Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования

Владимирский государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА
ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
КНИГА 14

В.П. БУГАКОВ, А.В. ТЕЛЬНЫЙ

ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ

Системы контроля и управления доступом

Учебное пособие

Под редакцией М.Ю. Монахова

Владимир 2007

УДК 004.056
ББК 32.97
Б90

Редактор серии – доктор технических наук,
профессор М.Ю. Монахов

Рецензенты:

Кандидат технических наук, доцент зав. кафедрой
оперативно-технической деятельности
Владимирского юридического института Федеральной
службы исполнения наказаний
К.Н. Курысев

Кандидат технических наук,
доцент кафедры информатики и защиты информации
Владимирского государственного университета
А.А. Воронин

Печатается по решению редакционно-издательского совета
Владимирского государственного университета

Бугаков, В. П.

Б90 Технические средства охраны : системы контроля и управления доступом : учеб. пособие / В. П. Бугаков, А. В. Тельный ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2007. – 148 с. (Комплексная защита объектов информатизации. Кн. 14 / под ред. М.Ю. Монахова).
ISBN 5-89368-713-2

Это четырнадцатая книга из серии «Комплексная защита объектов информатизации». В ней представлен систематизированный материал по первой части учебного курса «Инженерно-техническая защита информации» – методам и средствам систем контроля и управления доступом на объекты информатизации.

Предназначено для студентов специальности 090104 – комплексная защита объектов информатизации дневной формы обучения.

Табл. 4. Ил. 65. Библиогр.: 20 назв.

УДК 004.056
ББК 32.97

ISBN 5-89368-713-2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Одним из наиболее эффективных подходов к решению задачи инженерно-технической защиты информации на объектах является использование систем контроля и управления доступом (СКУД). Правильное использование СКУД позволяет закрыть несанкционированный доступ на территорию, в здание, отдельные этажи и помещения.

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 технического ограждения (ограждения, преграды, двери и воро-

та); исполнительного устройства (замки, приводы дверей, шлагбаумов, турникетов и т. д.).

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

В данном учебном пособии рассматриваются теоретические и практические вопросы общей организации СКУД, даются практические решения и рекомендации по выбору СКУД для оборудования объекта.

Пособие предназначено в первую очередь для студентов и аспирантов, специализирующихся в вопросах комплексной защиты объектов информатизации, а также может быть полезным в системе переподготовки и повышения квалификации инженерно-технических кадров.

Для более углубленного изучения следует обратиться к литературе, приведенной в библиографическом списке.

Глава 1. ОСНОВНЫЕ ПОНЯТИЯ СКУД

1.1. Термины и определения

Приведем ряд терминов и их определения, используемые в системах контроля и управления доступом (СКУД), которыми будем оперировать в дальнейшем.

Система контроля и управления доступом в общем случае является элементом, подсистемой безопасности объекта и сама выполняет дополнительные функции по обеспечению безопасности, например охранной сигнализации. В работе системы контроля и управления доступом участвует прежде всего объект или субъект, претендующий на право доступа к ресурсам, находящимся в некоторой зоне. С общей точки зрения, определения объекта и субъекта следующие.

Субъект – личность, человек как носитель каких-либо свойств.

Объект – философская категория, выражающая то, что противостоит субъекту в его деятельности. С точки зрения доступа, – это различные перемещаемые предметы, транспортные средства. В том числе сюда относятся и носители информации – магнитные и лазерные диски, магнитные ленты и т. п.

Объект или субъект должен получить доступ в некоторую зону.

Доступ – перемещение субъекта или объекта (живого существа, предмета, физического процесса) в некоторую зону или получение возможности взаимодействия с определенным материальным или информационным ресурсом. Например, проход на предприятие сотрудника или возможность пользоваться Интернетом и т. д.

Субъект доступа (СД)* или *объект доступа (ОД) – живое существо, предмет или физический процесс (например, человек, транспортное средство), претендующие на право доступа.

Наиболее распространенный СД – это человек (сотрудник организации, посетитель, покупатель, жилец дома и т. д.). Другой пример – автомашина. В этом случае может контролироваться право доступа либо водителя (субъекта доступа); либо автомашины, управляемой им (объекта доступа); либо пассажира с водителем; либо того и другого одновременно с автомашиной (субъект и объект доступа).

В дальнейшем будем пользоваться в основном термином «*субъект доступа»* как наиболее часто встречающимся. Однако при этом будет неявно предполагаться, что то же самое возможно и для объекта доступа (ОД).

Зона – часть контролируемого объекта (помещение, территория, канал связи, область на носителе информации), т. е. это территория контролируемого объекта или ее часть; помещение или группа помещений в контролируемом здании; доступные для использования каналы связи, зоны на носителях информации или сами носители и т. д.

Доступ субъекта/объекта контролируется и управляется СКУД. Для решения задачи контроля и управления доступом система должна выполнить ряд определенных процедур.

Контроль и управление доступом (КУД) – идентификация, аутентификация, контроль санкционированности и управление доступом в контролируемую зону. (Замечание: аутентификация не является обязательной).

Аутентификация – это процедура проверки правомочности владения субъектом или объектом, предъявленным идентификационным признаком (ИП) на соответствующем носителе, идентификаторе.

Верификация – сравнение идентичности двух разных субъектов доступа.

Идентификация – это процедура опознавания субъекта или объекта по присущему ему или некоторому носителю идентификационному признаку(ам).

Процедура идентификации состоит из следующих этапов:

- обнаружение и считывание ИП;
- сравнение обнаруженного ИП с эталонными признаками, находящимися в базе данных;
- принятие решения о правах доступа.

Для того чтобы в точке доступа можно было опознать, идентифицировать СД, последний должен обладать рядом идентификационных признаков.

Идентификационный признак (ИП) – набор характеристик и параметров, содержащих информацию, достаточную для решения задач идентификации и аутентификации.

Идентификационный признак наносится на некоторый носитель информации – идентификатор.

Идентификатор – носитель идентификационного признака. Это субъект или объект, определенные характеристики или параметры которого служат признаками, по которым осуществляется идентификация и аутентификация.

Идентификатором – носителем идентификационных признаков – может быть либо сам субъект или объект доступа, либо специальный предмет, на котором тем или иным образом нанесены идентификационные признаки (рис. 1).

Рис. 1. Идентификаторы

Действительный идентификатор – идентификатор с ИП, допускающий перемещение СД через данную точку доступа (ТД) в данный временной и календарный периоды.

Недействительный идентификатор **–** идентификатор с ИП, не допускающий перемещение СД через данную ТД в определенный временной и календарный периоды.

Как отмечалось ранее, идентификатором может служить как сам субъект или объект доступа, так и отдельные дополнительные предметы. Например, человек может идентифицироваться по отпечатку пальца, т. е. он сам является носителем ИП. Другой случай, когда субъект доступа имеет предмет, к примеру магнитную карту, на которой нанесены идентификационные признаки. В этом случае СД и носитель разделены.

В СКУД используются разнообразные носители идентификационных признаков (карты, брелоки и др.). Для записи последних применяют различные технологии (например, технологию магнитной записи, эффекты Виганда, проксимити и др.).

Система контроля и управления доступом (СКУД) – совокупность методов и средств контроля и управления доступом, функционирующих и взаимодействующих по определенным правилам. Иначе можно сказать, что это совокупность всех технических, программных, организационных и других методов и средств, необходимых для выполнения задачи контроля и управления доступом субъекта или объекта в некоторую зону.

Зоны, доступ в которые должен контролироваться, могут обладать различными особенностями, связанными с используемыми процедурами, характером функционирования, возможностью доступа того или иного субъекта или объекта.

Зона контролируемого доступа (ЗКД) – зона, доступ в которую контролируется СКУД. Например, прилегающая территория или определенные помещения предприятия.

Зона разрешенного (санкционированного) доступа (ЗРД) – зона, доступ в которую субъекту или объекту разрешен только в

определенные временные и календарные интервалы. К примеру, помещение на предприятии, в которое разрешен доступ сотруднику только в рабочие дни и рабочее время. Подчеркнем, что понятие ЗРД применимо только к конкретному субъекту или объекту доступа.

Зона неразрешенного (несанкционированного) доступа (ЗНД) – зона, доступ в которую определенному субъекту или объекту запрещен в определенные временные и календарные интервалы. Например, то же, упомянутое выше, помещение в нерабочее время или в выходные и праздничные дни становится ЗНД для того же субъекта доступа, т. е. одна и та же зона может быть зоной как разрешенного, так и неразрешенного доступа для определенного субъекта или объекта в зависимости от времени и даты.

Частный случай ЗНД – зона запрещенного доступа, т. е. зона, доступ в которую данному субъекту или объекту доступа запрещен всегда, независимо от времени и даты.

Зона свободного (неконтролируемого) доступа (ЗСД) – зона, доступ в которую не ограничивается.

Зона ограниченного по времени доступа (ЗОВД) – зона, доступ в которую ограничивается только временными и календарными интервалами. Например, доступ в торговые помещения магазина для покупателей ограничен только рабочими часами магазина, т. е. любой СД (покупатель) может посетить магазин, но только в определенные дни и часы. В то же время для продавцов временные рамки шире. Однако здесь появляется принципиальное отличие – речь идет уже только об ограниченном круге СД – сотрудниках магазина. Доступ разрешен только им.

Зона ограниченного доступа объектов (ЗОДО) – зона, доступ в которую ограничивается правилами запрета перемещения определенных объектов, предметов. Например, доступ в торговые помещения магазина самообслуживания ограничен (запрещен) для покупателей с большими сумками, т. е. любой субъект может посетить магазин, но есть ограничения на то, что он может

иметь при себе. Доступ в самолет запрещен пассажирам с оружием или предметами, представляющими опасность для пассажиров. Это аналогичный предыдущему случай, но с дополнительным ограничением круга СД – сюда входят только пассажиры самолета.

Санкционированный доступ – доступ, не нарушающий правила управления доступом (доступ СД, имеющего соответствующий уровень доступа). К примеру, проход сотрудников предприятия в рабочие часы в соответствующий отдел предприятия.

Несанкционированный доступ (НСД) – доступ, нарушающий правила управления доступом (доступ СД, не имеющего соответствующего уровня доступа). Примером может служить проход покупателя в складские помещения магазина или в торговый зал вне рабочего времени магазина.

Разграничение доступа – разрешение перемещения по одним маршрутам и запрет перемещения по другим. Например, разграничение потоков сотрудников предприятия, идущих на работу или с работы в часы максимальной загрузки начала и окончания рабочего дня, по разным проходным, т. е. это организация перемещения СД в одни и те же зоны по определенным маршрутам.

Точка доступа (ТД) – часть объекта, оборудованная соответствующими средствами, в которой осуществляются контроль и управление доступом. К примеру, проходная предприятия, где осуществляются контроль доступа и управление им. Возможность того или иного субъекта или объекта по перемещению через точки доступа определяются уровнем доступа этого СД. При этом можно выделить две основные составляющие уровня доступа: пространственную (маршруты перемещения) и временную (временные и календарные интервалы).

Уровень доступа (УД) – это совокупность разрешенных точек доступа и соответствующих им разрешенных временных и календарных интервалов.

Уровень доступа характеризует права субъекта или объекта доступа по перемещению через точки доступа в разные зоны контролируемого объекта, т. е. понятие УД определяет, куда (к чему) и когда разрешен доступ конкретного СД или ОД. Можно говорить, что уровень доступа включает в себя:

- перечень разрешенных зон контролируемого доступа;
- допустимые временные и календарные интервалы доступа в эти зоны;
- совокупность разрешенных точек доступа в эти зоны.

В качестве примера можно привести предприятие, доступ в различные отделы которого разрешен только в рабочее время и рабочие дни недели для сотрудников соответствующих отделов. Возможности доступа сотрудников охраны шире по временным и календарным рамкам. Например, они могут находиться на территории объекта и в нерабочее время, в том числе и в выходные дни. Но они имеют более жесткие ограничения по зонам. Например, ограничены перемещением только по коридорам и не имеют доступа непосредственно в отделы. В то же время доступ на территорию предприятия разным сотрудникам разрешен только через определенные, в общем случае разные, проходные (ТД).

1.2. Критерии оценки и классификация

Критериями оценки СКУД являются основные технические характеристики и функциональные возможности.

К основным техническим характеристикам относятся:

– уровень идентификации;

– количество контролируемых мест;

– пропускная способность;

– количество пользователей;

– условия эксплуатации.

По уровню идентификации доступа СКУД могут быть:

– *одноуровневые* – идентификация осуществляется по одному признаку, например по считыванию кода карточки;

– *многоуровневые* – идентификация осуществляется по нескольким признакам, например, по считыванию кода карточки и биометрическим данным.

По 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, имитостойкости и криптозащиты;

– автоматическая идентификация по признакам, свойственным субъекту доступа, например биометрия;

– 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 (табл. 1). В зависимости от особенностей объекта, конфигурации

СКУД, фирмы изготовителя набор функций в каждом классе может изменяться и дополняться функциями из других классов.

Таблица 1

Класс системы	Степень защиты от НСД	Выполняемые функции	Применение
1	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 соответствии с имеющимся идентификатором; – автоматическую регистрацию событий в собственном буфере памяти, выдачу тревожных извещений (при несанкционированном проникновении, неправильном наборе кода или взломе заграждающего устройства или его элементов) на внешние оповещатели или внутренний пост охраны; – автоматическое управление открытием/закрытием устройства заграждения	То же, что для СКУД 1-го класса. На объектах, где требуется учет и контроль присутствия сотрудников в разрешенной зоне. В качестве дополнения к имеющимся на объекте системам охраны и защиты

Окончание табл. 1

Класс системы	Степень защиты от НСД	Выполняемые функции	Применение
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 ТСВ 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 и интегрированных системах безопасности и управления системами жизнеобеспечения

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 компью-

тер. 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 «*Touch Memory*». 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. Типичный пример автономной СКУД – квартирные (подъездные) домофонные системы.

СКУД 2-го класса также малофункциональные 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. На объектах, оборудованных средствами и системами ОПС, СКУД 2-го класса применяются как самостоятельные системы и часто рассматриваются только как средства усиления режима обеспечения безопасности объекта. СКУД 3-го и 4-го классов обычно называются сетевыми, так как контроллеры объединены в локальную сеть, работающие в реальном времени и ведущие непрерывный диалог с периферийными устройствами, с ведущим контроллером или с управляющим компьютером, расположенным в пункте охраны. Системы этих классов – крупные и многоуровневые системы, рассчитанные на большое число пользователей (1500 человек и более).

Подобные системы применяются в случае, когда необходимо контролировать время прохода сотрудников и посетителей на объект и в помещения. При этом применяются более сложные

электронные идентификаторы (*Proxmity*, Виганд-карточки, 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 реализовывать 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, *USB* и дальность связи до 15 м.

Третий уровень – связь между контроллерами и считывающими устройствами. Здесь применяется интерфейс *RS* 485, *RS*-422 и др.

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.

Контрольные вопросы и задания

1. Дайте определение или толкование понятий: доступ, субъект доступа, объект доступа, контролируемая зона, аутентификация, идентификация, система контроля и управления доступом.
2. Что такое санкционированный доступ, разграничения доступа?
3. Приведите классификацию СКУД по техническим и функциональным признакам.

Глава 2. ОРГАНИЗАЦИЯ СКУД

В общем случае СКУД должна выполнить следующие процедуры:

- идентификацию субъекта или объекта;
- аутентификацию;
- проверку санкционированности доступа;
- разрешение или запрет доступа;
- протоколирование событий (результатов выполнения перечисленных ранее процедур).

Таким образом, в общем случае ставится задача идентифицировать субъект или объект, претендующий на право доступа в некоторую зону (к некоторому ресурсу), проверить правомочность владения им идентификатором, правомочность попытки такого доступа и в случае положительного решения разрешить доступ. Эта задача решается в точке доступа в зону контролируемого доступа. В свою очередь, ЗКД – это зона, доступ в которую разрешен только через точки доступа. Доступ в одну и ту же зону может осуществляться через несколько разных ТД. Для конкретных СД одни и те же ЗД могут быть зонами как разрешенного, так и неразрешенного доступа в зависимости от уровня доступа этого субъекта.

2.1. Обобщенная структурная схема

Для решения указанных выше задач контроля и управления доступом система (рис. 2) должна включать в себя три основных элемента:

- устройство считывания идентификационных признаков (считыватель);

• устройство анализа ИП и принятия решения (так называемый контроллер);

• устройство управления доступом.

Устройство управления доступом включает в себя:

• преграждающее управляемое устройство (дверь, турникет и тому подобные устройства и конструкции);

• исполнительное устройство для управления состоянием преграждающего устройства (например электромагнитный замок);

• элементы контроля состояния преграждающего устройства (к примеру магнитоконтактный датчик);

• элементы неконтролируемого управления состоянием преграждающего устройства.

Структура, приведенная на рис. 2, справедлива практически для любых реализаций СКУД, например технических (электронных, механических и т. п.) или автоматизированных систем с использованием человека как элемента общей системы КУД. Для подтверждения рассмотрим несколько примеров.

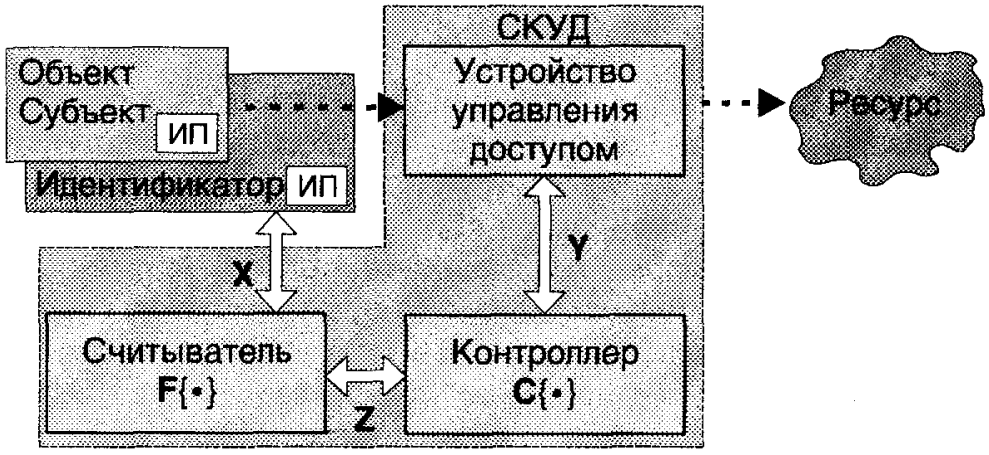


Рис. 2. Обобщенная структурная схема СКУД

Наиболее распространенная СКУД – обыкновенный механический замок, имеющий все необходимые элементы СКУД. Человек (субъект) владеет ключом (идентификатором), который яв-

ляется физическим носителем ИП. Сам идентификационный признак – это форма ключа. Механизм замка – считыватель и устройство принятия решения (контроллер). Засов и фиксатор – исполнительные устройства, которые приводятся в действие при соответствии формы ключа (т. е. ИП) параметрам механизма (образец ИП) и позволяют открыть дверь.

Другой уже упоминавшийся пример – вахтер на проходной. Человек предъявляет ему пропуск с различными идентификационными признаками – форма, цвет и размер пропуска, фотография, фамилия, специальные знаки, разрешающие доступ в различные подразделения, и др. Вахтер зрительно оценивает пропуск (считывает) на соответствие образцу, который он знает (процедура идентификации). Затем сравнивает фотографию с лицом реального человека (аутентификация). И, наконец, при соответствии сравниваемых параметров разблокирует турникет (доступ разрешен).

То же самое выполняют современные автоматизированные СКУД. Все или часть процедур: идентификации и аутентификации; проверки санкционированности доступа; управления исполнительными устройствами управления доступом; протоколирования событий – автоматизируются. Таким образом, частично или полностью исключается человеческий фактор – одно из самых слабых звеньев систем безопасности.

Основываясь на рассмотренном материале, можно сформулировать в общем виде алгоритм функционирования СКУД.

Как отмечалось ранее, для выполнения процедур идентификации и аутентификации субъекта или объекта он или идентификатор должен обладать идентификационным признаком или признаками, каждый из которых характеризуется в общем случае набором параметров или функций. В функциональной схеме (см. рис. 2) M идентификационных признаков x_{km} субъекта или объекта (идентификатора), имеющих K параметров, определяют-

ся в общем случае матрицей X. Элемент матрицы x_{km} представляет собой *k-й* параметр (функцию) *m-го* признака.

Считыватель СКУД преобразует информационные признаки x_{km} с носителями определенной физической природы в сигналы z_{km}, пригодные для дальнейшей обработки контроллером. Алгоритм преобразования определяется оператором F:

$$Z = F\{X\}.$$

Контроллер в общем случае сравнивает считанные признаки Z со всеми эталонами Z_i^o, хранящимися в базе данных, тем самым определяя номер i объекта/субъекта или фиксируя отсутствие эталона Z_i^o, соответствующего предъявленному Z.

На основании результатов сравнения (фактически по найденному значению i), т. е. информации об уровне доступа i-го объекта/субъекта, хранящейся в базе данных, контроллер формирует матрицу Y_i выходных сигналов:

$$Y_i = C\left\{Z, Z_i^o\right\}\Big|_{i=1\ldots I}.$$

В состав этих сигналов входят и сигналы, управляющие исполнительными устройствами. Исполнительные устройства разблокируют (в случае санкционированного доступа) преграждающие устройства, обеспечивая доступ. Уровень доступа определяет разрешенные зоны, а также временные и календарные интервалы доступа (когда, куда, к чему разрешен последний). Для детерминированной системы, каковой является СКУД, это определяет реакцию системы, т. е. процедуру функционирования преграждающих устройств, в свою очередь, приводимых в действие исполнительными устройствами.

Очевидно, что основные особенности СКУД будут зависеть прежде всего от характеристик объекта, на котором необходимо осуществлять контроль и управление доступом. Среди особенностей объекта основными являются структура (топология) и ре-

жим функционирования зон контролируемого доступа (маршруты перемещения, временной и календарный график, потенциальные возможности несанкционированных действий). С точки зрения СКУД, наиболее важны особенности собственно точек контроля доступа как основной ячейки любой системы КУД. Действительно, точка доступа обязательно содержит все основные элементы СКУД в целом. Поэтому от состава ее технических средств и принципов построения будут существенно зависеть и характеристики системы.

Рассмотрим упомянутые основные особенности объекта, влияющие на структуру СКУД и точек доступа (контроля и управления доступом), определяющие алгоритмы работы СКУД.

2.2. Структура зон доступа

Простая (*одиночная*) *зона*

Структура простой одиночной зоны z_j контролируемого доступа с одной точкой доступа d_i, принадлежащей этой зоне, показана на рис. 3.

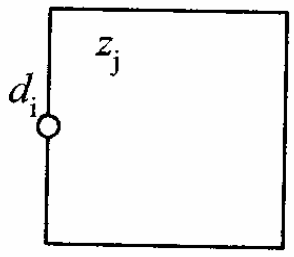


Рис. 3. Простая зона

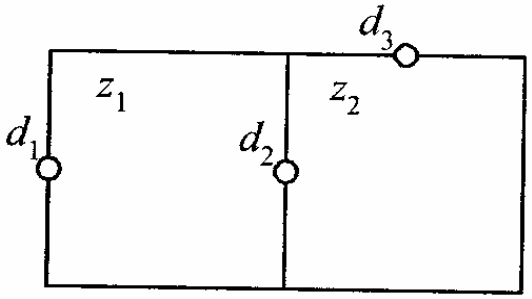


Рис. 4. Связанные зоны

Будем обозначать ТД кружком, подразумевая, что в общем случае она содержит все необходимые для решения задачи КУД элементы (считыватель, контроллер, устройство управления доступом). Зона имеет как минимум одну точку доступа. Форма зоны в общем случае может быть произвольной (как выпуклой, так

и нет). Кроме того, очевидно, что зона доступа может включать в себя несколько помещений с общим режимом функционирования, являющихся одной зоной.

Связанные зоны

В связанных зонах перемещение в одну из зон контролируемого доступа возможно через другие зоны контролируемого доступа. Связанные зоны (z и z_2 на рис. 4) имеют, по крайней мере, одну общую точку доступа d_2, принадлежащую обеим связанным зонам. Через нее осуществляется перемещение из одной ЗКД z_i в другую, связанную с ней зону z_2. Контроль и управление доступом в каждую из зон может происходить как через точки доступа, находящиеся по периметру связанных зон (d_1 и $< d_3$ на рис. 4), так и через общие ТД (d_2 в нашем примере), т. е. через точки доступа, принадлежащие рассматриваемой зоне или зонам.

Группы связанных зон

Для нескольких связанных зон могут быть различные частные случаи:

- последовательно связанные зоны, когда доступ в каждую следующую зону осуществляется из предыдущей (зоны z_1, z_2 и z_3, рис. 5);
- параллельно связанные – доступ в каждую зону осуществляется из одной и той же общей зоны (зоны z_2, z_3 и z_4 на рис 6);
- произвольно связанные зоны, являющиеся комбинацией предыдущих случаев.

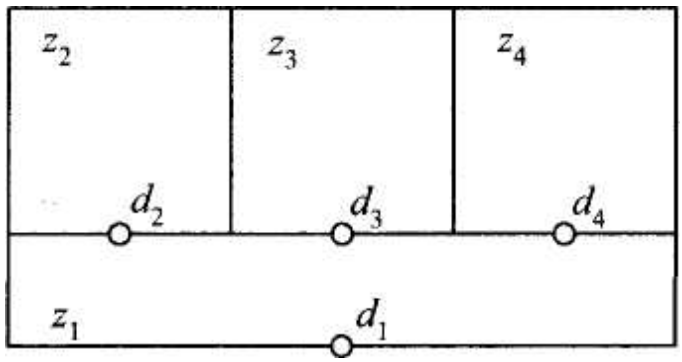


Рис. 5. Последовательно связанные зоны

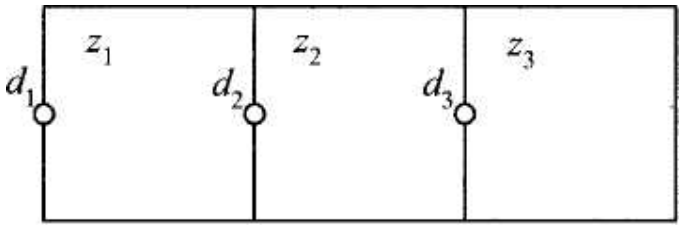


Рис. 6. Параллельно связанные зоны

Связанные зоны имеют свои особенности при выборе уровней доступа в них, рассматриваемых ниже.

Вложенные зоны

Вложенными называются зоны, когда одна или группа зон контролируемого доступа находятся внутри другой ЗКД (рис. 7). Вложенные зоны могут быть как простыми, так и связанными.

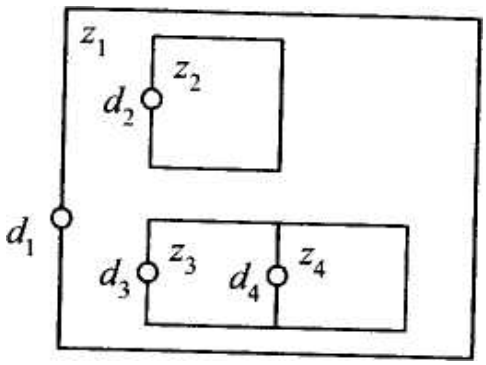


Рис. 7. Вложенные зоны

Типичным примером такой структуры является территория предприятия (зона z_1) и здания, находящиеся на ней (зоны z_2, z_3, z_4).

Заметим, что рассматриваемое понятие и рис. 7 отображают только взаимосвязь зон, а не их пространственное расположение. Так, на рис. 7 две группы вложенных зон могут быть разными этажами одного и того же здания, а внешний периметр – как периметром территории, так и границей одного здания. В последнем случае зона z_1 представляет собой общие помещения (холл, лестницы и т.п.).

Анализируя рассмотренные структуры зон, можно выделить два типа:

1. *Внешние зоны контролируемого доступа* – зоны, доступ в которые возможен из зон свободного доступа. Например, это зона z_1 на рис. 5 – 7.

2. *Внутренние зоны контролируемого доступа* – зоны, доступ в которые возможен только из других зон контролируемого доступа. Например, это зоны z_2, z_3 и z_4 на рис. 5 и 6.

