



Биометрическая защита: обзор технологии



УДК 004.56
ББК 28.04я73
С89



Антти Суомалайнен

С89 Биометрическая защита: обзор технологии – М.: ДМК Пресс, 2019. – 104 с.: ил.

ISBN 978-5-97060-762-6

Книга посвящена системам контроля доступа на основе биометрических и поведенческих характеристик (отпечатков пальцев, геометрии кисти руки, рисунка радужной оболочки и кровеносных сосудов сетчатки глаза, теплового изображения лица, клавиатурного почерка, динамики подписи, спектральных характеристик голоса и др.)

Подробно рассмотрены перспективные направления дистанционного определения личности в системе единой биометрической идентификации. Практически все это уже работает повсеместно, включая систему безопасности на правительственном уровне, контроль на границах и финансовую сферу. Рассмотрены риски биометрической защиты и даны полезные технические характеристики конкретных устройств и их модификаций.

Для широкого круга читателей.

УДК 004.56
ББК 28.04я73

Все права защищены. Никакая часть этой публикации не может воспроизводиться, сохраняться, копироваться и распространяться какими бы то ни было средствами – электронными, механическими, фотокопированием и любыми иными – без предварительного письменного разрешения автора или правообладателя.

Эта книга не может быть продана, выдана или иным способом распространена в любой форме, отличной от оригинального оформления, без предварительного разрешения автора или правообладателя.

Несмотря на то что содержание книги прошло тщательную подготовку, автор и издатель не несут никакой ответственности за возможный ущерб, понесённый кем-либо вследствие ошибок или неточностей в книге.

ISBN 978-5-97060-762-6

© Оформление, издание, перевод, ДМК Пресс, 2019

Содержание

https://t.me/it_boooks/2

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)	65
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



https://t.me/it_boooks/2

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.

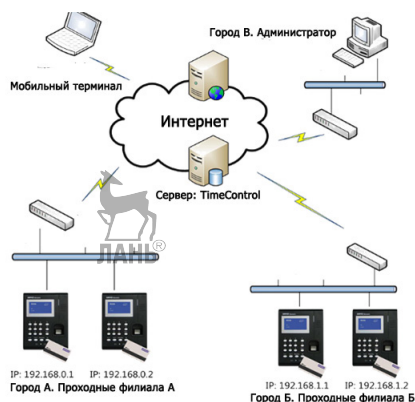


Рис. 1.2. Блок-схема контроля и администрирования в системе идентификации, действующей посредством интернета

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.

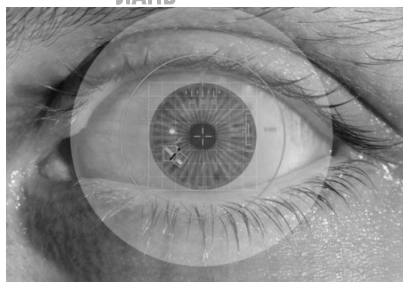


Рис. 1.3. Иллюстрация сканирования по геометрии лица человека

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.

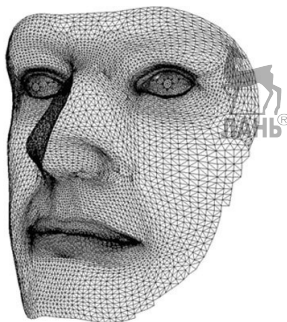


Рис. 1.4. Иллюстрация метода сканирования по оболочке и сетчатке глаза

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 СКВД 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 СКВД 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

СКУД работает с любыми произвольными считывателями уникальных идентификаторов (бесконтактных карт форматов EMarin, HID, Mifare, ключей Touch Memory, штрих-кодов), имеющих выходной формат Wiegand 26–48 бит. Этими считывателями также могут быть биометрические устройства, идентифицирующие человека по любому принципу (палец, ладонь, сетчатка, лицо) либо по совокупности признаков (биометрия плюс код карты). Главное условие для их включения в состав СКУД – формирование выходного формата Wiegand для подключения к контроллерам СКУД TSS-203/209.

Биометрические способы распознавания имеют более низкую надежность и скорость работы, нежели традиционная аутентификация по ключам или бесконтактным картам. Вероятность распознавания (для контроля доступа важен параметр FRR – False Rejection Rate – ложный отказ в доступе) имеет значение 1–2 на 100 человек (при традиционной регистрации по карте этот параметр равен 1 на 100 000).

Скорость – при большом числе сотрудников – несколько секунд, в отличие от долей секунды при карточной регистрации. Поэтому биометрию рекомендуется ставить на отдельных пунктах прохода с невысокой интенсивностью хождений, подобный жесткий контроль требуется выполнять либо на VIP-зонах, либо при доступе в особо важные помещения. Однако стремительное развитие электронных технологий приводит к тому, что появляются новые системы и информация меняется.

1.3.2. Принципы работы устройств в составе СКУД TSS2000

Схема интегрирования в СКУД очень проста: достаточно подключить такой считыватель к контроллеру TSS-203/209. После этого при успешном распознавании считыватель будет передавать на контроллер Wiegand-код. Для контроллера (и для СКУД в целом) равнозначно обычной процедуре считывания кода бесконтактной карты, по которому находится владелец карты, определяются его права доступа и принимается решение о допуске (то есть о включении реле, разблокирующего дверной замок или турникет).

Биометрические считыватели управляются собственным программным обеспечением, которое позволяет регистрировать пользователей и настраивать поведение системы (например, что важно для описываемой интеграции, настраивать формат выводимого кода). Считыватели обычно соединяются с настроечной программой посредством ЛВС, т. е. каждый из них должен быть подключен к локальной сети. Существуют считыватели, которые программируются с помощью мастер-карты, т. е. без компьютера.

Работа устройства в составе СКУД TSS2000 является полностью автономной, что позволяет системе функционировать и при выключенном сервере, и при нарушении связи по ЛВС. Наиболее распространены считыватели, которые передают Wiegand-код, прописанный при регистрации биометрических характеристик пользователя. Этот код либо считывается встроенным считывателем

карт и заносится в соответствующее поле, либо переписывается туда вручную с номера, написанного на самой карте.

В отличие от ряда других СКУД, которые предлагают программную интеграцию с биометрическими устройствами, сей код является неполным Wiegand-кодом (без битов четности и нечетности) и при пересылке на контроллер СКУД преобразуется в «правильный» Wiegand. Проверить правильность занесенного вручную кода можно с помощью утилиты из числа программ СКУД TSSKeyConvertor.exe (папка c:\ACS\utils\, тип преобразования 3, 4 или 9).

В табл. 1.4 приведен пример соответствия считывателям указанных кодов. Если на используемой карте номер не пропечатан, следует считать карту на любом считывателе СКУД и преобразовать полученный шестнадцатеричный код в соответствующий десятичный утилитой TSSKeyConvertor («Из TSS», тип преобразования 3, 4 или 9). Протестированы на возможность совместной работы со СКУД TSS2000 следующие считыватели (см. табл. 1.4).

Таблица 1.4. Считыватели, их типы, производители, функционал, которые были рассмотрены при написании книги

№ п/п	Название считывателя/системы	Производитель	Тип считывателя
1	BioEntry Plus / BioEntry W, BioEntry W2, BioStation A2	Suprema, Корея	Распознавание по отпечатку пальца
2	F11 ZKSoftware	КНР	Распознавание по отпечатку пальца
3	F710 Hanvon	КНР	3D-распознавание по лицу
4	FR020EM, FR030EMW, FR031EMW	Smartec, Китай	Распознавание по отпечатку пальца
5	FR040EM	Smartec, Китай	Распознавание по лицу, коду доступа и карте Em Marine
6	Recognition Systems HandKey II Schlage	США	По форме кисти руки
7	EyeSwipe-Nano Eyelock	США	По наружной оболочке глаза (Iris Scanner)

Подключение биометрических считывателей (терминалов) к контроллерам марки ТСС производится так же, как и любых считывателей с Wiegand-выходом. Примерные схемы подключения с комментариями приведены во второй главе нашей книги.

1.3.3. Организация работы с программой «Бюро пропусков»

Одна из проблем использования биометрических устройств в СКУД ТСС – параллельная работа в двух программных интерфейсах: регистрация сотрудников в ПО биометрической системы и в программном модуле СКУД «Бюро пропусков», см. рис. 1.6.



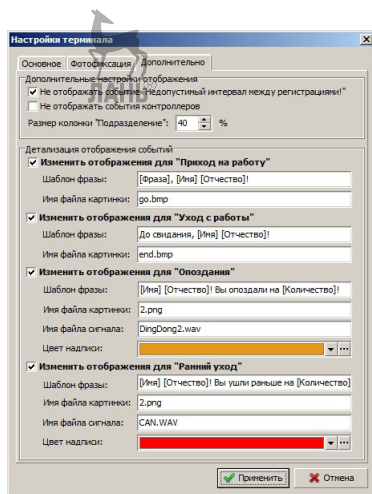


Рис. 1.6. Иллюстрация окна программы Бюро пропусков

Занесение биометрических характеристик производится с помощью ПО биометрического оборудования (например, для оборудования Smartec – это ПО Timex).

Занесение данных о сотрудниках и наделение их правами доступа, в том числе присвоение кода карты, выполняется в программе СКУД ТСС «Бюро пропусков». Для корректной работы СКУД необходимо, чтобы генерируемый биометрическим считывателем и поступающий на контроллер СКУД Wiegand-код совпадал с кодом, который посредством программы Бюро пропусков заносится в базу данных СКУД. Эта задача решается несколькими способами в зависимости от вариантов установки и использования СКУД.

Вариант 1 – биометрия как часть обычной СКУД

Если уже работающая СКУД дооснащается пунктом прохода с биометрической идентификацией, то необходимо, чтобы с биометрического считывателя поступал уже занесенный в базу СКУД код карты сотрудника. При этом не важно, будет выполняться двухфакторная идентификация (и по карте, и по пальцу) или только по биометрическому признаку (палец, лицо).

Для реализации этой задачи необходимо в биометрическом ПО в соответствующем поле карточки сотрудника занести некое число, которое при передаче на контроллер СКУД будет в точности совпадать с кодом из базы данных.

В разных ПО эти коды задаются по-разному. Поэтому невозможно дать единую схему описания кодов, мало того – для некоторых устройств передача заданного кода карты в требуемом формате в принципе невозможна.

! Внимание, пример!

К примеру, в ПО Тimeх для работы описанной схемы достаточно установить генерацию на выходе номера карты и прописать в карточке сотрудника число, пропечатанное на самой карте.

