - на центральный пульт с возможностью дублирования звуковым/световым оповещателем. Тревожное извещение должно выдаваться также при любом акте вандализма.

Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию секретности кода.

Устройства идентификации аналогично исполнительным устройствам должны быть защищены от влияния вредных внешних факторов и вандализма.

Идентификаторы должны быть защищены от подделки и копирования.

Производитель должен гарантировать, что данный код идентификатора не повторится или указать условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами.

В паспортах на конкретные виды идентификаторов, должен быть определен минимум кодовых комбинаций.

Для автономных систем пользователь должен иметь возможность сменить или переустановить открывающий код по мере необходимости, но не менее 100 раз. Смена кода должна быть возможна только после ввода действующего кода.

При выборе идентификаторов следует иметь в виду, что клавиатура обеспечивает низкий уровень безопасности, магнитные карточки - средний, карточки проксимити, Виганда и электронные ключи «тач-мемори» - высокий и биометрические карточки - очень высокий уровень безопасности.

3.2.3. Требования к устройствам контроля и управления доступом

Контроллеры, работающие в автономном режиме, должны обеспечивать прием информации от считывателей, обработку информации и выработку сигналов управления для устройств исполнительных.

Контроллеры, работающие в сетевом режиме, должны обеспечивать:

- обмен информацией по линии связи между контроллерами и управляющим компьютером или ведущим контроллером;
- сохранность памяти, установок, кодов идентификаторов при обрыве связи с управляющим компьютером (ведущим контроллером), отключении питания и при переходе на резервное питание;
- контроль линий связи между отдельными контроллерами и между контроллерами и управляющим компьютером.

Для гарантированной работы СКУД расстояние между отдельными компонентами не должно превышать величин, указанных в паспортах (если не используются модемы).

Протоколы обмена информацией и интерфейсы должны быть стандартных типов. Виды и параметры интерфейсов должны быть установлены в паспортах и/или других нормативных документах на конкретные средства с учетом общих требований ГОСТ 26139.

Рекомендуемые типы интерфейсов:

- между контроллерами - RS 485;
- между контроллерами и управляющим компьютером - RS 232.

Программное обеспечение должно обеспечивать:

- инициализацию идентификаторов (занесение кодов идентификаторов в память системы);
- задание характеристик контролируемых точек;
- установку временных интервалов доступа (окон времени);
- установку уровней доступа для пользователей;
- протоколирование текущих событий;
- ведение баз данных;
- сохранение данных и установок при авариях и сбоях в системе.

Уровень доступа - совокупность временных интервалов доступа (окон времени) и мест прохода (маршрутов перемещения), которые назначаются определенному лицу или группе лиц, которым разрешен доступ в заданные охраняемые зоны в заданные временные интервалы).

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

- отключение управляющего компьютера;
- программный сброс управляющего компьютера;
- аппаратный сброс управляющего компьютера;
- нажатие на клавиатуре случайным образом клавиш;
- случайный перебор пунктов меню программы.

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

Программное обеспечение должно быть защищено от преднамеренных воздействий с целью изменения установок в системе.

Вид и степень защиты должны быть установлены в паспортах на конкретные виды средств или систем. Сведения, приведенные в технической документации, не должны раскрывать секретность защиты.

Программное обеспечение при необходимости должно быть защищено от несанкционированного копирования.

Программное обеспечение должно быть защищено от несанкционированного доступа с помощью паролей. Количество уровней доступа по паролям должно быть не менее 3.

Рекомендуемые уровни доступа по типу пользователей:

- первый («администрация») - доступ ко всем функциям контроля и доступа;
- второй («оператор») - доступ только к функциям текущего контроля;
- третий («системщик») - доступ к функциям конфигурации программного обеспечения, без доступа к функциям, обеспечивающим управление устройств исполнительных.

При вводе пароля па экране дисплея не должны отображаться вводимые знаки.

Число символов пароля должно быть не менее 5.

3.2.4. Требования к электропитанию.

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

СКУД должны сохранять работоспособность при отклонениях напряжения сети от -15 до +10 % и частоты до ±1 Гц от номинального значения.

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

Электроснабжение технических средств СКУД осуществляется от свободной группы щита дежурного освещения. При отсутствии на объекте щита дежурного освещения или свободной группы на нем, заказчик устанавливает самостоятельный щит электропитания на соответствующее количество групп. Щит электропитания, устанавливаемый вне охраняемого помещения, должен размещаться в запираемом металлическом шкафу и быть заблокирован на открывание.

СКУД должны иметь резервное электропитание при пропадании основного электропитания. Номинальное напряжение резервного источника питания должно быть 12 или 24 В Переход на резервное питание и обратно должен происходить автоматически без нарушения установленных режимов работы и функционального состояния СКУД.

СКУД должны сохранять работоспособность при отклонениях напряжения резервного источника питания от-15 до +10 % от номинального значения.

Резервный источник питания должен обеспечить функционирование системы при пропадании напряжений в сети на время не менее 8 ч.

При использовании в качестве источника резервного питания аккумулятора должен выполняться автоматический подзаряд аккумулятора.

Аккумуляторные батареи (за исключением необслуживаемых), как правило, размещаются в специальных аккумуляторных помещениях на стеллажах или полках шкафа, в соответствии с требованиями ТУ 45-4-ДО.610.236-87 в поддонах, стойких к воздействию агрессивных сред.

Свинцовые аккумуляторы емкостью не более 72 А/ч и щелочные аккумуляторные батареи емкостью не более 100 А/ч и напряжением до 60 В могут

устанавливаться в общих производственных невзрыво- и непожароопасных помещениях в металлических шкафах с обособленной приточно-вытяжной вентиляцией.