Используя эти понятия, можно ввести еще один термин: *уровень вложения зон*, или *уровень доступа зон.* Так, если принять за нулевой уровень зоны свободного доступа, тогда:

• внешние зоны будут иметь первый уровень (доступ в них возможен непосредственно из ЗСД, следовательно, необходимо пройти один этап контроля доступа – одну ТД);

• внутренние зоны, непосредственно граничащие с внешними, т. е. имеющие общие ТД с внешними зонами, будут иметь второй уровень (чтобы попасть в них, надо пройти как минимум две точки доступа);

• третий уровень будут иметь зоны, доступ в которые возможен через две упомянутые выше зоны (т. е. необходимо преодолеть минимум три ТД) и т. д.

Рассматриваемое понятие хорошо иллюстрируется приведенным ранее рис. 5, на котором зона z_1 имеет первый уровень, z_2 – второй уровень, а z_3 – третий. Таким образом, понятие уровня вложения зон или уровня доступа зон характеризует необходимые требования к уровню доступа субъекта в эти зоны. Чем выше уровень доступа зоны, тем выше должен быть уровень доступа субъекта.

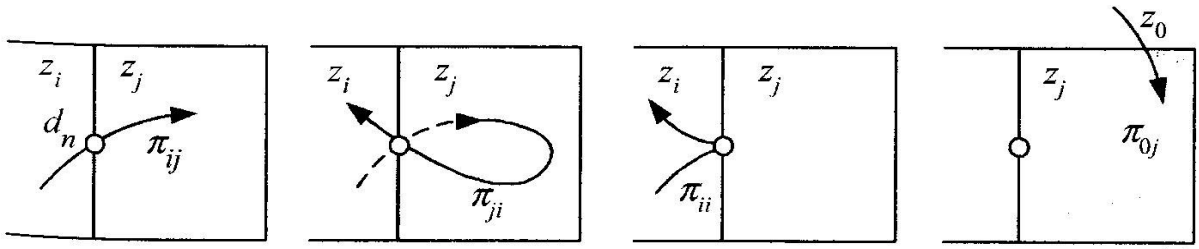
2.3. Маршруты перемещения субъекта доступа

Проанализируем возможные маршруты перемещения субъекта доступа на контролируемом объекте в контролируемых зонах. С функциональной точки зрения, конечная цель системы – это контроль и управление доступом в ЗКД, т. е. необходимо контролировать и управлять доступом субъекта в ЗКД, а также желательно знать, в какой именно зоне находится СД, и протоколировать события. Очевидно, что информацию для выполнения упомянутых процедур можно получить только в точках доступа.

Введем понятие перехода (перемещения) из одной зоны доступа (контролируемого или свободного) в другую. Обозначим такой переход из зоны z_i в зону z как n_{ir}. Нулевой индекс будет обозначать зону свободного доступа.

Начнем с простейшего случая одиночной зоны (см. рис. 3) с одной точкой доступа. На рис. 8 показаны различные возможные

варианты перемещения субъекта доступа через точку доступа. В первом случае (рис. 8, *а*) СД перемещается из зоны z_i в зону контролируемого доступа z_j через точку доступа d_n.



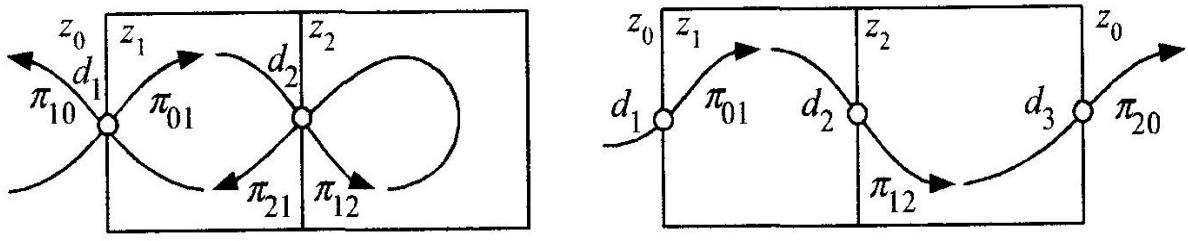
а) *б)* *в)* *г)*

Рис. 8. Возможные маршруты движения СД

В дальнейшем субъект может перемещаться внутри зоны и выйти из нее обратно через ту же ТД (рис. 8, *б*). Этот переход по аналогии с предыдущим можно обозначить как n_{ji}. Таким образом, переходы с разным порядком индексов отличаются направлением перемещения.

В ряде СКУД возможны также еще два случая. В первом (рис. 8, *в*) субъект доступа, пройдя идентификацию, остался в той же самой зоне z_i Такой переход обозначается n_n. Во втором (рис. 8, *г*) СД попадает (несанкционированно) в зону контролируемого доступа, минуя точку доступа.

Более сложные случаи перемещения СД в связанных зонах рассматриваются на рис. 9.



а) *б)*

Рис. 9. Маршруты движения СД

Таким образом, переход π_{ij} означает следующее:

- При $i \neq 0, j \neq 0$ – перемещение СД из *i*-й зоны контролируемого доступа в *j*-ю.
- При $i = 0, j \neq 0$ – перемещение СД из зоны свободного доступа в *j*-ю зону контролируемого доступа.
- При $i = j$ – возврат в ту же самую зону доступа (контролируемого или свободного) с идентификацией в точке доступа без перемещения через эту ТД.

Переходы π_{ij} и π_{ji} с разным порядком следования индексов отличаются направлением перемещения (порядком прохождения ТД).

Введем понятие маршрута субъекта доступа. *Маршрут субъекта доступа* – это конечная последовательность переходов, выполненных им.

Последовательность переходов, например для случая двух последовательно связанных зон (см. рис. 9, *а*), может быть записана следующим образом:

$$\pi_{01}, \pi_{12}, \pi_{21}, \pi_{10}. \qquad (1)$$

Зоны, с которых начинается и которыми заканчивается маршрут, называются *концевыми.* Остальные являются внутренними.

Приведенная последовательность переходов (1) определяет замкнутый маршрут движения субъекта доступа. Замкнутость означает возврат в ту же самую исходную зону доступа.

Замкнутый маршрут начинается и заканчивается в одной и той же зоне доступа. В противном случае маршрут называется *открытым.*

Полный маршрут начинается и заканчивается на внешних концевых зонах свободного доступа и включает в себя все переходы, выполненные в зонах контролируемого доступа на объекте.

Полный замкнутый маршрут начинается и заканчивается в одной и той же внешней концевой зоне свободного доступа, т. е. в частном случае полного маршрута концевые зоны доступа являются внешними зонами свободного доступа.

Маршрут может быть квазизамкнутым, когда субъект доступа перемещается в контролируемую зону из зоны свободного доступа через одну точку доступа, а выходит также в ЗСД, но через другую внешнюю ТД (рис. 9, *б*), т. е. вход и выход из ЗКД происходят в область вне контролируемого объекта, но через разные точки доступа. Рассмотренный пример квазизамкнутого маршрута может быть записан как

$$\pi_{01}, \pi_{12}, \pi_{20}. \qquad (2)$$

Мы рассматривали корректные (санкционированные) переходы. *Корректными* будем считать переходы, при которых перемещение субъекта доступа осуществляется по конструктивно предназначенным для этого элементам конструкции объекта. Примером могут служить двери, в том числе оборудованные средствами контроля и управления доступом, т. е. точки доступа.

В принципе могут быть также и *некорректные* (*несанкционированные*) *переходы* – перемещение по не предназначенным для этого элементам конструкции объекта, в том числе и с нарушением целостности конструкций, т. е., минуя точки доступа, например через окна. Пример такого некорректного перехода приведен на рис. 8, *г*. Маршрут, показанный на рис. 8, *в*, может быть как корректным (санкционированным), так и некорректным (несанкционированным) в зависимости от установленного режима функционирования СКУД.

Корректный (*санкционированный*) *маршрут* – это последовательность корректных переходов.

С общей точки зрения корректный маршрут субъекта доступа должен быть непрерывным: субъект должен пройти все последовательно связанные зоны на данном маршруте. Например, полный замкнутый маршрут (1) является непрерывным. Однако, к примеру, маршрут

$$\pi_{01}, \pi_{12}, \pi_{10} \qquad (3)$$

не является непрерывным. Субъект, находясь во второй из двух последовательных зон контролируемого доступа, оказался в первой без возврата в зону z_1 из z_2, т. е. отсутствует переход π_{21}.

Учитывая вышесказанное, можно сформулировать некоторые принципы функционирования систем контроля и управления доступом, следующие из рассмотренных особенностей.

1. *Санкционированные действия* – любые действия в СКУД должны подтверждаться соответствующим уровнем доступа.

2. *Осуществимость* – корректное перемещение субъекта доступа должно производиться только по конструктивно предназначенным для этого элементам объекта.

3. *Непрерывность* – санкционированное перемещение через точки доступа должно осуществляться только с последовательным прохождением подряд всех связанных зон и соответствующих принадлежащих этим зонам точек доступа без пропуска на данном маршруте (и в заданном временном интервале).

4. *Неповторяемость* – прохождение одной и той же точки доступа не может быть выполнено дважды подряд в одном и том же направлении без прохождения других ТД или этой ТД в обратном направлении.

Первые три принципа являются обязательными для СКУД. Выполнение четвертого может не контролироваться в упрощенных системах. Однако это приводит к снижению надежности СКУД. Например, невыполнение этого принципа дает возможность использовать один и тот же идентификатор для входа на объект нескольких человек.

2.4. Особенности точек доступа

Введем графические обозначения для основных элементов, влияющих на режим функционирования ТД. Будем обозначать на рисунках *j*-й считыватель *c* прямоугольником, а кнопку *m* управления выходом *k* – квадратом с точкой внутри (рис. 10). При этом предполагаем, что ис-

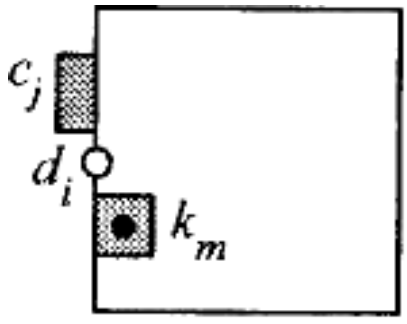


Рис. 10. Обозначение элементов оборудования точки доступа

полнительное и преграждающее устройства входят в состав ТД d_i, обозначенной кружком.

В зависимости от конфигурации и состава используемых для организации точки доступа технических средств, последняя может иметь различные особенности, от которых существенно зависят режимы функционирования этих средств

Точки доступа в зависимости от их особенностей можно классифицировать следующим образом.

По расположению на контролируемом объекте

- Внешние, через которые осуществляется перемещение из зон свободного доступа в зоны контролируемого доступа или выход из ЗКД в ЗСД.
- Внутренние, при прохождении которых субъект доступа не покидает пределов зон контролируемого или ограниченного по времени доступа.

Примерами внешних точек доступа могут служить точки доступа d_1 и d_3 на рис. 4 и d_1 на рис. 5 и 6. Соответственно, примеры внутренних точек доступа – это d_2 на рис. 4, d_2 и d_3 на рис. 5, а также d_2, d_3 и d_4 на рис. 6. Точки доступа вложенных зон d_2, d_3 и d_4 на рис. 6 также являются внутренними.

По характеру взаимодействия точек доступа друг с другом

- Связанные – точки доступа, алгоритм работы которых зависит от алгоритма работы других.
- Несвязанные – точки доступа, функционирующие независимо от других.

По направлению перемещения

- Однонаправленные, движение через которые осуществляется только в одном направлении.
- Ненаправленные, движение через которые может осуществляться в обоих направлениях.

По способу контроля направления перемещения

- С односторонним контролем доступа, в которых контроль доступа (идентификация и управление доступом) осуществляется

только в одном направлении. При перемещении СД в обратном направлении осуществляется только управление доступом (без контроля), причем непосредственно одним субъектом доступа.

• С двухсторонним контролем доступа. В этом случае при движении в любом направлении совершается полный цикл процедур КУД: идентификация (и, возможно, аутентификация), проверка санкционированности и управление доступом. При этом управление осуществляется самой системой КУД, а не субъектом доступа.

Поскольку последние особенности являются наиболее важными, рассмотрим их подробнее.

Точка доступа с односторонним контролем

В данном случае система контролирует перемещение субъекта доступа только в одном направлении. Перемещение в обратном направлении система не отслеживает.

Например, в неавтоматизированной системе для прохода на предприятие надо предъявить пропуск (идентификатор), а для выхода – нет. В автоматизированной системе субъект предъявляет идентификатор, СКУД проверяет уровень доступа и дает команду на устройство управления доступом. При перемещении субъекта в обратном направлении он либо движется по маршруту, не оборудованному устройствами управления доступом (преграждающими), либо управляет последними без предъявления идентификатора.

Таким образом, при санкционированном доступе разрешение на вход после идентификации субъекта дается собственно СКУД. В то же время для выхода – прохода в обратном направлении – достаточно нажать кнопку выхода, чтобы разблокировать замок двери или пройти через турникет с фиксированным направлением вращения, позволяющим проходить только в одном направлении, т. е. осуществляется неконтролируемый выход.

Пример подобной системы приведен на рис. 11, 12. Для контролируемого прохода необходимо предъявить действительный идентификатор, для выхода – просто нажать кнопку выхода. С точки зрения состава технических средств такая точка доступа должна быть оснащена только одним считывателем c_x на входе. На выходе необходим элемент неконтролируемого управления заграждающим устройством (например кнопка управления дверью или турникетом).

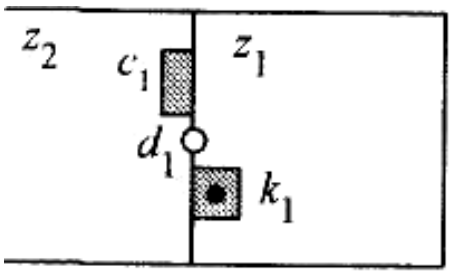


Рис. 11. Точка доступа с односторонним контролем

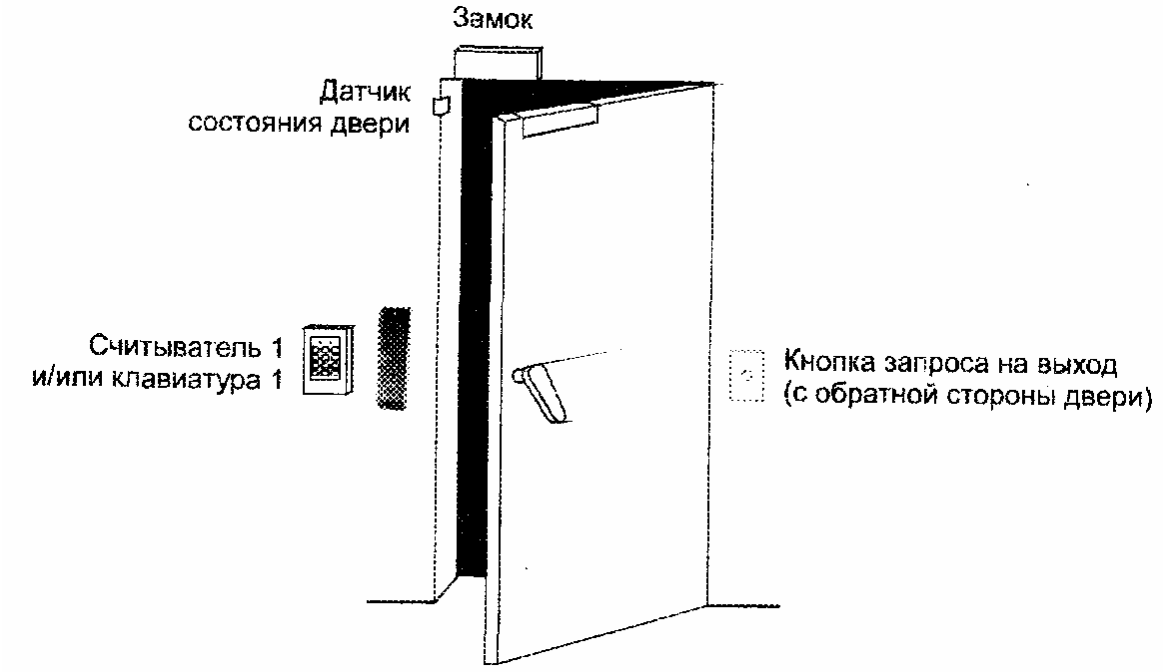


Рис. 12. Технические средства точки доступа с односторонним контролем

Рассмотренный случай является достаточно распространенным вариантом построения точки доступа, используемым во многих системах. Преимущество этого варианта – технически более простая система. С функциональной точки зрения он используется, когда нужно ограничить только вход на объект.

При этом имеется ряд недостатков:

• Неизвестно, где находится субъект/объект доступа – в контролируемой зоне z_1 или вне ее (в зоне z_2). Причина – выход не контролируется, и система не может фиксировать факт выхода субъекта, вошедшего на объект.

• Вследствие неконтролируемого выхода возникает возможность использования одного и того же идентификатора для многократного повторного прохода через эту точку доступа. К примеру, сотрудник проходит на объект (санкционирование), затем передает идентификатор другому, и он также (но уже несанкционированно) проходит на этот же объект, используя тот же самый идентификатор. Заметим, что эти рассуждения справедливы для СКУД, в которых не используется аутентификация – т. е. проверка правомочности владения субъектом предъявляемого идентификатора. А это достаточно распространенный вариант СКУД.

Точка доступа с двухсторонним контролем

Точки доступа с двухсторонним контролем перемещения позволяют устранить вышеперечисленные недостатки, в частности фиксировать факты попыток повторного прохода по одному и тому же идентификатору без предварительного выхода из зоны контролируемого доступа.

Как варианты могут быть два типа систем с двухсторонним контролем прохода:

1. Точка доступа, в которой контролируется и фиксируется только факт прохода, без определения направления. То есть используется, к примеру, один и тот же считыватель для контроля и управления проходом в обоих направлениях. В этом случае пройти как в прямом, так и в обратном направлении может только обладатель действительного идентификатора. Формально, поскольку применяется только один считыватель, для определения направления движения используется подсчет количества проходов субъекта с определенным идентификатором. Тогда направление прохода может фиксироваться по порядку прохождения точки доступа. Например, нечетные проходы соответствуют одному

направлению, скажем, входу на объект, а четные – другому направлению (выходу). Система, сравнительно редко используемая по ряду причин. К ним можно отнести потерю действительного направления при двукратном (подряд) предъявлении идентификатора, если вход не осуществлен по каким-либо причинам. В этом случае второе предъявление идентификатора будет восприниматься как выход, хотя субъект либо не был реально в контролируемой зоне, либо только вошел в нее. Другая причина – отсутствие в ряде случаев технической возможности использования одного и того же считывателя для входа и выхода.

2. Точка доступа, в которой контролируется и фиксируется также и направление перемещения. Для этого обычно используются отдельные считыватели для контроля и управления дверью при проходе с разных сторон (рис. 13, 14). В этом случае можно устранить упомянутые выше недостатки. В последней системе есть возможность фиксировать все переходы через ТД.

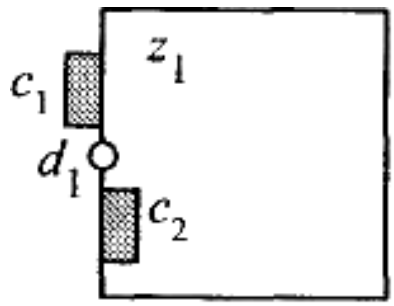


Рис. 13. Точка доступа с двухсторонним контролем

Рис. 14. Технические средства точки доступа с двухсторонним контролем

Для контролируемого двухстороннего прохода необходимо предъявить действительный идентификатор как при перемещении из зоны свободного в зону контролируемого доступа, так и при обратном перемещении. Например, предъявить идентификатор надо как для входа на предприятие, так и для выхода. Более того, сделать это нужно, используя отдельные считыватели. В этом случае можно контролировать местоположение субъекта доступа, поскольку направление, в котором он движется, точно определяется по считывателю, которому предъявлен идентификатор (остается, правда, возможность осуществить идентификацию, но не пройти через дверь).

Кроме контроля местонахождения субъекта есть возможность регистрировать попытки повторного прохода (в заданный временной интервал) как несанкционированное действие, запрещая проход.

Связанные точки доступа

Точку доступа с двухсторонним контролем можно рассматривать как две связанные точки доступа, имеющие общие устройства управления доступом. Кроме того, при использовании алгоритма запрета повторного прохода алгоритмы их функционирования также связаны, т. е. это две технически и алгоритмически связанные точки доступа. Обычно они обслуживаются одним контроллером.

Другой пример связанных точек доступа приведен на рис. 15. Как отмечалось, в общем случае переходы (или часть их) могут быть однонаправленными, т. е. разрешенное перемещение может осуществляться только в одном направлении. Особенность рассматриваемой

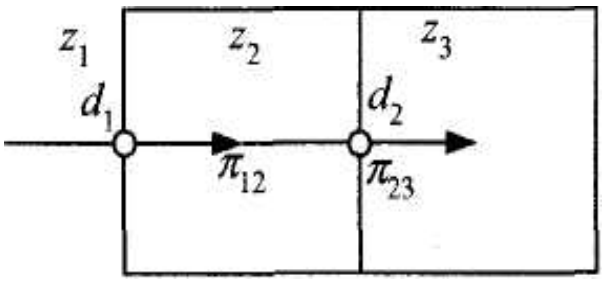


Рис. 15. Связанные точки доступа с направленным перемещением

структуры состоит в том, что переходы π_{12} и π_{23} являются последовательно однонаправленными, т. е. они могут быть выполнены только последовательно, один за другим с движением в одном направлении.

Практическим примером такой структуры может служить перемещение в зону контролируемого доступа z_3 через специальную зону z_2 или тамбур (специальное преграждающее устройство). В этом случае сначала открывается первая дверь (точка доступа d_1), посетители проходят в тамбур (зона z_2) из зоны z_1. Затем первая дверь закрывается, и только после этого может быть открыта вторая дверь (точка доступа d_2) для прохода в зону d_3. Такой режим используется, прежде всего, по двум основным причинам. Во-первых, для контроля (досмотра) посетителей или транспорта в закрытой зоне (например таможенной). Во-вторых, для исключения прорыва через одиночную точку доступа в зону контролируемого доступа группы людей вслед за субъектом, имеющим действительный идентификатор, после разблокирования замков двери. Тактика такого доступа называется шлюз.

Введем еще одно понятие, характеризующее зоны контролируемого доступа (для последовательно связанных зон), – понятие категории доступа зоны.

Категория доступа зоны – важность, значимость зоны контролируемого доступа. Для санкционирования доступа в ЗКД более высокой категории субъекту доступа необходимо иметь соответственно более высокий уровень доступа.

Наглядно это может быть продемонстрировано на примере последовательно связанных зон (см. рис. 5). Для доступа в каждую следующую зону субъекту доступа необходимо иметь более высокий уровень доступа.

В соответствии с определением, приведенным в п. 1.1, уровень доступа – это совокупность разрешенных точек доступа и соответствующих им разрешенных временных и календарных

интервалов. Эта совокупность может быть записана следующим образом:

$$\text{У}_i(d_1, d_2, \ldots, d_N, \Delta t_1, \Delta t_2, \Delta t_M, \Delta T_1, \Delta T_2, \Delta T_L). \quad (4)$$

Это выражение включает упомянутые совокупности точек доступа d_n, разрешенных временных Δt_m и календарных $\Delta t_{1'}$ интервалов.

В частном случае такие переменные, как временные и календарные интервалы, могут отсутствовать, т. е. минимальный набор переменных – это совокупность разрешенных точек доступа

$$\text{У}_i(d_1, d_2, \ldots, d_N). \quad (5)$$

Возвращаясь к понятию категории доступа зоны, можно говорить, что это понятие определяет требуемый для доступа набор параметров уровня доступа субъекта, приведенный в выражении (4). Так, для структуры объекта, приведенной на рис. 5, возможны три субъекта доступа с соответствующими уровнями

$$\text{У}_1(d_1), \text{У}_2(d_1, d_2) \text{ и } \text{У}_3(d_1, d_2, d_3). \quad (6)$$

Первому позволен проход в первую зону контролируемого доступа, второму – в первую и вторую, третьему – в любую. Аналогично определяются зоны разрешенного доступа для случая параллельно связанных зон (см. рис. 6).

Анализируя сказанное, можно сформулировать еще один принцип, которым должны удовлетворять алгоритмы СКУД для последовательно связанных зон, – *монотонность*.

Монотонность означает следующее:

• Категория доступа каждой следующей из последовательно связанных зон должна быть выше предыдущей. Иначе, возможно, категория доступа занижена или нет необходимости в точках доступа и зоны могут быть объединены.

• Субъект доступа, имеющий i-й уровень доступа (позволяющий перемещение через j-ю точку доступа), должен иметь и $(i - 1)$-й уровень доступа (для $i > 1$).

Примером, иллюстрирующим первую часть, может служить рис. 5. Если, например, категории доступа зон z_2 и z_3 одинаковы, то эти зоны могут быть объединены в одну. То же самое можно сказать о структуре на рис. 6 для любой из пар зон, в которые входят z_1 и одна из параллельных зон. Если категория любой пары зон совпадает, то они могут быть объединены. Другой пример (см. рис. 7): зоны, для которых должны выполняться сформулированные принципы, – это z_1, z_3, z_4 .

Исключением является случай, когда имеется не менее двух внешних точек доступа. Тогда сказанное справедливо для части объекта, от внешней точки до зоны контролируемого доступа с наиболее высокой категорией доступа.

Примером корректно присвоенных уровней доступа, соответствующих принципу монотонности, могут служить уровни доступа в выражении (6). Как пример некорректного уровня можно записать $У_3(d_1, d_3)$. Здесь разрешена третья ТД, но запрещена вторая.

2.5. Математическая модель системы

Для описания системы контроля и управления доступом воспользуемся математическим аппаратом теории множеств и представлением СКУД в виде графа. Такое представление основано на приведенных выше рассуждениях и понятиях.

Множества точек и зон доступа

В нашем случае совокупность точек доступа d всей СКУД может быть определена множеством D, которому принадлежат эти точки доступа $d \in D$. Обычно специфика объектов (особенно средней и большой емкости по количеству контролируемых зон) такова, что объект имеет несколько структурных подразделений (цехов, зданий, отделов и т. д.) с разными категориями доступа в

каждое из них. Следовательно, с учетом специфики функциональных особенностей объекта СКУД имеет несколько подсистем, отличающихся категориями доступа зон и, соответственно, разными уровнями доступа пользователей (субъектов доступа). Поэтому в общем случае множество D в свою очередь разделяется на I подмножеств D_i с элементами d_i. Подмножества $D_i \subset D, \quad i = 1,\ldots,I$ являются собственными подмножествами множества D.

Подмножества точек доступа D_i могут быть как пересекающимися, так и непересекающимися. Это зависит от того, имеют ли упомянутые структурные подразделения общие зоны доступа и, соответственно, общие точки доступа. С этой точки зрения можно записать следующее выражение:

$$(D_1 \cup D_2 \cup \ldots \cup D_I) = D.$$

Причем для непересекающихся подмножеств

$$d_i \in d_j, i = j;\ d_i \notin d_j, i \neq j.$$

Аналогично совокупность зон доступа z всей СКУД может быть определена множеством Z, которому принадлежат эти точки доступа $z \in Z$. Учитывая упомянутую выше специфику объектов (несколько структурных подразделений с разными категориями доступа зон), множество Z разделяется на J подмножеств Zj с элементами z_j. Подмножества $Z_i \subset Z, \quad j = 1,\ldots,J$ являются собственными подмножествами множества Z.

Как и подмножества точек доступа, подмножества Z_j могут быть как пересекающимися, так и непересекающимися, т. е.

$$(Z_1 \cup Z_2 \cup \ldots \cup Z_J) = Z.$$

При этом для непересекающихся подмножеств

$$z_i \in Z_j, i = j; z_i \notin Z_j, i \neq j.$$

Проиллюстрируем вышесказанное на примерах объектов со связанными зонами доступа, приведенными на рис. 5 и 6. Соответствующие подмножества D_1, D_2, D_3 точек доступа D_i показаны на рис. 16 и 17 диаграммами Эйлера – Венна с разной штриховкой.