Если выбранное биометрическое устройство присылает код, отличный от базового, то возможны следующие варианты привязки его к конкретному сотруднику:

- создание новой карты на данного человека. Недостаток этого варианта – невозможность создания отчета по сотруднику, с точки зрения системы две карточки – это два разных человека;
- добавить в СКУД ТСС опциональную возможность хранения в базе нескольких кодов.

Вариант 2 – полностью биометрическая СКУД

В данной конфигурации не важно, какой код приходит от биометрического терминала. Важно лишь считать его и занести в карточку сотрудника в программе Бюро пропусков. Способы занесения будут описаны ниже. На рис. 1.7 представлена иллюстрация работы с кодами непосредственно в программе.

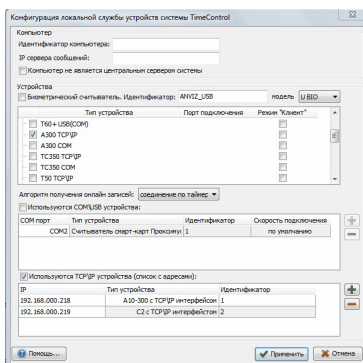


Рис. 1.7. Иллюстрация работы с кодами

В некоторых ПО возможна передача на Wiegand-выход кода, соответствующего ID сотрудника. К примеру, так, как это описано в разделе «Режимы идентификации».

Под «обычной» здесь подразумевается СКУД, построенная на считывателях кодов карт или ключей.

1.3.4. Варианты занесения кодов в ПО СКУД «Персонал»

В программе «Персонал» предусмотрены следующие способы занесения кода:

- с любого считывателя системы;
- с контрольного считывателя (подключенного к ПК БД «Персонал»);
- вручную.

Все эти способы применимы и к биометрическим считывателям. На рис. 1.8 представлена иллюстрация окна программы при работе с уровнями доступа.

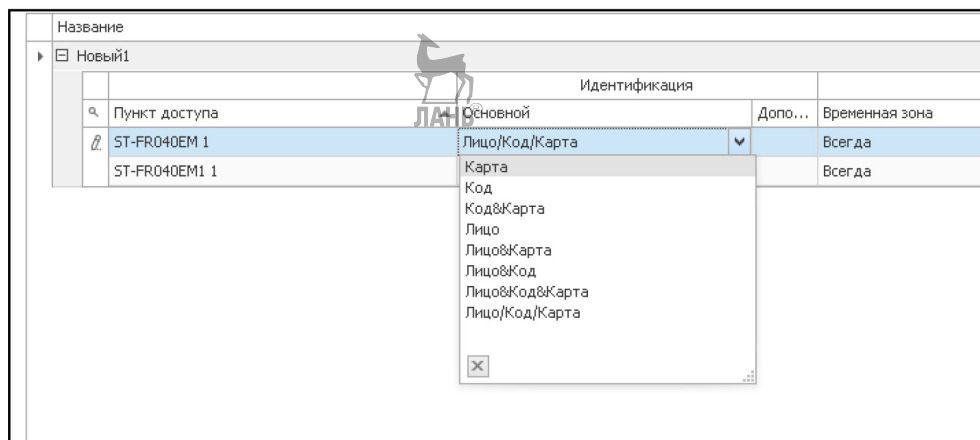


Рис. 1.8. Иллюстрация окна программы при работе с уровнями доступа

Самый простой вариант (но не самый удобный) – считать код с любого биометрического терминала. Последовательность работы здесь выглядит следующим образом.

1. Создаем карточку сотрудника в программе БД «Персонал».
2. Создаем карточку сотрудника в биометрическом ПО.
3. Регистрируем сотрудника в биометрическом ПО (лицо, палец).
4. В программе «Персонал» закрываем карточку сотрудника, следим, чтобы запись сотрудника в списке была текущей.
5. Нажимаем на панели инструментов клавишу **Читать ключ**. Загорится панель в левом верхнем углу с изображением ключа.
6. Просим сотрудника выполнить процедуру аутентификации на терминале.
7. Панелька с ключом погаснет. Код сотрудника запишется в поле **Ключ** его карточки.

Важно, чтобы никто не опередил регистрируемого сотрудника, иначе в его карточку запишется чужой код (при неопознанном коде) либо процедура сбросится (при наличии этого кода в базе).

Наиболее предпочтительный способ – занесение кода с контрольного считывателя. Для этого биометрический терминал должен быть подсоединен к ПК через интерфейсный модуль TSS GT7.5.

В этом случае достаточно проделать следующее.

1. Создаем карточку сотрудника в программе «Персонал».
2. Создаем карточку сотрудника в биометрическом ПО.
3. Регистрируем сотрудника в биометрическом ПО (лицо, палец).
4. В карточке сотрудника («Персонал») двойным кликом по полю **Ключ** активируем работу контрольного считывателя.
5. Просим сотрудника выполнить процедуру аутентификации на контрольном терминале.
6. Код сотрудника запишется в поле **Ключ** его карточки.

При ручном вводе в поле **Ключ** заносится код, прочитанный либо в программе «Дистанционный мониторинг», либо в «Консоль-мониторинг», либо в файле `SERVCONT_TRACE<ggggmmdd_ччммсс>.log`.

Можно пользоваться утилитой TSSKeyConvertor, которая перекодирует код, занесенный (или считанный) в поле **Ключ** биометрического ПО. При этом предполагается, что все установочные и монтажные работы выполнены: ПО установлено, СКУД работает, терминалы включены в ЛВС и подключены к контроллерам СКУД.

1.4. ПОПУЛЯРНЫЕ БИОМЕТРИЧЕСКИЕ СИСТЕМЫ

Стандартная связь со считывателями (терминалами) из программного обеспечения выполняется через ЛВС по IP-адресу устройства. Терминалы имеют предустановленный заводской IP-адрес (либо DHCP), указанный в документации. Чаще всего 192.168.1.n, где n – произвольное число.

Для замены адреса из рабочей группы конкретной ЛВС требуется связаться с терминалом с ПК, имеющим аналогичный адрес, т. е. 192.168.1.m. Только после этого программные средства разработчика позволят заменить адрес, к примеру, на 192.168.0.k.

Это проиллюстрировано на рис. 1.9.

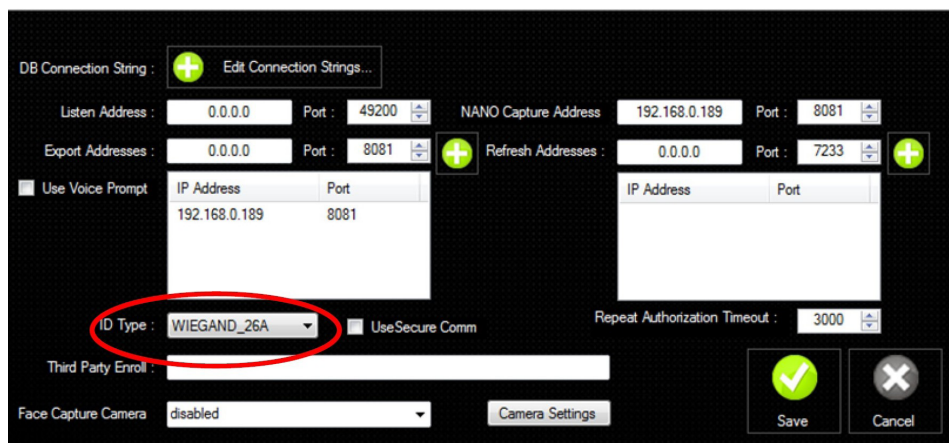


Рис. 1.9. Иллюстрация работы с утилитой в программе биометрической идентификации

Альтернативный вариант – добавление дополнительного IP-адреса в окне свойств TCP/IP-протокола (это возможно только при статическом IP-адресе). Далее приводятся лишь основные характеристики устройств и наиболее принципиальные моменты работы с ними, относящиеся в основном к настройкам корректного взаимодействия со СКУД ТСС.

Предполагается, что перед тестированием любых биометрических считывателей с выходом Wiegand считыватель уже подключен к управляющему контроллеру марки TSS. Также предполагается, что читатель внимательно изучил инструкции и руководства по работе с конкретными биометрическими устройствами и программным обеспечением к ним.



Внимание, важно!

Не рекомендуется устанавливать программное обеспечение биометрических считывателей на сервер СКУД. Основная работа в подобном ПО – это регистрация биометрических параметров сотрудников (лицо, отпечатки пальцев). Поэтому самое подходящее место для его установки – рабочее место оператора бюро пропусков. Допускается (и предполагается) его установка на том же компьютере, где установлена программа СКУД ТСС «Персонал».

1.4.1. Считыватели BioEntry Plus / BioEntry W / BioEntry W2 / BioEntry Station A2 (Suprema, Корея). Распознавание по отпечатку пальца

Любой из перечисленных считывателей сочетает дактилоскопический сенсор и встроенный считыватель карт в узком изящном корпусе. Является одним из центральных продуктов в линейке качественных высокопроизводительных биометрических устройств Suprema. Благодаря разнообразию интерфейсов (TCP/IP, RS485, Wiegand) и типов считывателей карт (Proximity (EM), HID Prox, Mifare, iClass) гибко подстраивается под логику работы вашей системы безопасности. Считыватели способны хранить в памяти от 100 до 500 000 пользователей (предполагая по два отпечатка для каждого). Это позволяет обеспечивать автономный режим работ биометрической подсистемы на крупных объектах.

Особенности работы с программой BioStar (v. 1.61)

Настройка устройства (Device)

Закладка **Wiegand**:

- в поле **FC Code** следует указать тип 18;
- в поле Input/Output выставить **Wiegand (User)**.

Настройка «Пользователя» (User) предполагает установку закладки **Details**: в поле **ID** вручную занести десятичное число, написанное на RFID-карте сотрудника.

Закладка **Отпечатки пальцев** (Fingerprints): «ввести» 1 или более пальцев пользователя для регистрации. После выполнения указанных действий на контроллер TSS придет корректный код карты, прописанный в карточке сотрудника в программе СКУД «Персонал». При наличии встроенного считывателя смарт-карт (формата Mifare) система позволяет записывать шаблон отпечатка пальца непосредственно на карту. При этом значительно повышается скорость принятия решения. Иллюстрация этого шага представлена на рис. 1.10.