Аккумуляторные установки должны быть оборудованы в соответствии с требованиями ПУЭ.

При использовании в качестве источника резервного питания аккумулятора или сухих батарей должна быть предусмотрена индикация разряда аккумулятора или батареи ниже допустимого предела. Для автономных систем индикация разряда должна быть световая или звуковая, для сетевых систем сигнал разряда аккумулятора должен передаваться на центральный пульт.

Химические источники тока (батарейки), встроенные в активные идентификаторы или обеспечивающие сохранность данных, должны обеспечивать работоспособность средств контроля и управления доступом не менее 5 лет.

4. Типовые варианты СКУД

4.1. СКУД для автономного режима работы

СКУД 1-го и 2-го классов, работающими в автономном режиме, обычно оборудуются: квартиры, коттеджи, небольшие офисы, магазины, аптеки, гостиницы и т. п. и мало значимые зоны на важных объектах. Это позволяет рационально уменьшить число каналов, обслуживаемых дорогостоящими СКУД 3-го и 4-го классов. Данные СКУД - это небольшие и недорогие системы, обслуживающие, как правило, до восьми устройств заграждения (дверей, ворот, турникетов и т. п.). СКУД 1-го и 2-го классов можно применять и на важных объектах или помещениях, если необходимый уровень безопасности обеспечивается системами охранной сигнализации и видеоконтроля.

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

Рис. 1. Оборудование СКУД помещения с одной дверью

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

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

При реализации данного варианта на объекте рекомендуется:

- использовать системы, имеющие прочный металлический корпус, кодонаборную клавиатуру с металлическими кнопками, встроенную индикацию режимов работы, антисаботажную защиту для предотвращения умышленного взлома корпуса контроллера и считывателя;
- использовать системы имеющие энергонезависимую память и позволяющие хранить данные длительное время;
- использовать системы позволяющие изменять время разблокировки дверей;
- программирование системы осуществлять с помощью мастер-карточки и клавиатуры.

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

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

На рис. 2 приведен вариант оборудования СКУД, работающей в автономном режиме, объекта с несколькими дверями.

Данный вариант построения системы отличается от предыдущего только лишь расширением функций и объемом памяти управляющего контроллера, а также его конструкцией. Считыватели и исполнительные устройства размещены в разных конструктивных блоках и управление ими осуществляется через общий контроллер. В систему могут быть введены дополнительные функции:

- контроль прохода в двух направлениях;

- автоматическое открытие и закрытие дверей при аварийных и тревожных ситуациях;
- передача тревожных сообщений на пост охраны;
- регистрация происходящих событий с помощью принтера, подключаемого к контроллеру.

Рис. 2. Оборудование СКУД объекта с несколькими дверями

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

В своем законченном виде данную систему можно легко включить в СКУД, работающую в сетевом режиме. Для этого необходимо использовать контроллер, позволяющий работать в сетевом режиме с другими контроллерами, или использовать дополнительный модуль связи, обеспечивающий объединение контроллеров через интерфейс RS 485.

4.2. СКУД для сетевого режима работы

СКУД 3-го и 4-го классов предназначены для оборудования крупных объектов, таких, как банки, крупные учреждения и фирмы. Несомненным достоинством этих систем является возможность практически неограниченного расширения. Такие системы позволяют обслуживать десятки тысяч пользователей.

В относительно небольших и недорогих системах 3-го класса используется построение системы СКУД, при котором в одну контролируемую линию интерфейса RS 485 включаются все контроллеры, а база данных загружается в один управляющий контроллер (мастер-контроллер).

Такое построение обеспечивает гибкость встраивания СКУД в интерьер помещений, минимизацию коммуникационных соединений и большие расстояния между объектами управления.

Эффективность работы СКУД 4-го класса обусловлена возможностью создавать разветвленные, достаточно многочисленные соединения контроллеров и управляющих компьютеров в единую систему. Модульность построения данных систем обеспечивает:

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

На рис. 3 приведена примерная структурная схема построения СКУД 3-го класса (64 контролируемые двери) на базе многофункционального контроллера, имеющего модульную конструкцию. На рис. 4-6 приведены варианты построения систем 4 класса.

Рис. 3. Примерная структурная схема построения СКУД 3-го класса

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

К одному контроллеру может быть подключено до 8 считывателей различного типа, например считыватель магнитных карточек, считыватель бесконтактных карточек, клавиатура (кодонаборник) и др. Подключение считывателей осуществляется через соответствующий считывающий модуль, работающий с двумя считывающими устройствами. Помимо считывателей, он также контролирует датчики состояния дверей и кнопки их открывания, другие вспомогательные устройства.

Информация о состоянии иных внешних устройств поступает в контроллер через модуль входа/выхода. Посредством этого же модуля контроллер управляет работой исполнительных устройств, устройством выдачи тревожных извещений. Модуль связи обеспечивает объединение контроллеров в единую систему, протяженностью до 1 км с помощью интерфейса RS 485, а также при необходимости объединение контроллеров и управляющего компьютера в компьютеризированную систему с помощью интерфейса RS 232. Модуль приемо-передачи управляет работой считывателей бесконтактных карточек (proximity).

Один контроллер может обслуживать до 10000 пользователей. Для увеличения числа пользователей может применяться модуль расширения памяти.

Системы 4-го класса обычно строятся на базе таких же многофункциональных контроллеров, которые используются для построения СКУД 3-го класса, объединенных в единую компьютерную сеть. При создании компьютерной сети контроллеры в количестве до 32 единиц могут быть объединены в одну ветвь в соответствии с рис. 4. В этом случае модуль связи включается в первый по порядку контроллер ветви. Через него осуществляется связь этого контроллера с компьютером по интерфейсу RS 232. Обмен информацией между контроллерами производит по интерфейсу RS 485. Кроме того, модуль связи осуществляет преобразование формата и скорости передачи данных RS 232/RS 485. Каждый контроллер в ветви имеет свой адрес.