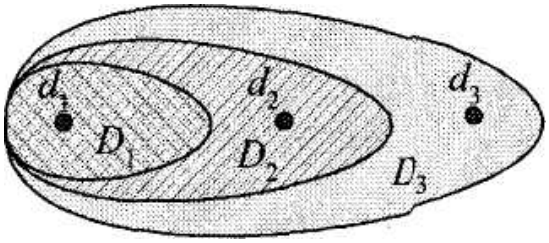


Рис. 16. Подмножества точек доступа последовательно связанных зон

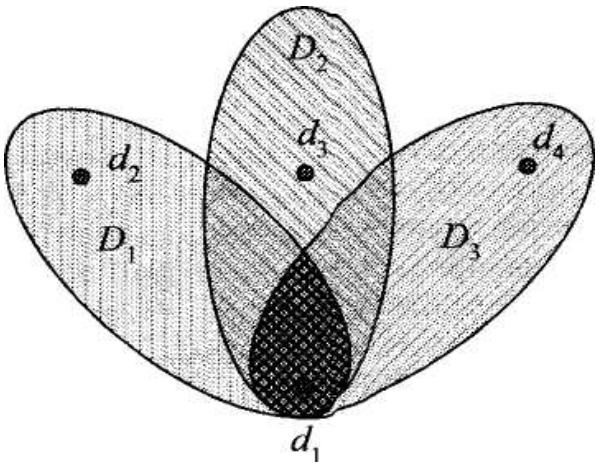


Рис. 17. Подмножества точек доступа параллельно связанных зон

Для случая объекта, показанного на рис. 5, подмножества D будут включать (см. рис. 16) следующие ТД:

$$(d_1) \in D_1,$$
$$(d_1, d_2) \in D_2,$$
$$(d_1, d_2, d_3) \in D_3.$$

Соответственно для объекта на рис. 5 подмножества D_i могут быть записаны (см. рис. 17) в виде

$$\begin{aligned}(d_1, d_2) &\in D_1,\\ (d_1, d_3) &\in D_2,\\ (d_1, d_4) &\in D_3.\end{aligned} \qquad (7)$$

Учитывая состав подмножеств D_i, нетрудно сделать вывод, что они пересекающиеся.

В обоих примерах подмножества D имеют общую ТД d_i, соответствующую области пересечения этих подмножеств: $d_1(D_1 \cap D_2 \cap D_3)$.

Ясно, что в общем случае может быть и другой состав подмножеств D_r. Для примера, на рис. 18 подмножество D_2 включает в себя три точки доступа $(d_1, d_3, d_4) \in D_2$.

Аналогичное представление может быть использовано и для подмножеств Z_j зон.

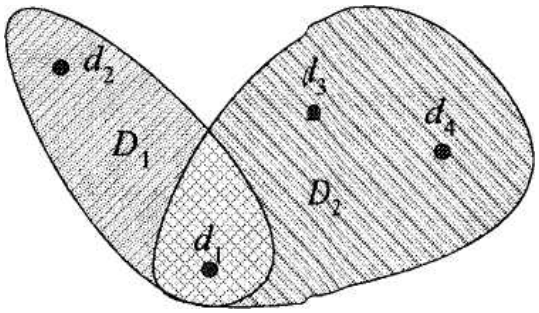


Рис. 18. Подмножества точек доступа

Представление СКУД в виде графа

В системе СКУД субъект доступа может перемещаться из одной зоны в другую через точки доступа. Такая система может быть представлена с помощью теории графов. Переходы (перемещения) p_{ij} субъекта доступа можно трактовать как ветви графа. Если говорить о вершинах графа, то при этом возможны два подхода. Они основаны на том, что выбирается в качестве вершин графа – зоны или точки доступа. Проанализируем, что же целесообразно выбрать за основу рассматриваемого представления.

Учтем, что система контроля доступа однозначно фиксирует факты регистрации в точках доступа. Однако факты прохода через точку доступа могут и не регистрироваться. В п. 2.2 были показаны примеры, когда субъект доступа, зарегистрировавшийся в точке доступа, не прошел ее. Другой пример, когда используется ТД с односторонним контролем. В этом случае также неизвестно точно, находится ли СД в зоне, в которую он переместился, или уже вышел в предыдущую.

Поэтому в общем случае в системе КУД при регистрации субъекта доступа в ТД возникает неопределенность, в какой зоне реально находится СД – из которой или в которую он переме-

щался. Как факт можно принять только то, что субъект зарегистрировался в *i*-й точке доступа. Следовательно, можно говорить о целесообразности выбора точек доступа в качестве вершин графа.

Другой подход, использующий зоны как вершины графа, также может использоваться в некоторых задачах.

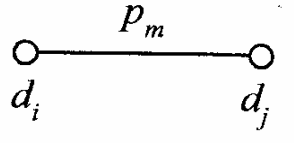


Рис. 19. Вершины и ветвь графа

Рассмотрим граф (рис. 19), вершины которого будут соответствовать точкам доступа D_i, а ребра – переходам p_m между этими ТД.

То есть переход p_m можно представить как ребро графа p_m, соединяющее две концевые вершины d_i и d_j графа – точки доступа $p_m = (d_i, d_j)$.

Совокупность возможных корректных переходов p_m, $m = 1, ..., M$ составляет множество P.

Таким образом, ребро определяет корректный переход между двумя точками доступа, т. е. возможность санкционированного перемещения субъекта доступа в системе. Некорректные переходы должны контролироваться другими средствами комплексной системы безопасности, к примеру охранной сигнализации или телевизионного наблюдения.

Тогда граф будет определяться соответствующими множествами точек доступа и корректных переходов между ними $G = (D, P)$.

Если два ребра графа (перехода) имеют общую концевую вершину (точку доступа), то они называются *смежными.* Ребра с одинаковыми концевыми вершинами называются *параллельными.* В СКУД это соответствует наличию нескольких путей перемещения между одними и теми же точками доступа. Если в СКУД нет нескольких путей перемещения между двумя ТД, то граф называется *простым.*

Маршрут субъекта доступа в графе $G = (D, P)$ представляет собой конечную чередующуюся последовательность точек доступа и переходов между ними $d_o, p_1, d_l, p_2, ..., d_{n-1}, p_n, d_n$, причем d_{n-1} и d_n являются концевыми вершинами ребра p_n.

Маршрут называется *открытым*, если его концевые вершины различны, в противном случае называется *замкнутым*, а если он начинается и оканчивается в разных внешних точках доступа, то *квазизамкнутым*.

В случае СКУД граф может быть:

- *неориентированным* или *ненаправленным*, если точка доступа допускает корректные перемещения в любом направлении;
- *ориентированным* или *направленным*, если перемещение через точку доступа допускается только в одном направлении;
- *смешанным*.

Граф называется *пленарным*, если его можно нарисовать на плоскости таким образом, что его ребра пересекаются только в вершинах. Основная часть СКУД может быть представлена пленарными графами.

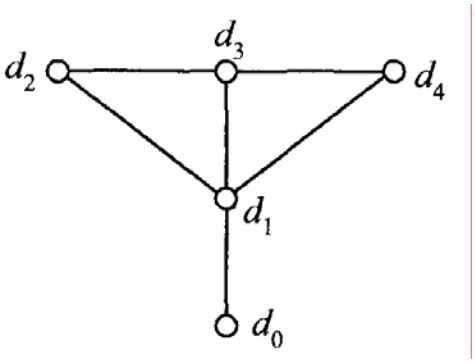


Рис. 20. Граф СКУД с параллельно связанными зонами

Порядок графа определяется количеством вершин, т. е. точек доступа (или, что то же самое, количеством элементов множества *D*).

На рис. 20 приведен пример графа для объекта, изображенного на рис. 6. Исходная зона свободного доступа обозначена как нулевая точка доступа.

Рассмотрим, для примера, некоторый объект, имеющий два этажа, план которого показан на рис. 21. В левой части здания расположен основной вход из зоны свободного доступа,

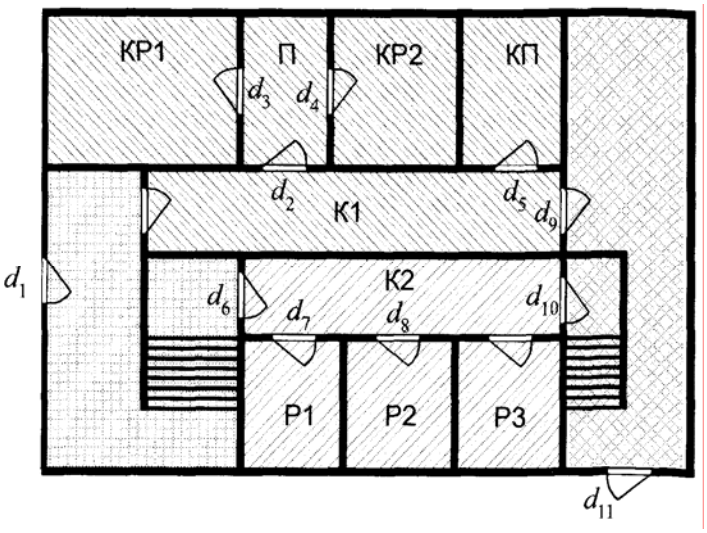


Рис. 21. План контролируемого объекта

контролируемый точкой доступа d_1. В правой – аварийный (пожарный) выход (точка доступа d_{11}). Двери пожарного выхода, закрытые в штатной ситуации, разблокируются при срабатывании системы пожарной сигнализации, обеспечивая свободный выход для всех пользователей системы.

На первом этаже расположены кабинеты руководства КР1 и КР2. Доступ в них осуществляется из коридора К1 через приемную П. Контроль доступа в приемную и кабинеты реализуется соответственно точками доступа d_2, d_3 и d_4. Из коридора К1 возможен проход в комнату переговоров КП через ТД d_5.

На втором этаже расположен коммерческий отдел. Для контроля прохода в коридор служит ТД d_6. Доступ в рабочие комнаты отдела Р1, Р2 контролируемого (в пределах отдела) доступа (d_7, d_8) и не контролируемого Р3 осуществляется из коридора К2. При этом в комнату Р3 возможен свободный доступ из коридора К2 (в том числе и для лиц, имеющих доступ в комнаты Р1 и Р2).

Как из коридора К1, так и К2 в аварийной (пожарной) ситуации возможен выход через соответствующие точки доступа d_9 и d_{10}, которые становятся автоматически доступными в упомянутой ситуации.

В рассматриваемом примере имеется три подсистемы КУД. Две контролируют первый и второй этажи. Третья, аварийная, контролирует пожарные выходы (в правой части здания).

Взаимосвязь точек доступа может быть в общем виде представлена графом, ветви которого определяют возможные пути перемещения субъектов через точки доступа (т. е. возможные корректные маршруты прохождения системы КУД). На рис. 22 представлен планарный граф, соответствующий рассматриваемому объекту и определяющий взаимосвязь множества ТД.

На графе диаграммами Эйлера – Венна с разной штриховкой показана взаимосвязь подмножеств D_i (подсистем) множества точек доступа D рассматриваемой СКУД. В этом примере имеем три пересекающихся подмножества точек доступа. Пересечение

первого D_1 и второго D_2 определяет главный вход как общую точку d_1 доступа.

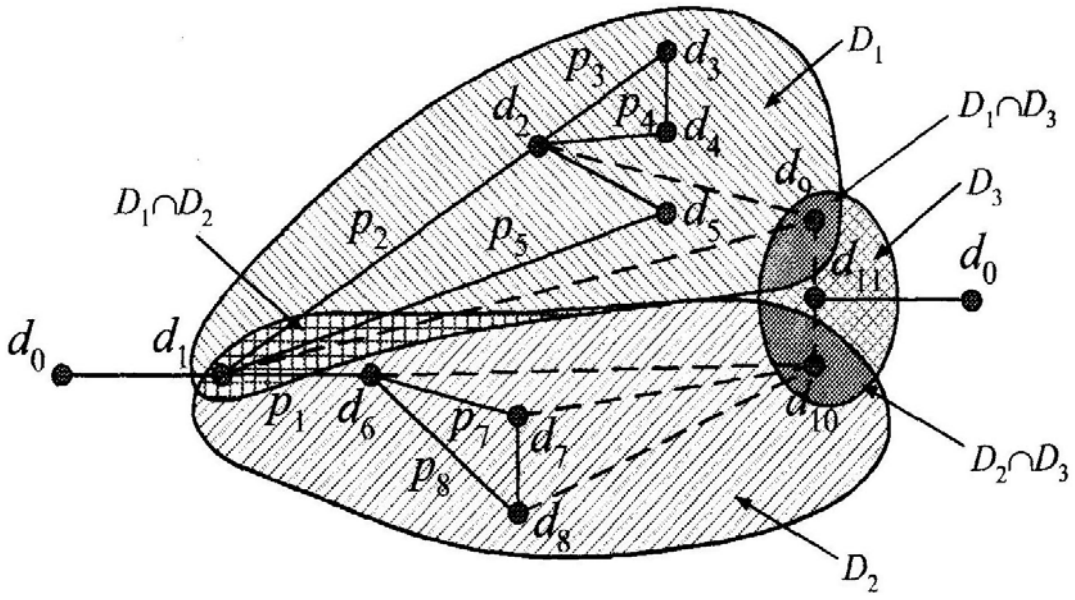


Рис. 22. Граф, определяющий взаимосвязь точек доступа

Таким образом, ТД d_1 принадлежит как подмножеству D_1, так и D_2, т. е.

$$d_1 \in (D_1 \cap D_2).$$

Кроме того, пересекаются подмножества D_1 и D_3 аварийной подсистемы, а также D_2 и D_3:

$$d_9 \in (D_1 \cap D_3),$$
$$d_{10} \in (D_2 \cap D_3).$$

Соответствие рис. 21 и 22 поясняется штриховкой соответствующих диаграмм Эйлера – Венна на графе и помещений на плане объекта.

Ребра графа с концевыми вершинами d_9, d_{10} и d_{11}, т. е. переходы, используемые только в аварийной ситуации, обозначены пунктиром.

Рассмотренный граф – это неориентированный (ненаправленный) пленарный граф 11-го порядка.

Математическая модель процесса идентификации

Формализуем процессы считывания и обработки информации в системе контроля и управления доступом, используя структурную схему, приведенную ранее на рис. 2.

Идентификационные признаки *m*-го объекта/субъекта определяются в общем случае матрицей *X* параметров ИП или функций, характеризующей его. Пусть *M* – количество информационных признаков, а *K* – максимальное количество параметров одного из признаков. Тогда можно записать выражение для матрицы

$$X = \begin{bmatrix} x_{11} & x_{21} & \cdots & x_{K1} \\ x_{12} & \cdots & \cdots & x_{K2} \\ \cdots & x_{km} & \cdots & \cdots \\ x_{1M} & \cdots & \cdots & x_{KM} \end{bmatrix}.$$

Элемент x_{km} представляет собой *k*-й параметр (функцию) *m*-го признака. Количество параметров разных ИП может быть различным, т. е. часть элементов матрицы *X* может быть равна нулю.

Считыватель СКУД преобразует информационные признаки x_{km} с носителями определенной физической природы в сигналы z_{km}, пригодные для дальнейшей обработки контроллером. Алгоритм преобразования определяется оператором *F*:

$$Z = F\{X\}, \text{ где } \quad Z = \begin{bmatrix} z_{11} & z_{21} & \cdots & z_{K1} \\ z_{12} & \cdots & \cdots & z_{K2} \\ \cdots & z_{km} & \cdots & \cdots \\ z_{1M} & \cdots & \cdots & z_{KM} \end{bmatrix}.$$

В частном случае одного ИП матрица *Z* представляет собой матрицу-строку. Например, для числового пароля из шести цифр 052830 соответствующие элементы единственной строки матрицы *Z* будут совпадать с цифрами введенного пароля *Z* = [052830].

Отметим, что в общем случае критерии сравнения могут быть различными для разных ИП одного и того же субъекта/объекта.

Контроллер осуществляет сравнение по определенному алгоритму матрицы Z с эталонными Z_i^o (i – порядковый номер субъекта доступа $i = 1...I$; o – количество субъектов доступа), хранящимися в базе данных. Критерий сравнения обозначим оператором C, который должен учитывать возможные допуски ΔZ на изменение значений параметров ИП, которые подвержены случайным изменениям в силу объективных или субъективных обстоятельств (наличие шумов воздействия помех, временные изменения идентификационных признаков и так далее). В общем случае контроллер сравнивает матрицу Z со всеми эталонами Z_i^o по очереди, тем самым определяя номер i субъекта доступа, обладающего этим идентификатором, или фиксируя отсутствие эталона Z_i^o, соответствующего предъявленному Z. Отметим, что критерии сравнения могут быть различными для разных информационных признаков одного и того же объекта/субъекта.

На основании результатов сравнения (фактически по найденному значению i) и информации об уровне доступа i-го объекта/субъекта, хранящейся в базе данных, контроллер формирует матрицу Y_i выходных сигналов:

$$Y_i = C\left\{Z, Z_i^o\right\}\Big|_{i=1...I}.$$

В состав этих сигналов, прежде всего, входят сигналы, управляющие исполнительными устройствами.

Уровень доступа СД определяет разрешенные зоны доступа, а также временные и календарные интервалы доступа (т. е. когда, куда, к чему разрешен доступ). Для детерминированной системы, каковой является СКУД, это определяет реакцию системы на действия субъекта доступа. То есть процедуру функционирования заграждающих устройств, в свою очередь приводимых в действие исполнительными устройствами.

Учитывая, что большинство современных СКУД используют цифровую обработку, на выходе считывателя будем иметь матрицу Z, элементы которой представляют собой цифры в той или иной системе счисления. Тогда реально алгоритм сравнения C во многих случаях упрощается и сводится к сравнению элементов матриц Z и Z_i^o с целью выявления совпадающей с эталонной. Или, что то же самое, должно быть определено значение i, при котором выполняется условие

$$Z - Z_i^o = 0.$$

Однако в общем случае это будет многоальтернативная проверка гипотез обнаружения, оценки параметров или распознавания образов.

Контрольные вопросы и задания

1. Приведите обобщенную структурную схему СКУД. Опишите принцип функционирования.
2. Какие структуры зон контролируемого доступа вы знаете? Охарактеризуйте кратко каждую.
3. Проанализируйте возможные перемещения субъекта доступа в контролируемых зонах.
4. Что такое точка доступа в контролируемую зону? Перечислите их особенности в СКУД.
5. Опишите математическую модель СКУД.

Глава 3. МЕТОДЫ И СРЕДСТВА ИДЕНТИФИКАЦИИ В СКУД

Идентификационные признаки, по которым можно решить задачи идентификации и аутентификации субъекта доступа, обычно находятся на некотором материальном носителе-идентификаторе. Это могут быть либо физически нанесенные на какой-либо идентификатор те или иные идентификационные признаки, либо непосредственно принадлежащие субъекту доступа физически или виртуально. Считыватель является устройством, позволяющим считать эту информацию с идентификатора. Очевидно, что эти пары устройств – идентификатор и считыватель – жестко связаны между собой физическим принципом нанесения или передачи идентификационных признаков и считывания их. Поэтому будем рассматривать эту пару упомянутых устройств как устройство идентификации.

3.1. Методы и типы идентификации

Рассмотрим, что может служить идентификатором (непосредственным носителем ИП) и что может быть использовано в качестве собственно идентификационных признаков. Для этого выделим самые общие группы носителей идентификационных признаков как с точки зрения практической реализации, так и с позиции защищенности от основных угроз несанкционированных действий (НСД): копирования, принуждения, кражи носителя, потери или передачи его другому лицу и других. Заметим, что последние угрозы весьма реальны и позволяют в ряде случаев достаточно легко несанкционированно преодолеть СКУД.

Итак, для идентификации может использоваться следующее.

• Некий материальный носитель, предмет (ключ, карточка, радиобрелок, номерной знак автомашины и тому подобное), в общем случае не связанный непосредственно с субъектом доступа, на который тем или иным образом нанесены идентификационные признаки.

• Знания субъекта, например буквенно-цифровой пароль, являющийся идентификационным признаком.

• Собственно субъект или объект доступа – его характерные и, по возможности, уникальные индивидуальные особенности (отпечаток пальца или ладони, параметры пульса для человека; форма предмета, например автомашины и т. п.), которые могут служить информационными признаками.

Если говорить о наиболее часто встречающемся случае, когда речь идет о контроле доступа людей (субъектов), то используются три общих принципиально разных метода, основанных на том, что:

1) пользователь имеет;

2) пользователь знает;

3) характеризует его как индивидуума.

К идентификаторам, использующим первый метод, можно отнести карты доступа с различными физическими принципами записи информации (идентификационных признаков), брелоки, пропуска и тому подобные предметы.

В качестве знаний пользователя наиболее широко используются различные буквенно-цифровые пароли, например набираемые на клавиатуре СКУД.

В последнем методе, в свою очередь, можно говорить о двух группах биометрических признаков. Во-первых, о *квазистатических* признаках, мало меняющихся во времени (например, форма лица, отпечатки пальцев или ладони и аналогичные), и, во-вторых, о *квазидинамических* признаках, подверженных достаточно значительным временным изменениям (форма и динамика нанесения подписи, спектральный состав речи, тип походки, параметры пульса и тому подобные признаки).

Имитостойкость и криптозащита СКУД

Прежде всего рассмотрим возможные несанкционированные действия с носителями ИП, которые могут тем или иным образом привести к несанкционированному преодолению СКУД. Часть этих действий, такие как наблюдение, манипулирование, копирование, принуждение, повреждение, сформулированы в соответствующем государственном стандарте. Приведем определения этих терминов.

Наблюдение – действия, выполняемые с устройствами контроля и управления доступом без прямого доступа к ним, целью которых является получение действующего кода.

С общей точки зрения, такие действия – лишь частный случай съема информации по визуальному каналу. Поскольку съем информации о СКУД в целом и, в частности, об идентификационных признаках является одним из видов несанкционированных действий и может привести к несанкционированному преодолению СКУД, будем пользоваться более общим термином *«съем информации».* Этот известный термин более корректно определяет несанкционированное действие, определяемое в стандарте, поскольку может быть не только «наблюдение» за набором кода на клавиатуре, но и съем информации, к примеру, по радиоканалу для бесконтактных карт с соответствующим принципом действия.

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.

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 преграждающие управляемые устройства. Устройства контроля и управления доступом при этом могут функционировать нормально.

Повреждение – разрушающее воздействие без использования инструментов, а также с помощью ручных и других типов инструментов.

Однако в стандарте отсутствует такой достаточно опасный с точки зрения преодоления СКУД вид несанкционированного доступа, как кража идентификатора.

Защищенность

Под *защищенностью* идентификатора будем понимать скрытность его использования, устойчивость к несанкционированным действиям, сложность съема информации об идентификационных признаках и их параметрах и использования тем или иным способом этой информации или самого идентификатора для несанкционированных действий в СКУД.

Проанализируем защищенность и уязвимость различных носителей ИП от НСД. Прежде всего отметим, что для любых способов реализации упомянутых выше методов наиболее опасно принуждение, т. е. насильственные действия над лицом, имеющим право доступа.

Материальный носитель (т. е. то, что пользователь имеет) может быть потеряно, украдено или передано другому лицу. Таким образом, с точки зрения несанкционированного завладения и использования носителя такого типа СКУД достаточно слабо защищены. Кроме кражи для некоторых способов реализации первого метода представляет опасность и копирование носителя ИП.

Для метода, использующего знания пользователя, наиболее опасен съем информации, в частности по визуальному каналу (например путем наблюдения за набором пароля на клавиатуре).

Также практически неконтролируема передача этого пароля владельцем другому лицу. Может представлять опасность и манипулирование (например подбор пароля при отсутствии защиты от этого).

Наибольшая защищенность достигается при использовании биометрических признаков.

Важно представлять пути улучшения защищенности средств, использующих различные методы идентификации, от разных угроз.

В табл. 2 приведено сравнение рассматриваемых методов по устойчивости к различным видам несанкционированных действий.

Таблица 2

Основа метода идентификации	Защищенность от НСД						Возможность аутентификации
	Кража	Съем информации	Манипулирование	Копирование	Принуждение	Повреждение	
То, что пользователь имеет	Н	В	В	Н...В	Н	Н...В	Н
То, что пользователь знает	В	Н	С...В	В	Н	Н...В	Н
То, что характеризует пользователя	В	В	В	П...В	Н	Н...В	В

В таблице использованы следующие обозначения защищенности:

Н – низкая,

С – средняя,

П – повышенная,

В – высокая.

В некоторых позициях таблицы указан диапазон изменения, так как степень защищенности будет зависеть от конкретно выбранного технического способа реализации метода и от его параметров.

Классификация идентификаторов

Идентификаторы могут классифицироваться по ряду признаков, связанных, прежде всего, со способом технической реализации, непосредственно зависящим от принципа действия. К числу этих признаков можно отнести следующие.

Способ взаимодействия идентификатора и считывателя:

- бесконтактные (дистанционного действия);
- контактные (с непосредственным взаимодействием).

Физический принцип действия. По технологии нанесения – считывания или передачи – приема информации различают:

- магнитную запись;
- оптический (в том числе инфракрасный);
- радиочастотный;
- штриховые коды;
- проксимити-технологию;
- смарт-технологию;
- технологию Виганда;
- механическое кодирование;
- точ-мемори (*touch-memory*);
- биометрический (квазистатический и квазидинамический);
- кодонаборные способы.

Ниже рассматриваются основные типы идентификаторов. При этом, поскольку наиболее важным является физический принцип действия, от которого во многом зависят эксплуатационные характеристики как идентификатора, так и считывателя, то в дальнейшем за основу возьмем именно физический принцип действия. Однако надо помнить, что это не исключает, а наоборот

требует учета как метода идентификации, так и способа его технической реализации при выборе идентификатора для конкретной системы контроля доступа.

3.2. Пассивная радиочастотная технология идентификации

В современных системах контроля и управления доступом радиочастотный принцип (технология) идентификации получает все большее распространение благодаря своим возможностям и преимуществам. Другой термин, часто используемый на практике, – проксимити (*proximity*). В разных источниках встречаются и другие названия: бесконтактная, или дистанционная, технология. Однако все они недостаточно полно отражают физический принцип, используемый в таких системах. Например, технологию идентификации человека по радужной оболочке глаза также можно назвать бесконтактной, или дистанционной, так как считывание в современных системах может осуществляться на расстояниях порядка метра. Термин «радиочастотный принцип идентификации» представляется наиболее правильным, поскольку, во-первых, он отражает физический принцип, используемый в таких системах (данные от идентификатора на считыватель передаются на радиочастоте), и, во-вторых, соответствует используемому в зарубежной литературе общему для данного класса систем определению *Radio Frequency Identification* (*RFID*). В дальнейшем мы будем использовать термины *радиочастотная технология идентификации* и *проксимити-технология.*

Устройство считывателя и идентификатора

Как и в других системах идентификации, использующих материальный носитель идентификационного признака ИП, в системах радиочастотной идентификации есть считыватель и идентификатор (карта, брелок или метка). В идентификаторе находится микросхема с фиксированным или перепрограммируемым ко-

дом, катушка индуктивности и конденсатор, представляющие собой резонансный колебательный контур (рис. 23).

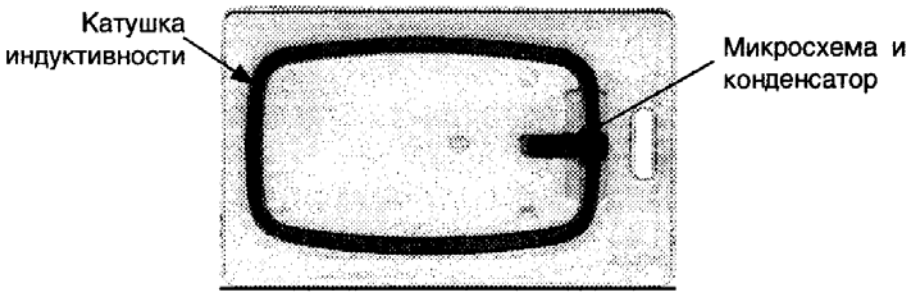


Рис. 23. Устройство карты радиочастотной идентификации (проксимити)

Индуктивность в зависимости от используемого диапазона частот может выполняться в виде катушки или печатных проводников. В диапазоне частот порядка сотен килогерц необходима индуктивность катушки в несколько миллигенри, в то время как на частоте 13,56 МГц достаточно катушки с индуктивностью в несколько микрогенри. В литературе обычно катушку индуктивности называют антенной, хотя реально в упомянутых диапазонах частот таковой она не является. Чтобы в этом убедиться, достаточно сравнить ее размеры с рабочей длиной волны.