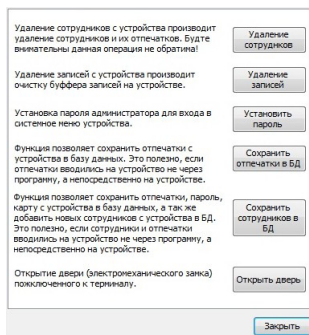


Рис. 10. Иллюстрация работы с введением кодов и «привязкой» отпечатков пальцев в программе СКУД

Особенности работы с программой BioStar (v. 2.6.2)

Настройка устройства (Device) – раздел **Расширенный** (Advanced) – панель **Wiegand**:

опцию **Код ошибки** следует включить при необходимости получения информации о попытках прохода по считывателю (неверный отпечаток, неверная карта). При этом на контроллер будет приходить код 1, что позволит впоследствии анализировать попытки несанкционированных проходов.

При выставлении опции **Режим вывода** в положение **Нормальный** считыватель будет передавать коды карты на контроллер СКУД только в случае наличия этого кода (или отпечатка) в базе считывателя.

При выставлении данной опции в положение **Bypass** считыватель будет работать в прозрачном режиме прямой передачи кода карты на контроллер СКУД. Этот режим является предпочтительным, если биометрический считыватель в основном используется как обычный считыватель карт, по пальцам же проходят лишь VIP-лица. Преимущество здесь заключается в том, что нет необходимости загружать в память считывателя коды карт.

Регистрация пользователей и задание выходного Wiegand-кода выполняются на панели **Люди** (Users) – **Добавить пользователя** (Add user) – **Личные настройки** (Credential).

После регистрации пальцев (клавиша + **Отпечаток**) необходимо задать код карты на выходе (клавиша + **Карта**).

Далее возможны два варианта занесения кода. Первый – это чтение непосредственно со встроенного считывателя карт. При этом в поле **Регистрация альтернативы** (Registration Option) должно стоять значение **Регистрация с помощью считывателя** (Register by Card reader).

! Внимание, важно!

Для чтения карты формата Em-marin в поле Тип карты (Card Type) необходимо выставить значение Серийный номер карты (CSN). Для чтения карты формата HID в поле Тип карты (Card Type) необходимо выставить значение Wiegand. В случае если карта пользователя отсутствует, можно прописать код вручную (Enter Manually). Для этого в поле ID карты следует занести код, полученный с помощью вышеупомянутой утилиты TSSKeyConvertor (тип преобразования 3, 4 или 9).

При проверке соответствия кодов (например, в тестовой программе NewTest) пользователь увидит, что со считывателя BioEntry (порт 1) приходит то же значение, что и с обычного считывателя (порт 2).

1.4.2. Биометрический считыватель F11 (ZKSoftware, Китай). Распознавание по отпечатку пальца

Устройство предназначено для использования совместно с любой системой контроля доступа, поддерживающей подключение считывателей по интерфейсу Wiegand. Выходной Wiegand-формат может произвольно конфигурироваться пользователем с длиной кода от 26 до 64 бит. Программирование и ввод пользователей осуществляются с использованием идущего в комплекте (бесплатного) программного обеспечения на русском языке с поддержкой неограниченного количества считывателей по сети Ethernet или подключаемых по RS232/485. Считыватель может использоваться и автономно, т. к. имеет реле управления замком и вход подключения кнопки выхода. Памяти для хранения событий нет.

Особенности работы

Принцип работы с ПО системы Access Control Software аналогичен предыдущему примеру. В настройках устройства (закладка **Wiegand**) выставляется выходной формат Wiegand-26, в поле **Output** – значение **ID**. В карточке пользователя в поле ID следует занести десятичный код, напечатанный на карте.

1.4.3. Биометрический считыватель F710 (Hanvon, Китай). 3D-распознавание по лицу

Биометрический сканер лица (Face Recognition) FaceId F710 для систем контроля доступа имеет как реле управления замком, так и стандартный интерфейс типа Виганд (Wiegand-26 или Wiegand-34 выбирается через меню при установке на объекте), что позволяет использовать лицевой сканер и в качестве ав-

тономной системы контроля доступа на одну дверь, и в качестве компонента системы со множеством точек прохода.

Двойной сенсор (две видеокамеры) и передовая технология распознавания лиц обеспечивают низкие FAR (ложный допуск) $< 0,0001\%$ и FRR (ложный отказ) $< 1\%$. Инфракрасная подсветка обеспечивает распознавание лиц в любых условиях освещенности, даже в полной темноте. Дружественный интерфейс: эргономичный дизайн, экран, на который проецируется изображение со встроенных видеокамер, и система подсказок – максимально облегчает идентификацию пользователей биометрической системы. Память на 500 пользователей.

Время идентификации менее 1 с. Лог событий содержит до 70 000 записей с изображениями, которые могут быть автоматически выгружены по локальной сети. Встроенный бесконтактный считыватель формата EM-марин (MIFARE под заказ) и клавиатура позволяют организовать различные правила доступа: только лицо, код и лицо, карта и лицо, только карта. Питание 12 В, при максимальном токе потребления 1 А, размеры 200×115×95 мм, рабочая температура в диапазоне 0...+40 °С.

Особенности работы считывателя

Сканер настраивается и работает автономно (возможно копирование базы на флеш-носитель). Возможна работа с ПО производителя оборудования HAMS (Hanvon Attendance Management System). Принцип работы с ней аналогичен описанным ранее.

В любых вариантах распознавания (лицо, карта, pin-код и их сочетания) передает на контроллер СКУД Wiegand-код, сформированный из facility-кода (т. н. «номер пачки»), всегда равным 100 и ассерт кода (номер пользователя), равного номеру пользователя, задаваемого при его регистрации в базе сканера. Для занесения согласования пользователя, занесенного в сканер, и пользователя СКУД TSSProfi необходимо в учетной карточке последнего (в программе «Персонал») задать соответствующий код ключа. Для этого в программе TSSKeyConvertor следует выбрать тип преобразования 3 и в верхнем поле задать число формата:

100xxxxx,

где xxxxx – номер пользователя в базе сканера, дополненный слева нулями до пяти знаков. К примеру, для пользователя с номером 1–10000001, для номера 499–1000499.

Преобразованный код из нижнего поля должен быть вставлен в поле **Ключ** карточки сотрудника.

1.4.4. Биометрический считыватель FR020EM, FR030EMW, FR031EM (Smartec, Китай). Распознавание по отпечатку пальца

Мультитехнологичное биометрическое устройство Smartec ST-FR020EM способно идентифицировать пользователей по отпечаткам пальцев и картам

доступа стандарта Em Marine. Оно может работать как в автономном режиме, так и в составе сетевых СКУД, а через Wiegand-интерфейс имеется возможность интегрировать биометрический считыватель в системы доступа любых производителей. Помимо ридеров двух типов, STFR020EM имеет встроенный контроллер и набор входов/выходов для подключения к нему внешних устройств, в том числе и дополнительного био-/RFID-считывателя. Прочный металлический корпус обеспечивает ему степень защиты IP54 и позволяет эксплуатировать считыватель в неотапливаемых помещениях при температуре от -10 до $+50$ °C и влажности до 90 %.

ST-FR020EM оснащен высокоточным оптическим сканером отпечатков пальцев и может хранить в памяти до 1500 биометрических шаблонов. К примеру, если на каждого пользователя заносить в базу по 2 шаблона, то биометрический считыватель сможет обслуживать до 750 человек. При этом время идентификации одного отпечатка пальца составляет менее 1 с. Чтобы повысить вероятность корректного распознавания отпечатков, производитель рекомендует заводить в базу шаблоны указательного, среднего или безымянного пальца пользователя.

Все рассмотренные в разделе 1.4 считыватели работают в программе Таймекс (Timex).

Особенности работы с программой Timex

Для работы используется условно-бесплатное ПО Таймекс (Timex). Основные принципы работы рассмотрим далее.

Как добавить устройство считывания (терминал)? Помните, что для успешного поиска его в ЛВС необходимо указать IP-адрес из рабочего диапазона адресов пользовательской сети. При необходимости измените его в окне настроек в правой части экрана. В группе настроек Wiegand – выход укажите **Формат** – Wiegand 26 бит, **Тип данных** – CardNo.

Затем создайте различные по статусу уровни доступа. Для работы в составе СКУД необходимо установить тип идентификации «Отпечаток & карта» (если вы хотите использовать возможность дополнительного контроля пользователя) или «Отпечаток/карта» (для идентификации только по пальцу или только по карте). Затем добавьте пользователя. Сделать это можно так.

На закладке **Идентификаторы – Карта/код** введите код карты сотрудника из БД СКУД (программа «Персонал»), преобразованный утилитой TSSKeyConversion по алгоритму 9 к десятичному виду.

Если на картах доступа нанесен номер, можно ввести его в соответствующие поля **Card code** и **Site code**. Рекомендуется далее проверить корректность преобразования кодов в программе NewTest или в модуле СКУД Дистанционный мониторинг: коды от обычного считывателя и от данного биометрического должны совпадать. Эти действия на примере проиллюстрированы на рис. 1.11 в окне программы Таймекс (Timex).

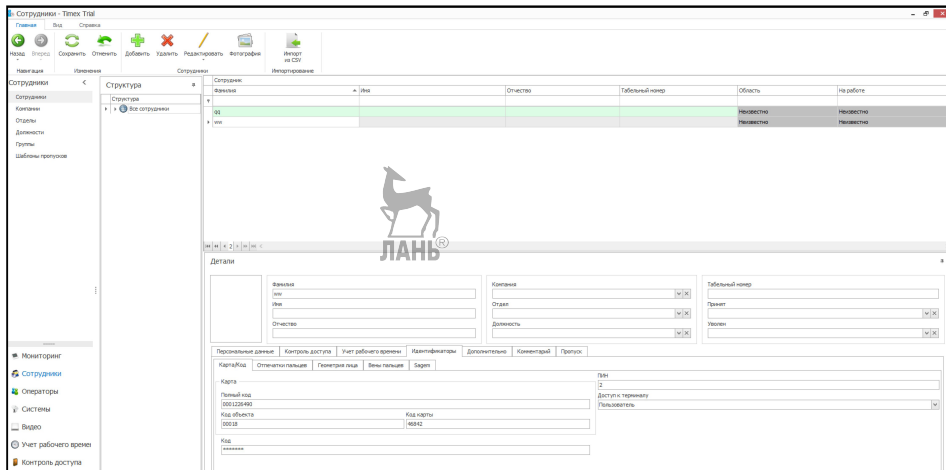


Рис. 1.11. Окно программы Таймекс (Timex)

Операция по регистрации самих отпечатков выполняется на закладке **Идентификаторы – Отпечатки пальцев**.