Рис. 4. Примерная структурная схема построения СКУД 4-го класса с одной ветвью

Дальнейшее наращивание системы возможно путем организации нескольких (до 10) ветвей контроллеров. Пример организации двух ветвей показан на рис. 5. Модуль связи первого контроллера преобразовывает с одной стороны

поток данных, посылаемых с управляющего компьютера на контроллер, а с другой - поток выходных данных, параллельно подаваемых на адресные модули связи в ветвях. Каждый адресный модуль связи обменивается данными с контроллерами в ветвях и модулями связи. Такая расширенная сеть позволяет обслуживать до 320 контроллеров и 2048 контролируемых точек.

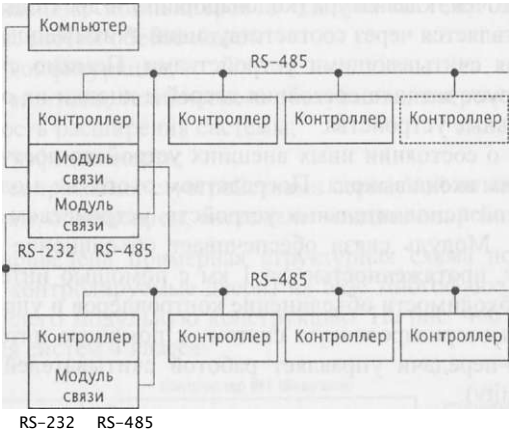


Рис. 5. Примерная структурная схема построения СКУД 4-го класса с несколькими ветвями

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

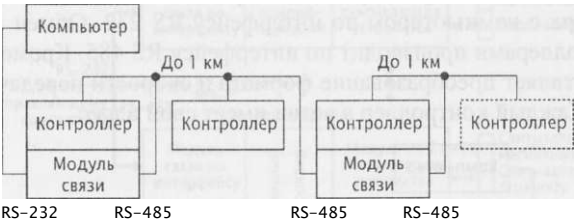


Рис. 6. Увеличение длины ветви при использовании двух модулей связи

При организации компьютеризированных СКУД рекомендуется применять IBM-совместимые компьютеры типа PENTIUM с ОЗУ 16 МБ и более, с двумя последовательными портами и объемом винчестера не менее 528 МБ. Компьютеры этого типа удовлетворяют потребностям любой системы и позволяют модернизировать ее в будущем.

Наличие описанных модулей многофункционального контроллера создает большие возможности по управлению разнообразной периферией системы.

В качестве контролируемых точек могут выступать считывающие головки, ПИН-клавиатуры, замкнутые/разомкнутые контакты кнопок, реле, выходные контакты различных объемных или поверхностных извещателей. В качестве исполнительных устройств могут использоваться электрозамки дверей, исполнительные устройства шлагбаумов, турникетов, устройства тревожного оповещения и освещения, телевизионные камеры и т. д.

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

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

5. Размещение технических средств СКУД на объекте

5.1. Устройства центрального управления

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

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

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

При объединении компьютеров в сеть целесообразно разделять функциональные возможности среди пользователей сети и в соответствии с этим размещать компьютеры в помещениях объекта (рис. 7).

Компьютер контрольно-пропускного пункта
Идентификация персональной корточки и фотографии ее владельца. Контроль открытия/закрытия устройств заграждения
Компьютер центрального поста охраны
Мониторинг несанкционированного доступа, аварийных и чрезвычайных ситуаций с автоматическим выводом тревожной графики на монитор
Компьютер отдела кадров
Оформление, печать пропусков и внесение в базу данных фотографий попьзователей. Учет рабочего времени
Сервер службы безопасности
Программирование всей системы. Сбор, обработка и регистрация всей поступающей информации
Компьютеры администрации
Получение необходимых для них сводок.

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

5.2. Устройства контроля и управления

Ведущие контроллеры и контроллеры, работающие на несколько устройств заграждения, рекомендуется размещать в специальных запираемых металлических шкафах или нишах, на высоте удобной для технического обслуживания. При этом следует дверцы данных шкафов или ниш блокировать охранной сигнализацией на возможное открытие или пролом. Контроллеры, совмещенные в одном корпусе с исполнительными или считывающими устройствами, рекомендуется оборудовать антисаботажными кнопками, предотвращающими несанкционированное вскрытие корпуса. Корпус данных контроллеров должен быть выполнен из ударопрочного материала, предотвращающего контроллер от актов вандализма. Контроллеры, управляющие работой считывателей или исполнительных устройств одной двери в двух направлениях, рекомендуется устанавливать с внутренней стороны охраняемого помещения.

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

При работе устройств контроля и управления в сетевом режиме необходимо учитывать возможность появления помех и сбоев в работе из-за непра-

вильного 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.

5.3. Считыватели и устройства исполнительные

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

На рис. 8 и 9 приведены некоторые варианты размещения и монтажа считывателей и устройств исполнительных.