Когда идентификатор оказывается вблизи считывателя, два контура (идентификатора и считывателя) становятся индуктивно связанными. Контур считывателя можно рассматривать как первичный, а идентификатора – как вторичный. Индуктивная связь катушек приводит к появлению взаимной индуктивности. Следовательно, появление в магнитном поле первичного контура катушки индуктивности вторичного приводит к изменению параметров первичного контура считывателя, которые могут регистрироваться. Таким образом, изменяя параметры вторичного контура, например осуществляя расстройку или шунтирование вторичного контура, можно организовать информационный обмен между считывателем и идентификатором.

Для изменения параметров вторичного контура идентификатора, т. е. для модуляции, используется специальная микросхема, коммутирующая вторичный контур в соответствии с запрограммированным в ее памяти кодом. Внутри микросхемы (рис. 24) находятся: цепь синхронизации; энергонезависимая память для хранения кода идентификатора; выпрямитель и стабилизатор напряжения с буферным конденсатором; схема модуляции, изменяющая параметры контура; детектор команд в носителях с двухсторонним обменом информацией.

Считыватель представляет собой обычно микропроцессорное устройство, содержащее первичный колебательный контур и электронную схему, позволяющую детектировать сигнал, модулированный кодом карты. Используемый частотный диапазон существенно влияет на характеристики системы.

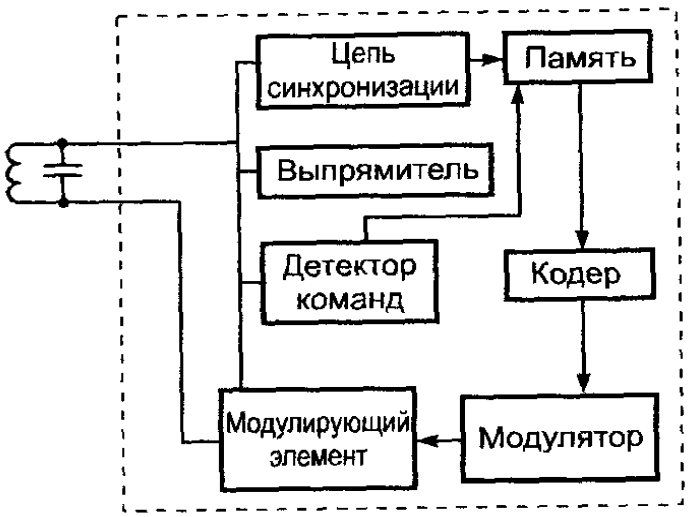


Рис. 24. Функциональная схема бесконтактного идентификатора

В диапазонах длинных и коротких волн для двухстороннего обмена информацией между считывателем и идентификатором используется индуктивная (или трансформаторная) связь (рис. 25). В этом состоит основное отличие физического принципа проксимити-технологии от приемопередающих радиоканальных устройств. Идентификатор не является передатчиком, а лишь модулирует амплитуду несущей частоты считывателя в соответствии с запрограммированным в его памяти кодом.

В диапазоне СВЧ для обмена информацией между считывателем и идентификатором используется радиоканал.

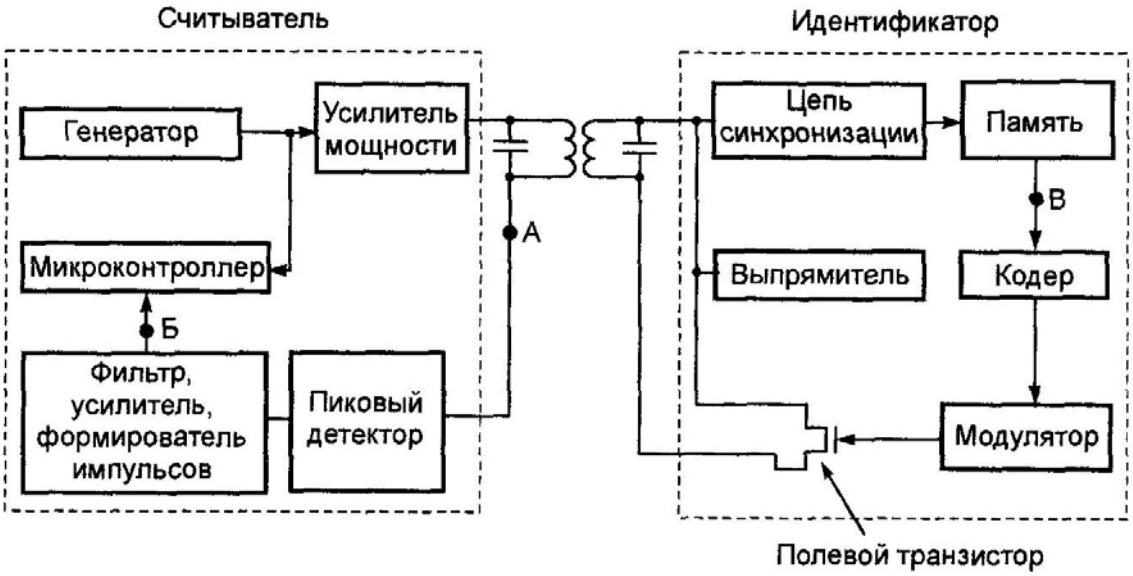


Рис. 25. Функциональная схема радиочастотного устройства идентификации

Типичный сеанс связи между считывателем и картой состоит из следующих этапов.

1. Считыватель формирует колебания несущей частоты, непрерывно контролируя наличие модуляции в сигнале. Модуляция сигнала будет означать обнаружение карты в зоне действия считывателя (рис. 26).

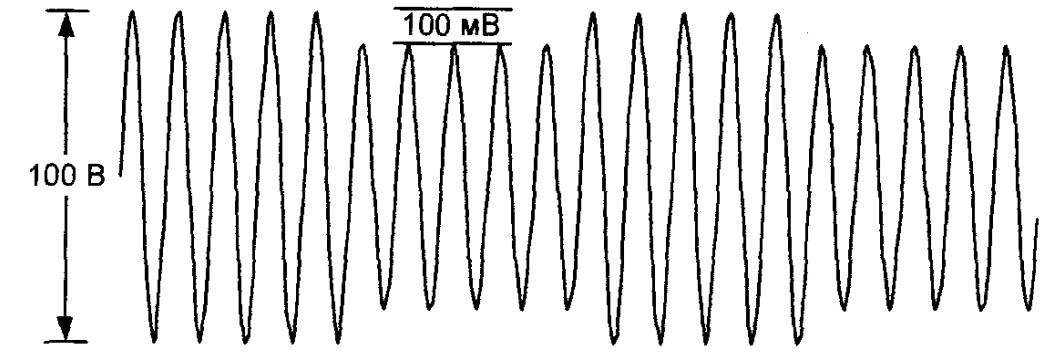


Рис. 26. Амплитудно-модулированный сигнал

2. Карта попадает в поле считывателя. После накопления энергии, достаточной для работы микросхемы и синхронизации, начинается управление транзистором, шунтирующим контур.

3. Шунтирование контура осуществляется в соответствии с информационным кодом, записанным в памяти микросхемы карты. Это приводит к изменению напряжения несущего колебания в контуре считывателя.

Кодирование информации в системах радиочастотной идентификации

Выбор способа кодирования влияет на возможность обнаружения и исправления ошибок при приеме, занимаемую сигналом полосу частот, возможность синхронизации, стоимость реализации и другие параметры системы. Существует много способов кодирования, однако в системах радиочастотной идентификации наибольшее распространение получили следующие три (рис. 27).

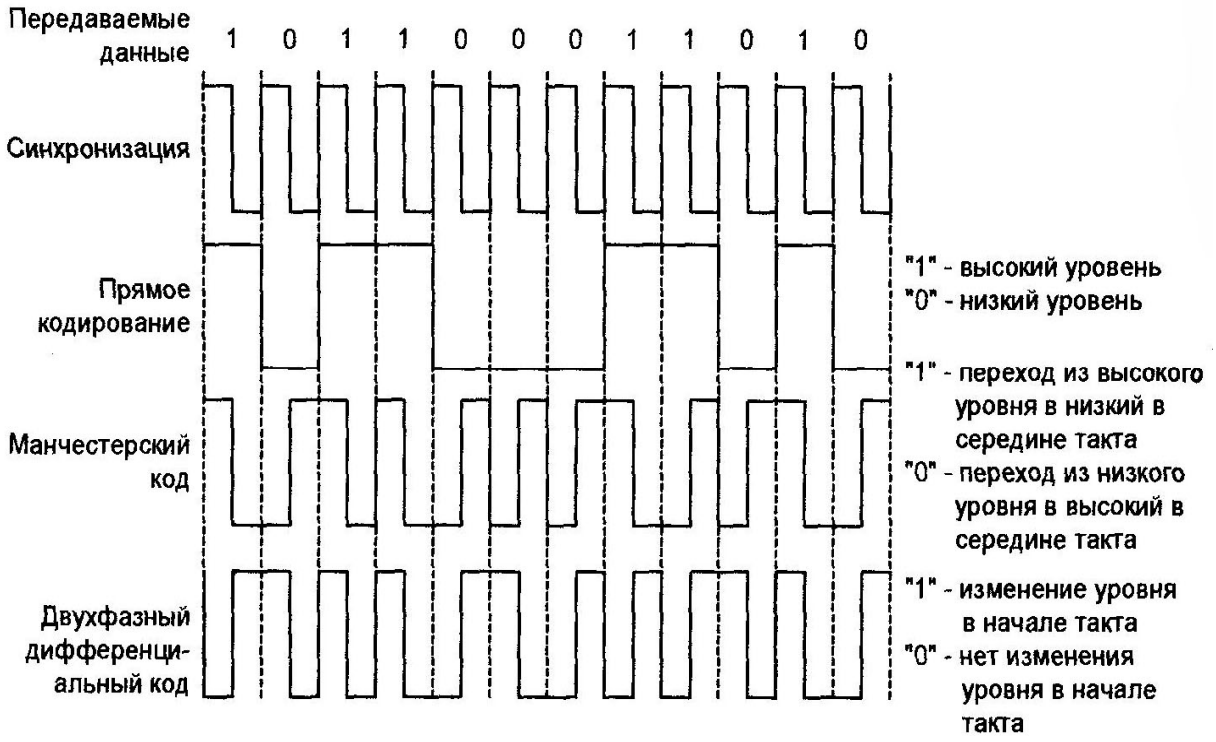


Рис. 27. Способы кодирования данных

1. *Прямой код.* В этом случае простейшего двухуровневого кода нулю соответствует низкий уровень сигнала, единице – высокий. Информационные переходы совпадают с границей бит. В зарубежной литературе этот код обозначается как «*NZR*» (*Non Return to Zero*), т. е. кодирование «без возврата к нулю». Достоинство такого способа кодирования – его простота: двоичный код сообщения не надо подвергать дополнительным преобразованиям. Однако этот код не обеспечивает синхронизации, и это является самым большим его недостатком.

2. *Дифференциальный двухфазный код.* Существует несколько разновидностей способа кодирования, использующего этот код, но в общем случае изменение уровня сигнала происходит каждый такт синхронизации, причем логические значения «0» и «1» различаются по переходам напряжения в середине такта синхронизации. Поскольку переходы осуществляются каждый такт вне зависимости от значения бита («0» или «1»), этот метод используется для синхронизации считывателя с потоком передаваемых данных (самосинхронизирующийся код). Также он обеспечивает возможность обнаружения ошибок.

Манчестерский код – разновидность дифференциального двухфазного способа кодирования. Он также является самосинхронизирующимся кодом. Единица соответствует переходу сигнала из высокого уровня в низкий, нуль – обратному переходу. Важная особенность манчестерского кода – отсутствие у сигнала постоянной составляющей при передаче длинной последовательности единиц или нулей.

В некоторых системах радиочастотной идентификации в зоне действия считывателя может присутствовать одновременно несколько идентификаторов. В этом случае возникает коллизия – попытка модуляции несущего сигнала считывателя двумя идентификаторами одновременно. Для корректного считывания информации со всех идентификаторов используются специальные алгоритмы, позволяющие предотвращать коллизии. Алгоритмы

основаны на временном разделении сигналов от различных идентификаторов. Задача усложняется, когда требуется не только считывание, но и запись данных на идентификаторы.

Факторы, влияющие на дальность считывания

Рассмотрев особенности функционирования считывателей и идентификаторов, можно сформулировать факторы, влияющие на дальность считывания в системах радиочастотной идентификации с пассивными идентификаторами.

1. Рабочая частота и конструкция антенны считывателя.
2. Добротность контура антенны считывателя.
3. Взаимная ориентация антенн считывателя и идентификатора в пространстве.
4. Величина тока и напряжения в катушке считывателя.
5. Чувствительность приемника считывателя.
6. Алгоритм кодирования/декодирования данных и используемый способ модуляции сигнала.
7. Длина кодовой посылки (количество бит в коде идентификатора).
8. Окружающие условия (наличие близкорасположенных металлических предметов, электромагнитных помех и т. п.).

3.3. Штриховые коды

Штриховые коды достаточно широко используются для идентификации. Наиболее хорошо известно такое их применение, как маркировка товаров.

Штриховой код представляет собой группу полос различной ширины (рис. 28), наносимых на поверхность идентификатора.

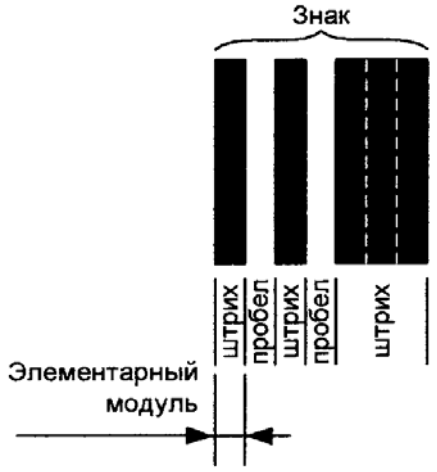
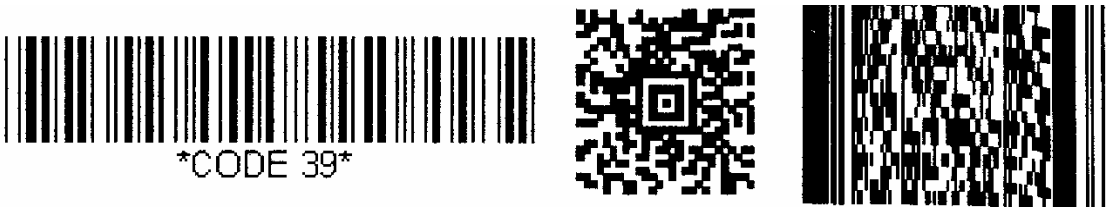


Рис. 28. Знак штрихового кода

Информационным параметром в штриховом коде является соотношение ширины темных полос (штрихов) и ширины светлых полос (пробелов между штрихами), что соответствует широтной импульсной модуляции. Каждая цифра кодируется определенным количеством штрихов и пробелов. Отведенное для каждой цифры кода место называется знаком и является основной единицей информации в штриховом коде. Все знаки обычно имеют одинаковую ширину и состоят из элементарных модулей, поэтому ширина штрихов и пробелов всегда кратна элементарному модулю. Элементарный модуль – это самый узкий элемент (штрих или пробел).

Существуют различные способы кодирования информации, называемые штрих-кодовыми кодировками. Различают одномерные (линейные) и двумерные штриховые коды (рис. 29).



а) *б)* *в)*

Рис. 29. Примеры штрих-кодов: а – одномерного; б, в – двумерных

Одномерными (линейными) называются штрих-коды, читаемые в одном направлении (по горизонтали поперек штрихов). Наиболее распространенные линейные кодировки (символики): *EAN*, *UPC*, *Code* 39, *Code* 128, *Codabar*, *Interleaved* 2 *of* 5. Линейные символики позволяют кодировать небольшой объем информации (до 20 – 30 символов, обычно цифр).

Двумерными называются штрих-коды, разработанные для кодирования большого объема информации (до нескольких тысяч символов).

Двумерный код считывается при помощи специального сканера и позволяет быстро и безошибочно вводить большой объем

информации. Декодирование такого кода проводится в двух измерениях (по горизонтали и по вертикали). К двумерным штрих-кодам относятся *PDF*417 *Aztec*, *Data Matrix* и др.

Использование штриховых кодов является наиболее дешевой технологией идентификации, поэтому они широко применяются для маркировки товаров в магазинах и на складах, в системах учета оплаты проезда и на автоматизированных парковках благодаря низкой стоимости идентификатора. В современных системах контроля доступа штриховой код используется преимущественно в сочетании с другими способами идентификации, например на пластиковой карте со штрих-кодом может располагаться фотография пользователя.

Считывание кода осуществляется оптическим способом в видимом или инфракрасном диапазоне волн. Считыватель содержит источник света, фотодетектор и устройство обработки сигнала (рис. 30). Источник света излучает свет с определенной длиной волны на штриховой код. Отраженный свет возвращается обратно и фокусируется на фотодетекторе. Фотодетектор преобразует оптическую информацию в электрический сигнал, который обрабатывается и преобразуется в формат, пригодный для передачи в устройство обработки (контроллер) для принятия решения.

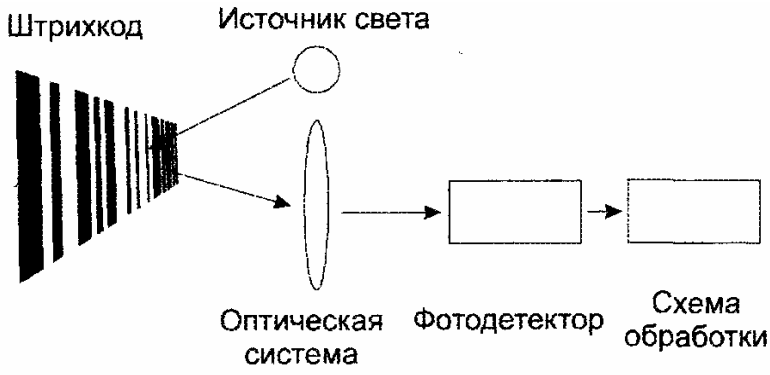


Рис. 30. Устройство считывателя штрих-кода

Существуют различные типы штриховых кодов. Каждый тип разработан для определенной области применения и обладает своими преимуществами и особенностями. Так, некоторые коды имеют высокую плотность записи информации, позволяющую разместить на ограниченном пространстве большой объем данных. Существуют коды с возможностью проверки считанной информации, обеспечивающие контроль ошибок при чтении. Неко-

торые штриховые коды позволяют записывать как цифровую, так и символьную информацию.

В системах контроля и управления доступом наиболее часто используются штриховые коды *Interleaved* 2 *of* 5 и *Code* 39. Первый из них позволяет кодировать только цифровую информацию, а второй – цифровую и символьную.

Код Interleaved 2 *of* 5

Этот код (известный также как *USSITF*2/5, *ITF* и 1-2/5) является непрерывным штрих-кодом переменной длины и позволяет кодировать цифры от 0 до 9. Он относится к кодам с высокой плотностью записи и позволяет записывать до 18 цифр на дюйм при ширине элементарного модуля 0,19 мм. Высокая плотность достигается за счет исключения пробелов, разделяющих соседние знаки (рис. 31).

Рис. 31. Примеры штрихового кода Interleaved

Код *Interleaved* используется во многих областях для кодирования цифровых данных и является стандартным международным кодом для маркирования тары и упаковки единиц поставки. Код *Interleaved* широко применяется в автоматизированных системах для идентификации предметов складирования, багажа в аэропортах, нумерации авиационных билетов, идентификации почтовых отправлений и др. Он принадлежит к семейству кодов «2 из 5» (2 *of* 5) и имеет пять элементов в знаке, два из которых являются широкими.

Особенность кода *Interleaved* – представление пар цифр в знаках штрихового кода с помощью пяти штрихов и пяти промежутков. При этом используется чередование цифр: на нечетных позициях (считая слева направо) знаки изображаются штрихами,

а на четных – пробелами (рис. 32). От этого произошло название кода – *Interleaved* («перемежающийся»). При кодировании данных с нечетным количеством знаков впереди записывается «0». В двоичном изображении широкий штрих или широкий промежуток идентичен «1», узкий штрих или узкий промежуток – «0». Соотношение ширины широкого и узкого элементов составляет не менее 2,5:1.

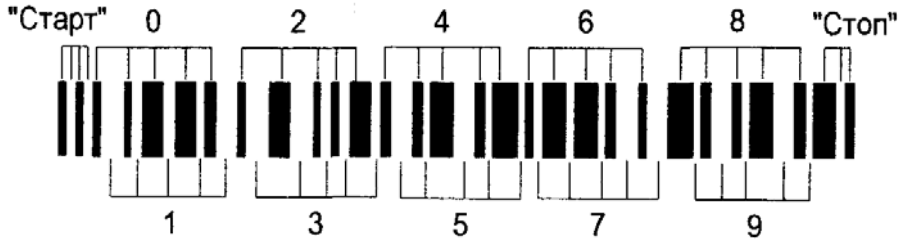


Рис. 32. Структура штрихового кода Interleaved

Знак «Старт» состоит из двух узких штрихов и двух узких промежутков. Знак «Стоп» состоит из одного широкого штриха, одного узкого штриха и одного узкого промежутка.

В коде *Interleaved* для повышения надежности считывания обычно используется контрольный знак. Контрольный знак располагается непосредственно после информационных знаков перед знаком «Стоп». Если добавление контрольного знака делает количество знаков в кодируемых данных нечетным, впереди кодовой строки непосредственно после знака «Старт» добавляется «0».

Код Code 39

Штриховой код *Code* 39 является кодом переменной длины и позволяет отобразить 43 символа, среди которых цифры, 26 символов английского алфавита и 7 служебных символов. Этот код может быть расширен для кодирования всех 128 символов *ASCII* путем удвоения числа знаков, приходящихся на один символ.

Этот код иногда называют «*Code* 3 *of* 9». Наименование штрихового кода связано со структурой изображения знаков

«3 из 9» (рис. 33), где три элемента знака (два штриха и один пробел) из девяти являются широкими, а остальные шесть – узкими. Каждый символ начинается и заканчивается темным штрихом, состоит из пяти темных и четырех светлых штрихов. Отношение ширины узкого и широкого штриха может составлять от 2,2:1 до 3:1.

Рис. 33. Примеры кода Code 39

Достоинством этого кода является его очень высокая достоверность чтения, которая может быть увеличена добавлением в символ контрольного знака. Согласно некоторым исследованиям, проведенным за рубежом, вероятность ошибки считывания составляет не более $3{,}33 \cdot 10^{-7}$.

Двумерный штрих-код Aztec

Этот код с высокой плотностью записи относится к двумерным, так как его считывание и декодирование осуществляется в двух измерениях. Он позволяет кодировать до 3750 символов полного набора *ASCII*-символов (256 байт). Штрих-код представляет собой квадратную матрицу с концентрическими квадратами в центре, которые служат для определения позиции кода относительно считывающего устройства. Данные в виде черных и белых модулей (элементарных квадратов черного или белого цвета) размещаются на различном расстоянии от центра по периметру опорных квадратов (рис. 34).

Рис. 34. Примеры штрихового кода Aztec

Такой способ размещения модулей позволяет кодировать различный объем данных, который пропорционален размерам матрицы. Кроме этого могут использоваться различные способы обнаружения и коррекции ошибок на основе кодов Рида – Соломона. Параметрами для штрих-кода *Aztec* являются размеры элементарного модуля и способ обнаружения и коррекции ошибок. Минимальные размеры штрих-кода составляют 15×15 модулей (что позволяет кодировать 12 *ASCII*-символов с 40%-ной избыточностью), максимальные – 151×151 (до 3750 символов с 25%-ной избыточностью).

Здесь приведены примеры только наиболее широко используемых штриховых кодов. Количество различных типов штриховых кодов составляет несколько десятков. Выбор конкретного типа штрих-кода зависит от многих параметров: объема и состава записываемых данных, требуемой надежности считывания, допустимых размеров штрих-кода, стоимости считывающей аппаратуры и других.

К преимуществам штриховых кодов можно отнести:

- низкую стоимость идентификатора и устройства для печати;
- возможность записи на идентификатор цифровой и символьной информации различной длины.

Основным недостатком штрихового кода является слабая защита от копирования или подделки. Штрих-код может быть скопирован с помощью копировального аппарата или другого оптического устройства считывания. В некоторых системах печати штрих-код закрывается пленкой, непрозрачной для видимого света, но позволяющей прочитать штрих-код в инфракрасном диапазоне. Принтер для печати штриховых кодов может наносить изображение кода с низкой контрастностью относительно окружающего фона, что не позволит просто воспроизвести код с помощью копировального аппарата. Все параметры штриховых кодов стандартизированы (ширина линий, расстояние между ними, количество линий, кодирующих один символ, и т. п.), поэтому формиро-

вание или воспроизведение штрихового кода с необходимыми данными не представляет сложности. Аналогами штрих-кодов в настоящее время являются голографические этикетки (марки) для защиты товаров.

3.4. Карты Виганда

В 1975 г. американский ученый Джон Виганд (*John R. Wiegand*) в результате 40-летних исследований открыл эффект быстрого изменения магнитных полей с помощью специально обработанных ферромагнитных проводников малого диаметра и их регистрации. Конструкция чувствительного элемента запатентована и для формирования сигналов требует всего лишь несколько простых элементов: пару постоянных магнитов и катушку индуктивности, расположенную между магнитами, вдоль которых перемещаются отрезки проволоки Виганда.

В начале восьмидесятых годов стали выпускать карты и считыватели, основанные на Виганд-эффекте. Устройство карт и считывателей иллюстрирует рис. 35.

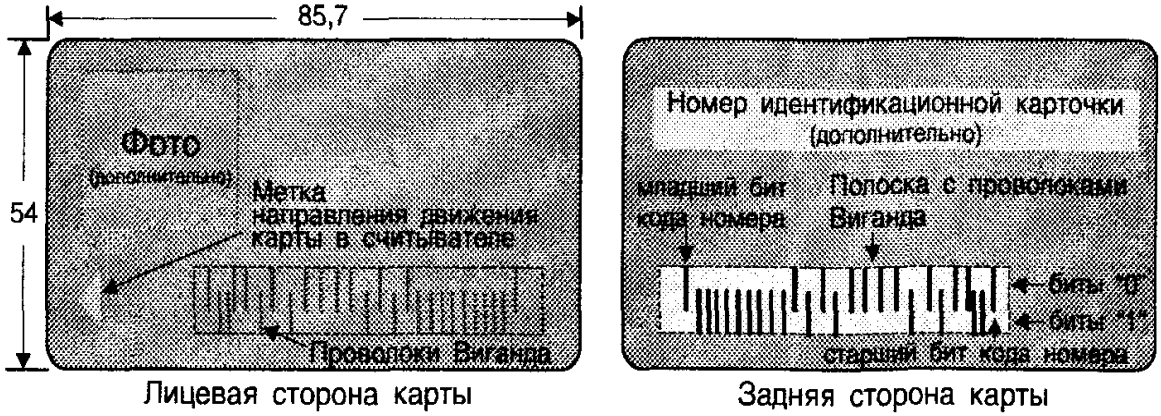


Рис. 35. Конструкция карты Виганда

В определенное место пластиковой карты толщиной 0,76 мм запрессованы два ряда отрезков проволоки Виганда. В считывателе предусмотрены чувствительные элементы для каждого ряда.

Количество отрезков и расстояние между ними определяют идентификационный код карточки. Обычно используются 26-битовые коды, что определяет количество отрезков проволоки в карте. Информационная емкость такой карты определяет 67 108 864 возможных комбинаций и практически сводит вероятность приобретения двух карт с одинаковым номером к нулю (теоретически вероятность меньше чем 2-10-8). Таким образом, эти карты относятся к уровню повышенной устойчивости по отношению к несанкционированным действиям согласно ГОСТ Р 51241 (не менее 107).

Эффект Виганда

Проволока Виганда производится из холоднообработанной ферромагнитной проволоки диаметром около 0,2 мм на основе сплава кобальта, железа и ванадия (викаллой). Процесс холодной обработки состоит из большого количества этапов скручивания и раскручивания проволоки в напряженном состоянии. При такой обработке максимальная деформация будет иметь место в поверхностном слое. Как следствие, магнитные свойства проводника будут изменяться в зависимости от расстояния до центра. Таким образом, эта процедура приводит к тому, что проволока Виганда имеет магнитомягкую сердцевину (стержень) и поверхность с высокой коэрцитивной силой (оболочка). При воздействии на проволоку внешнего продольного магнитного поля достаточной напряженности магнитное поле стержня будет переключать свою полярность, формируя импульсы Виганда.