Программный комплекс учета рабочего времени и контроля доступа TimeControl позволяет автоматизировать процесс учета рабочего времени сотрудников, контролировать доступ через контрольно-пропускные пункты и вести учет посетителей.

Благодаря поддержке большого спектра оборудования система позволяет решать задачи как небольшого офиса, так и крупного предприятия со множеством проходных и большим количеством сотрудников. Программный комплекс позволяет автоматизировать структурированную организацию с филиальной сетью. При этом отчеты могут быть сформированы централизованно с учетом работы всех филиалов.

Учет рабочего времени и контроль доступа для филиальной сети

В системе заложена возможность гибкого разделения прав доступа сотрудников по работе с программой. Представлено более 30 отчетов по учету рабочего времени (опоздания, ранние уходы, прогулы, выполнение и невыполнение заданного графика и т. д.), контроля доступа, расчету заработной платы и т. д. При необходимости, по желанию заказчика, могут быть добавлены новые отчеты и скорректированы существующие:

- монитор событий позволяет отображать видео с IP-камеры, что дает возможность контролировать сотрудников на пропускном пункте и получать фотографию сотрудника с IP-камеры;
- использовать звуковое оповещение. Терминал позволяет использовать звуковое оповещение при регистрации прихода, ухода или ошибочной регистрации (недопустимый интервал, не найден в базе и т. д.). Файлы,

используемые для звукового оповещения, находятся в папке **Sound**. В настройках указывается только имя файла из этой папки;

- использовать ПС-спикер для оповещения. Звуковое оповещение выдается при помощи спикера в системном блоке;
- время отображения статуса регистрации. В данной настройке указывается интервал отображения статуса регистрации в секундах;
- отображать фотографию сотрудника. По умолчанию терминал отображает фотографии сотрудников, но можно отключить возможность, если не используете фотографии сотрудников и хотите уменьшить локальный трафик;
- фильтр проходных. Если в фильтре указаны проходные, то терминал будет реагировать только на события, связанные с выбранными проходными;
- фильтр подразделений. Если в фильтре указаны подразделения, то терминал будет реагировать только на события, связанные с сотрудниками выбранных подразделений;
- отображать статус рабочего интервала сотрудника вместо подразделения и проходной в списках «Приход\Уход», «По проходным». По умолчанию в списках «Приход\уход» и «По проходным» отображаются колонки «Подразделение» и «Проходная». Если данная настройка включена, то вместо этих колонок будет отображаться колонка «Статус интервала» (иллюстрация на рис. 1.6–1.7 в первой главе);
- вызывать внешний модуль при регистрации события. Если включена данная настройка и указан путь к файлу, то при регистрации событий «Приход», «Уход» и «Проход» вызывается указанный внешний модуль. В качестве параметров передаются код пользователя, дата и время события и тип прохода. Пример строки вызова с параметрами: «с:\test.exe UID=123 DATETIME=2012-01-15-14-32 INOUT=1». Значения INOUT=1 – приход 2 – уход 0 – проход;
- ручная регистрация прихода/ухода из монитора событий. Возможность нажатием кнопки в мониторе событий зафиксировать приход или уход сотрудника с работы без использования считывателей;
- сбрасывать статус регистрации после удачной регистрации. Если в мониторе событий используется ручной выбор статуса регистрации, то после фиксирования регистрации статус будет выставлен на статус по умолчанию;
- автоматический запуск терминала при старте компьютера. Запускать или нет терминал учета рабочего времени при запуске компьютера. Для сохранения настройки учетная запись в Windows Vista и Windows 7–10 должна обладать правами администратора. Поэтому запускают приложение EventMonitor с правами администратора (закладка **Совместимость** в свойствах ярлыка);

- поверх всех окон при регистрации события – если данная настройка включена, то при регистрации прихода/ухода появляется поверх всех окон, оповещающая о событии;
- отображать ФИО сокращенно. Формат отображения изменяется на сокращенный – фамилия, инициалы;
- сворачивать окно после отображения события – если данная настройка включена, то после регистрации и отображения события окно монитора событий автоматически будет свернуто.

Дополнительные настройки монитора событий Terminal Options-add

Настройки терминала «Дополнительно»

- Не отображать событие «Недопустимый интервал между регистрациями!». Событие будет игнорироваться монитором.
- Не отображать события контроллеров (настройка относится к карточным считывателям M2 Net и контроллеру Z5R WEB) – при включении этой настройки в мониторе событий не будут отображаться такие события, как «Открытие двери с кнопки», «Карта не найдена в банке ключей» и др.
- Размер колонки «Подразделение» в процентах. Процентный размер колонки «Подразделение» в мониторе событий относительно ширины всей таблицы.
- Детализация отображения событий. Уместно настроить разные звуковые сообщения, цвета сообщения и текст в зависимости от типа события. Параметр (фраза) принимает значения «Доброе утро», «Добрый день» и «Добрый вечер» в зависимости от времени суток.

Настройка локальных устройств позволяет определить устройства, с которыми работает система. После внесения изменений необходимо перезагрузить компьютер или перезапустить службу «Service for device control».

Общие правила прикладывания пальца к устройству: необходимо прикладывать к устройству не кончик пальца, не его основание, а подушечку, при этом слегка прижимая ее к стеклу сканера. Не нужно отдергивать палец сразу после того, как вы его приложили, дождитесь, пока устройство сообщит о результате операции, а затем уберите палец.

Перенос отпечатков сотрудников с одного терминала на другой

В случаях использования биометрических сетевых терминалов в филиальных сетях необходимо перенести отпечатки одного или нескольких сотрудников из одного филиала на другой. Такая необходимость возникает, когда сотрудник может работать сразу в нескольких филиалах, а отпечатки были получены на терминале его основного филиала. Подробно о переносе отпечатков в системе мы с примерами и иллюстрациями работы ПО говорили в главе 1.

Для того чтобы разослать полученные отпечатки на другие терминалы, нажмите **Сервис – Устройства – Обновить выбранных сотрудников**

на устройствах. Выберите нужных сотрудников и нажмите **Обновить**. После этого отпечатки сотрудников будут переданы на терминалы других филиалов.

Система также позволяет оперативно осуществить перенос отпечатков всех сотрудников через конфигуратор устройств. В этом случае последовательность действий оператора (администратора) должна быть такой.

1. Зайдите в конфигуратор устройств и выберите устройство, данные с которого нужно перенести на другие терминалы.
2. Нажмите кнопку **Управление** и затем **Сохранить сотрудников в БД**.



Внимание, важно!



Одного пользователя создаем с правами администратора, только после этого терминал перейдет в штатный режим работы (т. е. перестанет после каждого отключения питания требовать регистрации мастер-карты). Для занесения отпечатков пальцев пользователей используется USB-считыватель типа ST-FE700. Для занесения кодов карт используется USB-считыватель типа ST-CE011EM. Он заносит код карты непосредственно в текстовое поле, поэтому для занесения кода следует поставить курсор в поле **Полный код**.

В результате выполненных операций в СКУД будет приходить одинаковый код как от прикладывания карты, так и при распознавании пальца пользователя. Обратите внимание, что считыватель будет присылать код только при удачном распознавании.

Данный тип биометрического считывателя работает также и с внешним считывателем с интерфейсом Wiegand, форматами Emarin и HID по описанному алгоритму.

1.4.5. Биометрический считыватель FR040EM (Smartec, Китай). Распознавание лиц, кодов доступа и карт Em Marine

Биометрический считыватель ST-FR040EM марки Smartec выполняет распознавание геометрии лица, а также идентификацию пользователей по коду доступа и картам стандарта Em Marine. Устройство предназначено для работы в системах контроля доступа и учета рабочего времени, а наличие встроенного контроллера позволяет ему выполнять функции СКУД в автономном режиме. При сетевой работе для программирования ST-FR040EM используется ПО Timex, а при автономной – встроенное меню и экранная клавиатура.

Память считывателя рассчитана на хранение до 500 шаблонов, обеспечивающих распознавание лиц, а также на хранение до 10 000 кодов идентификационных карт. Благодаря наличию режима распознавания геометрии лица этот считыватель можно отнести к классу устройств, получивших название Hands Free («свободные руки») и способных считывать идентификационную информацию на значительном расстоянии. Таким образом, при проходе через точку

доступа руки сотрудника остаются свободными, что позволяет, например, беспрепятственно перенести тяжелый груз, а медперсоналу провести пациента в палату. Поэтому функция «распознавание лиц» – это в первую очередь удобство для пользователя, а при использовании совместно с другими методами идентификации – обеспечение высокой надежности системы контроля доступа в целом. На передней панели считывателя под небольшим углом к вертикальной плоскости расположены две камеры: обычная цветная и камера, фиксирующая изображение в ИК-диапазоне.

При этом распознавание лиц выполняется с помощью обработки кадров, зафиксированных ИК-камерой. Для этого в процессор устройства заложен специальный алгоритм, обеспечивающий анализ и сравнение полученного изображения с шаблонами, хранящимися в базе ST-FR040EM.

Конфигурирование системы

Все биометрические терминалы компании Smartec работают под управлением ПО Timex. Поэтому изложенное в настоящем разделе во многом относится и к другим устройствам, к примеру таким, как FR30 и 31.

Терминал ST-FR040EM благодаря дисплею очень удобен в настройках, особенно в автономном режиме. При добавлении пользователя регистрируются его карта и лицо. В рабочем режиме при прикладывании карты и распознавании лица (или только распознавании лица) на контроллер СКУД передается Wiegand-код, указанный при регистрации пользователя в программе СКУД «Бюро пропусков».

ST-FR040EM работает под управлением ПО Timex. В дальнейшем изложении предполагаю, что пользователь внимательно ознакомился с инструкцией по работе с данным ПО. Обратим внимание на ключевые моменты настройки и взаимодействия со СКУД.

Рекомендуется следующая последовательность работы со считывателем:

- включить считыватели в локальную сеть;
- на каждом считывателе задать корректный для пользовательской ЛВС IP-адрес.

Адрес устройства по умолчанию – 192.168.1.241. Изменение адреса производится выбором на экране дисплея считывателя кнопок **Меню** – **Связь** – **Связь**.

В ПО Timex в разделе **Система** – **Терминалы** последовательно добавлять устройства. Рекомендуется сразу протестировать наличие связи с устройством одноименной клавишей. Если связь отсутствует, добавленный в таблицу считыватель будет помечен красным цветом.

