

Содержание

Глава 1. Методы геометрического считывания информации	7
1.1. Идентификация человека посредством электроники.....	7
1.1.1. Сравнение с шаблоном и технические ошибки	8
1.1.2. Верификация и ошибки верификации	8
1.2. Методы считывания информации для анализа в системе кодового доступа	10
1.2.1. Отпечаток пальца.....	10
Оптический метод	10
Емкостный метод.....	11
Радиометод	11
Нажимной метод.....	11
Микроэлектромеханический метод.....	11
1.2.2. Геометрия лица человека	12
1.2.3. Радужная оболочка и сетчатка глаза	12
1.2.4. Идентификация по рисунку вен ладони и ее геометрии.....	13
1.2.5. Дополнительная идентификация по штрих-коду	14
1.3. Устройства считывания информации. Взаимодействие со СКУД	15
1.3.1. Идентификация по бесконтактным картам.....	15
Физическое исполнение	15
Протокол взаимодействия (формат).....	16
Используемые считыватели и формат идентификаторов	16
Возможность синхронизации и дальность считывания информации.....	17
Выходной интерфейс	17
Особые условия эксплуатации	17
Дизайн	17
1.3.2. Принципы работы устройств в составе СКУД TSS2000	18
1.3.3. Организация работы с программой «Бюро пропусков».....	19
Вариант 1 – биометрия как часть обычной СКУД	20
Вариант 2 – полностью биометрическая СКУД.....	21
1.3.4. Варианты занесения кодов в ПО СКУД «Персонал».....	21
1.4. Популярные биометрические системы	23
1.4.1. Считыватели BioEntry Plus / BioEntry W / BioEntry W2 / BioEntry Station A2 (Suprema, Корея). Распознавание по отпечатку пальца	24
Особенности работы с программой BioStar (v. 1.61)	24
Особенности работы с программой BioStar (v. 2.6.2)	25
1.4.2. Биометрический считыватель F11 (ZKSoftware, Китай). Распознавание по отпечатку пальца.....	26

Особенности работы	26
1.4.3. Биометрический считыватель F710 (Hanvon, Китай). 3D-распознавание по лицу	26
Особенности работы считывателя	27
1.4.4. Биометрический считыватель FR020EM, FR030EMW, FR031EM (Smartec, Китай). Распознавание по отпечатку пальца	27
Особенности работы с программой Timex.....	28
Учет рабочего времени и контроль доступа для филиальной сети.....	29
Дополнительные настройки монитора событий Terminal Options-add	31
Перенос отпечатков сотрудников с одного терминала на другой	31
1.4.5. Биометрический считыватель FR040EM (Smartec, Китай). Распознавание лиц, кодов доступа и карт Em Marine	32
Конфигурирование системы	33
Режимы идентификации	34
1.4.6. Биометрический считыватель Recognition Systems – считыватель HandKey II по форме кисти руки.....	35
Особенности работы	36
1.4.7. Биометрический считыватель компании Eyelock (США) EyeSwipe- Nano – по радужной оболочке глаза (Iris Scanner)	36
Особенности работы	37
Таблицы перекодировки	37

Глава 2. Биометрическая идентификация: практика

и возможности использования.....	38
2.1. Введение в технологию.....	38
2.2. Состав, конфигурация и задачи единой биометрической системы.....	39
2.3. Температурный метод сканирования	40
2.4. Как работает система регистрации и сопоставления.....	41
2.5. Дополнительные возможности интеграции со смарт-картами	43
2.6. Конфигурирование считывателей в системе ЕБС.....	45
2.7. Риски и ошибки идентификации.....	46
2.8. Практическая работа и перспективы	47
2.9. Практические примеры коммутируемых соединений	49
2.10. Практический пример	51
2.10.1. Установка и эксплуатация устройства HN-F1ME со считывателем отпечатков пальцев и считывателем карт Proximity	51
Практическая установка и монтаж	52
Схема подключения	53
Функционал устройства в режиме «Мастер».....	54
Удаление пользователей	55
Действия с помощью пульта ДУ и добавление пользователей	55
Удаление пользователей с помощью пальца и по ID	56
Сохранение изменений и выход из режима программирования	56