Петля гистерезиса проволоки состоит из большого количества дискретных переходов, которые происходят в течение переключений полярности стержня и оболочки. Эти переходы известны как эффект Баркгаузена, суть которого заключается в том, что ферромагнетики, находясь в магнитном поле, напряженность которого изменяется непрерывным образом, изменяют свою намагниченность дискретно.

Существуют два способа формирования эффекта Виганда: симметричное и асимметричное магнитные переключения.

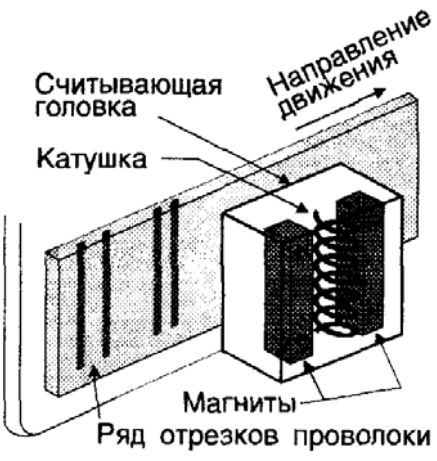


Рис. 36. Конструкция считывателя

При *симметричном* переключении для намагничивания и активизации проволоки Виганда используются магнитные поля одинаковой напряженности и противоположной полярности. Эти поля формируются, например, постоянными магнитами, установленными на стационарной головке считывателя. Проволоки Виганда перемещаются относительно головки (рис. 36).

Сначала насыщающее магнитное поле первого магнита одной полярности ориентирует полярности стержня и оболочки в одном направлении (этап А, рис. 37).

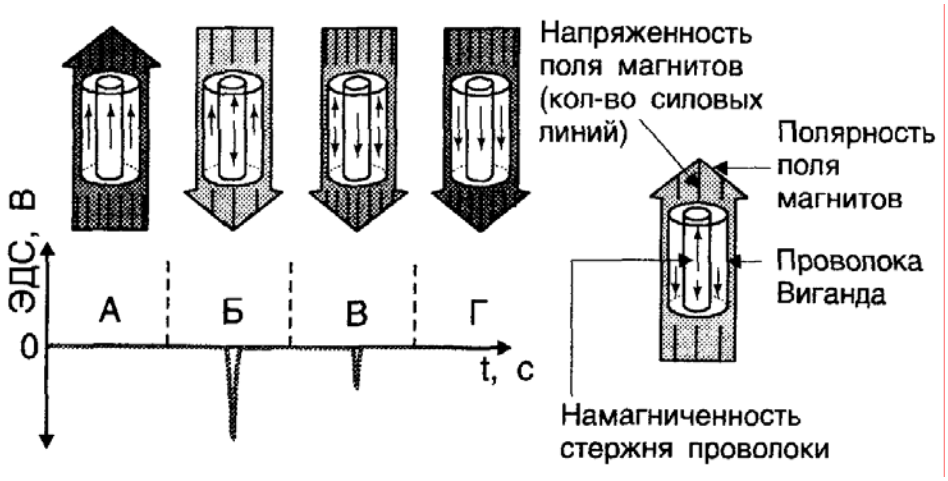


Рис. 37. Процесс формирования сигналов

В ходе перемещения проволоки к следующему магниту противоположной полярности изменяется полярность приложенного к проволоке поля. При приближении ко второму магниту напря-

женность вновь приложенного внешнего поля увеличивается. Это приводит к тому, что сначала переключается полярность стержня (этап Б, рис. 37) и генерируется импульс напряжения в катушке считывателя. Затем при дальнейшем увеличении напряженности поля (по мере дальнейшего приближения ко второму магниту) переключается полярность оболочки, генерируя импульс напряжения меньшей величины. Амплитуда этого импульса значительно меньше предыдущего (на порядок и более). В итоге магнитное поле второго магнита полностью насыщает проволоку Виганда.

При асимметричном режиме переключения проволока Виганда намагничивается и активизируется магнитными полями противоположной полярности и разной напряженности. Насыщающее магнитное поле первого, более мощного магнита одной полярности ориентирует полярности стержня и оболочки в одном направлении. Затем поле второго магнита противоположной полярности, но меньшей напряженности переключает полярность стержня (но не оболочки) и тем самым формирует импульс напряжения меньшей амплитуды в катушке считывателя. После этого насыщающее поле восстанавливает прежнюю полярность, одновременно переключая полярность намагниченности стержня, формируя импульс большей амплитуды.

Практически в большинстве случаев используется режим симметричного переключения из-за простоты подбора постоянных магнитов.

При магнитном переключении проволоки Виганда в катушке считывателя наводится электродвижущая сила (ЭДС) индукции продолжительностью порядка 10 мкс (рис. 38). Амплитуда ЭДС индукции катушки может составлять от 2 до 8 В в зависимости от конструкции

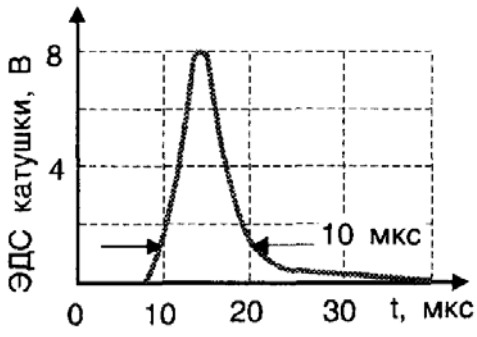


Рис. 38. Импульс ЭДС катушки считывателя

считывающей головки и сопротивления нагрузки. Важно отметить, что амплитуда ЭДС индукции не зависит от напряженности (если его значение больше напряженности насыщения) и полярности продольного магнитного поля. Зазор между головкой считывателя и проволоками Виганда, как правило, не превышает 1,3 мм.

Считыватели могут иметь и иные варианты своего исполнения. В другом варианте конструкции используется одна считывающая головка для обоих рядов отрезков проволоки (с одним магнитом и катушкой на каждый ряд) и одним общим насыщающим магнитом, расположенным вблизи головки и имеющим полярность, противоположную магнитам головки. Общий магнит устанавливается так, чтобы поляризовать определенным образом все отрезки проволоки до их прохождения перед головкой.

Области применения

На основе эффекта Виганда кроме СКУД работают некоторые типы измерителей расхода газов, жидкостей, датчиков скорости, измерителей положения и другие, в том числе датчики, применяемые в системах управления машинами и механизмами. Эффект Виганда наблюдается при температуре от –80 до +260 °С. Диапазон рабочих температур конкретного типа устройства определяется свойствами используемых элементов и не зависит от свойств проволоки Виганда. При соответствующей конструкции головки и расположении катушки относительно магнитов можно дополнительно контролировать направление перемещения проволок Виганда путем анализа полярности импульсов Виганда.

К преимуществам устройств на основе эффекта Виганда также можно отнести следующие:

- Отсутствие внешнего источника питания и двухпроводное подключение считывающей головки.
- Способ считывания, который исключает механический износ деталей считывающей головки.

- Высокая техническая надежность, определяемая простотой конструкций карт и считывателей.
- Высокая устойчивость карт к внешним воздействиям, в том числе электрическим и магнитным. Для того чтобы испортить карту, ее надо механически разрушить.
- Невозможность подделки карт вне заводских условий, при недоступности необходимой информации о технологии изготовления проволоки и используемых материалах, а также незнании последовательности расположения отрезков проволоки.

Характеристики интерфейса

При большом количестве производителей идентификаторов и считывателей, использующих различные физические принципы действия, весьма важным становится вопрос совместимости этих устройств. Поскольку в 80-х гг. подавляющее большинство СКУД использовали считыватели Виганда, то интерфейс для передачи данных от считывателя к контроллеру (интерфейс Виганда) стал «де-факто» стандартом среди производителей контроллеров. На сегодняшний день практически все современные контроллеры и считыватели, в том числе магнитных и проксимити-карт, поддерживают интерфейс Виганда. Интерфейс определяет совместимость различных устройств по электрическим параметрам и формату представления данных. Он использует две сигнальные линии, по одной из которых передаются импульсы, соответствующие «0» двоичного кода данных, а по другому – «1». Считыватель содержит схему, преобразующую электрические параметры интерфейса и формат представления данных от считывающего элемента (магнитной головки считывателя, схемы бесконтактного считывания и т. п.) в соответствующие параметры интерфейса Виганда. Для согласования скорости поступления информации от считывающего элемента со скоростью приема информации контроллером используется буфер. Скорость, с которой данные передаются на контроллер, фиксирована и не зависит от

скорости предъявления карт и быстродействия электронной схемы считывателя. В нормальном состоянии на обеих сигнальных линиях интерфейса удерживается потенциал +5 В относительно общего провода. При передаче бита данных сигнальная линия соединяется с общим проводом (потенциал 0 В). Уровни сигналов соответствуют логическим уровням ТТЛ. Типичная длительность импульса – 20 – 100 мкс, а интервала между импульсами – 0,2 – 200 мс. Точные значения длительностей могут отличаться в зависимости от производителя считывателя. Пакеты данных от различных карт отделяются друг от друга временными интервалами порядка 500 мс.

На рис. 39 показана временная диаграмма на выходе считывателя при передаче двоичного числа «01101». Каждый импульс соответствует изменению логических уровней напряжения с 5 до 0 В.

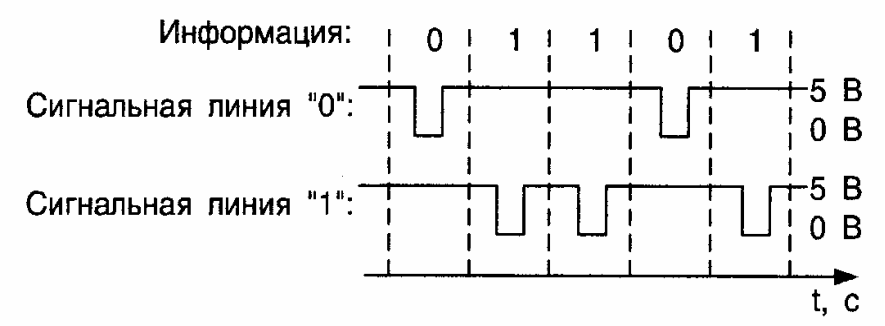


Рис. 39. Временная диаграмма импульсов на выходе считывателя

Формат представления данных определяется общим числом записанных на карте бит информации и их распределением по группам (полям) данных. Один из наиболее распространенных – 26-битный интерфейс Виганда. Соответственно, при этом на карте записано 26 бит информации.

26-битный формат карт Виганда был разработан сравнительно давно. В настоящее время он является наиболее популярным и поддерживается подавляющим большинством контроллеров различных фирм-производителей. Данный формат является откры-

тым, т. е. любая компания может заказать у производителя карты с любым системным кодом и номером. В связи с этим существует потенциальная возможность дублирования номеров карт и несанкционированного доступа на объект. Для исключения возможности повторения номеров карт многие производители карт и считывателей разработали свои собственные форматы, содержащие большее количество бит данных. Производители таких карт могут практически гарантировать, что каждая карта имеет уникальный номер. Рассмотрим форматы на примере компании *HID* – одного из ведущих производителей бесконтактных карт и считывателей. Компания предлагает следующие стандартные форматы карт, совместимые со всеми типами производимых считывателей:

- 26-разрядный формат;
- 37-разрядный формат *HID*;
- формат *Corporate* 1000 (35 бит);
- формат *Long* (до 84 бит).

Кроме них *HID* предлагает специальные форматы для производителей систем контроля доступа. Так, например, для компании *Northern Computers* выпускаются 34-разрядные карты. Помимо системного кода, номера карты и битов контроля четности, на карте может быть записан также номер выпуска карты (*issue code*).

Магнитные карты

Магнитная карта представляет собой пластиковую карту стандартных размеров с нанесенной на нее магнитной полосой. На магнитной полосе могут находиться от одной до трех дорожек записи (рис. 40), причем положение доро-

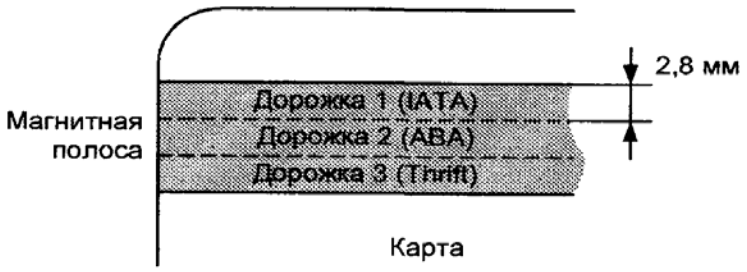


Рис. 40. Размещение дорожек на магнитной полосе карты

жек, их ширина и глубина записи регламентируются стандартами *ANSI* (*American National Standards Institute*) и *ISO* (*International Standard Organization*).

Дорожка 1 используется для записи и хранения цифровой и символьной информации. Она применяется в случае, когда на карте требуется хранить информацию об имени и фамилии ее владельца. Стандарт на запись данных на эту дорожку был разработан Международной ассоциацией воздушного транспорта (*IATA – International Air Transportation Association*), которая использовала пластиковые карты для бронирования авиабилетов. В банковских картах на этой дорожке обычно хранятся имя и фамилия владельца, номер карты и срок действия. Данные записываются с плотностью записи 210 бит на дюйм (*BPI*), каждый символ кодируется 7 битами. Всего на эту дорожку можно записать до 79 символов.

Формат записи на *дорожку 2* стандартизован Американской банковской ассоциацией (*ABA – American Banking Association*) и предусматривает запись цифровых данных с плотностью 75 *BPI*. На дорожке размещается до 39 символов, для кодирования каждого используется 5 бит. В банковских картах на этой дорожке также обычно хранятся номер карты и срок ее действия.

Дорожка 3 используется крайне редко, в основном для применений, связанных с постоянной перезаписью информации на карте. Цифровые данные длиной до 107 бит записываются с плотностью 210 *BPI* (5 бит на символ).

Стандарт *ANSI* определяет формат записи информации на дорожку. Для примера рассмотрим запись на дорожку 2. В начале полосы находится последовательность из нулей, используемая для калибровки считывателя. Первое значение «1» является первым битом данных. Этот первый бит входит в стартовую метку (преамбулу), представляющую собой шестнадцатеричное значение «B» (последовательность бит «1011»). За этой меткой следует информационная часть, которая может иметь длину до 37 деся-

тичных символов. Каждый символ состоит из 4 бит данных и одного бита контроля нечетности в пределах символа. После информационной части идет завершающая метка, представляющая собой шестнадцатиричное «*F*» (последовательность бит «1111»). Завершает кодовую посылку бит контроля четности. Рассмотрим пример записи информации на магнитной полосе. Пусть последовательность двоичных символов, записанных на карте, содержит 10 десятичных символов:

1101001000000101001101101110011111000100000010111001001111111100001

Каждый символ кодируется 5 битами, из которых 4 являются информационными, а пятый служит для контроля четности:

11010 01000 00010 10011 01101 11001 11100 01000 00010 11100 10011 11111 00001

После деления кодовой посылки на блоки по 5 бит осуществляется преобразование информации в десятичный формат. Из каждого блока удаляется бит контроля четности «Ч», а первые 4 бита переставляются в обратном порядке (рис. 41). Полученные блоки преобразуются в десятичную форму.

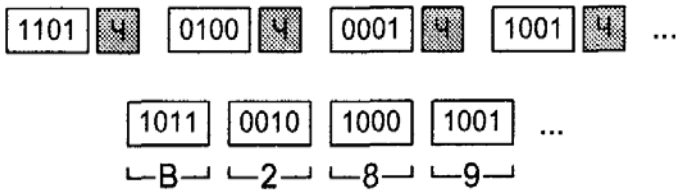


Рис. 41. Преобразование данных

Запись информации на магнитную полосу осуществляется с помощью устройства записи магнитных карт (в англоязычной литературе встречается термин *encode*). Магнитная головка состоит из сердечника с обмоткой. В сердечнике имеется зазор шириной 0,1 – 10 мкм. При протекании через обмотку тока записи в области зазора возникает магнитное поле рассеяния, которое воздействует на прилегающую к головке область рабочего слоя магнитной полосы карты. Поле записи через определенные промежутки времени изменяет свое направление на противоположное. В ре-

зультате под действием поля рассеяния магнитной головки происходят намагничивание и перемагничивание отдельных участков движущегося магнитного носителя. При периодическом изменении направления поля записи в рабочем слое носителя возникает цепочка чередующихся участков с противоположным направлением намагниченности, которые соприкасаются друг с другом одноименными полюсами. Ширина каждого участка при плотности записи 75 бит на дюйм составляет 0,338 мм. Если в пределах одного участка направление намагниченности изменяется один раз, это соответствует двоичному «О», а если два раза – «1». На рис. 42 показано распределение поляризации магнитного поля на дорожке, соответствующее двоичной строке «000101010».

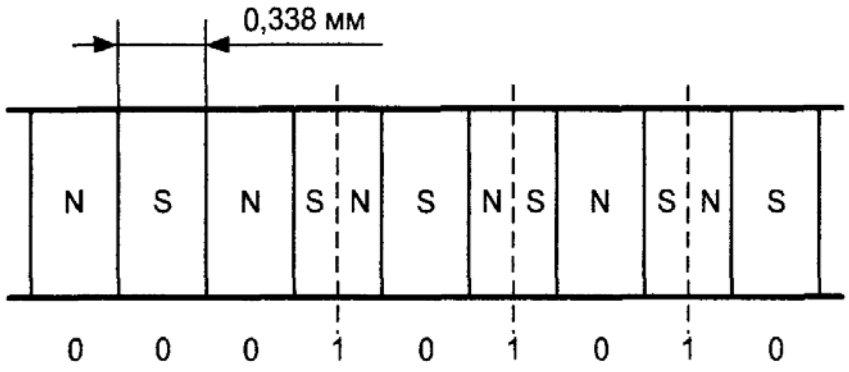


Рис. 42. Поляризация магнитного поля на дорожке

Основные достоинства устройств идентификации на картах с магнитной полосой:

- невысокая стоимость карт;
- возможность изменения кода на карте в процессе эксплуатации с помощью устройства записи.

Основные недостатки:

- невысокая защищенность карт от подделки;
- контактный способ считывания, не всегда удобный, например для контроля движущегося автотранспорта;
- невысокая пропускная способность считывателей;

- магнитные головки со временем могут засоряться и смещаться;
- карты требуют бережного хранения, поскольку магнитная полоса на карте чувствительна к воздействию электромагнитных полей, а также механическим воздействиям.

Использование карт с магнитной полосой в современных системах контроля и управления доступом может быть целесообразным в случае, когда нужно обеспечить минимальную стоимость карт, например, в автоматизированных парковках, в качестве пропусков в метро, на выставках и т. п. В остальных случаях из-за указанных недостатков карты с магнитной полосой используются сравнительно редко. Стоимость считывателей карт с магнитной полосой в настоящее время сопоставима с простыми моделями считывателей проксимити-карт.

3.5. Бесконтактные смарт-карты

Бесконтактные смарт-карты совмещают в себе достоинства бесконтактных проксимити- и смарт-карт. Запись и чтение информации с микросхемы карты осуществляется бесконтактным способом, аналогичным используемому в проксимити-картах. Так же, как и проксимити-карты, бесконтактные смарт-карты являются пассивными устройствами, т. е. не имеют встроенного источника питаний. Питание микросхемы карты при обмене информацией со считывателем происходит за счет переменного электромагнитного поля, генерируемого считывателем (рис. 43).

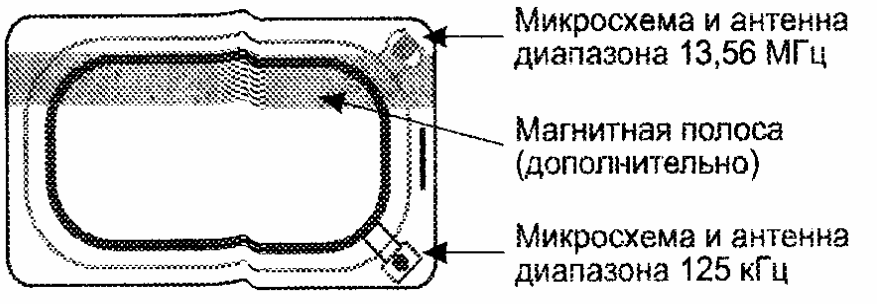


Рис. 43. Комбинированная бесконтактная смарт-карта

Первоначально бесконтактные смарт-карты разрабатывались для использования в платежных системах (например для оплаты проезда в транспорте), а затем получили распространение и в системах контроля и управления доступом. В настоящее время наибольшее распространение получили карты стандартов *MIFARE* фирмы *Philips Electronics* и *iCIass* фирмы *HID*.

Рассмотрим принцип действия и основные характеристики карт и считывателей *MIFARE*. Рабочая частота последних составляет 13,65 МГц, при этом максимальная дальность считывания – около 10 см. Скорость обмена данными между картой и считывателем – 106 кбит/с. Физический принцип обмена информацией со считывателем аналогичен проксимити-картам, использующим диапазон частот 13,56 МГц. Основное отличие от проксимити-карт состоит в объеме памяти карты, способе хранения информации и организации сеанса связи со считывателем. Карта может перемещаться в поле действия антенны считывателя без прерывания сеанса обмена данными.

Электронные таблетки

Электронные таблетки (*touch memory*) получили достаточно широкое распространение благодаря своей простоте (а следовательно, и дешевизне) и надежности, стойкости к механическим воздействиям. Впервые такие идентификаторы были разработаны компанией *Dallas Semiconductor*.

Конструктивно электронная таблетка (рис. 44) представляет собой металлический корпус цилиндрической формы. Одна часть – торцевая – отделена от основной части корпуса изолятором. Таким образом, имеются две изолированные токопроводящие части, образующие пару из сигнальной и общей линии.

Считыватель (рис. 45) должен иметь гнездо, соответствующее электронной таблетке. При этом сама таблетка и гнездо считывателя должны иметь такую форму, которая практически исключает короткое замыкание.

Сама таблетка обычно крепится на некотором держателе, позволяющем упростить процесс пользования (удобнее держать в руке) и крепить электронную таблетку, например на связке ключей. Внутри корпуса располагается электронная часть схемы, которая может включать в себя в зависимости от модификации все или часть нижеперечисленных основных элементов:

- Постоянное запоминающее устройство (ПЗУ), данные в которое записываются при изготовлении и не могут быть изменены в процессе эксплуатации.
- Энергонезависимое перепрограммируемое запоминающее устройство (ППЗУ).
- Буферная память для защиты от возможного нарушения контакта во время процесса записи/считывания.
- Интерфейс для приема и передачи информации с функциями контроля целостности данных.
- Схема синхронизации и часы.
- Встроенный источник питания для ППЗУ.

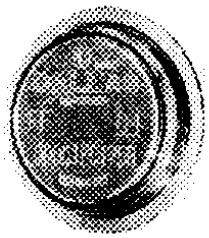


Рис. 44. Электронная таблетка

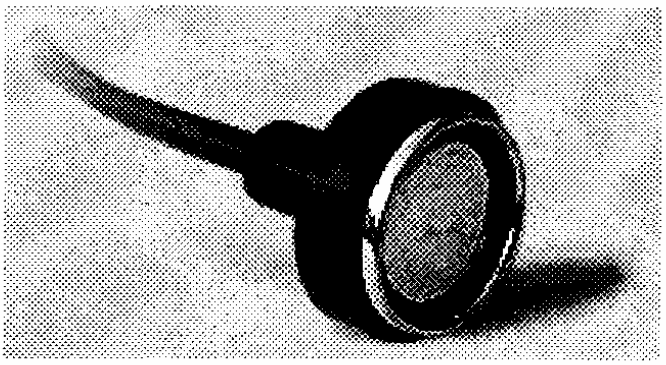


Рис. 45. Считыватель

В зависимости от типа устройства часть элементов может отсутствовать, например ППЗУ или схема синхронизации и часы. Объем памяти составляет обычно от 64 бит (ПЗУ) до десятков килобит.

Жестких требований к габаритам таких устройств не предъявляется, поэтому и существенных технологических сложностей с реализацией соответствующей схемотехники практически нет.

Питание электронной части осуществляется от считывателя при прикосновении к нему. Таким образом, необязательно иметь основной встроенный источник питания в самом идентификаторе. Однако следует учитывать возможность нестабильного контакта при работе. Этим, в частности, и обусловлена необходимость в буферной памяти для идентификаторов, имеющих ППЗУ. Запоминающие устройства должны иметь защиту от несанкционированного доступа. Последняя обычно реализуется с помощью ключей.

Поскольку как для питания, так и для обмена информацией могут использоваться только два контакта, необходимо разделение постоянного (питание) и переменного (информация) токов, что достаточно просто реализуется технически. Например амплитудной модуляцией тока потребления. Таким образом, питание, прием и передача данных осуществляется по одной паре проводников.

Передача или прием информации осуществляется в полудуплексном режиме. Взаимодействие организовано по принципу «ведомый-ведущий», при этом ведущим является считыватель.

Металлический корпус, а следовательно, и высокая механическая прочность, отсутствие источника питания обусловливают широкое применение таких идентификаторов на практике, в первую очередь – в массовых системах, например в домофонных системах идентификации.

Смарт-карты

Контактные смарт-карты, так же как и электронные таблетки, получили весьма широкое применение. Конструктивно такой

идентификатор (рис. 46) выполнен в виде пластиковой карты, на которой закреплена микросхема с несколькими (обычно 6 – 8) контактами (рис. 47).

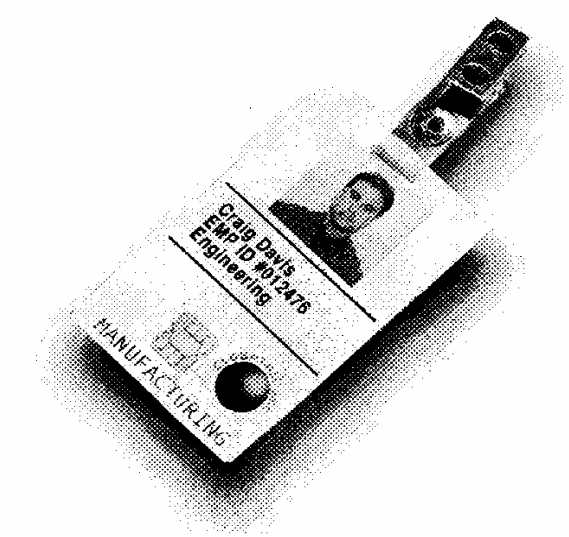


Рис. 46. Контактная смарт-карта

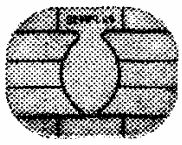


Рис. 47. Контакты микросхемы

Это пассивное устройство, не имеющее встроенного источника питания. Отличие от рассмотренного выше случая состоит, прежде всего, в наличии нескольких контактов, а значит, в возможности запитывать микросхему, передавать данные и принимать их по раздельным каналам. Соответственно, и скорость обмена будет выше, и упрощается интерфейсная часть идентификатора. В таких идентификаторах достаточно просто реализовать не только двухсторонний обмен информацией, но и перезапись данных, к примеру списывание со счета денежных средств по мере их расходования.

Технологические требования к размеру микросхемы здесь выше – она должна быть достаточно плоской, не намного превышать толщину собственно пластиковой карты. Кроме того, должны быть более жесткие требования к материалу покрытия контактов. Считыватель должен иметь группу скользящих контактов, соответствующую по расположению контактам карты.

Можно выделить несколько типичных разновидностей смарт-карт, которые определяются прежде всего функциональными возможностями и структурой памяти карты:

- С фиксированной информацией, имеющие только ПЗУ, данные в котором не могут меняться в процессе эксплуатации.
- С перезаписываемой информацией. Имеют не только ПЗУ, но и перепрограммируемую память, информация в которой может изменяться в процессе эксплуатации.
- Микропроцессорные карты с широкими возможностями не только непосредственно по решению задач контроля доступа, но и других. В любом случае необходимы меры по защите информации от несанкционированного доступа, копирования или модификации. Средства защиты могут быть различными – от системы ключей до использования сложных специальных криптографических алгоритмов. Вплоть до блокирования или самоуничтожения информации. Уровень защиты зависит от условий конкретной задачи.