- Изменить значение Wiegand-выхода – **Формат** на **Wiegand-26** (для каждого терминала).
- Нажать клавишу **Сохранить**.

В разделе **Контроль доступа** – **Уровни доступа** создать список пунктов доступа. Для нашего примера с двумя терминалами это будет выглядеть так.

В разделе **Сотрудники** добавить необходимое число пользователей системы, задать им права доступа, сохраняя каждую запись в считывателе. Можно

выполнить полную загрузку списка сотрудников в терминалы в разделе **Система – Терминалы** – клавиша **Загрузить сотрудников**. В этом случае база данных всех устройств будет предварительно очищена.

На одном из терминалов выполнить последовательно регистрацию лиц всех сотрудников.

В карточке сотрудника задать имя терминала, на котором зарегистрированы шаблоны лиц, и нажать клавишу **Импортировать**. Если все предыдущие операции были выполнены корректно, его шаблон занесется в карточку, и условная фигура приобретет зеленый контур.

Нажатие клавиши **Сохранить** загрузит шаблон лица данного сотрудника во все остальные терминалы, к которым он имеет доступ.

Затем необходимо выполнить описанную операцию для каждого сотрудника.

Режимы идентификации

Терминалы FR040 позволяют идентифицировать пользователей по трем признакам: по лицу, по коду карты, по цифровому коду, набранному на панели дисплея. Возможны любые варианты использования этих признаков: по всем одновременно, по любому или только по одному из них, по их произвольному сочетанию.

Режим идентификации выбирается в разделе **Контроль доступа – Уровни доступа** из выпадающего списка для каждого пункта прохода. Независимо от выбранного режима возможно 2 варианта, передаваемых контроллеру СКУД Wiegand-кода:

- передается ID (pin) сотрудника;
- передается номер карты, заданный сотруднику.

Настройка исходного кода производится при описании свойств терминалов. Видно, что для одного считывателя выбран ID сотрудника, для второго – номер карты. При выборе ID передается уникальный код сотрудника из поля ПИН.

В случае если выбран номер карты, он обязательно должен быть введен в карточке сотрудника. Оба числа при передаче преобразуются в формат Wiegand-26, то есть к их двоичному представлению справа и слева добавляются биты, дополняющие две части кода (асерт и facility) соответственно до четного и до нечетного значения. Поэтому PIN будет приходить на контроллер СКУД в преобразованном виде: PIN (dec) ПИН (bin) Бит четности Wiegand (bin) Wiegand (hex) – так, как показано в табл. 1.5.

Таблица 1.5. Распределение кодов по ID и номеру карты

1	1	1	11	2
2	10	1	101	5
3	11	0	110	6
4	100	1	1001	9
5	101	0	1010	A
6	110	0	1100	C



Аналогичным, но более сложным образом будет преобразован и занесенный номер, напечатанный на карте. Заранее понять, какой код придет в СКУД, возможно с помощью утилиты TSSKeyConvertor.

В тестовой программе NewTest (входит в поставку СКУД TSS2000) увидим оба кода, соответствующих показанным на рисунках настройкам. Здесь показано, что на контроллер с адресом 7 на порт номер 1, к которому подключен терминал с именем ST-FR040EM, приходит код карты, заданный конкретному сотруднику.

К порту № 2 подключен терминал с именем ST-FR040EM1, который формирует код, соответствующий ID сотрудника (PIN равен 1, Wiegand-код равен 2). Эти коды приходят при любом способе идентификации данного сотрудника, в том числе и по карте.

1.4.6. Биометрический считыватель Recognition Systems – считыватель HandKey II по форме кисти руки

Биометрические считыватели HandKey распознают персонал по размеру и форме кисти руки, что обеспечивает высокий уровень безопасности в силу уникальности строения кисти руки каждого человека. Для того чтобы биометрическая система могла произвести считывание, человек должен положить ладонь руки на панель устройства, а специальные штырьки-фиксаторы помогают скорректировать ее расположение. Встроенные светодиоды на панели считывателя сигнализируют о корректности расположения ладони, что упрощает взаимодействие человека с устройством.

В отличие от обычных проксимити-считывателей, биометрические системы доступа осуществляют процедуру идентификации личности в два взаимосвязанных этапа: набор уникального идентификационного номера, состоящего из 1–10 цифр, и непосредственно сканирование кисти руки на панели считывателя. В сравнении с традиционными системами контроля доступа, использующими считыватели различных электронных карт, биометрические системы требуют только запоминания кода.



Внимание, важно!

Второй этап идентификации – сканирование кисти руки пользователя полностью исключает несанкционированный проход в охраняемые помещения по чужой или украденной карте доступа.

Двухэтапная процедура идентификации пользователя, с одной стороны, существенно повышает уровень безопасности, а с другой – позволяет практически мгновенно осуществить проверку из базы данных. Таким образом, набирая свой индивидуальный код на клавиатуре системы (или, как вариант, используя карту доступа), человек, перед тем как пройти верификацию по форме кисти руки, заранее «сообщает» биометрическому считывателю,

с каким именно шаблоном сравнивать полученные данные. Таким образом, время верификации по форме кисти руки не превышает 1 с, а общее время идентификации в системе с учетом набора кода или использования электронной карты составляет 1–5 с.

По состоянию на 2019 год биометрические считыватели HandKey II выпускаются в двух модификациях – для установки в помещении и на улице. Для защиты от несанкционированного вскрытия корпуса биометрические системы оснащены датчиками вскрытия.

Особенности работы

Для включения режима передачи Wiegand-кода на контроллер необходимо включить режим **Для эмуляции считывателя карт** (For card RDR out) в меню настроек (2 Setup Menu).

Выходной код формируется из ID, установленного каждому пользователю при регистрации ладони, и дополнительного кода (facility), равного по умолчанию 50 (можно установить любое другое значение facility-кода). К примеру, для пользователя с номером 1 будет сформирован код 5000001, который при преобразовании в Wiegand даст 2640002.

1.4.7. Биометрический считыватель компании Eyelock (США) EyeSwipe-Nano – по радужной оболочке глаза (Iris Scanner)

EyeSwipe Nano-TS является турникетным устройством идентификации и аутентификации личности в наборе решений от компании-производителя Eyelock, которое осуществляет в реальном времени считывание и анализ радужной оболочки глаза на расстоянии и в движении. Устройство было разработано для установки на турникетах или других системах с большой пропускной способностью и имеет широкий диапазон захвата для повышения простоты в использовании во время движения. EyeSwipe Nano-TS включает в себя интегрированный кардридер для поддержки старых пользователей персональных карт и обеспечивает плавный переход к использованию биометрических технологий допуска.

Как и все средства аутентификации личности Eyelock, EyeSwipe-Nano TS является нейтральным по отношению к используемым алгоритмам и может использоваться в сочетании с любыми алгоритмами или существующими базами данных.

Основные параметры:

- питание через Ethernet Plus (PoE +);
- возможность хранения 50 000 записей в памяти;
- встроенный ридер поддерживает HID Prox или MiFare и других распространенных форматов;
- регистрация и проверка соответствия самим устройством – «OnBoard»;
- сканирование радужной оболочки глаза встроенными видеокамерами;
- соединение через Wiegand, F/2/F, реле и Ethernet для простой интеграции со всеми существующими платформами.

Особенности работы

В фирменном программном обеспечении при регистрации каждого пользователя задается код карты, который будет приходить на контроллер ТСС при успешном распознавании глаза. Код задается вручную с подписанного на карте значения формата 123.56789, где 123 – код пачки (facility-код, одноименное поле), 56789 – номер карты (ID или ассерт-код, поле badge на рисунке).

Для корректной работы в окне настроек в поле **ID type** следует установить значение **Wiegand-26**.

Таблицы перекодировки

Таблица перекодировки «номер карты – Wiegand-код» (пример). Полезные сведения даны в табл. 1.6.

Таблица 1.6. Таблица перекодировки

№ п/п	Номер карты	Wiegand-код
1	0001216491	2251FD7
2	0001209214	224E6FD
3	0001227821	225785B

При преобразовании с помощью утилиты TSSKeyConvertor выбирается тип преобразования 9.

Таблица 1.7 перекодировки «номер пачки.номер карты – Wiegand-код» (пример) представлена ниже.

Таблица 1.7. Таблица перекодировки «номер пачки.номер карты – Wiegand-код»

№ п/п	Номер, нанесенный на карту	Номер карты для конвертации	Wiegand-код
1	018.36843	01836843	2251FD7
2	018.29566	01829566	224E6FD
3	018.48173	01848173	225785B
4	100.00001	10000001	2C80002
5	100.00499	10000499	2C803E6

Примечание. При преобразовании с помощью утилиты TSSKeyConvertor выбирается тип преобразования 3.



Глава 2

.....

Биометрическая идентификация: практика и возможности использования



https://t.me/it_boooks/2

Среди многообразия интегрированных систем электроники и автоматики получили популярность системы контроля доступа и идентификации человека по отпечатку пальца; их используют во всем мире для контроля доступа в закрытые помещения или хранилища. Совершенствование этих систем приводит к появлению новых моделей не только таких контроллеров, но и непосредственно электронных исполнительных устройств, управляемых контроллерами. В главе рассматриваются вопросы комплексной защиты с помощью контроллеров отпечатка пальца, а также вариативные возможности подключения к ним периферийных исполнительных устройств.

2.1. ВВЕДЕНИЕ В ТЕХНОЛОГИЮ

Технология электронного сканирования отпечатков пальцев получила новый импульс развития после разработки Atmel Grenoble (французским подразделением компании Atmel) считывателей FingerChip.

В разработке использован тепловой метод считывания отпечатков пальцев, основанный на свойствах пироэлектрических материалов преобразовывать разность температур в напряжение. Малые размеры объекта сканирования, относительно низкая стоимость, высокая точность, отсутствие специального и дорогостоящего обслуживания, низкое энергопотребление – такие качества способствовали признанию лидерства технологии в стационарных и портативных системах безопасности, включая системы контроля доступа, кассовые терминалы, общественный транспорт, компьютеры, карманные компьютеры, считыватели смарт-карт и транспортные средства. FingerChip является семейством миниатюрных датчиков для оцифровки отпечатка пальца и имеет преимущества по сравнению с другими технологиями систем безопасности.