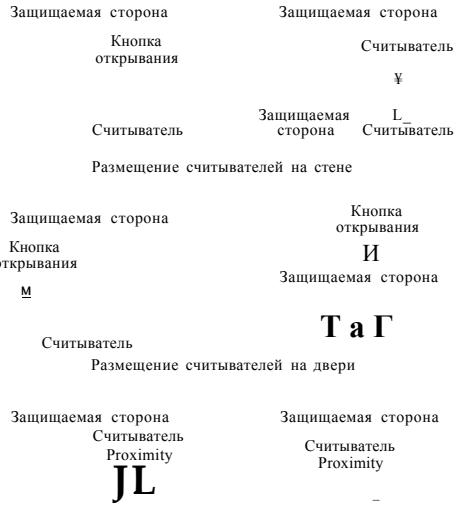


Рис. 8. Варианты размещения считывателей

Считыватели Proximity удобнее всего размещать на стене, скрытно в стене перед устройствами заграждения или даже с внутренней стороны устройства заграждения, например на внутренней стороне неметаллической двери, если ее толщина не превышает 10 см При монтаже считывателя на металле рекомендуется, чтобы между основанием считывателя и металлической поверхностью расстояние было не менее 25 мм. В случае, когда стена, за которой установлен считыватель, оказывается слишком толстой или изготовлена из металла (содержит металлическую арматуру), считыватель допускается устанавливать на расстоянии, на котором должна быть обеспечена необходимая защита от возможного несанкционированного прохода.

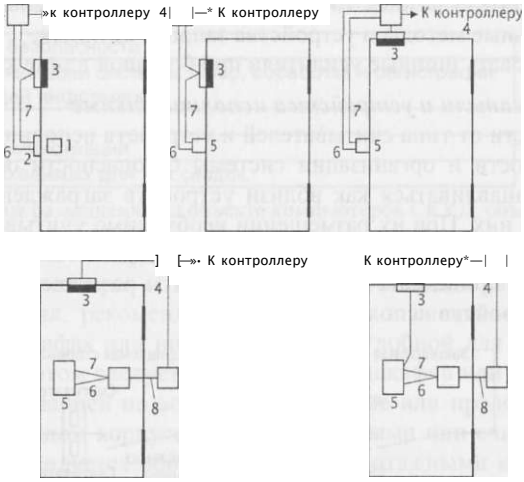


Рис. 9. Варианты размещения исполнительных устройств на дверных конструкциях: I - механический замок; 2 - электромагнитная защелка; 3 - магнитоконтактный датчик открытия двери (СМК); 4 - соединительная коробка; 5 - электромеханический или электромагнитный замок; 6 - кабель питания замка (для дверей из сгораемого материала - двойная изоляция ПХВ или металлорукав); 7 - цепи управления и контроля; 8 - гибкий переход (кабелепровод)

Считыватель магнитных карточек, карточек Виганда и электронных ключей и клавиатуру рекомендуется размещать на стене или непосредственно на устройстве заграждения на высоте, удобной для пользования.

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

Электромагнитные защелки рекомендуется монтировать в косяке дверной коробки Данная установка позволяет блокировать ригель замка, установлен-

ного в двери, при закрывании двери и разблокировать замок при подаче сигнала от контроллера. Кроме этого, 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. Обычно чаще всего электромеханические замки устанавливают на двери (накладной или врезной замок), но иногда эти замки устанавливаются и на дверной коробке.

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

При совместном использовании магнитноконтактных извещателей (типа СМК) в качестве датчиков положения двери с электромагнитными и электромеханическими замками они должны быть разнесены друг от друга как можно дальше.

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

6. Монтаж электропроводок технических средств СКУД на объекте

6.1. Электропроводки технических средств СКУД

Электропроводки технических средств СКУД представляют собой совокупность кабельных линий и линий проводов электрических соединителей, трубопроводов и коробов, проложенных и закрепленных на элементах зданий и сооружений, для прокладки кабелей и проводов, устройств их крепления и защиты от механических повреждений.

Для монтажа электропроводок рекомендуется применять кабели и провода, перечень которых приведен в табл. 2, за исключением случаев когда кабельная и проводная продукция входит в комплект поставки или оговорена в технической документации на СКУД.

Следует помнить, что при большой длине электропроводок (более 50 м) для борьбы с электромагнитными помехами необходимо использовать экранированные кабели и провода, витые пары. Сечение (диаметр) проводников выбирается исходя из длины электропроводки и нагрузки.

Выбор видов электропроводки, проводов, кабелей, труб и коробов с проводами и кабелями и способов их прокладки должен осуществляться с учетом требований электро- и пожарной безопасности.

Электропроводки СКУД подразделяются на:

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

6.2. Монтаж линий связи, низковольтных цепей питания

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

Таблица 2. Рекомендуемый перечень проводов и кабелей

Марка кабеля	*Число жил (пар)*	*Сечение жил, мм^2 (диаметр, мм)*	*Способ прокладки*	*Область применения*	*Примечание*
АВВГ, АГ1ВГ; ГОСТ 16442-80	2,3	2,5-50	Внутри помещений, в тоннелях, каналах	Силовые цепи электропитания	Допускается прокладка в земле в трубах
АВРГ, АНРГ, ВРГ; ГОСТ 433-73Е	2; 3	2,5-50	Внутри помещений, в тоннелях, в каналах	Силовые цепи электропитания	
АПВ; ГОСТ 6323-79Е		2,5-50	В стальных пустотных каналах строительных конструкций	Монтаж электрических цепей	
КРВГ, КНРГ, АКРНГ, КРВГ, АКПсВГ, КВВГ, КПВГ, КПсВГ; ГОСТ 1508-78Е	4; 5; 7; 10, 14; 19; 27; 37	0,75-2,5	Внутри помещений, в тоннелях, в каналах	Цепи управления и сигнализации	Допускается прокладка в земле в трубах