Контактные смарт-карты получили широкое распространение как идентификаторы для оплаты телефонных разговоров в автоматах, на транспорте и для других применений.

Контрольные вопросы и задания

1. Что может служить носителем идентификационных признаков в СКУД?
2. Какие действия с носителями ИП могут привести к несанкционированному преодолению СКУД?
3. Проанализируйте защищенность и уязвимости носителей ИП от НСД.
4. На чем основана пассивная радиочастотная технология идентификации? Приведите примеры схем устройств.
5. Что из себя представляет штриховой код? Какие штрихкодовые кодировки вы знаете?

6. Как работает устройство считывания штрих-кода?
7. Какие штриховые коды используются в современных СКУД?
8. Что такое карта Виганда? На каких принципах основано ее функционирование?
9. Как используются магнитные карты в СКУД? Поясните принцип функционирования.
10. Что такое бесконтактные смарт-карты и как их используют в СКУД?
11. Назовите разновидности и принципы действия бесконтактных идентификаторов.
12. Какие формы передачи данных распространены в СКУД?

Глава 4. ОСОБЕННОСТИ ПОСТРОЕНИЯ БИОМЕТРИЧЕСКИХ СИСТЕМ ИДЕНТИФИКАЦИИ

В последние годы биометрический метод контроля доступа развивается весьма активно. Он основан на использовании характерных и уникальных физиологических особенностей или поведенческих характеристик человека, с помощью которых осуществляется идентификация его личности. Важным преимуществом этого метода является то, что с высокой степенью вероятности одновременно решаются задачи как идентификации, так и аутентификации.

Можно говорить о двух группах систем, использующих биометрический метод идентификации. К первой следует отнести биометрические системы, анализирующие статические характеристики человека, например папиллярный узор пальцев, геометрию ладони или рисунок радужной оболочки глаза. Эти идентификационные признаки являются практически постоянными физическими характеристиками человека и подвержены крайне слабым изменениям со временем. Поэтому их можно назвать *квазистатическими.*

Ко второй группе относятся биометрические системы, анализирующие динамические идентификационные признаки человека при выполнении им определенных действий. Ими могут быть динамика воспроизведения подписи, параметры речи, клавиатурный почерк (временные характеристики ввода пользователем информации с клавиатуры) и др. Эти признаки находятся под влиянием как выполняемых действий (контролируемых, управляемых), так и психологических факторов (менее управляемых). Поэтому их можно называть *квазидинамическими*. Поскольку квазидинамические характеристики могут изменяться с течением времени, зарегистрированный биометрический образец должен периодически обновляться при его использовании.

При всех серьезных преимуществах биометрического метода идентификации следует учитывать в ряде случаев и этическую сторону вопроса. Пользователи не всегда согласны, чтобы их отпечатки пальцев или другие физиологические характеристики фиксировались в системе. Отметим еще один важный момент. Перед тем как анализировать выбранные биометрические идентификационные признаки человека (квазистатические или квазидинамические), нужно удостовериться, что предъявленные характеристики действительно принадлежат живому существу: во-первых, что предъявленный образ действительно принадлежит человеку (а не имитирован, скажем, с помощью муляжа пальца, руки, глаза и т. п.), а во-вторых, что его характеристики соответствуют именно живому существу.

Если система не позволяет с достаточно высокой степенью достоверности определять, что предъявленные для идентификации биометрические признаки соответствуют живому существу, существуют три потенциальные угрозы для такой системы идентификации. Первая из них заключается в том, что предъявленный муляж может являться копией биометрического признака уполномоченного пользователя системы. Например, получив отпечаток пальца действующего пользователя, потенциальный нарушитель может изготовить муляж пальца и воспользоваться им для доступа. Не менее важной является опасность добавления муляжа при занесении биометрических признаков пользователей в систему. Уполномоченный пользователь может предъявить системе не свой носитель биометрических признаков, а муляж, которым впоследствии может воспользоваться нарушитель или группа нарушителей для получения доступа. И последняя по порядку, но не по важности угроза связана с тем, что действующий пользователь системы может отказаться от факта получения им доступа (зарегистрированного системой), если носитель биометрических признаков может быть подделан.

4.1. Биометрический метод идентификации

При занесении биометрических признаков в память системы необходимо проверить достаточность считанной информации для успешной идентификации. Вводимые эталонные биометрические признаки должны содержать достаточное количество информации для возможности сравнения их со считываемыми и принятия решения с требуемой вероятностью. Например, при идентификации по отпечаткам пальцев необходимо убедиться, что эталонный отпечаток не был смазан и содержит достаточное количество характерных деталей (завитков, пересечений папиллярных линий и т. п.), позволяющих однозначно идентифицировать пользователя. Если эталонный исходный образ не обладает необходимой достаточностью характеристик, система должна предложить пользователю либо повторить ввод, либо ввести новый образец (например другой палец).

Если считанный эталонный образ соответствует указанным требованиям, осуществляется его преобразование в форму, удобную для поиска в базе данных и сравнения. Обычно считанный образ содержит большое количество избыточной информации, которая может быть безболезненно удалена при сохранении возможности идентификации. Иначе, если не использовать преобразование и сжатие образа, размер памяти, необходимой для хранения всех образов, может оказаться слишком большим, а время выборки необходимого образа из памяти слишком продолжительным.

Итак, процесс занесения биометрических образов в память системы состоит из следующих этапов:

1. Поиск и считывание биометрических признаков.

2. Проверка соответствия предъявленных биометрических признаков живому человеку.

3. Проверка достаточности считанной эталонной информации для успешной идентификации человека.

4. Преобразование считанного образа в форму, удобную для дальнейшей работы и хранения, т. е. формирования образца идентификационных признаков.

5. Занесение образца в память системы.

Виды ошибок идентификации

Рассмотрим, какие события могут иметь место при принятии решения в системе биометрической идентификации (как, впрочем, и в любой другой). Существуют две гипотезы:

- предъявленный биометрический идентификатор принадлежит уполномоченному пользователю;
- предъявленный биометрический идентификатор не принадлежит уполномоченному пользователю.

Система принимает решение о разрешении или запрете доступа (табл. 3).

Таблица 3

Гипотеза	Решение системы идентификации			
	Разрешение доступа		Запрет доступа	
Предъявлен действующий идентификатор	Правильное разрешение доступа	$P_{\text{п.р}}$	Ложный отказ в доступе	$P_{\text{л.о}}$
Предъявлен недействующий идентификатор	Несанкционированный доступ	$P_{\text{н.д}}$	Правильный отказ в доступе	$P_{\text{о.д}}$

Вероятность разрешения доступа при предъявлении действующего идентификатора характеризует *вероятность правильного разрешения доступа* ($P_{\text{п.р}}$). Запрет доступа при предъявлении действующего идентификатора называется *ложным отказом в доступе* (характеризуется вероятностью $P_{\text{л.о}}$). Эти два события образуют полную группу, т. е.

$$P_{\text{п.р}} + P_{\text{л.о}} = 1.$$

Аналогично вероятность разрешения доступа при предъявлении недействующего идентификатора называется *вероятностью несанкционированного доступа* ($P_{\text{н.д}}$), а вероятность запрета доступа при предъявлении недействующего идентификатора – *вероятностью правильного отказа в доступе* ($P_{\text{о.д}}$). Эти события также образуют полную группу

$$P_{\text{н.д}} + P_{\text{о.д}} = 1.$$

В зарубежной литературе вероятность $P_{\text{н.д}}$ обозначается как *FAR* (*False Acceptance Rate*) или *FMR* (*False Match Rate*), а $P_{\text{л.о}}$ – как *FRR* (*False Rejection Rate*) или *FNMR* (*False Non-Match Rate*). Ложный отказ в доступе и несанкционированное разрешение доступа называются ошибками первого и второго рода соответственно.

Очевидно, что в любой системе крайне желательно иметь вероятности $P_{\text{н.д}}$ и $P_{\text{л.о}}$ как можно меньшими, однако эта задача оказывается противоречивой. Ясно, что при попытке снизить вероятность несанкционированного доступа увеличивается вероятность отказа в доступе действующему пользователю системы, и наоборот, снижение вероятности отказов в доступе уполномоченным пользователям неизбежно приводит к увеличению вероятности несанкционированного доступа.

В некоторых биометрических системах имеется возможность настраивать характеристики для соответствия решаемой задаче. Например в системах, где требуется высокая пропускная способность, имеет смысл снизить $P_{\text{л.о}}$ для того, чтобы избежать задержек при проходе пользователей. На объектах повышенной категории надежности, не требующих высокой пропускной способности, необходимо уменьшить $P_{\text{н.д}}$. Возможно, при этом системе потребуется несколько попыток чтения биометрических характеристик пользователя для его достоверной идентификации.

Еще одна характеристика, которая используется для систем биометрической идентификации, – вероятность отказа в регист-

рации пользователя в системе $P_{\text{о.р}}$. При занесении эталонного образца идентификационных характеристик пользователя возможна ситуация, когда полученной от него биометрической информации оказывается недостаточно для его дальнейшей однозначной идентификации (точнее, с заданной вероятностью). Эта ситуация может возникнуть, например, если отпечаток пальца содержит мало характерных элементов, используемых для сравнения отпечатков между собой, или палец был поврежден или загрязнен. В англоязычной литературе для данной характеристики используется аббревиатура *FTE* (*Failure To Enroll Rate*).

4.2. Идентификация на основе квазистатических признаков

Идентификация по отпечатку пальца

Кожа человека состоит из двух слоев, при этом нижний слой образует множество выступов. На основной части кожи выступы располагаются хаотично и поэтому трудно наблюдаемы. На отдельных участках кожи конечностей выступы строго упорядочены в линии (гребни), образующие уникальные папиллярные узоры. Идентификация личности на основе папиллярных рисунков пальцев рук впервые была предложена Г. Фулдсом (*H. Faulds*) и В. Гершелем (*W. Herschel*) в статье английского журнала «*Nature*» в 1880 г. В настоящее время этот метод идентификации широко известен и распространен в первую очередь в криминалистике.

Системы идентификации по отпечаткам пальцев (также известные под названием *дактилоскопические*) получили наибольшее распространение среди биометрических систем благодаря удобству пользования, небольшим габаритам считывающих устройств, быстроте идентификации и сравнительно невысокой стоимости. Они широко используются в системах разграничения доступа к компьютеру, банковских приложениях и других. Развитие микроэлектроники позволило существенно уменьшить раз-

меры считывающих элементов. Структурная схема системы изображена на рис. 48.

Рис. 48. Структурная схема считывателя отпечатка пальцев

С помощью чувствительного элемента считыватель снимает папиллярный рисунок с пальца человека. Типичная разрешающая способность, которую имеют современные считывающие элементы, составляет порядка 500 точек на дюйм, что соответствует размерам элементарного чувствительного элемента 50×50 мкм. Это значение рекомендовано Федеральным бюро расследования (ФБР) США для интегрированных автоматизированных систем идентификации по отпечаткам пальцев. Ширина папиллярных выступов составляет примерно 450 мкм, поэтому теоретически достаточно было бы иметь разрешающую способность чувствительного элемента порядка 112 точек на дюйм (элементарный чувствительный элемент 225×225 мкм), однако для полной реализации всех возможностей алгоритмов сравнения этой разрешающей способности недостаточно. Спецификации ФБР также рекомендуют сканирование папиллярного рисунка с 256 градациями серого на каждый элемент. Однако в реальных условиях обычно достаточно 64 градаций серого (каждая точка кодируется 6 битами). Существуют системы, использующие бинарное квантование изображений отпечатков.

Исходный отпечаток, полученный со считывающего элемента с разрешением 500 точек/дюйм и 256 градациями серого, за-

нимает сравнительно большой объем памяти. Например, изображение размером 2×3 см содержит около 400×600 элементов, что требует для хранения в памяти 240 кбайт. Для 10 отпечатков пальцев потребуется более 2 Мбайт. Очевидно, что хранение таких больших объемов информации приведет к значительному удорожанию устройства, а поиск и сравнение изображений такого размера будут занимать много времени и требовать больших вычислительных ресурсов. Кроме того, крайне нежелательно хранить отпечатки в исходном виде из соображений конфиденциальности. Обычно пользователям нравится анонимность, они не хотят, чтобы отпечатки пальцев были без их согласия переданы правоохранительным органам или просто похищены злоумышленниками. Поэтому производители используют специальные методы обработки и хранения полученных данных, которые не позволяют восстановить исходный отпечаток.

Для сжатия исходного изображения обычно используется Вейвлет-преобразование. Коэффициент сжатия выбирается таким образом, чтобы избежать потерь информации, необходимой для успешной идентификации. Обычно его максимальное значение составляет порядка 10. После сжатия размер изображения составляет десятки килобайт. Объем хранимой информации об отпечатке пальца может быть еще существенно уменьшен, если осуществить классификацию на характерные типы папиллярных рисунков и выделить на отпечатке характерные особенности, представляющие собой начала (окончания) папиллярных линий или их слияния (разветвления). На папиллярных рисунках выделяют несколько типов характерных элементов: пересечение, соединение и разветвление линий, окончания линий, островки и дельты (рис. 49). Современные алгоритмы обработки соединяют характерные точки изображения векторами и описывают их свойства и взаиморасположение. При этом используются относительные расстояния между характерными точками изображения, что позволяет сделать процесс сравнения отпечатков инвариантным к

повороту пальца относительно считывающего элемента. Обычно в отпечатке выделяется порядка 30 – 40 характерных точек, что позволяет создать образец отпечатка размером от 40 байт до 1 кбайта. По такому образцу невозможно восстановить исходный отпечаток, однако можно сравнивать отпечатки друг с другом.

Рис. 49. Характерные особенности отпечатка пальца

Идентификация пользователей осуществляется путем сравнения образа предъявленного отпечатка пользователя с эталонными образцами, хранящимися в памяти считывателя. При этом возможны два алгоритма работы:

1. Сравнение образа считанного отпечатка со всеми образцами, хранящимися в памяти. Если такой образец не найден, принимается решение об отказе в доступе. Достоинством такого алгоритма является возможность работы только по отпечатку пальца без использования дополнительных идентификаторов.

2. Сравнение образа считанного отпечатка с одним конкретным образцом из памяти. В этом случае биометрический считыватель до анализа образа отпечатка пальца должен иметь информацию о том, какой пользователь будет предъявлять палец для идентификации. Обычно это достигается за счет совмещения считывателя отпечатка пальца с кодонаборным устройством (клавиатурой) или считывателем, например проксимити-карт. Каждому пользователю назначается уникальный пароль или при-

сваивается номер карты, пользователь вводит пароль или предъявляет карту, после чего прикладывает палец к считывающему элементу. Считыватель на основе введенного пароля или номера карты выбирает из памяти образец отпечатка, соответствующий данному пользователю, и осуществляет сравнение.

Такой алгоритм имеет следующие достоинства:

- возможность использования одновременно двух различных методов идентификации;
- более высокое быстродействие по сравнению с предыдущим алгоритмом, поскольку осуществляется сравнение считанного образа только с одним эталонным, а не перебор всех образцов;
- возможность хранения в базе данных информации о большом количестве пользователей;
- меньшая стоимость считывателя.

На сегодняшний день известны несколько основных технологий считывания отпечатков пальцев. Опишем их в порядке появления. Самый первый и один из самых распространенных сегодня способов основан на использовании оптической системы – призмы и нескольких линз со встроенным источником света. Структура такого считывателя показана на рис. 50.

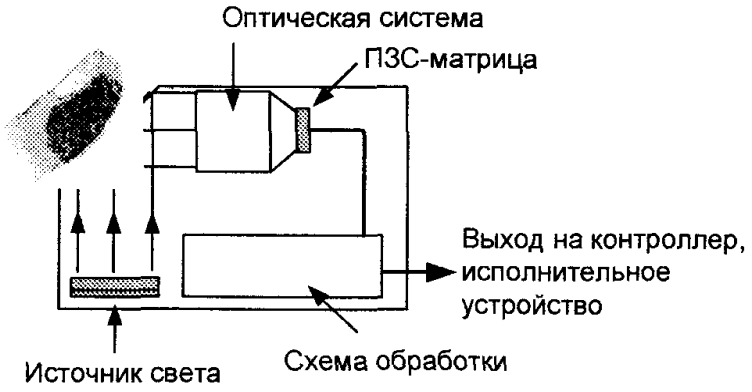


Рис. 50. Функциональная схема оптического считывателя

Свет, падающий на призму, отражается от поверхности соприкасающейся с пальцем пользователя, и выходит через другую сторону призмы, попадая на оптический датчик (обычно это монохромная камера на основе ПЗС-матрицы), где формируется изображение.

Преимуществом такого способа считывания является сравнительно невысокая стоимость реализации по сравнению с другими. Недостатки подобной системы следующие. Коэффициент отражения значительно зависит от параметров кожи: сухости, присутствия масла, бензина, других химических элементов. Кроме того, место контакта пальца с призмой со временем загрязняется, что приводит к ухудшению качества получаемых изображений.

Другой способ основан на измерении разности электрических потенциалов между гребнями и впадинами на коже пальца с использованием полупроводниковой пластины. Палец в считывателе выступает в качестве одной из пластин конденсатора (рис. 51). Другая пластина конденсатора – это полупроводниковая поверхность чувствительного элемента, содержащая несколько десятков тысяч конденсаторных пластин с плотностью считывания порядка 500 элементов/дюйм. В результате получается изображение гребней и впадин кожи на пальце.

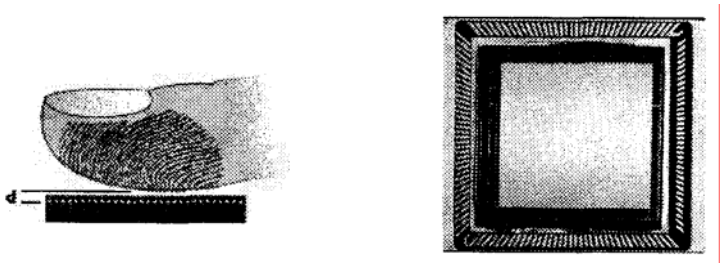


Рис. 51. Полупроводниковый считыватель

В данном случае жировой баланс кожи и степень чистоты рук пользователя не играют столь существенной роли, как в предыдущем случае. Кроме того, можно реализовать более компактную систему. Если говорить о недостатках метода, то полупроводниковый чувствительный элемент требует эксплуатации в герметичной оболочке, а дополнительные покрытия уменьшают чувствительность системы. На изображение могут оказать влияние сильное внешнее электромагнитное поле и повышенная влажность.

Существуют полупроводниковые чувствительные элементы, позволяющие фиксировать разницу температур между гребнями и впадинами кожи на пальце. Преимуществом этой технологии

является высокая устойчивость к электромагнитным помехам, загрязнениям, влажности. Такие считывающие элементы производятся фирмой *Atmel* (серия *FingerChip*).

Существует еще один метод реализации считывающих систем. Его разработала компания *Ethentica Inc*. В качестве считывающего элемента используется электрооптический полимер (система *TactileSense*). Этот материал позволяет получать оптическое изображение отпечатка пальца с высоким разрешением, которое затем переводится в цифровой формат и обрабатывается. Метод также нечувствителен к состоянию кожи 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.

Дополнительная задача, которая решается в считывателях отпечатка пальца – определение принадлежности пальца живому человеку (а не имитация с помощью муляжа). Это достигается за счет анализа электропроводности кожи, ее температуры.

Примером современного считывателя отпечатков пальцев является модель *VeriPass*, предлагаемая фирмой *Northern Computers*. Этот считыватель позволяет хранить в памяти до 200 отпечатков пользователей.

Чтобы уменьшить время анализа, считыватели отпечатка пальца оснащаются дополнительно клавиатурой, на которой пользователь набирает свой личный пароль, или считывателем карты. В этом случае время анализа существенно снижается, так как происходит только сравнение считанного образа с одним образцом, извлеченным из базы данных, а не перебор всех возможных образов. Использование комбинации «пароль + биометрический признак» или «карта + биометрический признак» позволяет также снизить стоимость считывателя, поскольку существенно снижаются требования к быстродействию аппаратного обеспечения считывателя. Примером устройства, использующего комбинацию «карта + отпечаток пальца», является устройство *VeriProx*

*VP*1000. Оно представляет собой считыватель отпечатка пальца, комбинированный со считывателем бесконтактных (*proximity*) карт НЮ. Совмещение двух технологий позволило получить низкую вероятность ошибки (0,0005), малое время идентификации (менее секунды) и большое количество отпечатков, хранимых в памяти считывателя (4500), по сравнению со считывателями, использующими только отпечаток пальца.

Особенности считывателей *VeriPass*, *VeriProx*, *VeriFlex* и *VeriSmart*:

- достаточно надежное считывание отпечатка пальца, в том числе при наличии на пальцах загрязнений, влаги, порезов;
- защищенность от попыток имитации пальца искусственными материалами (резиной, латексом и т. п.);
- светодиодная и звуковая индикация считывания;
- возможность использования для расширения существующей системы контроля доступа;
- добавление пользователей в систему с помощью мастер-карт или программного обеспечения *VeriAdmin*;
- возможность объединения нескольких считывателей в сеть по интерфейсу *RS* 485 для ведения общей базы данных отпечатков пальцев (исключает необходимость ввода отпечатков пальцев во все считыватели системы) – до 31 считывателя в сети с максимальной длиной 1200 м.

Последнее время получает распространение технология хранения отпечатка пальца непосредственно на бесконтактной смарт-карте. Для идентификации пользователь предъявляет карту, считыватель считывает с нее данные отпечатка пальца, а затем прикладывает палец к чувствительному элементу. Считыватель осуществляет сравнение предъявленного отпечатка пальца с его эталонными данными, полученными с карты, и принимает решение о правомочности владения пользователем карты.

Такой способ имеет два основных преимущества. Во-первых, снимается ограничение на количество пользователей в системе, поскольку вся информация об отпечатках пальцев хранится на

картах пользователей. Во-вторых, при работе нескольких считывателей исключается необходимость прокладки специализированного кабеля между считывателями в системе для пересылки отпечатков. В качестве примера таких устройств можно привести считыватели *VeriSmart* и *BioAccess*, предлагаемые фирмой *Northern Computers*. В обоих устройствах используются карты *Mifare Standard*, имеющие память на 1 кбайт.

Недостатками подобных считывателей являются более высокая стоимость карт *Mifare* по сравнению с обычными проксимити-картами, а также необходимость иметь в системе устройство записи на бесконтактные смарт-карты.

Технические характеристики считывателей сведены в табл. 4.

Таблица 4

Показатель	Значение			
Модель	*V-Pass*	*V-Prox*	*V-Sman*	*BioAcoees*
Фирма-производитель	*Bioscrypt*	*Bioscrypt*	*Bioscrypt*	*Northern Computers*
Технология считывания	Только отпечаток	Карта + отпечаток (хранится в считывателе)	Карта + отпечаток (хранится на карте *Mifare*)	Карта + отпечаток (хранится на карте *Mifare*)
Поддерживаемые интерфейсы	Виганда, *RS* 232, *RS* 485			Виганда, магнитных карт, *RS* 232, *RS* 485
Типы карт для считывателя	–	26 или 34 бит *HID*	*Mifare Standard*	*Mifare Standard*
Количество пользователей в системе	100 (возможность расширения до 200)	4500	Не ограничено	Не ограничено
Время добавления нового пользователя	Менее 3 с	Менее 3 с	Менее 5 с	Менее 10 с
Время идентификации пользователя	Менее 1 с (при 100 отпечатках)	Менее 1 с	Менее 2 с	Менее 1 с

Окончание табл. 4

Показатель	Значение			
Вероятность несанкционированного доступа ($P_{н.д}$)	0,002	–	–	Менее 0,0005
Вероятность ложного отказа в доступе	0,01	–	–	Менее 0,01
Эквивалентная вероятность ошибки	–	0,001	0,001	–
Напряжение питания	7 – 24 В пост. тока		8 – 12 В пост. тока	12 – 24 В пост. тока
Потребляемый ток в дежурном режиме	200 мА при 12 В	60 мА при 12 В	200 мА при 12 В	110 мА при 12 В
Потребляемый ток в режиме добавления пользователей	250 мА при 12 В	250 мА при 12 В	250 мА при 12 В	250 мА при 12 В
Размеры, мм	130×50×65,5		130×118×63,5	125×68×61

Радужная оболочка глаза

Радужная оболочка глаза человека (*iris*) – это мембрана, окружающая глазной зрачок. Ее диаметр обычно составляет около 11 мм. Радужная оболочка глаза имеет свой неповторимый рисунок, практически не меняющийся после достижения человеком одного года. Уникальность этого рисунка обусловлена генотипом личности, и существенные отличия рисунка радужной оболочки наблюдаются даже у близнецов. Вероятность, что существуют две радужные оболочки с одинаковым рисунком, составляет 10^{-72}. Рисунок содержит большое количество мелких деталей, по которым можно идентифицировать человека, и при этом очень стабилен на протяжении всей его жизни, а сама радужная оболочка является наиболее защищенным и оберегаемым органом. Врачи используют рисунок и цвет радужной оболочки для диагностики и выявления генетической предрасположенности к некоторым заболеваниям.

Системы идентификации человека по радужной оболочке глаза считаются одними из самых надежных среди всех биометрических технологий. Вероятность ложного допуска в системах, представленных на современном рынке, составляет 0,000001 и менее при вероятности отказа в доступе уполномоченному пользователю порядка 0,02.

Система идентификации использует видеокамеру, считывающую рисунок радужной оболочки глаза. Современные считыватели позволяют делать это с расстояния от 10 сантиметров до одного метра. При этом наличие у человека очков или контактных линз не оказывает существенного влияния на качество считанного изображения. В простейшем случае система аутентификации состоит из объектива, черно-белой телевизионной камеры и платы ввода видеоизображения в компьютер. Подсветка глаза осуществляется несколькими маломощными светодиодами, излучающими инфракрасное излучение (обычно в диапазоне от 700 до 900 нм). Наведение камеры достигается за счет системы зеркал, а фокусировка – объективом с трансфокатором. В некоторых моделях считывателей наведение камеры происходит автоматически при приближении объекта на расстояние ближе полуметра. После наведения камеры считыватель анализирует изображение и выделяет в нем внешнюю границу радужной оболочки, зрачковую область и центр зрачка (рис. 52).

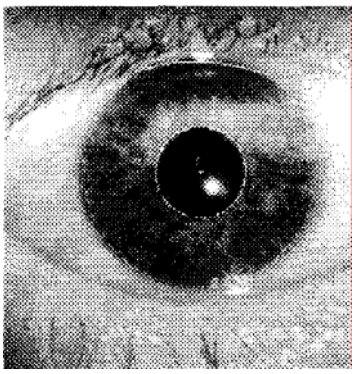


Рис. 52. Полная область считывания

Затем определяется область радужной оболочки, которая будет использоваться для дальнейшего анализа. При этом исключаются области, закрытые веками, теневые и отражающие области. В современных считывателях высокие характеристики распознавания достигаются, если для анализа доступно менее 40 % поверхности радужной оболочки. Вся информация обрабатывается в полярной системе ко-

ординат. Полученное оптимизированное изображение преобразуется в цифровой образец идентификационных признаков, занимающий несколько сотен байт памяти.

При сравнении считанного образа с эталонным образцом из памяти считывателя происходит вычисление расстояния Хемминга, которое характеризует степень различия между двумя образами. Каждый из 2048 бит образа, полученного при считывании, попарно сравнивается с битом образа из памяти, а полученное значение вычисляется по логике «Исключающее ИЛИ» (рис. 53).