Добавление мастер-пальца	56
Добавление пользователей последовательно	57
Удаление отпечатков пальцев и карт	57
Удаление всех пользователей	57
Установка группового кода	57
Установка типа замка и времени переключения реле двери	57
Установка контроля состояния двери	58
Установка блокировки двери	58
Установка режима шлюза	58
Установка времени выхода тревоги	58
Действия пользователя на открывание двери и отключение тревоги	58
2.10.2. Другие способы применения контроллера	59
Подключение дополнительного считывателя к контроллеру HN-F1ME	60
Установка двух контроллеров HN-F1ME на одну дверь	60
Организация шлюза на двух контроллерах TS-RDR-Bio1	61
Сброс контроллера на заводские установки	62
2.11. Выводы	64

Глава 3. Практическое подключение к единой биометрической системе (ЕБС)

3.1. Обоснование создания и особенности ЕБС	65
Строение ЕБС	67
3.2. Биометрические контроллеры и их характеристики	67
3.2.1. HN-F1ME	67
3.2.2. Биометрический считыватель F16 MIFARE ZKTECO	68
3.2.3. Биометрический считыватель ST-SC110EKF SMARTEC	69
3.2.4. Биометрический считыватель FR1200 ZKTECO	70
3.2.5. Биометрический считыватель ST-FR015EM SMARTEC	72
3.2.6. Биометрический считыватель MA300 EM ZKTECO	72
3.2.7. Биометрический считыватель BIOSMART 5M-E-EM	73
3.2.8. Биометрический считыватель BIOSMART 4-O-EM-N-L	74
3.2.9. Биометрический считыватель ST-FR040EM SMARTEC	74
3.2.10. Биометрический считыватель ST-FR032EK SMARTEC	75
3.2.11. Биометрический считыватель BIOSMART MINI-O-EM	76
3.2.12. Биометрический считыватель ST-FR030EMW SMARTEC	77
3.2.13. Биометрический считыватель C2000-BIOACCESS-F18 БОЛИД	78
3.2.14. Биометрический считыватель TF1600 ZKTECO	79
3.2.15. Биометрический считыватель TF1700 ZKTeco	81
3.2.16. FE-MA300 биометрический считыватель Falcon Eye	82
3.2.17. Биометрический считыватель C2000-BIOAccess-MA300 Болид	83
3.2.18. Биометрический считыватель ST-FR031EM Smartec	84
3.3. Автономные контроллеры-считыватели биометрических данных	86
3.3.1. TS-RDR-Bio 2 контроллер-считыватель Tantos	86

3.3.2. TS-RDR-Bio 1 контроллер-считыватель Tantos	87
3.4. Многофункциональные считыватели	88
3.4.1. Контроллер F16 ZKTeco	88
3.4.2. Инновационный контроллер MA300 Mifare ZKTeco	89
3.4.3. Контроллер Optimus SKF-010	91
3.4.4. Контроллер ST-FR015E Smartec	92
3.5. Портативные и переносные считыватели.....	93
3.5.1. Настольный контроллер Hikvision DS-K1F820-F	93
3.5.2. Контроллер Smartec ST-FE800	94
3.5.3. Контроллер Smartec ST-FR015EM	95
3.5.4. Контроллер Smartec ST-FE700	96
3.6. Варианты исполнительных устройств.....	97
3.6.1. Дверные замки и защелки.....	99
3.6.2. Варианты применения для сейфовых хранилищ	100
Сетевой контроллер Эра-2000GSM	100
3.7. Выводы	102
Опорная литература.....	103

Глава 1

Методы геометрического считывания информации

Применение для идентификации разных подходов предоставляет свои преимущества: признаки, по которым происходит идентификация, нельзя потерять или забыть, передать третьим лицам, в отличие от обычных бесконтактных карт, практически невозможно подделать или украсть. Но существуют также и недостатки, к которым относятся отсутствие возможности 100%-ной достоверности идентификации, относительно высокая стоимость считывателей и зачастую слишком продолжительное время процесса идентификации. В этой главе рассмотрим популярные и развивающиеся методы считывания информации электронным способом, отличительные особенности и перспективы разных методов.

1.1. Идентификация человека посредством электроники

Принцип работы систем опознавания основан на получении изображения со сканера биометрического считывателя и его преобразовании в шаблон в электронной форме, который затем сравнивается с заранее составленным электронным банком данных. Шаблоны могут храниться как в базе данных СКУД, так и во встроенной памяти считывающего устройства или в памяти карты доступа.