Результирующее изображение обладает высоким качеством даже при сухости и других проблемах с отпечатком пальца. Кроме того, FingerChip является единственным самоочищающимся датчиком отпечатка пальца, т. к. на поверхности сканирования не остается скрытых отпечатков.

Разумеется, Atmel не единственная компания, результативно действующая в партнерской сети производителей комплексного оборудования (ОЕМ), компаний, занимающихся разработкой и применением датчиков отпечатка пальца, приложений, аппаратного обеспечения и микропроцессоров. В наши дни считыватели FingerChip – в составе систем обеспечения безопасности – используются везде, где требуется быстрая, надежная и точная идентификация или аутентификация личности, в том числе при идентификации групп большой численности.

2.2. Состав, конфигурация и задачи единой БИОМЕТРИЧЕСКОЙ СИСТЕМЫ

Среди специфических применений электронного сканирования отпечатков пальцев важно отметить:

- защиту компьютерных систем любой конфигурации, в том числе КПК и ККМ, смартфонов и интернет-приложений от несанкционированного доступа, использования секретной или ограниченного пользования информации;
- защиту транспортных средств и ценного имущества от несанкционированного доступа или использования;
- предотвращение хищений и подлогов при финансовых транзакциях, особенно при электронных транзакциях, включая оплату кредитными картами и оплату через интернет;
- ограничение доступа посторонних лиц к производственным площадям, складам и закрытым зонам, таким как военные и иные сооружения с особым режимом охраны;
- контроль пассажиропотока в общественном транспорте, в том числе при воздушных перевозках;
- идентификация конкретных лиц в особых условиях доступа, к примеру в пенитенциарной системе;
- подтверждение подлинности владельцев документов, в том числе водительских удостоверений, лицензий, медицинских полисов, идентификационных карт и др.

Уникальная идентификация личности, иначе аутентификация – подтверждение того, что человек является тем, кто имеет допуск, кто внесен в электронную базу как носитель оригинального отпечатка пальца. Причем электронное «дактилоскопирование» при создании банка данных, имеющих допуск к объекту (оборудованию), осуществляется сразу в полном объеме – сканируются все пальцы и даже внутренняя поверхность кисти рук. Забегая немного впе-

ред, скажу, что контроль отпечатков пальцев в системах безопасности и доступа не единственная, а комплексная часть охранных мероприятий; среди иных комплексных мер в наши дни используются контроль с помощью биометрии лица человека, сканирование зрачка (радужной оболочки и сетчатки глазного яблока), идентификация рисунка вен на ладони. Все это для того, чтобы в комплексе мер исключить ошибку идентификации, которая в ряде случаев может слишком дорого стоить. Подробно и теоретически эти вопросы были рассмотрены в первой главе книги.

Уникальность субъекта, претендующего на допуск, в биометрической электронной системе определяется посредством измерения физических и поведенческих свойств («живой образец»), получения и последующего сравнения с эталоном образца измерений в стандартном формате данных. Этот образец сравнивается с эталоном (подписью), полученным измерением тех же параметров, признан уникальным идентификатором личности и сохранен в базе данных системы безопасности. Близкое сходство образца и эталона означает подтверждение подлинности личности. Физические характеристики, по уникальности которых можно быстро идентифицировать личность, в дополнение к биометрии, – это особенности голоса, походки. К слову, идентификация по ДНК не входит в этот список, поскольку анализ ДНК длителен по времени и связан с пробой биологического материала физического тела.

Защита информации (носителей информации) и объектов (оборудования) является основной задачей комплексной системы безопасности при удостоверении личности; эта система получила название ЕБС (единой биометрической системы). Сегодня с развитием ЕБС ушли в прошлое такие методы-анахронизмы эпохи, как проверка специальных пропускных документов (паспортов, нагрудных знаков и т. п.), контроль закрытой информации (пароля, персонального кода, подписи и т. п.) или личное опознание сотрудниками службы охраны, ибо бывшие еще 3–6 лет назад традиционными подходы работали только в границах основных предъявляемых требований. В отличие от устаревших и не обеспечивающих уже адекватных ответов на вызовы времени методов, перспективная биометрия дает возможность удобного, надежного и недорогого способа аутентификации и применяется даже в неконтролируемых и удаленных местах.

Технологий электронного снятия отпечатков пальцев несколько: оптический, емкостный, радио-, нажимной, микроэлектромеханический и температурный способы. Выбрав для нашего обзора качественный продукт FingerChip, далее рассмотрим температурный способ как наиболее перспективный. А об альтернативных способах мы подробно поговорили в главе 1.

2.3. ТЕМПЕРАТУРНЫЙ МЕТОД СКАНИРОВАНИЯ

Температурный метод имеет преимущества. Среди них – высокая устойчивость к электростатическому разряду, отсутствие необходимости облучать

кончик пальца. Температурный датчик эффективен и надежен как при предельных, в том числе отрицательных, так и при комнатных температурах. Его практически невозможно обмануть искусственной имитацией пальца. Почему? Как я уже отметил выше, пирозлектрический материал преобразовывает разницу температур в напряжение. Эффект используется также в инфракрасных камерах. Температурный сканер отпечатков пальцев измеряет разницу температур между чувствительными элементами, контактирующими с выступами кожи (линиями), и элементами под впадинами, то есть неконтактирующими.

Недостатком «температурной» технологии является то, что изображение быстро исчезает. При прикладывании пальца в первый момент разница температур (следовательно, уровень сигнала) значительна, но за короткое время (менее 0,1 с) изображение исчезает, поскольку палец и датчик приходят в температурное равновесие. Это одна из причин того, что на практике иногда бывает необходимо дважды (трижды) приложить палец к считывателю. К примеру, такая ситуация весьма распространена на пограничном контроле в пунктах перехода границы (я ее знаю на примере финской границы) или при применении устройств с мобильными считывателями (пограничники в поездах, пересекающих границы).

2.4. КАК РАБОТАЕТ СИСТЕМА РЕГИСТРАЦИИ И СОПОСТАВЛЕНИЯ

Отпечаток, или набор данных, характеризующих его, известен как эталон (или зарегистрированный эталон) человека. При создании электронного банка (базы) данных регистрируются отпечатки пальцев идентифицированных лиц. При работе системы происходит сопоставление – отпечатки пальцев считываются и программным методом сравниваются с зарегистрированными отпечатками из базы данных или с некоторой их частью (как минимум с единственным зарегистрированным отпечатком).

Как при регистрации, так и при сопоставлении данные обрабатываются в одинаковой последовательности, описанной ниже применительно к FingerChip.

Функционал считывателей FingerChip основан на распознавании узора линий и выделении деталей на подушечке пальца, ибо отпечаток характеризуется фрагментами, такими как дуги, спирали, завитки, разветвлениями, дельтами (Y-образными соединениями) и окончаниями выступов. В рисунке от 30 до 40 мелких деталей. Они характеризуются своим положением (координатами), типом (разветвление, дельта или окончание) и ориентацией (см. рис. 2.1).



Рис. 2.1. Иллюстрация функционала биометрических считывателей FingerChip

Устройства сочетают дактилоскопический сенсор и встроенный считыватель карт. Благодаря разнообразию интерфейсов (TCP/IP, RS485, Wiegand) и типов считывателей карт (Proximity (EM), HID Prox, Mifare, iClass) гибко подстраивается под логику работы системы безопасности.

Получение отпечатка в электронном виде – посредством биометрического считывателя завершается создание растрового изображения с требуемым разрешением всего отпечатка или его части. Метод FingerChip отличается последовательностью горизонтальных кадров размером 8×220 точек при разрешении 4 бита на точку, которые все вместе дают изображение отпечатка. При условии что палец перемещался по датчику с приемлемой скоростью, элементы изображения, повторяющиеся на смежных кадрах, дают возможность реконструировать изображение отпечатка в целом. Эта операция выполняется программным методом, в частности в составе комплекта FingerChip. Реконструированное изображение имеет глубину до 16 бит, получаемую при обработке кадров.

Atmel и FingerChip создали приложения для адаптации датчика отпечатка пальца для конкретных конфигураций оборудования. В табл. 1 представлена информация о наиболее популярных и востребованных биометрических температурных датчиках семейства FingerChip.

Таблица 2.1. Температурный датчик отпечатка пальца семейства FingerChip

AT77C101B	Температурный датчик отпечатка пальца с чувствительной областью 0.4×14 мм ($0.02'' \times 0.55''$) и цифровым выходом (встроенный АЦП)
AT77C102B	Температурный датчик отпечатка пальца из семейства FingerChip с размерами чувствительной поверхности 0.4×14 мм и цифровым выходом (встроенный АЦП)
AT77C104B	Температурный датчик отпечатка пальца из семейства FingerChip с функциями органа управления и интерфейсом SPI
AT77C105A	Температурный датчик отпечатка пальца из семейства FingerChip с функциями органа управления и расширенным диапазоном питания ввода-вывода (1,8–3,3 В)
AT77SM0101BCB02VKE	Модуль биометрического датчика отпечатка пальца FingerChip

В дополнение к сказанному необходимо добавить, что имеется возможность объединения FingerChip для мобильных приложений: самое низкое потребление питания (4,5 мА макс.), очень маленькая зона сканирования, даже если встраивать в трубку телефона, высоконадежное защитное покрытие, цвет которого можно выбрать, чтобы соответствовать новым разработкам внешнего вида трубок.

Да, отпечаток состоит из гребешков и бороздок кожи, при проведении пальца по датчику отпечаток последовательно передается по пикселям. Когда палец проходит над сканирующей областью FingerChip, возникают одна за другой разницы температуры между элементом под гребешком, т. е. контактирующим, и элементом под бороздкой, т. е. неконтактирующим.

Эти разницы температур вызывают разницу электрических зарядов в пирoeлектрическом материале датчика, выполненном по КМОП-технологии, бла-

годаря чему возможно произвести идентификацию. Черные и белые пиксели с выводов датчика – как достоверная копия отпечатка пальца.

Преимущества технологии: высококачественное изображение, самые широкие рабочие температуры (от -40 до $+85$ °C), самая низкая потребляемая мощность на рынке и способности усилить датчик, полностью защищенный полупроводник с очень прочным покрытием.

FingerChip Atmel интегрирован в первый массовый биометрический КПК, а именно в серию iPAQ 5450 и затем iPAQ 5550. Таким образом фирма HP укрепила биометрические функциональные возможности на некоторых из своих известных карманных компьютерах iPAQ.