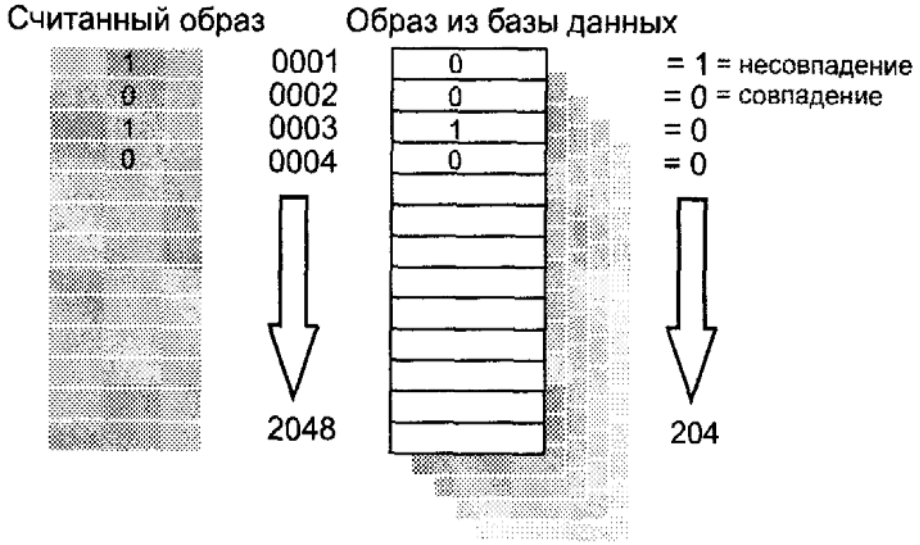


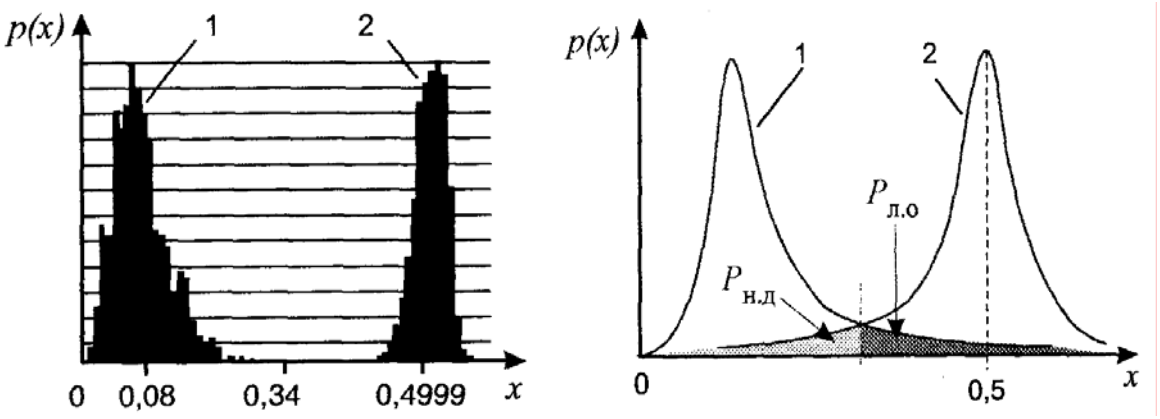
Рис. 53. Вычисление расстояния Хемминга

Например, если первый бит считанного образа равен «1», а первый бит образа из памяти «0», то это означает, что совпадения нет, и в результат записывается «1». Если есть совпадение, в результат записывается «0». Далее сравниваются вторые биты образов, затем третьи и т. д. В реальных системах сравнение всех 2048 пар бит происходит достаточно редко, поскольку радужная оболочка не полностью доступна для сканирования. После сравнения всех доступных пар бит количество полученных несовпадений делится на общее число сравнений. Полученное значение называют расстоянием Хемминга. Например, если в результате

сравнения 2048 пар бит было найдено 204 несовпадения, расстояние Хемминга вычисляется как 204:2048 = 0,1. Это значит, что два образа различаются на 10 %.

Логическая операция «Исключающее ИЛИ» просто реализуется и быстро выполняется на современных процессорах, например, 32-разрядный процессор может за одну машинную операцию выполнить действие «Исключающее ИЛИ» для двух целых десятичных чисел из диапазона от 0 до 4294967295. На процессоре с тактовой частотой 300 МГц за одну секунду можно выполнить сравнение приблизительно 100 000 рисунков радужных оболочек.

На основании экспериментальных данных при выборке сравнений образов радужных оболочек порядка 10^6 были построены гистограммы плотности вероятностей, которые оценивали степень соответствия предлагаемого для идентификации образа и эталонного образца из базы данных. Соответствующие гистограммы показаны на рис. 54, *а*. Плотность вероятности (рис. 54, *б*) иллюстрирует случай, когда предлагаемый для идентификации образ соответствовал эталонному. Плотность вероятности *2*, имеющая среднее значение порядка 0,5, отражает случай, когда предлагаемый образ не соответствовал эталонному (расстояние Хемминга 0,5 соответствует случайному распределению совпадений). Среднее значение распределения *1* близко к 0,08 (или 8 %).



а) *б)*

Рис. 54. Распределение степени соответствия предлагаемых для идентификации образов и эталонного образца из базы данных

Особенностью обоих распределений является малое значение дисперсии, которое выражается в малой ширине обоих распределений. Так, для 1 среднеквадратическое отклонение равно 0,038, а для 2 – 0,032. Расстояние Хемминга, равное 0,342, соответствует равенству вероятностей ошибок первого и второго рода и составляет $8{,}33 \cdot 10^{-7}$.

4.3. Идентификация на основе квазидинамических признаков

Основной специфической особенностью идентификации и аутентификации человека на основе квазидинамических биометрических признаков является возможность существенного изменения этих идентификационных признаков во времени. Эти изменения могут быть связаны с большим количеством факторов как внешних, воздействующих на человека, так и собственно его физиологических особенностей (физическое состояние, настроение и т. п.).

Анализ подписи

Подпись человека давно использовалась для установления его личности. Работа по автоматизации этого процесса показала, что для достижения требуемой надежности идентификации необходимо учитывать не только саму форму подписи, но и динамику движения пера, степень нажима и др. Только при этом достигается высокая надежность идентификации личности. Действительно, научиться подписываться похожей подписью не настолько уж и сложно. Однако воспроизвести эту подпись с той же динамикой крайне сложно.

Очевидно, что идентификация на основе подписи не может найти широкого применения в системах контроля доступа на объект в связи с низкой пропускной способностью. Такие системы применяются в банковских приложениях.

Голосовая идентификация

Очевидная привлекательность данного метода состоит в удобстве применения. Основной сложностью, связанной с этим способом, является достижение требуемой точности идентификации. Спектральный состав речи определяется не только рядом физиологических и поведенческих факторов, но и возможными помехами – окружающим шумом. При этом подверженность речи влиянию этих факторов может создать проблемы для процесса идентификации. Например, человек с простудой может испытывать трудности при использовании данных систем.

Нельзя не учитывать и достаточно слабую защищенность этого способа от съема информации по акустическому каналу – от возможной записи с последующим воспроизведением для несанкционированного преодоления СКУД. В настоящее время идентификация по голосу используется для управления доступом в помещения с низкими и средними требованиями к безопасности. Идентификация по голосу – удобный, но в то же время не такой надежный способ идентификации, как, например, использование отпечатка пальца или радужной оболочки глаза.

Идентификация по походке

Одно из новых направлений разработок систем идентификации. Хотя достаточно очевидное, если вспомнить широко применяемую фразу «узнаю по походке». Это направление связано прежде всего с автоматизированным выявлением определенных субъектов среди других. Например, для поиска лиц, находящихся в розыске.

Примером может служить радиолокационная система распознавания людей по походке, как одна из разработок Пентагона в области антитеррористической деятельности. Она основана на уникальности в достаточной степени походки человека. Оценка эффективности такой системы – 80 – 90 % правильного распознавания. При этом учитываются ряд индивидуальных характеристик и параметров тела человека, таких как физические размеры, масса тела, характерные особенности движений и др.

К сложностям использования таких систем можно отнести трудности в распознавании людей с четкой походкой.

Из других проектов, находящихся в стадии разработок, можно отметить распознавание людей по контуру на расстоянии до 150 м с оценочной вероятностью правильной идентификации 90 %; разработки, связанные с трехмерным отслеживанием движения тела, и ряд других.

4.4. Перспективные направления

Исследования, ведущиеся в области биометрических технологий, могут дать существенное расширение списка применяемых принципов идентификации.

Существуют действующие системы, которые идентифицируют личность по клавиатурному почерку. Этот метод основан на том, что при быстром наборе текста на клавиатуре компьютера интервалы между нажатиями клавиш и их отпусканиями, а также длительности удержания клавиш уникальны для каждого человека. Этот метод позволяет сочетать два независимых метода идентификации – основанный на знаниях человека (пароль или кодовая фраза, вводимая с клавиатуры) и на его физических характеристиках как личности (клавиатурный почерк).

Одним из активно развивающихся направлений аутентификации является использование индивидуальных особенностей генетического кода личности. Сегодня методы анализа генетического кода применяются только в криминалистике, так как они сравнительно дороги и пока не позволяют получать результат в реальном масштабе времени. Тем не менее стоимость технологий экспресс-анализа биологических материалов и время анализа снижаются достаточно быстро. Вполне возможно, что методы идентификации личности по генетическому коду скоро станут коммерческими технологиями.

В целом, если говорить о биометрической идентификации личности, необходимо помнить и об этических аспектах (например о соблюдении конфиденциальности), которые тесно связаны с задачами контроля доступа и безопасности.

Контрольные вопросы и задания

1. На чем основан биометрический метод идентификации? Перечислите основные этапы занесения информации о биометрических образах в память распознающей системы.

2. Проанализируйте способ идентификации по отпечатку пальца. Как работает реализующее его устройство идентификации?

3. Проанализируйте способ идентификации по геометрии руки.

4. В чем заключается способ идентификации по радужной оболочке глаза? Приведите структурную схему устройства и поясните принцип его функционирования.

5. Проанализируйте способы идентификации по сетчатке глаза и по геометрии лица.

6. Опишите способы идентификации на основе квазидинамических признаков.

Глава 5. ВЫБОР СКУД ДЛЯ ОБОРУДОВАНИЯ ОБЪЕКТА

5.1. Обследование объекта

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

– 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.

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.

Условия эксплуатации

Учитывать вредное воздействие окружающей среды следует лишь для исполнительных устройств, считывателей и контроллеров, предназначенных для работы вне отапливаемых закрытых помещений либо в особых условиях (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.

Интегрированные системы охраны (*ИСО*)

В настоящее время любой крупный и особенно важный объект имеет весь набор технических средств безопасности. 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 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 и аппаратном уровнях, возможность организации линий связи стандартных интерфейсов *RS* 485 и *RS* 232 (при значительной удаленности панелей систем сигнализации и управления доступом).

5.2. Требования к основным компонентам СКУД

Требования к исполнительным устройствам

Исполнительные устройства 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 исполнительных устройствах должна предусматриваться возможность питания от резервного источника тока, а также механическое аварийное открывание 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.

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 заданную 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, *Proximity*, Виганд-карточки и электронные ключи *Touch Memory* – высокий и биометрические – очень высокий уровень безопасности.

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 исполнительных устройств.

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 осуществлять:

– 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 трех.

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 исполнительных устройств.

При вводе пароля на экране дисплея не должны отображаться вводимые знаки.

Число символов пароля должно быть не менее пяти.

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 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 восьми часов.

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 пяти лет.

5.3. Типовые варианты СКУД

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. 55 приведен вариант контроля доступа в помещение с одной дверью. В систему входят: 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.

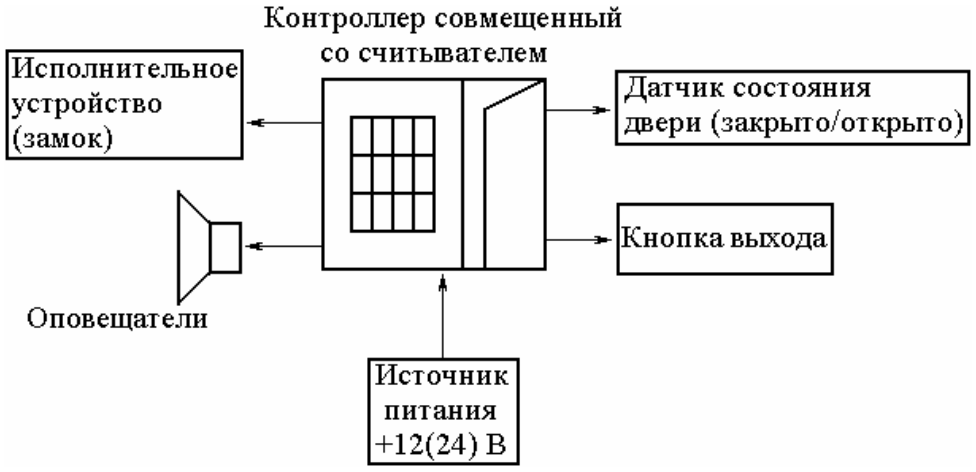


Рис. 55. Оборудование СКУД помещения с одной дверью

Система обеспечивает два способа контроля доступа: проверку только карточек или двойную проверку – карточек и кодо-

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

При реализации данного варианта на объекте рекомендуется:

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

– использовать системы, имеющие энергонезависимую память и позволяющие хранить данные длительное время;

– использовать системы, позволяющие изменять время разблокировки дверей;

– программирование системы осуществлять с помощью мастер-карточки и клавиатуры.

Данный состав СКУД может варьироваться в широких пределах и в минимуме состоять из одного конструктивно законченного блока (в виде замка), в котором размещены считыватель, контроллер, исполнительное устройство (запор, ригель, задвижка и т. п.), индикаторы режимов работы. При этом СКУД работает в режиме обычного замка, т. е. при совпадении кодов идентификатора и считывателя запорный механизм срабатывает и разблокирует дверь, разрешая через нее проход. В процессе расширения системы дополнительно может устанавливаться еще один считыватель для контроля прохода в обратную сторону (или организации многоуровнего контроля доступа), выносные световые/звуковые оповещатели, устройства автоматического открывания/закрывания двери и т. д.

На рис. 56 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.

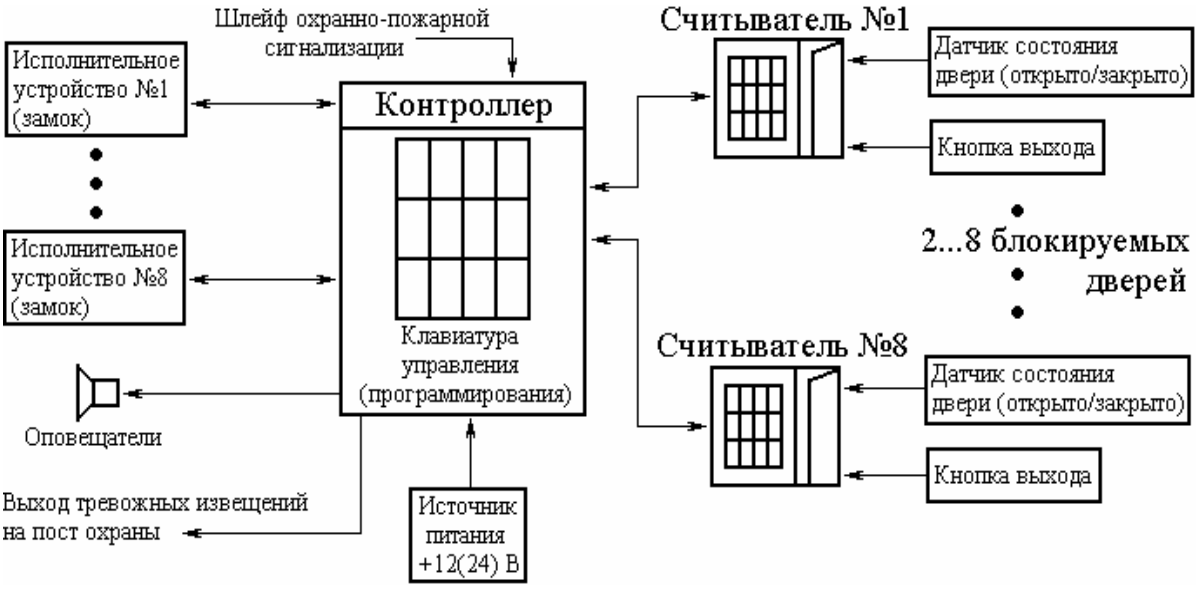


Рис. 56. Оборудование СКУД объекта с несколькими дверями

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.

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. 57 приведена примерная структурная схема построения СКУД 3-го класса (64 контролируемые двери) на базе многофункционального контроллера, имеющего модульную конструкцию. На рис. 58 приведены варианты построения систем 4-го класса.

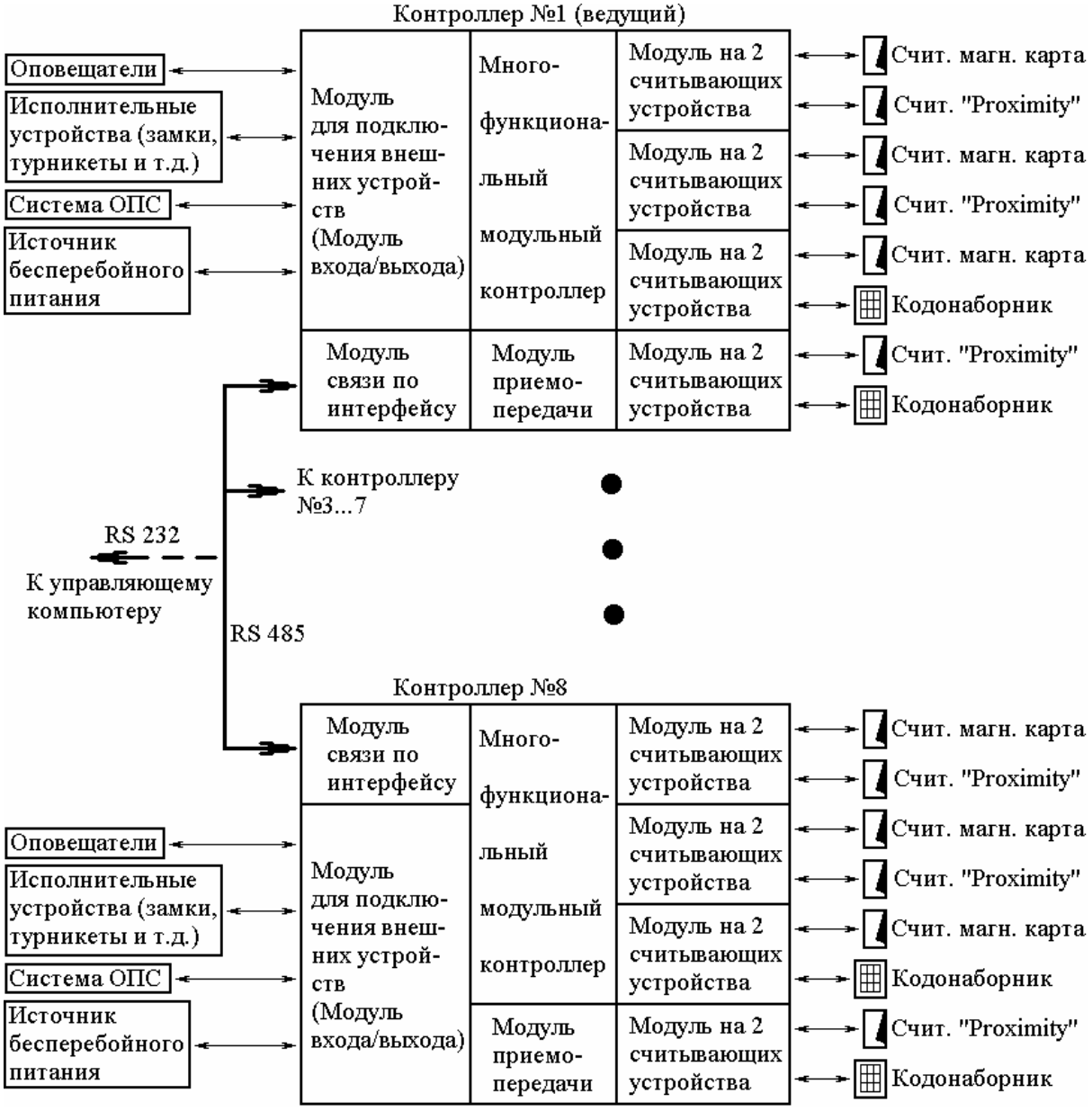


Рис. 57. Структурная схема СКУД 3-го класса

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 восьми 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.

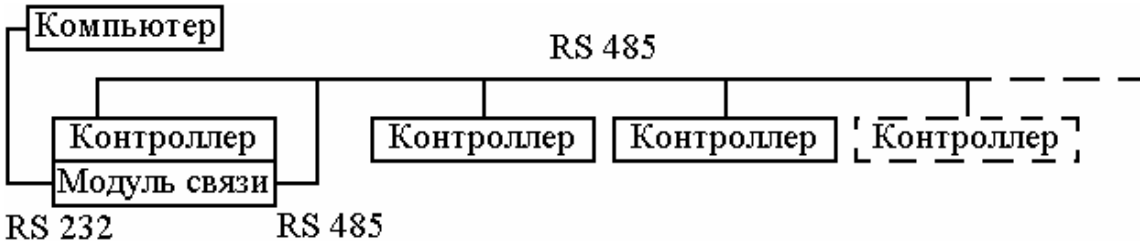


Рис. 58. Примерная структурная схема построения СКУД 4-го класса с одной ветвью

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 одного километра с помощью интерфейса *RS* 485, а также при необходимости объединение контроллеров и управляющего компьютера в компьютеризированную систему с помощью интерфейса *RS* 232. Модуль приемопередачи 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 по-

строения 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. 58. 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.

Дальнейшее наращивание системы возможно путем организации нескольких (до 10) ветвей контроллеров. Пример организации двух ветвей показан на рис. 59.

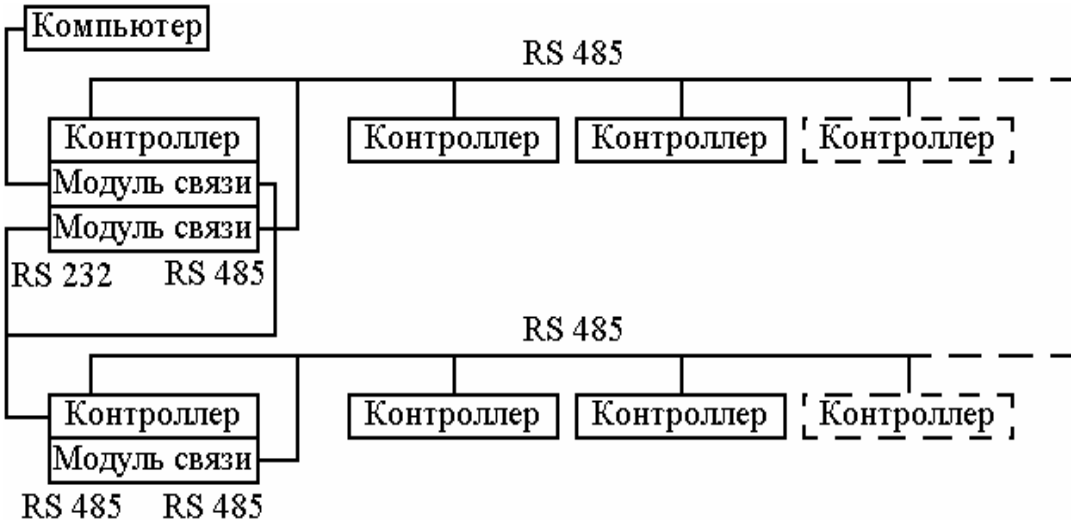


Рис. 59. Структурная схема построения СКУД 4-го класса с несколькими ветвями

Модуль связи первого контроллера преобразовывает с одной стороны поток данных, посылаемых с управляющего компьютера на контроллер, а с другой – поток выходных данных, параллельно подаваемых на адресные модули связи в ветвях. Каждый адресный модуль связи обменивается данными с контроллерами в ветвях и модулями связи. Такая расширенная сеть позволяет обслуживать до 320 контроллеров и 2048 контролируемых точек.

При необходимости ветвь контроллеров может быть увеличена еще на один километр. Для этого удлиняемая ветвь (рис. 60) подключается к первому контроллеру новой ветви через модуль связи (интерфейс *RS* 485).

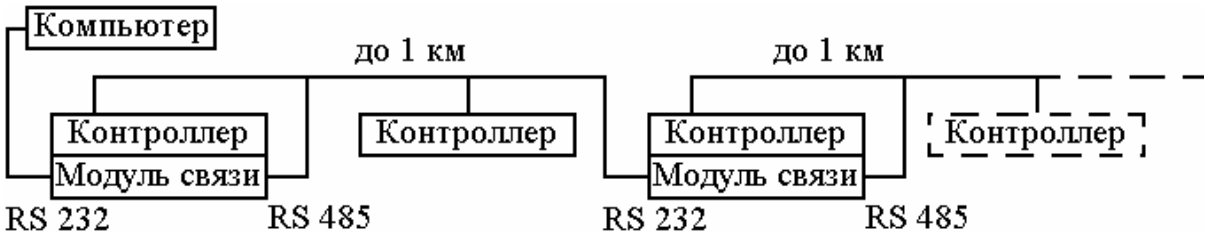


Рис. 60. Увеличение длины ветви при использовании двух модулей связи

Наличие описанных модулей многофункционального контроллера создает большие возможности по управлению разнообразной периферией системы. В качестве контролируемых точек могут выступать считывающие головки, *Pin*-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 флаговых регистров, временные интервалы регистраторов событий и т. д.) прямо с клавиатуры компьютера. Это дает возможность реализовывать различные варианты организации контроля и управления доступом, гибко меняя их в соответствии с текущими требованиями.

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

Размещение технических средств СКУД на объекте

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. 61).

Ведущие контроллеры и контроллеры, *работающие на несколько устройств заграждения*, рекомендуется размещать в

специальных запираемых металлических шкафах или нишах, на удобной для технического обслуживания высоте. При этом дверцы данных шкафов или ниш следует 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, защищающего контроллер от актов вандализма. Контроллеры, управляющие работой считывателей или исполнительных устройств одной двери в двух направлениях, рекомендуется устанавливать с внутренней стороны охраняемого помещения.

Рис. 61. Размещение компьютеров СКУД, объединенных в сеть, на объекте

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 демпфирующих 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 неправильного монтажа соединительных линий и их длины. Для нормальной работы рекомендуется:

– для шины *RS* 485 использовать высококачественный экранированный кабель витой пары;

– при значительной длине соединительного кабеля подключать к шине оконечные и согласующие элементы. Необходимое точное значение величины этих элементов зависит от характеристик кабеля;

– заземлять устройства и экранированные оплетки кабелей в одной точке (во избежание возникновения блуждающих токов), желательно у ведущего контроллера. При большой длине кабелей заземление можно производить в разных точках, но при этом обязательно нужно использовать специальные методы и устройства защиты от помех;

– использовать шинные усилители при большой длине кабеля.

Считыватели и исполнительные устройства. В зависимости от их типа, пропускной способности и организации системы безопасности объекта в целом они могут устанавливаться как вблизи устройств заграждения, так и непосредственно на них. На рис. 62 и 63 приведены некоторые варианты размещения и монтажа считывателей и исполнительных устройств.

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.