Для идентификации живого объекта (человека) в биометрических системах контроля доступа используются параметры, уникальные для каждого человека. Наиболее распространенными являются системы, идентифицирующие граждан по следующим признакам:

- отпечатки пальцев;
- рисунок вен или геометрии руки;
- радужная оболочка или сетчатка глаза;
- геометрия или термограмма лица.

Причем идентификация по отпечаткам пальцев на сегодняшний день имеет уже достаточно много готовых и реализованных устройств (сетей), по анализу, функционалу и практической работе которых уже можно составить как описания, так и выводы, разъяснить возможные перспективы развития отрас-

ли электронной промышленности именно в этом конкретном направлении. Идентификации по отпечатку пальцев в книге посвящен основной материал.

На рис. 1.1 представлена иллюстрация работы одной из интегрированных электронных систем, а именно системы учета рабочего времени, элементы и части которой взаимодействуют онлайн.



Рис. 1.1. Блок-схема элементов системы учета рабочего времени

В этой схеме за сканирование отпечатков отвечают системы Bio-lait, Bio pass и сетевые терминалы. Общая система сервера с условным названием Time Control включает несколько взаимосвязанных частей (см. рис. 1.1) и может применяться как в таком виде, так и в виде различных конфигураций оборудования, где одна система «страхует» от ошибок или обеспечивает верификацию – в дополнение к другой. О возможных ошибках и верификации поговорим далее.

1.1.1. Сравнение с шаблоном и технические ошибки

При распознавании происходит сравнение изображения, полученного со сканера или камеры, с ранее зарегистрированными данными (шаблонами). Существует два метода сравнения. Полученное изображение сравнивается с большим количеством шаблонов, сохраненных в базе данных системы (один ко многим). Отвечает на вопрос, кто это; занимает больше времени, содержит большее количество ошибок.

1.1.2. Верификация и ошибки верификации

Полученное изображение сравнивается с зарегистрированным шаблоном конкретного человека (один к одному). Отвечает на вопрос, тот ли это, с кем

сравнивается отпечаток; гораздо быстрее по времени, безошибочнее, но требует ввода дополнительного идентификатора, к примеру карты или пин-кода.

В момент сравнения полученного изображения с шаблоном возможно появление ошибок. Различают ошибки верификации первого (первичные) и второго (вторичные) рода. Ошибочное отклонение верификации (FRR – False Rejection Rate), когда сканер не может распознать зарегистрированного пользователя. Несильно критичны для системы безопасности, создают неудобства из-за необходимости проведения вторичной верификации. Частота возникновения выше, чем у ошибок второго типа.

Ошибочное принятие верификации (FAR – False Acceptance Rate), когда незарегистрированный пользователь определяется системой как зарегистрированный. Критичны для системы безопасности, поскольку злоумышленник может получить доступ к системе.

Появление ошибок FRR и FAR определяется такими характеристиками, как качество и разрешение сканирования, область сканирования, математические алгоритмы, используемые для сравнения, количество сравниваемых деталей, а соотношение этих показателей позволяет оценить применимость выбранного метода идентификации на подконтрольном объекте.

Для исключения ошибок дополнительно используются различные наборы тестов, определяющих реальность объекта биометрии. Для сканеров пальцев это может быть проверка рельефности, давления или температуры пальца, для сканеров глаза – проверка аккомодации зрачка, для сканеров лица – термограмма лица.

На рис. 1.2 представлена блок-схема системы удаленного доступа и контроля, реализованная с помощью интернета. По этой иллюстрации несложно понять, как происходят считывание данных, контроль и администрирование, в общих чертах.

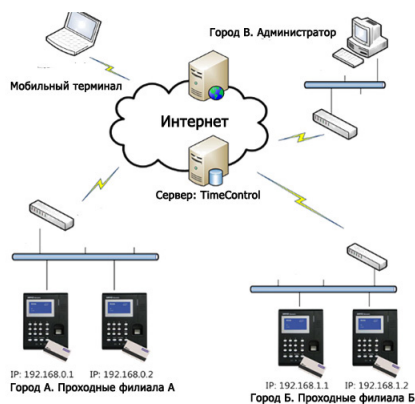


Рис. 1.2. Блок-схема контроля и администрирования в системе идентификации, действующей посредством интернета

1.2. МЕТОДЫ СЧИТЫВАНИЯ ИНФОРМАЦИИ ДЛЯ АНАЛИЗА В СИСТЕМЕ КОДОВОГО ДОСТУПА

1.2.1. Отпечаток пальца

Этот вид идентификации наиболее изучен, он основан на получении изображения рисунка папиллярных узоров пальцев людей, которые обладают свойствами индивидуальности, относительной устойчивости и восстанавливаемости. На протяжении всей книги будем говорить именно об этом – о различных современных методах идентификации человека по отпечатку пальца и всех связанных с этим вопросах и рисках.