Продолжение табл. 2

Марка кабеля	*Число жил (пар)*	*Сечение жил, мм' (диаметр, мм)*	*Способ прокладки*	*Область применения*	*Примечание*
АКВВГ, АКПВГ; ГОСТ 1508-78Е	4; 5; 7	2,5	Внутри помещений, в тоннелях, в каналах	Цепи управления и сигнализации	Кроме пожаровзрывоопасных помещений
ТСВ; ТУ 16—К71—005—87	(5; 10; 20; 30; 41; 103)	0,5	Монтаж оборудования	Цепи сигнализации	
ПРППМ; ТУ 16.505.755-80		(0,8; 1,0; 1,2)	Внутри помещения по стенам зданий, в земле	Цепи управления и сигнализации	С медными жилами
ТРП; ТУ16.К04.005-89	2	0,4-0,5	Внутри помещений и по наружным стенам зданий	Абонентская телефонная распределительная сеть	
ТПП, TUB; ГОСТ 22498-88Е	(10; 20, 30; 50; 100)	(0,5; 0,7)	Внутри помещений, в канализации, по стенам зданий, на опорах	Цепи сигнализации, местные телефонные сети	
ТППБ, ТППБГ; ГОСТ 22498-88Е	(10; 20; 30; 50; 100)	(0,5; 0,7)	В земле в траншее	Цепи сигнализации	
ТРВ; ТУ 16.К04.005-89	2	(0,4; 0,5)	Внутри помещений и по наружным стенам зданий	Абонентская телефонная распределительная сеть	
РК—75—2—12; ГОСТ 11326.70-79		(2)	Внутри помещений, по стенам зданий, в канализации	В телевизионных установках	Коаксиальный кабель
РК—75—2—13; ГОСТ 11326.71-79		(2)			
РК—75—4—11; ГОСТ 11326.8-79		(4)			

Продолжение табл. 2

Марка кабеля	*Число жил (пар)*	*Сечение жил, мм² (диаметр, мм)*	*Способ прокладки*	*Область применения*	*Примечание*
РК—75—4—12; ГОСТ 11326.9-79		(4)			
РК—75—4—15, ГОСТ 11326.22-79		(4)			
РК-75-4-16; ГОСТ 11326.23-79		(4)			
РК-75-7-15; ГОСТ 11326.24-79		(7)			
РК-75-7-16; ГОСТ 11326.25-79		(7)			
РК-75-9-12; ГОСТ 11326.26-79		/Q\ *(«I*			
РК-75-9-13; ГОСТ 11326.12-79		(9)			
РПШ; ТУ 16-505-670-74	2; 8; 10; 12; 14	0,5; 0,75; 1,0	В канализациях, по стенам зданий	Цепи управления телевизионных установок и СКУД	
н в	1	0,8-1,0		Монтаж оборудования	
н в м, ГОСТ 17515-72Е	1	0,8-2,5			
МГШВ; ТУ-16-505.437-82	1	0,2-1,5		Внутриприборный и межприборный монтаж	
МКШ, МКЭШ; ГОСТ 10348-80	2; 3; 5; 7; 10; 14	0,35; 0,5; 0,75	Для прокладки внутри помещений открыто, в трубах	Монтаж приборов	
ПРППА; ТУ 16.505-755-80	2	1,6	Внутри помещения по стенам здании, в земле открыто и в трубах	Цепи сигнализации и управления	

Окончание табл. 2

Марка кабеля	*Число жил (пар)*	*Сечение жил, мм (диаметр, мм)*	*Способ прокчадки*	*Область применения*	*Примечание*
АППВ; ГОСТ 6323-79Е	2,3	2,0-6	Негибкий монтаж электрических цепей	Цепи электропитания	
ППВ ; ГОСТ 6323-79Е	2,3	0,75-4	Негибкий монтаж элек цепей	Цепи электропитания	
ПВ-1; ГОСТ 6323-79Е	1	0,5-95	В стальных трубах, пустотных каналах строительных конструкций, на лотках	Монтаж силовых и осветительных цепей	
ПВ-3; ГОСТ 6323-79	1	0,5-95	В стальных трубах, пустотных каналах строительных конструкций, на лотках	Гибкий монтаж цепей, гибкий монтаж при скрытой и открытой прокладке	
ШВВП; ГОСТ 7399-80Е	2-3	0,5-0,75	Внутри помещений	Присоединения машин и приборов к сетям напряжением до 380 В	
ЛСВ; ТУ 16.705.403-85	2,4, 10	0,4 - 0,5	Внутри помещений, по стенам зданий	Монтаж цепей сигнализации и управления	
ПКСВ	2,3,4	0,5	Внутри помещений, по стенам зданий	Монтаж цепей сигнализации и управления	

Аббревиатуры, использованные в тексте

АВВГ кабель с изоляцией и оболочкой из поливинилхлоридного пластиката, без защитного покрова с алюминиевой жилой, гибкий,

АПВГ кабель с изоляцией из полиэтилена, оболочкой из поливинилхлоридного пластиката, без защитного покрова с алюминиевой жилой, гибкий.