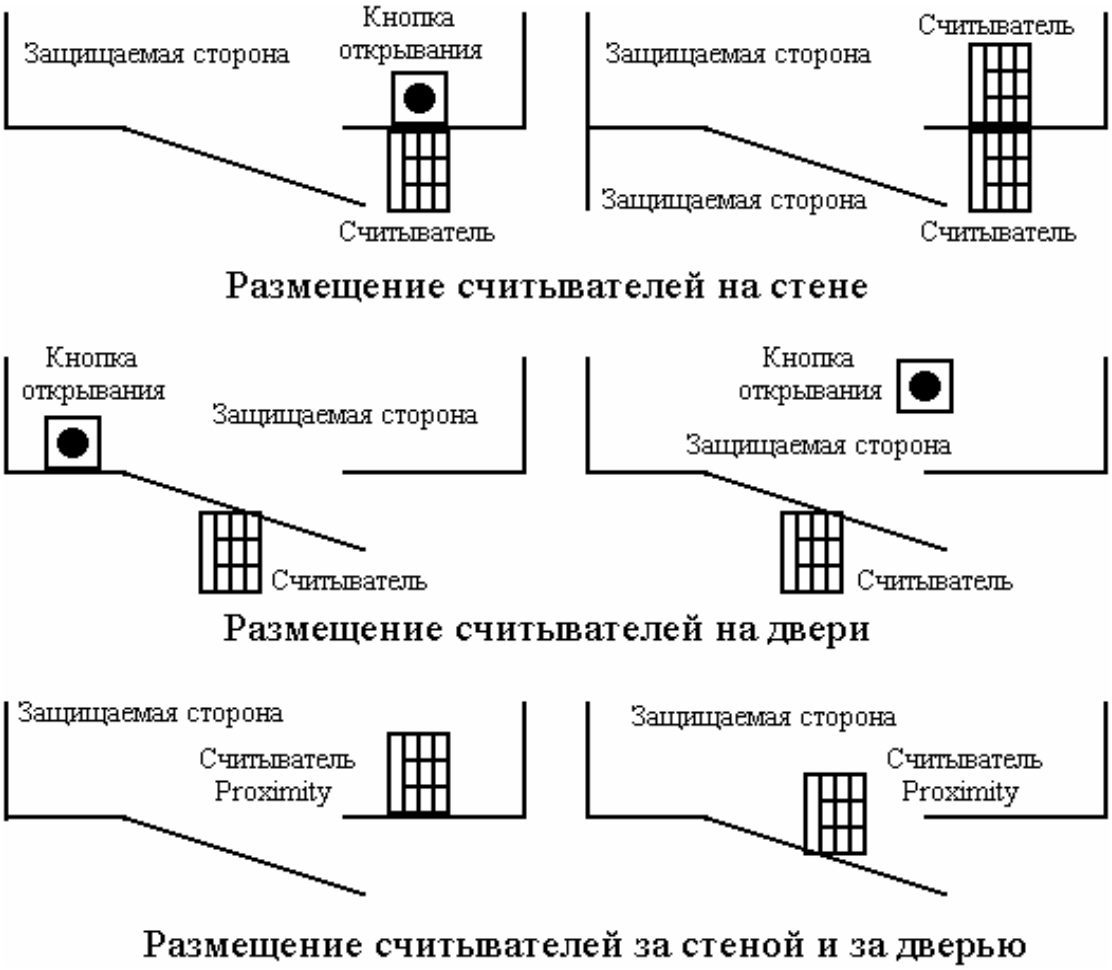
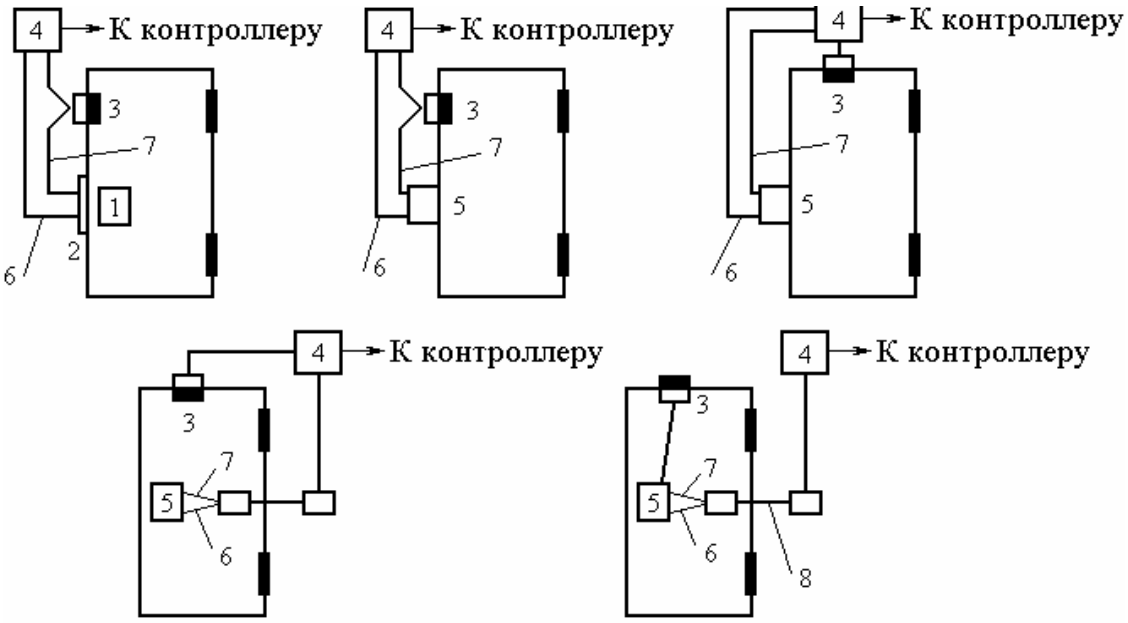


Рис. 62. Варианты размещения считывателей

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



Условные обозначения:
1 – механический замок;
2 – электромагнитная защелка;
3 – магнитоконтактный датчик открытия двери (СМК);
4 – соединительная коробка;
5 – электромеханический или электромагнитный замок;
6 – кабель питания замка (для дверей из сгораемого материала двойная изоляция ПХВ или металлорукав);
7 – цепи управления и контроля;
8 – гибкий переход (кабелепровод)

Рис. 63. Варианты размещения исполнительных устройств на дверных конструкциях

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.).

Электомагнитные защелки рекомендуется монтировать в косяке дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери при закрывании двери, и разблокировать замок при подаче сигнала от контроллера. Кроме того, такая установка защелки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромеханические замки рекомендуется устанавливать на деревянных и металлических дверях массой до 100 кг при условии средней нагруженности (до 100 – 200 проходов в день). Применение этих замков для дверей с высокой нагруженностью неэффективно по причине высокого механического износа и как следствие снижения надежности и срока службы. Обычно электромеханические замки устанавливают на двери (накладной или врезной замок), но иногда 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 магнитно-контактных 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).

Контрольные вопросы и задания

1. Перечислите основные требования к исполнительным устройствам СКУД.
2. Перечислите основные требования к устройствам идентификации доступа.
3. Перечислите основные требования к устройствам контроля и управления доступом.
4. В чем заключается специфика построения СКУД для автономного режима работы? Приведите типовой состав оборудования СКУД.
5. В чем заключается специфика построения СКУД для сетевого режима работы? Приведите типовые структурные решения таких систем.
6. Назовите основные принципы размещения оборудования СКУД на объекте.

Глава 6. УСТРОЙСТВА ПРЕГРАЖДАЮЩИЕ УПРАВЛЯЕМЫЕ

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 тому подобные конструкции).

Исполнительные устройства (ИУ) являются наиболее важными компонентами УПУ СКУД, поскольку именно это оборудование реализует активную часть управления доступом в охраняемую зону и/или помещение по командам устройств управления (контроллеров). Исполнительные устройства в основном определяют уровень и качество выполнения функции задержания и оказывают существенное влияние на быстродействие системы и стоимость СКУД в целом. В этой связи необходимо наиболее аккуратно подходить к вопросу выбора и применения исполнительных устройств.

Все ИУ по степени их применения можно разделить на три основных класса:

– используемые для организации доступа в помещения;

– предназначенные для организации доступа на пешеходных контрольно-пропускных пунктах (КПП);

– предназначенные для организации доступа на транспортных КПП.

6.1. Исполнительные устройства, применяемые для контроля доступа людей в помещения

К таким исполнительным устройствам относятся средства, обеспечивающие управляемое отпирание/запирание и открыва-

ние/закрывание дверей. Такими устройствами являются электрические замки разных типов и доводчики, в том числе различные электрические и механические приводы. Доводчик является тем необходимым элементом, который автоматически осуществляет закрывание двери после прохода через нее. Для того чтобы доводчик надежно выполнял свою основную функцию (закрывал дверь после прохода через нее и оберегал замок от механических ударов), при его выборе следует учитывать такие основные параметры, как масса и тип двери, частота срабатываний, требуемая скорость закрывания. Для обеспечения блокирования двери при отсутствии проходов через нее и возможности автоматического ее отпирания при разрешении прохода применяются электрические управляемые замки и защелки, которые делятся на *электромеханические* и *электромагнитные*.

Основное различие данных средств заключается в том, что в электромеханических замках в основном применяются те же принципы, что и в обычном механическом замке, только управление ригелем может осуществляться как механически (используя обыкновенно ключ), так и с использованием электричества. В электромагнитном замке удержание двери осуществляется посредством притягивания стальной пластины (якоря), размещенной на двери, к электрическому магниту (собственно замку), установленному на коробке за счет создаваемого магнитного поля.

Важным для оценки правильности применения того или иного замкового устройства (ЗУ) является то, что при отключении питания электромеханические замки, как правило, остаются в закрытом состоянии, в то время как электромагнитный замок при отключении питания, наоборот, отпирается. В этой связи электромагнитные замки чаще всего ставят на дверях, выполняющих функции аварийных выходов на случай экстренной эвакуации людей.

При выборе конкретного ЗУ необходимо учитывать особенности подачи сигнала управления и/или питания. Так, для управ-

ления электромеханическим замком, как правило, необходимо прокладывать провод в полотне двери или на ее поверхности с внутренней стороны. В этом случае дополнительно используются специальные кабелепроводы или контактные группы проводов для подачи питания от коробки двери до замка. Вместе с тем следует отметить, что некоторые производители выпускают электромеханические замки, в которых питание подается через запорную планку. Подводка питания и сигнальных цепей к электромагнитным замкам и электромеханическим защелкам осуществляется только путем прокладки кабеля в дверной коробке и не требует вмешательства в полотно двери. Отдельно следует упомянуть об автоматических раздвижных дверях, монтируемых в специально подготовленные дверные проемы. В таких ИУ вся механическая часть привода, как правило, размещается в верхней части конструкции двери. Автоматические раздвижные двери являются, по сути, достаточно сложным устройством и характеризуются определенной (довольно низкой) скоростью открывания/закрывания, ресурсными показателями, типом полотна двери, формой (плоская, сферическая), шириной дверного проема, наличием дополнительных сервисных функций.

При выборе замка учитываются такие особенности, как материал, из которого изготовлен замок, его стойкость к взлому, климатические условия эксплуатации, параметры управляющего сигнала и требуемого источника питания, наличие органов аварийной разблокировки, совместимость по уровню питающих напряжений и управляющих сигналов с контроллерами СКУД, дизайн и ряд других характеристик. Наиболее важными параметрами, характеризующими любой замок, главным образом электромеханический, и в основном определяющими его стоимость, являются его функциональные и технические, а также ресурсные показатели. Некоторые производители выпускают замки с более развитыми сервисными функциями, позволяют отслеживать положение ригеля ЗУ, двери (открыто/закрыто) и т. п.

6.2. Исполнительные устройства, применяемые для организации доступа на пешеходных КПП

При выборе таких ИУ необходимо четко представлять тот круг задач, который пользователь хочет решить за счет применения данного вида оборудования. В противном случае может оказаться, что или пропускное устройство (ПУ) не решает поставленной задачи, или можно было применить более простое и, следовательно, менее дорогостоящее оборудование. Рассмотрим основные задачи, которые, как правило, приходится решать потребителю.

В том случае, когда необходимо разделить поток людей и иметь информацию о времени и направлении прохода того или иного человека, т. е. фактически решать задачи контроля рабочего времени (табельного учета), наиболее эффективным является использование поясных (полуростовых) турникетов.

Поясные турникеты бывают «нормально закрытые» и «нормально открытые». Разница между ними заключается в том, что первый тип турникетов всегда заблокирован в режиме ожидания. В случае получения разрешения на проход его ЗУ разблокируется, а после прохода через него ЗУ опять блокирует турникет. В свою очередь, в зависимости от типа преграждающего устройства данный вид турникетов можно разделить на трехштанговые и роторные.

В ***трехштанговых турникетах*** (чаще называемых триподами) функцию преграждающего устройства выполняют штанги, расположенные на специальной головке под углом 120 градусов друг к другу, при этом одна из штанг в режиме ожидания всегда находится в горизонтальном положении, создавая барьер, препятствующий проходу (рис. 64). Для исключения преодоления таких турникетов путем подлезания под штангой и/или перелезания над ней некоторые производители устанавливают дополнительное средство обнаружения, контролирующее зону прохода под и/или над штангой.

Роторный турникет – это конструкция с вертикально расположенной вращающейся осью, на которой закреплены три или четыре лопасти, образующие перегородки, препятствующие проходу (рис. 65). Роторные турникеты по сравнению с триподами исключают возможность осуществить их преодоление путем подлезания под горизонтально расположенным брусом, в таких турникетах либо устанавливается несколько брусьев, либо применяется сплошное заполнение перекрываемой области пространства, например ударопрочным стеклом или пластиком.

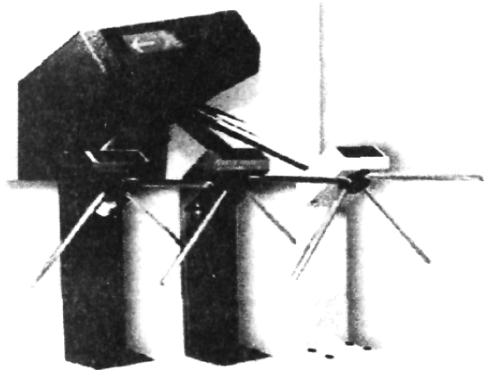


Рис. 64. Трипод электромеханический PERCO

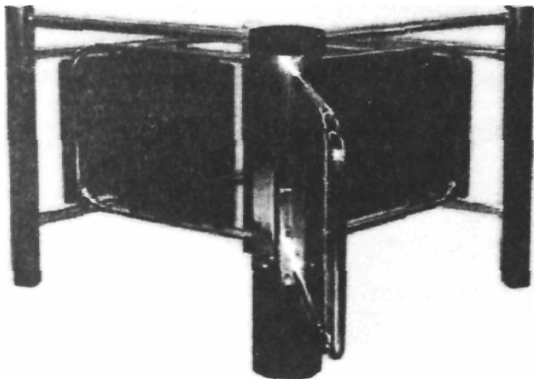


Рис. 65. Турникет роторный электромеханический полуростовый с приводом

Нормально открытые турникеты (например установленные в московском метро) оставляют зону прохода всегда открытой. В случае попытки несанкционированного прохода из стоек турникета выдвигаются специальные преграждающие устройства. Нормально открытый турникет обладает, как правило, более высокой пропускной способностью и надежностью, а также лучшими ресурсными показателями, нежели нормально закрытый турникет. Другим преимуществом нормально открытого турникета является постоянная готовность его использования для эвакуации людей. В триподах для реализации аварийного прохода обычно применяется специальный механизм «антипаника», обеспечивающий «перелом» преграждающего бруса при оказании на него воздействия в определенном направлении.

Учитывая тот факт, что полуростовые турникеты не являются серьезным препятствием для нарушителя, производители предлагают более совершенные устройства для обеспечения ужесточенных требований по организации пропускного режима на КПП. Речь идет о полноростовых турникетах и шлюзовых пропускных устройствах.

Полноростовые турникеты представляют собой трех- или четырехлопастную вертушку, выполненную в полный рост человека. В исходном положении дверь заблокирована специальной электромеханической защелкой. После предъявления личностных атрибутов и получения разрешения на проход блокировка с защелки снимается и пользователь проходит, толкая дверь от себя. После прохода дверь вновь блокируется защелкой.

Преодоление данного типа турникета является более проблематичным, чем в случае полуростовых, однако опытный нарушитель достаточно свободно может преодолеть и такой тип турникетов.

В идеальном случае пропускные устройства СКУД должны обеспечивать реализацию принципа шлюзования каждого проходящего, т. е. осуществлять попеременное открывание дверей тамбура с реализацией обязательной фазы временного блокирования в зоне контроля любого лица. В этом случае обеспечивается максимальный уровень требований по управлению доступом. Принцип шлюзования с применением весоизмерительного устройства позволяет практически полностью исключить проход по одному пропуску двух и более лиц и обеспечить надежное задержание несанкционированных лиц до выяснения обстоятельств, связанных с задержанием.

Полноростовые пропускные устройства шлюзового типа обычно выполняются в виде пропускных кабин, снабженных двумя дверьми, выходящими: одна – на неохраняемую, вторая – на охраняемую территорию зала КПП. Между запертыми дверьми и стенками такого устройства образуется зона контроля, в которой находится пользователь во время его идентификации. В случае выявления причин, требующих задержания, он остается заблокированным в зоне контроля.

Полноростовые трехлопастные турникеты блокирующего типа обеспечивают создание зоны контроля и реализуют принцип шлюзования проходящих лиц при каждом цикле поворота ротора на 120 градусов. Однако такие устройства менее удобны в пользовании и имеют во многом худшие характеристики по сравнению с пропускными кабинами.

В настоящее время на рынке есть интегрированные пропускные устройства шлюзового типа, обеспечивающие дополнительно к выполнению основной функции – управления доступом проходящих лиц – реализацию задач обнаружения проноса оружия, взрывчатых веществ и радиоактивных материалов.

При выборе типа пропускного устройства следует учитывать:

– решение основной функции доступа (исключение несанкционированного прохода с учетом приведенных выше рекомендаций), так как от ее правильной оценки во многом зависит стоимость оборудования;

– пропускную способность УПУ, от которой зависит количество устройств, необходимое для приобретения (целесообразно предусматривать также некоторый резерв их на случай выхода какого-либо устройства из строя или для снижения пиковых перегрузок при проведении регламентных и ремонтных работ);

– коэффициент использования площади зала КПП (при установке оборудования с более высоким значением данного коэффициента в одном и том же зале КПП потребитель может разместить большее количество УПУ или дополнительное досмотровое оборудование);

– габаритные размеры прохода, массу устройства, вероятность проноса предметов с определенными габаритными размерами, возможность использования ПУ в качестве основных и/или запасных эвакуационных проходов, эргономические показатели удобства движения при проходе, количество преодолеваемых преград и т. п.

Шлюзовой тамбур – это система из двух дверей, управляемая электроникой, которая позволяет открывать одну из дверей только в том случае, когда вторая закрыта.

Характерные особенности различных шлюзовых тамбуров:

– различная ширина прохода;

– система взвешивания, позволяющая обнаружить предмет, оставленный в тамбуре, и ограничить количество одновременно проходящих через кабину людей:

– система зашиты от несчастных случаев;

– возможность работы кабины как в ручном, так и в полностью автоматическом режиме;

– двухсторонняя связь (клиент-охранник);

– цифровой металлодетектор;

– детекторы взрывчатых веществ;

– синтезатор речевых сообщений;

– выносной пульт ручного управления шлюзовой кабиной;

– логический блок управления дверьми;

– режим аварийного выхода;

– гарантированное питание – встроенный аккумулятор большой емкости позволяет не нарушать работу системы даже в случае длительного отключения напряжения.

6.3. Электрозамки

Для управления процессом прохода в двери в СКУД используются специализированные электрозамки (замки с электрическим управлением). К исполнительным устройствам можно также отнести дверные доводчики;

Типы исполнительных устройств (электрозамков):

– электромагнитные замки;

– электромоторные замки;

– соленоидные замки;

– электромеханические (курковые) замки;

– электрозащёлки.

Электромагнитный замок представляет собой мощный электромагнит, закрепленный на дверном косяке. Ответная часть – якорь – крепится на двери (как правило, в верхней части). При наличии напряжения в обмотке замка он способен удерживать дверь с усилием 200 – 2000 кг. При выключении питания дверь разблокируется. Одним из главных достоинств данного устройства является отсутствие движущихся механических частей и, как следствие этого, значительный ресурс наработки на отказ.

Электромагнитный замок *ML*-194.01/*P* построен на базе микроконтроллера и предназначен для использования в системах контроля доступа. В качестве идентификаторов могут использоваться электронные ключи *iButton DS*1990*A* или *Proximity*-карты (для модели *ML*-194.01/*P*) при наличии *Proximity*-считывателей серии *AD* производства ООО «АККОРД-2001».

Соленоидные замки фактически представляют собой мощный металлический стержень, выдвинутый в нормальном состоянии из замка. При подаче питания он задвигается внутрь. Достоинства: высокое усилие удержания, высокая скорость, надежность. Недостатки: высокий скачок напряжения в момент открытия, а также то, что соленоид бывает только «нормально закрытым» и не может долго находиться под напряжением – сгорит.

Электромеханические (курковые) замки имеют специальный взводящий ригель, выполняющий функцию взвода пружины замка, для этого дверь необходимо открыть и снова закрыть. Данные модели недороги и эффективны, но имеют существенный недостаток: если пользователь решил выйти (считал карточку и замок разблокировал дверь), а потом передумал, и дверь не была открыта, она останется в открытом состоянии, и для того чтобы привести ее в исходное состояние, необходимо вручную открыть ее и снова закрыть. В качестве примера таких замков ниже приведены характеристики накладных электромеханических замков фирмы *ISEO* (Италия). Фирмой *ISEO* выпускается более 30 типов накладных электромеханических замков, ниже приведены харак-

теристики наиболее интересных моделей, отобранных в результате многолетнего опыта инсталляции этого оборудования.

Все замки имеют рабочий ригель, защелку и взводящий ригель, обеспечивающий сжатие рабочей пружины при закрывании двери. Различные модели отличаются способами открывания замка с внутренней стороны: кнопка или цилиндр + кнопка. Для электрического управления замком необходимо подать на него напряжение 12 В, 15 Вт.

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 последняя может быть открыта изнутри поворотом ручки без подачи управляющего напряжения на защелку. В качестве примера приведены параметры и характеристики электрозащелок серии 30 фирмы *OPENERS & CLOSERS* (Испания). Защелки данной серии предназначены, прежде всего, для алюминиевых и нетяжелых стальных дверей. Они отличаются миниатюрностью и высокой надежностью. Все защелки данной серии имеют регулировку положения запирающей планки. Это позволяет подогнать положение планки и ригеля замка после установки защелки. Отличительные черты серии: модификации с механической разблокировкой модификации с фиксацией открывания (*open hold*), модификации на различные напряжения и токи потребления, широкая номенклатура конструкций планок.

Дверные доводчики (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 от-

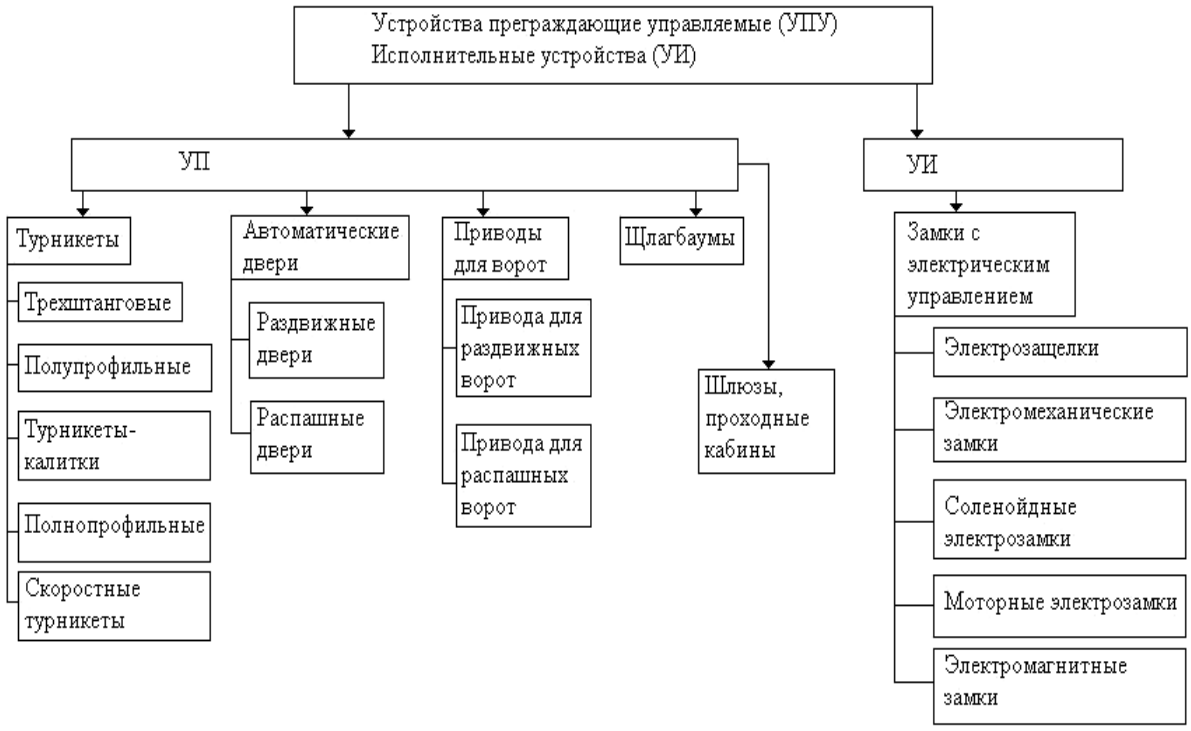
личаются конструктивным исполнением, дизайном, рядом дополнительных функций: фиксация двери в положении «открыто», ускорение в завершающей фазе закрывания – «прихлоп» и др. Некоторые их модификации (электромоторные доводчики) позволяют также еще и открыть дверь дистанционно.

Контрольные вопросы и задания

1. Охарактеризуйте исполнительные устройства, применяемые для контроля доступа людей в помещения.
2. Перечислите и проанализируйте исполнительные устройства, применяемые для организации доступа на пешеходных КПП.
3. Какие типы электрозамков используются для управления процессом прохода в двери в СКУД?
4. Для каких целей в СКУД служат дверные доводчики?

ЗАКЛЮЧЕНИЕ

Обобщая изложенное в данном пособии, можно представить основные структурные части СКУД в следующем виде:



Стремительное развитие СКУД обусловлено, с одной стороны, наличием многочисленных актуальных задач, а с другой – быстрым развитием технологий, позволяющих реализовать все более сложные задачи. А современные технологии позволяют реализовать все более сложные и совершенные алгоритмы идентификации, в первую очередь связанные с теорией распознавания образов.

Кроме технических вопросов, организация системы контроля доступа в ряде случаев требует решения и других проблем. Так, в настоящее время имеются планы введения специальных иденти-

фикаторов с основными биометрическими характеристиками в паспорта. Очевидно, что это позволит решить две основные задачи: с одной стороны, существенно упростить процесс идентификации и аутентификации личности при одновременном повышении надежности идентификации, а с другой – заметно усложнить возможность подделки паспортов.

Следующий шаг – создание глобальной базы данных для решения визовых проблем. Соответственно весьма важным становится другой аспект – морально-этический. Фактически это будет означать создание системы глобального контроля за перемещением человека.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК*

1. ГОСТ Р 50739-95. Защита от несанкционированного доступа к информации. Общие технические требования. – М. : Госстандарт России : Изд-во стандартов, 1998.

2. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – М. : Госстандарт России : Изд-во стандартов, 1999.

3. Методические рекомендации. Применение систем контроля и управления доступом в охране объектов. – М. : НИЦ «ОХРАНА» МВД России, 2004.

4. Методические рекомендации. Выбор и применение систем контроля и управления доступом. – М. : НИЦ «ОХРАНА» МВД России, 1998.

5. *Волковицкий, В. Д. WIN-PAK-Pro International*. Программное обеспечение для систем контроля доступа и комплексных

* Печатается в авторской редакции.

систем безопасности : справ. пособие / В. Д. Волковицкий. – СПб. : Экополис и культура, 2002.

6. *Волковицкий, В. Д.* Системы контроля и управления доступом / В. Д. Волковицкий, В. В. Волхонский. – СПб. : Экополис и культура, 2003.

7. *Арманд, В. А.* Штриховые коды в системах обработки информации / В. А. Арманд, В. В. Железнов. – М. : Радио и связь, 1989.

8. *Абрамов, А. М.* Системы управления доступом / А. М. Абрамов, О. Ю. Никулин, А. Н. Петрушин. – М. : Оберег-РБ, 1998. – 192 с.

9. *Свами, М.* Графы, сети и алгоритмы / М. Свами, К. Тхуласираман. – М. : Мир, 1984.

10. Интернет: *http*://*www.biometricsgroup.com*
11. Интернет: *http*://*www.bioscript.com*
12. Интернет: *http*://*www.cor-net.ru*
13. Интернет: *http*://*www.sec.ru*
14. Интернет: *http*://*www.aamsystems.ru*
15. Интернет: *http*://*www.shelni.ru*
16. Интернет: *http*://*www.domofon.ru*
17. Интернет: *http*://*www.accordsb.ru*
18. Интернет: *http*://*www.perco.ru*
19. Интернет: *http*://*www.elics.ru*
20. Интернет: *http*://*www.appolo-seccurity.com*

Учебное издание

Комплексная защита объектов информатизации. Книга 14

БУГАКОВ Виктор Петрович
ТЕЛЬНЫЙ Андрей Викторович

ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ
Системы контроля и управления доступом

Учебное пособие

Подписано в печать 18.05.07.
Формат 60x84/16. Усл. печ. л. 8,60. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета.
600000, Владимир, ул. Горького, 87.