Существуют два основных алгоритма распознавания отпечатков пальцев: по отдельным деталям (характерным точкам) и по рельефу всей поверхности пальца, причем по получаемому в результате обработки цифровому коду нельзя воссоздать первоначальный отпечаток.

Разнообразие биометрических считывателей отпечатков пальцев обусловлено широким спектром сенсоров (сканеров), использующихся для получения изображения. Среди инновационных решений есть бесконтактные считыватели, которые не требуют прикосновения, и считыватели 10 пальцев одновременно, но они довольно дороги при своей точности и комфортности для пользователя.

«Минусом» такой идентификации является зависимость качества распознавания отпечатка от состояния поверхности пальца и внешних условий (температура, влажность, пыль), нежелание некоторых людей оставлять свои отпечатки, а также наличие людей (порядка 2 % от общего количества) с врожденными плохо выделяющимися отпечатками пальцев.

Для примера рассмотрим СКУД «Sigur», где доступна глубокая интеграция со считывателями отпечатков пальца BioSmart, которая позволяет в рамках программного интерфейса СКУД «Sigur» заносить отпечатки пальцев сотрудников в систему.

Среди методов идентификации рисунка линий на пальце человеческой руки наиболее популярны следующие.

Оптический метод

Для получения оптического изображения отпечатка пальца может быть использовано устройство, подобное цифровой камере. Кончик пальца прикладывается к стеклянной пластине, освещенной должным образом. Необходимо только объектив, способный работать в непосредственной близости от объекта съемки. Изображение захватывается при помощи матрицы элементов с зарядовой связью (CCD) или элементов нужного разрешения (CMOS) и преобразуется в изображение в оттенках серого цвета (от 2 до 16 оттенков обычно вполне достаточно). Недостаток этой технологии заключается в том, что незаметный отпечаток пальца остается на поверхности стекла и может быть использован

повторно. Другая сложность состоит в том, чтобы отличить настоящий палец от хорошо выполненной имитации.

Емкостный метод

Когда кончик пальца прикладывается к матрице элементов, чувствительных к электрическому заряду, разница в электропроводности выступов (содержащих много воды) и впадин (содержащих воздух) приводит к локальному изменению емкости элементов. Это позволяет определить положение выступов и впадин и построить изображение отпечатка. Несмотря на подверженность этого метода электростатическим разрядам и прочим паразитным электрическим полям, он остается одним из наиболее популярных для получения изображений отпечатков пальцев. Однако такие сканеры сравнительно легко обмануть имитированным отпечатком или скрытым отпечатком на поверхности сканера.

Радиометод

Если облучить кончик пальца радиоволнами низкой интенсивности, то разницу в расстоянии между поверхностью выступов и впадин можно определить с помощью матрицы правильно настроенных антенных элементов. При этом требуется, чтобы кончик пальца контактировал с излучающим элементом датчика (обычно по периферии). Поскольку метод основан на физиологических свойствах кожи, его трудно обмануть имитацией пальца. Слабым местом метода является необходимость качественного контакта пальца и кольца передатчика, которое может быть весьма горячим.

Нажимной метод

Для получения узора отпечатка прикладываемого пальца может применяться и матрица пьезоэлектрических элементов, чувствительных к нажатию. Несмотря на многие недостатки этого метода (низкая чувствительность, неспособность отличить настоящий палец от имитации, подверженность повреждениям из-за чрезмерных прилагаемых усилий и т. п.), некоторые компании продолжают придерживаться этого метода в прототипах своей продукции.

Микроэлектромеханический метод

Микроэлектромеханический метод (MEMS) по состоянию на начало 2019 года – в промежуточной стадии между научно-исследовательскими работами и внедрением. Для определения выступов и впадин отпечатка пальца в лабораториях разработана матрица микромеханических датчиков, но пока еще нет уверенности в их устойчивости. Таким методом также невозможно отличить настоящий палец от имитации.