АВРГ	кабель с поливинилхлоридной оболочкой с алюминиевой жилой, гибкий
АНРГ	кабель с резиновой маслостойкой оболочкой, не распространяющей горение, с алюминиевой жилой, гибкий.
ВРГ	кабель с поливинилхлоридной оболочкой, с медной жилой, гибкий.
АПВ	провод с алюминиевой или алюминиевой, плакированной медью, жилой с поливинилхлоридной изоляцией.
ПВ1	провод с медной жилой с поливинилхлоридной изоляцией.
ПВ2	провод с медной жилой с поливинилхлоридной изоляцией повышенной гибкости.
КРВ1	кабель с изоляцией из резины, оболочкой из полпвинилхлоридного пластиката, с медной жилой, гибкий.
КРНГ	кабель с изоляцией из резины, оболочкой из резины не распространяющей горение, с медной жилой, гибкий.
АКРНГ	кабель с изоляцией из резины, оболочкой из резины не распространяющей горение, с алюминиевой жилой, гибкий.
КРВГ	кабель с изоляцией из резины, оболочкой из полпвинилхлоридного пластиката, с медной жилой, гибкий.
АКПсВГ	кабель с изоляцией из самозатухающего полиэтилена, оболочкой из полпвинилхлоридного пластиката, с алюминиевой жилой, гибкий.
КВВГ	кабель с изоляцией и оболочкой из полпвинилхлоридного пластиката, с медной жилой, гибкий.
КПВГ	кабель с изоляцией из полиэтилена, оболочкой из поливинилхлоридного пластиката с медной жилой, гибкий.
KI 1cBI	кабель с изоляцией из самозатухающего полиэтилена, оболочкой из поливипилхлоридного пластиката с медной жилой, гибкий.
АКВВГ	кабель с изоляцией и оболочкой из полпвинилхлоридного пластиката, с алюминиевой жилой, гибкий.
АКПВГ	кабель с изоляцией из полиэтилена, оболочкой из поливинилхлоридного пластиката, с алюминиевой жилой, гибкий.
ТПП	кабель телефонный с полиэтиленовой изоляцией в полиэтиленовой оболочке с алюминиевым экраном.
ТПВ	кабель телефонный с полиэтиленовой изоляцией с алюминиевым экраном, в поливинилхлоридной оболочке.
ТППБ	кабель телефонный с полиэтиленовой изоляцией в полиэтиленовой оболочке, с алюминиевым экраном, бронированный стальными лентами, с наружным защитным покровом.
ТППБГ	кабель телефонный с полиэтиленовой изоляцией в полиэтиленовой оболочке с алюминиевым экраном, бронированный стальными лентами с противокоррозионным покрытием, гибкий.
НВ	провод монтажный с жилой из медных луженных проволок с изоляцией из полпвинилхлоридного пластиката.
НВМ	провод монтажный с жилой из медных проволок с изоляцией из полпвинилхлоридного пластиката.
МКШ	кабель с изоляцией и оболочкой из полпвинилхлоридного пластиката.
МКЭШ	кабель с изоляцией и оболочкой из поливинилхлоридного пластиката, экранированный.

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

При открытой параллельной прокладке проводов или кабелей линий связи и силовых линий питания и освещения расстояние между ними должно быть не менее 0,5 м, в противном случае должна быть обеспечена защита от наводок. Это требование относится и к низковольтным цепям питания, если они запитывают мощные индуктивные нагрузки (электромагниты, соленоиды и т. п.) устройств заграждения.

Трассы проводок необходимо выбрать наикратчайшими, с учетом расположения электроосветительных, радиотрансляционных сетей, водопроводных и газовых магистралей, а также других коммуникаций.

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

Электропроводки, проходящие по наружным стенам на высоте менее 2,5 м или через помещения, которые не подлежат защите, должны быть выполнены скрытым способом или в металлических трубах.

При пересечении силовых и осветительных сетей кабели и провода СКУД должны быть защищены резиновыми или полихлорвиниловыми трубками, концы которых должны выступать на 4-5 мм с каждой стороны перехода. При пересечении кабели большей емкости должны прилегать к стене, а меньшей емкости огибать их сверху. Кабели меньшей емкости допускается пропускать под кабелями большей емкости при прокладке их в штробах.

Не допускается прокладка по стенам распределительных кабелей емкостью более 100 пар

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

При прокладке кабелей в местах поворота под углом 90° (или близких к нему) радиус изгиба должен быть не менее семи диаметров кабеля.

Кабели и провода должны крепиться к строительным конструкциям при помощи скреб или скоб из тонколистовой оцинкованной стали, полиэтиленовых эластичных скоб. Установка крепежных деталей должна производится с помощью шурупов или клея.

При прокладке нескольких проводов по одной трассе допускается располагать их вплотную друг к другу.

Для соединения и ответвления провода и шин рекомендуется применять распределительные и соединительные коробки.

Расстояние от кабелей и изолированных проводов, прокладываемых открыто, непосредственно по элементам строительной конструкции помещения до мест открытого размещения (хранения) горючих материалов, должно быть не менее 0,6 м.

При пересечении проводов и кабелей с трубопроводами расстояние между ними должно быть не менее 50 мм, а с трубопроводами, содержащими горючие или легковоспламеняющиеся жидкости и газы, - не менее 100 мм.

При параллельной прокладке расстояние от проводов и кабелей до трубопроводов должно быть не менее 10 мм, а до трубопроводов с горючими или легковоспламеняющимися жидкостями и газами - не менее 400 мм.

6.3. Прокладка электропроводок в трубах

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

Стальные трубы, прокладываемые в помещениях с химически активной средой, внутри и снаружи должны иметь антикоррозийное покрытие, стойкое в условиях данной среды. В местах выхода проводов из стальных труб следует устанавливать изоляционные втулки

Для ответвления и соединений стальных трубных проводок (как открытых гак и скрытых), следует применять коробки, ящики и т. п. изделия.

Расстояние между протяжными коробками (ящиками) не должно превышать:

50 м - при наличии 1 изгиба труб;

40 м - при наличии 2 изгибов труб;

20 м - при наличии 3 изгибов труб.

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

2.5 м - для труб с условным проходом до 20 мм;

3 м - для труб с условным проходом до 32 мм;

4 м - для труб с условным проходом до 80 мм;

6 м - для труб с условным проходом до 100 мм.

Расстояние между точками крепления металлорукавов не должно превышать:

0,25 м - для металлорукавов с условным проходом до 15 мм;

0,35 м - для металлорукавов с условным проходом до 27 мм,

0,45 м - для металлорукавов с условным проходом до 42 мм;

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

в приборы - не далее 0,8 м;

в соединительные и протяжные коробки - не далее 0,3 м;

в гибкие металлические рукава - 0,5 - 0,75 м.