В выпущенный Pocket PC hx2750 интегрирован датчик AT77C104B фирмы Atmel с SPI-интерфейсом. Разрешая достоверную идентификацию пользователя, FingerChip интегрирован в целый программный пакет, который включает алгоритм идентификации Cogent Systems, подстановку пароля Credant Technologies и набор программного обеспечения для кодирования данных.

FingerChip фирмы Atmel дает возможность защитным функциям ProtectTools новых HP iPAQ hx2750 достигнуть новых перспектив.

2.5. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ИНТЕГРАЦИИ СО СМАРТ-КАРТАМИ

Даже в смарт-карту может быть загружен эталон отпечатка пальца ее владельца. Далее поговорим о том, как биометрическая аутентификация может быть интегрирована в систему безопасности смарт-карт и транзакций банковских инструментов. Такая процедура известна как «совпадение с картой». Основное отличие комплексного метода – в том, что зашифрованный эталон никогда не передается за пределы карты, а образец передается в карту для сравнения только в зашифрованном виде.

При использовании смарт-карты владелец (кстати, в дополнение к PIN-коду) предоставляет образец отпечатка пальца считывателю смарт-карты для аутентификации. Интегральные схемы используются в смарт-карте и в считывателе в виде ASSP или стандартных продуктов.

Смарт-карта содержит защищенный 8-битный микроконтроллер AT90SC со встроенной флеш-памятью. В дополнение к программам и данным «память» содержит зашифрованный эталон отпечатка пальца, записанного при регистрации владельца смарт-карты. Считыватель смарт-карт построен на основе микроконтроллера AT91 ARM с флеш-памятью AT49BV для хранения программ и данных. Связь между AT90SC и AT91 осуществляется через интерфейс промышленного стандарта ISO 7816. Получение и оцифровка изображения отпечатка пальца осуществляются схемой AT77C101B FingerChip.

Последовательность действий в этом случае показана на рис. 2.2.

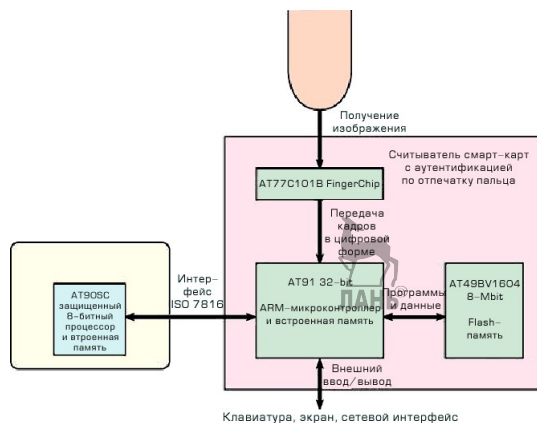


Рис. 2.2. Блок-схема взаимодействия функций считывателя

При начале операции аутентификации AT91 в считывателе активирует AT90SC в смарт-карте, и выполняется обычный ввод и проверка PIN-кода. Это осуществляется через интерфейс ISO 7816. Таким образом обеспечивается начальный уровень проверки того, что претендент на допуск является тем, за кого себя выдает.

Затем отпечаток пальца человека, заявляющего себя как владельца смарт-карты, считывается схемой FingerChip, оцифровывается и передается в микроконтроллер AT91. Контроллер AT91 реконструирует изображение из последовательности кадров и извлекает из него образец. Затем он шифрует образец и передает его в AT90SC в смарт-карте. Контроллер AT90SC сравнивает зашифрованный образец, полученный от считывателя, с зашифрованным эталоном, хранящимся в его защищенной памяти. Если уровень соответствия превышает пороговое значение, он посылает подтверждение в AT91 считывателя. Личность считается удостоверенной, и разрешается соответствующая транзакция.



Внимание, важно!

Среди множества достоинств единой биометрической системы – малое количество элементов, которое приводит к снижению размеров, энергопотребления и стоимости. Схемы взаимосвязи контроллеров AT91 и AT49BV могут быть объединены в один модуль для снижения размеров и стоимости. Важно, что использование ASSP и стандартных продуктов снижает единовременные затраты на проектирование и разработку. Флеш-память в смарт-карте и считывателе допускает модернизацию программного обеспечения. Порог отказа/допуска может быть выставлен программным методом – в зависимости от требований безопасности, а задача получения и проверки второго отпечатка в сомнительных случаях решается введением дополнительного блока в программу

или введением новых элементов комплексного контроля. Отличие ЕБС на основе рассмотренных методов в том, что в считывателе не хранятся постоянно образцы или эталоны, зашифрованный эталон никогда не передается за пределы смарт-карты, а образцы стираются из памяти сразу после аутентификации. Нет необходимости иметь базу данных зарегистрированных эталонов, что снижает возможности внедрения потенциальных злоумышленников.



2.6. КОНФИГУРИРОВАНИЕ СЧИТЫВАТЕЛЕЙ В СИСТЕМЕ ЕБС

Все биометрические терминалы одной компании работают под управлением единого ПО. К примеру, терминалы Smartec работают под управлением ПО Timex. Иллюстрация считывателя представлена на рис. 2.3.



Рис. 2.3. Считыватель смарт-карт Smartec с аутентификацией по отпечатку пальца

Терминал ST-FR040EM благодаря дисплею очень удобен в настройках, в том числе в автономном режиме. При добавлении пользователя регистрируются его карта и лицо. В рабочем режиме при прикладывании карты и распознавании лица (или только распознавании лица) на контроллер СКУД передается Wiegand-код, указанный при регистрации пользователя в программе СКУД Бюро пропусков.

ST-FR040EM работает под управлением ПО Timex.

Рекомендуется следующая последовательность работы со считывателем.

1. Включить считыватели в локальную сеть.
2. На каждом считывателе задать корректный для ЛВС IP-адрес. Адрес устройства по умолчанию – 192.168.1.241. Изменение адреса производится выбором на экране дисплея считывателя кнопок **Меню – Связь – Связь**.

В ПО Timex в разделе **Система – Терминалы** последовательно добавить устройства. Рекомендуется сразу протестировать наличие связи с устройством одноименной клавишей. Если связь отсутствует, добавленный в таблицу считыватель будет помечен красным цветом.

2.7. Риски и ошибки идентификации

Отпечаток пальца – это структура, состоящая из выступов, содержащих поры, и впадин между ними. Непосредственно под этой структурой располагается структура кровеносных сосудов. Индивидуальная форма отпечатка пальца связана с электрическими и температурными характеристиками кожи. Для получения изображений отпечатков пальцев могут быть использованы свет, тепло и электрическая емкость (их сочетание). Отпечаток пальца человека формируется в эмбриональном состоянии, он не меняется с возрастом и восстанавливается в прежнем виде после повреждения. При достижении взрослого возраста отпечаток пальца сохраняет свой постоянный размер. Даже у близнецов нет одинаковых отпечатков пальцев.

При идентификации шахтеров, музыкантов, лиц иных профессий, где возможна деформация кожного покрова и рисунка подушечки пальца из-за внешних воздействий на пальцы, могут возникать сложности для систем распознавания отпечатков пальцев.

Итак, набор характеристик мелких деталей служит эталоном отпечатка пальца. Такие характеристики измеряются достаточно точно, поэтому вероятность того, что для двух разных отпечатков составятся одинаковые эталоны, крайне мала.

Однако существуют риски невозможности идентификации по отпечатку пальца (осужденный в местах заключения «стирает» палец о стену, у временно нетрудоспособного кисть в гипсе, или отсутствие рук у лиц с ограниченными возможностями здоровья). Но эти случаи скорее частные, чем типичные, и для решения конкретной задачи обеспечения безопасности в подобных ситуациях может применяться индивидуальный контроль доступа или контроль на основе комплекса идентификационных мероприятий (по другим, кроме биометрии, элементам).

Биометрическое изображение может быть получено, как минимум, двумя способами: объект (палец) может выступать «неподвижным» или «сканируемым».

В первом способе используют неподвижный чувствительный элемент (считыватель биометрических данных) размером с отпечаток и прикладывают

к нему палец на время, необходимое для электронного сканирования изображения. Достоинство этого способа – в том, что изображение целиком и комплексно передается для анализа базы одновременно.

Недостаток метода – в том, что требуется чувствительный элемент относительно большого размера, следовательно, и более дорогой, а также то, что на поверхности считывателя остается незаметный отпечаток пальца, мешающий в дальнейшем идентификации других лиц, претендующих на допуск.

Мы понимаем, что регистрация заключается в получении и сохранении эталонных вариантов отпечатков пальцев идентифицированного человека. Чтобы максимально исключить возможные риски некорректной идентификации (намеренной замены отпечатка), регистрацию проводят в специальных помещениях, исключающих получение эталонного отпечатка у подставного лица или изменения каким-либо образом полученных эталонных данных.

2.8. ПРАКТИЧЕСКАЯ РАБОТА И ПЕРСПЕКТИВЫ

В качестве сопутствующих примеров оборудования остановлюсь на считывателе отпечатков пальцев Bioki и считывателе смарт-карт с проверкой по отпечатку пальца Biothentic. Считыватель отпечатков пальцев Bioki (см. рис. 2.4) от IDS обеспечивает защищенный доступ к ПК.



Рис. 2.4. Считыватель отпечатков пальцев Bioki (IDS)

Работает как периферийное устройство, подключенное к порту USB3.0. Используя интегральную схему FingerChip и биометрическое программное обеспечение IDS, устройство оперативно считывает отпечатки пальцев, может регистрировать, анализировать и допускать на объекты авторизованных пользователей.

Биометрический считыватель FR020EM, FR030EMW, FR031EM (Smartec, Китай) осуществляет распознавание по отпечатку пальца и картам доступа стандарта Em Marine. Внешний вид устройства представлен на рис. 2.5.



Рис. 2.5. Считыватель отпечатков пальцев FingerChip

Устройство может работать как в автономном режиме, так и в составе сетевых СКУД (система кодового удаленного доступа), а через Wiegand-интерфейс имеется возможность интегрировать биометрический считыватель в системы доступа любых производителей. Помимо ридеров двух типов, STFR020EM имеет встроенный контроллер и набор входов/выходов для подключения к нему внешних устройств, в том числе и дополнительного био-/RFID-считывателя. Прочный металлический корпус обеспечивает ему степень защиты IP54 и позволяет эксплуатировать считыватель в неотапливаемых помещениях при температуре от -10 до $+50$ °C и влажности до 90 %.

ST-FR020EM оснащен высокоточным оптическим сканером отпечатков пальцев и хранит в памяти до 1500 биометрических шаблонов.