1.2.2. Геометрия лица человека

Биометрическая идентификация лиц в плане технической реализации представляет собой более сложную и дорогую задачу (по сравнению с отпечатками пальцев) и базируется на построении двухмерных или трехмерных моделей лица на основании снимков, сделанных видеокамерой. Она является самой комфортной и не всегда заметной для пользователя, не требует физического контакта с устройством.

На рис. 1.3 представлена иллюстрация сканирования по геометрии лица человека.

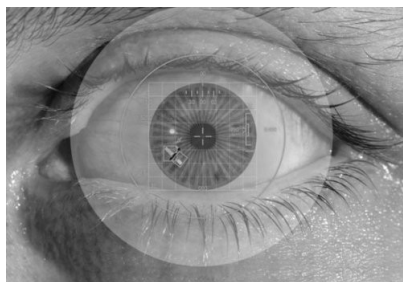


Рис. 1.3. Иллюстрация сканирования по геометрии лица человека

При построении двухмерной модели получается плоское изображение, такие системы более требовательны к освещению и положению лица при сканировании, в связи с чем происходит довольно много ошибок.

При построении трехмерной модели получается объемное изображение, что позволяет добиться большей точности распознавания за счет минимизации влияния таких факторов, как изменение цвета кожи (в том числе и с помощью косметики), ношение бороды или усов, изменение поверхности лица при болезни и др., обеспечивая при этом достаточную скорость построения 3D-модели лица.

Для повышения достоверности распознавания лиц дополнительно может использоваться термограмма лица (сканирование лица в инфракрасном диапазоне), которая компенсирует наличие очков, шляпы или накладных элементов.

1.2.3. Радужная оболочка и сетчатка глаза

Идентификация по радужной оболочке – одна из самых надежных, но дорогих технологий биометрической идентификации. Радужная оболочка уникальна, наиболее защищена от повреждений и не изменяется во времени. Очки и контактные линзы не влияют на получение изображения, даже слепой человек может быть идентифицирован таким способом.

На рис. 1.4 представлена иллюстрация этого метода.

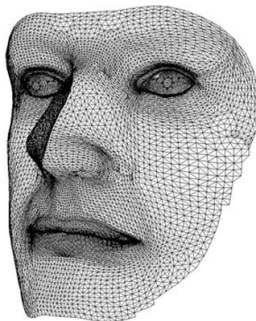


Рис. 1.4. Иллюстрация метода сканирования по оболочке и сетчатке глаза

После получения изображения происходит выделение частотных или других данных о рисунке радужной оболочки глаза, которые сохраняются в шаблон. Такой метод достаточно комфортен, поскольку не требует физического контакта с устройством и при этом отсутствует поток яркого света, направленный в глаз. При использовании камеры, разрешение которой превышает 3 Мп, можно захватывать 2 глаза на одном кадре, что заметно повышает уровень достоверности распознавания.

Этот принцип является быстрым и комфортным, по сравнению с идентификацией по сетчатке глаза, и может использоваться на объектах численностью в несколько десятков тысяч человек. В настоящее время активно развивается благодаря своей перспективности.

При идентификации по сетчатке глаза используется узор кровеносных сосудов, расположенных на поверхности глазного дна (сетчатке), получаемый путем просвечивания кровеносных сосудов на задней стенке глаза лазерным лучом мягкого излучения. Сетчатка – один из наиболее стабильных физиологических признаков организма, однако этот метод очень дорог, имеет невысокую пропускную способность и не является комфортным, так как пользователю приходится неподвижно сидеть и смотреть в окуляр в течение нескольких секунд. В настоящее время идентификация по сетчатке глаза в СКУД используется редко.

1.2.4. Идентификация по рисунку вен ладони и ее геометрии

Идентификация по рисунку вен ладони основана на получении шаблона при фотографировании внешней или внутренней стороны руки инфракрасной камерой. Из-за бесконтактной составляющей этот метод является достаточно комфортным для пользователя, при этом практически отсутствует возможность подделки, но болезни вен могут затруднять или искажать результат идентификации.

На рис. 1.5 представлена иллюстрация сканирования ладони по ее геометрии и рисунку вен.



Рис. 1.5. Иллюстрация сканирования ладони по ее геометрии и рисунку вен

Степень достоверности распознавания сравнима с идентификацией по радужной оболочке глаза, хотя стоимость оборудования гораздо ниже.