Приваривать стальные трубы к металлоконструкциям не допускается.

Прокладку проводов и кабелей в неметаллических (пластмассовых) трубах следует выполнять в помещениях при температуре воздуха не ниже минус 20 °С и не выше плюс 60 °С.

Применяемые для защиты электропроводок от механических повреждений трубопроводы должны изготавливаться из негорючих трудносгораемых материалов с нагревостойкостыо не менее 105 °С согласно требованиям ГОСТ 8865-87.

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

1 м - для труб диаметром 20 мм;

1 , 1 м - для труб диаметром 25 мм,

1,4 м - для труб диаметром 32 мм;

1.6 м - для труб диаметром 40 мм;

1.7 м - для труб диаметром 50 мм;

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

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

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

6.4. Прокладка электропроводок в коробах

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

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

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

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

При скрытых прокладках следует применять глухие короба.

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

При вертикальном расположении коробов крепление проводов и кабелей необходимо выполнять с расстоянием в 1 м.

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

6.5. Прокладка электропроводок напряжением 220 В

Для электроснабжения технических средств СКУД допускается использовать провода и кабели:

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

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

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

При монтаже электропроводок не допускается:

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

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

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

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

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

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

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

6.6. Монтаж электропроводок на территории объекта

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

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

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

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

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

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

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

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

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

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

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

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

Расстояние между протяжными коробками (ящиками), крепление труб, их изгиб и т. п. производится в соответствии с изложенным выше.

Перед прокладкой кабельных линий непосредственно в земле, траншее в случае скальных грунтов устраивается подсыпка из разрыхленной земли или песка толщиной не менее 100 мм.

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

Глубина укладки кабеля не менее 0,6 м. При пересечении кабеля другими кабельными линиями они разделяются слоем земли толщиной не менее 0,5 м. При прокладке в одной траншее двух или более кабелей следует их располагать параллельно с расстоянием между ними не менее 100 мм.

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

На прокладку кабелей в траншее составляется акт на скрытые работы.

Прокладка кабелей в сооружениях подземной канализации, тоннелях и коллекторах должна осуществляться в соответствии с проектом, требованиями СНиП 3.05.06-85, гл. 2-3 ПУЭ-87.

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

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

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

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные документы

1. ГОСТ Р 51241-98. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
2. РД 78.36.005-99. «Выбор и применение систем контроля и управления доступом».
3. РД 78.36.003-2002. Руководящий документ «Инженерно-техническая укрепленность Технические системы охраны Требования и нормативы проектирования по защите объектов от преступных посягательств».
4. ГОСТ «Устройства преграждающие управляемые - УПУ».

Литература

5. Тихонов В А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Уч. пособие. М.: Гелиос АРВ, 2006.
6. Абалмазов Э. И. Энциклопедия безопасности. Справочник каталог, 1997.
7. Тарасов Ю Контрольно-пропускной режим на предприятии. Защита информации // Конфидент, 2002. № 1. С. 55-61.
8. Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // Информост - радиоэлектроники и телекоммуникации, 2001. № 3 (16).
9. Татарченко И. В., Соловьев Д. С. Концепция интеграции унифицированных систем безопасности // Системы безопасности. № 1 (73). С. 86-89.
10. Мащенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие. М.: Горячая линия - Телеком, 2004
11 Горлицин И. Контроль и управление доступом - просто и надежно КТЦ «Охранные системы», 2002.
12. Барсуков В. С. Интегральная защита информации // Системы безопасности, 2002. №5, 6.
13. Стасенко Л. СКУД - система контроля и управления доступом // Все о вашей безопасности. Группа компаний «Релвест» (Sleo@relvest.ru).
14. Абрамов А. М., Никулин О. Ю, Петрушин А. И. Системы управления доступом. М.: «Оберег-РБ», 1998.
15. Предтеченский В И , Рыжухин Д. В , Сергеев М. С. Анализ возможности использования кодонаборных устройств (клавиатур) в системах контроля и управления доступом высокого уровня безопасности. М.: МГИФИ, 2005.
16. Гинце А. Новые технологии в СКУД // Системы безопасности, 2005. № 6
17. Защита информации. Выпуск 1. М.: МП «Ирбис-11», 1992.

18. Злотник Е. Touch Memory - новый электронный идентификатор // Монитор, 1994. №6 С. 26-31.
19 Филипп Х. Уокер Электронные системы охраны. Наилучшие способы предотвращения преступлений / Пер. с англ. М.: «За и против», 1991
20. Флорен М. В. Организация управления доступом // Защита информации «Конфидент», 1995. № 5. С. 87-93.
21 Барсуков В. С. Биоключ - путь к безопасности // Специальная техника, 2003. №2.
22. Крахмалев А. К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ «Охрана» ГУВО МВД России. 2003.
23. Мальцев И. В. Системы контроля доступом // Системы безопасности, 1996. № 1. С. 43-45.
24 Омельянчук А. Пущать или не пущать[9] Этот вопрос решают системы контроля доступа. Мир безопасности, 1997. № 5. С. 39^14.
25. Ситников С. С. Алгоритм оснащения современного объекта охраны СКУД // Системы связи и телекоммуникаций, 2002. Июнь-июль. С. 50-53.
26. Комплексные системы безопасности. Каталог. М.: Научно-производственный центр «Нелк», 2001.
27. Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. 2002. №2.
28. Филипс П. Д., Мартин Э., Уилсон С. Л., Пржибоки М. Введение в оценку биометрических систем // Открытые системы, 2000. № 3. С. 21-27.
29. Торокин А. А Инженерно-техническая защита информации. М.: Гелиос АРВ, 2003.
30. Абапмазов Э. И. Концепция безопасности: тактика высокоэффективной защиты. Стоимость стратегии, стратегические ресурсы, тактика защиты, сопоставимость тактических решений // Системы безопасности, 1995 №4.
31. Алексеенко В. Н. Современная концепция комплексной защиты. Технические средства защиты. М.: МИФИ, 1994.
32. Барсуков С. В Интегральная защита информации // Системы безопасности, 2002. № 5, 6.
33. Барсуков В. С. Биоключ - путь к безопасности // Специальная техника, 2003 №3. С. 26-35.
34. Гинце А. Биометрические считывания - практика применения. ААМ Системз. 2004.
35. Филипс П. Джонатан и др. Введение в оценку биометрических систем // Открытые системы, 2000. № 3.
36. Широчинин В. П., Кулик А. В., Марченко В. В. Динамическая аутентификация на основе клавиатурного почерка // Вестник национального технического университета Украины «Информатика, управление и вычислительная техника», 1999. № 32.