Метод идентификации по геометрии ладони основан на измерении отдельных параметров формы руки, таких как ширина ладони, радиус окружности, вписанной в центр ладони, длина пальцев и высота кисти руки, учитываются также пять основных линий, существующих на любой ладони.

Надежность этого метода сравнима с идентификацией по отпечатку пальца и тоже сильно зависит от состояния объекта, поскольку распухание тканей или ушибы руки могут исказить исходную структуру, руки могут изменяться с возрастом.

К плюсам использования можно отнести отсутствие влияния на процесс сканирования температуры, влажности и загрязненности, хотя в настоящее время идентификация по геометрии руки в СКУД используется редко.

1.2.5. Дополнительная идентификация по штрих-коду

Штрих-код представляет собой набор закодированных цифровых или алфавитно-цифровых символов в виде геометрических фигур, например последовательность черных и белых полос. Штрих-коды бывают разных видов, отличающихся тем, какой объем и какой тип информации можно с их помощью закодировать.

В системах контроля доступа обычно применяются самые простейшие штрих-коды, поскольку, как правило, не стоит задача передавать через идентификатор большое количество данных. Среди таких – Code 39, Code 128, EAN-13.

Штрих-код может наноситься практически на любую поверхность, например распечатываться обычным принтером на листе бумаги или вовсе отображаться в электронном виде на экране смартфона. Кроме этого, штрих-код может быть легко передан по электронным каналам связи, к примеру по электронной почте или факсу. Это делает использование штрих-кодов в СКУД очень дешевым. С другой стороны, такие идентификаторы никак не защищены от копирования, а также имеют низкую износостойкость. Исходя из данных особенностей, штрих-коды в СКУД обычно используются в качестве разовых пропусков для посетителей.

1.3. УСТРОЙСТВА СЧИТЫВАНИЯ ИНФОРМАЦИИ. ВЗАИМОДЕЙСТВИЕ СО СКУД

Существует большое количество сканеров штрих-кода. В зависимости от целей использования они различаются по технологии считывания и способу исполнения, характеризуются также разрешением, скоростью и дальностью сканирования, а также интерфейсом подключения.

В СКУД есть ряд общепринятых интерфейсов, с помощью которых различные считыватели могут взаимодействовать с контроллерами, это Weigand или Dallas Touch Memory. Как правило, сканеры штрих-кодов имеют либо USB-выход для подключения напрямую к рабочему месту (компьютеру), либо интерфейс RS232, с помощью которого сканер можно подключить к контроллерам СКУД через специальный промежуточный преобразователь интерфейсов.

В СКУД поддерживаются оба варианта подключения:

- напрямую к клиентскому месту через USB в режиме эмуляции набора с клавиатуры;
- к контроллерам через конвертер RS232 – Weigand. В качестве такого устройства может быть использован преобразователь Elsys.

1.3.1. Идентификация по бесконтактным картам

Среди идентификаторов, применяющихся в системах контроля доступа, распространение получили бесконтактные карты. Они удобны в использовании, бывают выполнены в разных формах и видах, а использование криптоалгоритмов в некоторых форматах карт существенно снижает риск их копирования и подделки.

Ниже рассмотрены основные особенности такого типа идентификаторов.

Физическое исполнение

Кроме представленных ниже, также существуют и другие исполнения идентификаторов (метки, наклейки, болты, колбы, ярлыки), однако в качестве отдельных элементов в системах контроля доступа они используются нечасто. В табл. 1.1 представлены сведения по различным идентификаторам.

Таблица 1.1. Различные современные идентификаторы и их особенности

Толстые карты (Clamshell card)	Брелки
Бесконтактные карты стандартных размеров толщиной 1,6 мм. Самые недорогие идентификаторы, дальность считывания – самая высокая из представленных (для формата EM Marine имеется исполнение повышенной дальности считывания – до 1,5 м). Для персонализации могут использоваться специальные наклейки	Брелки обычно дороже карт, при этом имеют меньшую дальность чтения. Могут иметь фирменный дизайн исполнения, однако возможность персонализации таких идентификаторов практически отсутствует. По сравнению с картами, брелки более устойчивы к физическому воздействию – меньше ломаются, могут прикрепляться к ключам
Тонкие карты (ISO card)	Браслеты
Бесконтактные карты стандартных размеров толщиной 0,76 мм. Стоимость немного выше, чем у толстых карт, однако дальность считывания ниже. Идеально подходят для персонализации посредством прямой печати на самих картах (сублимационной либо ретрансферной)	Стоимость немного выше, чем у брелков, дальность считывания примерно одинаковая. Могут закрепляться на теле человека, иметь фирменный дизайн. Из-за удобства ношения, как правило, применяются в различных фитнес-центрах, бассейнах, аквапарках и прочих спортивных учреждениях