37. Завгородний В В., Мельников Ю. Н. Идентификация по клавиатурному почерку // Банковские технологии, 1998. № 9.
38. Гинце А. А. Выбираем турникеты // Все о вашей безопасности, 2006. №5.
39 Гинце А. А. Особенности СКУД систем доступа крупных распределенных объектов. ААМ Системз, 2005.
40. Магауенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: Уч. пособие. М.: Горячая линия - Телеком, 2004
41. Мальковский М. Г. Лингвистический процессор и лингвистическая база знаний системы распознавания речи. ЦНИТ ГО: webmaster@phi-lol.msu.ru. 24 января 2000.
42. Кондратьев Д. Р. Биометрические устройства для СКУД // Системы безопасности, 2004. № 1.

Оглавление

Вышли в свет и имеются в продаже:

Журин С.И. **Практика и теория использования детекторов лжи. -** М.: Горячая линия - Телеком, 2004. - 143 е.: ил.. ISBN 5-93517-182-1.

Приведены интересные сведения о детекторах лжи: история их создания во многих странах мира; особенности работы с ними. Описаны способы применения детекторов в различных случаях, рассказано о том, что могут и что не могут детекторы лжи. Рассмотрены отдельные методы формирования вопросов и определения виновности проверяемого, а также некоторые аспекты применения детекторов лжи (правовая база).

Для широкого круга читателей. Особый интерес представляет для служб безопасности различных организаций, может быть полезна всем, чья профессия тем или иным образом связана с психологией или безопасностью.

Магауенов Р.Г. **Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие.** - 2-е изд., перераб. и доп. - М.: Горячая линия - Телеком, 2008. - 496 е.: ил., ISBN 978-5-9912-0025-7.

Содержатся систематизированные сведения по учебному курсу «Системы и средства охранной сигнализации». Большое внимание уделено задачам разработки и эксплуатации технических средств охранной сигнализации, вопросам методологии их создания и применения как элементов технических систем обеспечения комплексной безопасности объектов охраны. В основу книги положены материалы лекций, читаемых автором по названной учебной программе начиная с 1999 г. Настоящее издание (первое вышло в 2004 г.) дополнено информацией по применению быстроустанавливаемых технических средств охраны и словарем основных терминов и понятий, используемых в охранной сигнализации и других элементах систем физической защиты.

Для студентов вузов, может быть полезна инженерам, специализирующимся в области создания и эксплуатации технических средств и систем охранной сигнализации, а также руководителям и сотрудникам служб безопасности (охраны) объектов.

Магауенов **Р.**Г. **Охранная сигнализация и другие элементы систем физической защиты. Краткий толковый словарь.** - М.: Горячая линия - Телеком, 2006. - 97 е., ISBN 5-93517-333-6.

Краткий толковый словарь по системам охранной сигнализации и другим элементам систем физической защиты, содержит определения, современную трактовку и пояснения более 600 терминов и понятий, удовлетворяющих требованиям «актуализации нормативных документов». Книга преследует учебно-методические цели и не является нормативным документом, однако может быть полезна для разработки общероссийского стандарта открытого типа, предназначенного упорядочить терминологию по системам физической защиты.

Для специалистов в области создания и эксплуатации технических средств и систем охранной сигнализации, а также руководителей и сотрудников служб безопасности (охраны) объектов, студентов и аспирантов соответствующих специальностей.

Сайт издательства:

Серия книг «Обеспечение безопасности объектов» содержит систематическое изложение основных вопросов современной теории и практики обеспечения безопасности важных объектов и предназначена для использования при организации работ по защите предприятий, вычислительных центров, узлов связи, банков, офисов, коммерческих объектов, жилых домов, транспортных средств.

Книга 1 - «Концептуальные основы создания и применения системы защиты объектов»

В книге изложен широкий круг вопросов, связанных с организацией контрольно-пропускного режима на различных объектах и применением систем контроля и управления доступом (СКУД).

Большое внимание уделено средствам идентификации и аутентификации. Описаны устройства идентификации (считыванием) различных типов; средства биометрической аутентификации личности и особенности их реализации; различные виды контроллеров и исполнительные устройства СКУД. Приведен обзор различных вариантов реализации СКУД. Даны основные рекомендации по выбору средств и систем контроля доступа. В приложении приведены ключевые выдержки из официальных нормативных материалов связанных с использованием СКУД.

Книга 3 ~ «Технические средства наблюдения в охране объектов»
Книга 4 - «Инженерно-техническая защита объектов»
Книга 5 - «Технические системы охранной и пожарной сигнализации»
Книга 6 - «Охранные подразделения»
Книга 7 - «Интегрированные системы безопасности»

Для специалистов в области создания и применения систем защиты объектов, руководител
а также студентов учебных зав?
квалификации.