Протокол взаимодействия (формат)

Правильный выбор формата имеет непосредственное влияние на уровень безопасности системы. Получило распространение несколько форматов, отличающихся рядом параметров, они сведены в табл. 1.2.

Таблица 1.2. Особенности различных форматов и их параметров

Формат	Внутренняя перезаписываемая память	Защита от копирования	Механизм антиколлизии	Цена	Диапазон выбора считывателей
EM Marine	нет	нет	нет	★☆☆☆☆	★★★★★
HID ProxCard II, HID ISO Prox	нет	нет	нет	★★★★☆	★★★★☆
HID iClass	да	да	да	★★★★☆	★★☆☆☆
Mifare	да	да	да	★★☆☆☆	★★★★★

Кроме перечисленных форматов, есть и другие, к примеру Legic или Indala, однако они мало распространены в России.

Возможна поддержка сразу нескольких форматов одним идентификатором. Наиболее дешевым и имеющим самый широкий диапазон выбора считывателей является формат EM Marine, однако он никак не защищен от копирования. В отличие от него, идентификаторы Mifare не намного дороже, но имеют внутреннюю перезаписываемую память, правильное использование которой в совокупности со специально настроенными считывателями позволяет организовать защищенную идентификацию.

Используемые считыватели и формат идентификаторов

При организации СКУД следует подбирать оборудование и использующиеся идентификаторы, исходя из требований, предъявляемых к безопасности системы.

Выбор считывателя обуславливается несколькими основными параметрами.

Считыватели могут поддерживать как один, так и несколько форматов одновременно. При выборе идентификатора Mifare считывателям необходимо поддерживать работу с ним в защищенном режиме.

Возможность синхронизации и дальность считывания информации

Используется для исключения влияния считывателей друг на друга при установке на близком расстоянии, к примеру при монтаже на тонких стенах.

Стандартная дальность составляет не более 10 см, но бывают считыватели повышенной дальности до 1,5 м.

Выходной интерфейс

За счет большей дальности и помехоустойчивости самым предпочтительным является Wiegand. Интерфейс связи Dallas Touch Memory (iButton) имеет более низкие характеристики, а OSDP пока редок в использовании. Встречаются считыватели с проприетарным интерфейсом, которые работают с контроллерами только этого же производителя. Для подключения к ПК и заведения карт в систему могут использоваться считыватели с USB-интерфейсом.

Особые условия эксплуатации

Считыватели могут использоваться как в помещении, так и на улице, поэтому производятся с различными значениями рабочей температуры, влагоустойчивости и вандалостойкости.

Дизайн

Количество решений, подходящих под любые требования, вариативно и практически не ограничено.

Далее представлены примеры популярных в России считывателей, обладающих различными характеристиками. Эти данные сведены в табл. 1.3.

Таблица 1.3. Сведения о считывателях с различными характеристиками

Наименование	Ironlogic CP-Z2L	Prox EM Reader	Rosslare AY-K12	Ironlogic Matrix V	Prox 13	Cinintec CN560
Формат идентификатора	EM Marine	EM Marine	EM Marine, радиобрелки	EM Marine (повышенная дальность), радиобрелки Keeloq и CAME	Mifare Classic	Mifare Classic, Mifare DESFire, Mifare Plus
Возможность синхронизации	нет	есть	нет	нет	есть	–
Дальность считывания	3–6 см	10–12 см	8 см	EM Marine – до 50 см, радиобрелки – до 10 м	4–6 см	6–8 см
Корпус, использование	обычный, в помещениях	обычный, в помещениях	влагостойкий, всепогодный, уличный	влаго- и пылезащищенный, вандалостойкий, уличный	обычный, в помещениях	обычный, в помещениях
Ориентировочная цена, руб.	750	3000	3500	13 000	4000	12 500