К примеру, если на каждого пользователя заносить в базу по 2 шаблона, такой биометрический считыватель сможет обслуживать до 750 человек. Другие устройства могут обслуживать до 100 тыс. отпечатков. При этом время идентификации одного отпечатка пальца составляет менее 1 с. Чтобы повысить вероятность корректного распознавания отпечатков, производитель рекомендует заводить в базу шаблоны указательного, среднего или безымянного пальца пользователя.

Оперативные службы на примере пограничников, осуществляющих свои функции в пунктах пограничного пропуска граждан (в частности, в мобильных пунктах – в поезде Санкт-Петербург–Хельсинки, где пограничный и таможенный контроль пассажиров с российской стороны осуществляется в движении на перегоне между станциями Санкт-Петербург – Финляндский – Выборг, а с финской стороны – на перегоне между станциями на финской территории Вайниккала и Коуволла), снабжены «карманными» компьютерами.

Такой КПК представляет собой электронное устройство IPAQR h5400 от HPR (см. рис. 2.6) – мультимедийный карманный компьютер со встроенным устройством FingerChip для доступа в систему по результатам биометрической аутентификации. Он освобождает владельца от необходимости помнить логины и пароли и делает практически невозможным использование украденного компьютера посторонними лицами.



Рис. 2.6. Мобильный КПК HP IPAQR h5400 с FingerChip для биометрической аутентификации

Среди прочих особенностей модели h5400 – беспроводная сеть LAN на контроллере AT76C503A IEEE802.11b/USB фирмы Atmel.

Ключевым элементом ЕБС является электронный контроллер небольшого размера, считывающий данные с рисунка на пальце. Идентифицировав его носителя, контроллер передает сигнал на аналитический блок (рис. 2.6), который конфигуративно может быть совмещен с исполнительным устройством – электромагнитным замком или электронной инвертированной защелкой.

Контроллер (в ЕБС) является «шлюзом», с помощью которого цифровые данные вводятся в контроллеры на базе ПК и интегрированные системы. Контроллеры выпускаются нескольких видов: встраиваемые, с клеммником для подключения, клавиатурные (с разъемами USB/microUSB), контроллеры в модулях PCMCIA в ПК и КПК и др.

2.9. ПРАКТИЧЕСКИЕ ПРИМЕРЫ КОММУТИРУЕМЫХ СОЕДИНЕНИЙ

Пример подключения оборудования двухридерной двери с биометрическим считывателем ST-FR040EM и электромагнитным замком со встроенным управлением (нормально запитанным исполнительным устройством) к главной плате контроллеров TSS-209–2WNE/p и TSS-203–2W/p представлен на рис. 2.7.

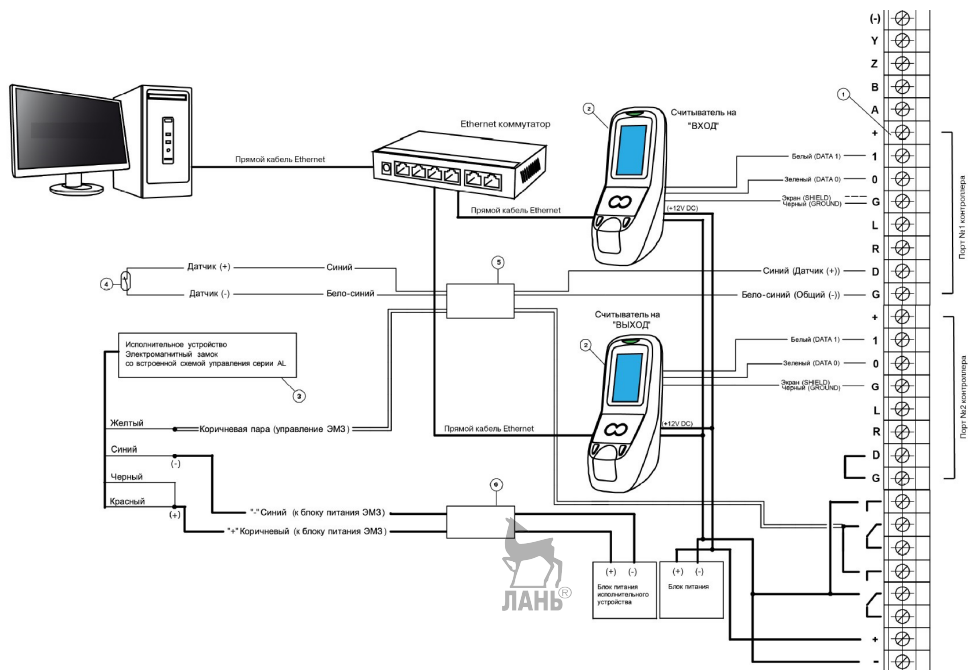


Рис. 2.7. Схема управления с биометрическим считывателем ST-FR040EM и электромагнитным замком

На схеме:

- 1) порт для подключения оборудования пункта прохода – на «вход» и «выход» (используются два порта контроллера);
- 2) биометрический считыватель (терминал) на «вход» и «выход» соответственно;
- 3) нормально запитанное исполнительное устройство (электромагнитный замок) со встроенным управлением, ЭМЗ серии «Алеко» или серии ML (подключение замка к СКУД производится в соответствии с рекомендациями в паспорте на соответствующий электромагнитный замок);
- 4) нормально замкнутый датчик двери (геркон);
- 5) кабель к датчику двери (геркону) и управлению исполнительным устройством (например, неэкранированный кабель типа витая пара UTP или КСПВ 4×0,4);
- 6) кабель питания электромагнитного замка (к примеру, кабель типа ШВВП 2×0,5; 2×0,75 или ПВС 2×0,75).

Пример подключения биометрического считывателя ST-FR040EM к контроллерам TSS-209 и TSS-203 при использовании экранированного кабеля типа «витая пара» (FTP, STP) представлен на рис. 2.8.

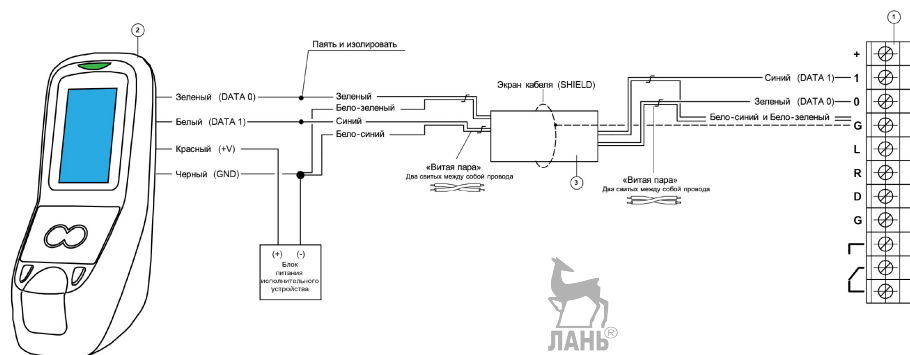


Рис. 2.8. Пример подключения биометрического считывателя ST-FR040EM

На схеме соединений (рис. 8) указаны:

- 1) порт для подключения оборудования пункта;
- 2) биометрический считыватель (терминал);
- 3) экранированный кабель «витая пара» (FTP, STP) для подключения считывателя.

На практике при предоставлении доступа в помещение электронный контроллер снимает питание с замка, обесточивая его, и дверь может быть без затруднений открыта усилием мускульной силы человека.

В качестве «запорного» устройства для бесконтактных электронных контроллеров можно использовать не только электромагнитный замок (к примеру, AL150/AL300, ЭМЗ-4, ML-100 и др.), но и любую активную нагрузку, рассчитанную на соответствующее напряжение питания.

Как правило, все устройства в рассматриваемом сегменте адаптированы для питания в диапазоне 10–16 В постоянного тока. К примеру, система кодового доступа, реализованная на модулях IronLogic, рассчитана на подключение в качестве нагрузки исполнительного устройства, питающегося постоянным напряжением $12\text{ В} \pm 20\%$ и током потребления до 5 А.

2.10. ПРАКТИЧЕСКИЙ ПРИМЕР

2.10.1. Установка и эксплуатация устройства HN-F1ME со считывателем отпечатков пальцев и считывателем карт Proximity

СКУД HN-F1ME обеспечивает управление контролем доступа по отпечаткам пальцев и картам EM RFID. Использование высокочувствительных электронных компонентов, оригинальных технологических решений обеспечивает высокую точность и надежность устройства, а также простую установку и его про-

граммирование с помощью отпечатка пальца «менеджера», мастер-карты EM 125 кГц либо с дистанционного ИК-пульта управления.

Практические возможности устройства определяются как:

- металлический, антивандальный корпус;
- поддержка до 3000 пользователей, включая 1000 отпечатков пальцев и 2000 RFID-карт доступа;
- Weigand-26 вход и выход;
- возможность подключения к другим контроллерам как дополнительного считывателя;
- ИК-пульт управления и мастер карты для программирования;
- светодиодная индикация режимов работы.

Практическая установка и монтаж

Внешний вид устройства представлен на рис. 2.9.



Рис. 2.9. Внешний вид считывателя отпечатков пальцев HN-F1ME

Установка и монтаж производятся в такой последовательности:

- снимите заднюю крышку устройства, используя специальную отвертку, входящую в комплект поставки;
- высверлите в стене 4 отверстия для шурупов и 1 отверстие для вывода кабелей;
- установите заднюю крышку устройства на стену, используя 4 самореза с потайной головкой;
- протяните кабели через ранее подготовленное отверстие под него;
- установите устройство на заднюю крышку.

В табл. 2.2 представлены сведения о назначении проводников шлейфа для подключения СКУД.

Таблица 2.2. Назначение проводов шлейфа для подключения СКУД

№ п/п	Цвет	Функция	Описание
1	Зеленый	D0	Порт Wiegand D0
2	Белый	D1	Порт Wiegand D1
3	Серый	Alarm-	«Минус» выхода тревоги
4	Желтый	Open	Кнопка запроса на выход
5	Коричневый	D_IN	Дверной контакт
6	Красный	+12V	«Плюс» питания от стабилизированного источника питания
7	Черный	GND	Общий провод («минус» питания)
8	Голубой	GND	Общий провод кнопки запроса на выход и дверного контакта
9	Пурпурный	L-	«Минус» электрозамка
10	Оранжевый	L+/Alarm+	«Плюс» замка / «плюс» выхода тревоги

Схема подключения

Схема подключения СКУД с обычным источником питания представлена на рис. 2.10.

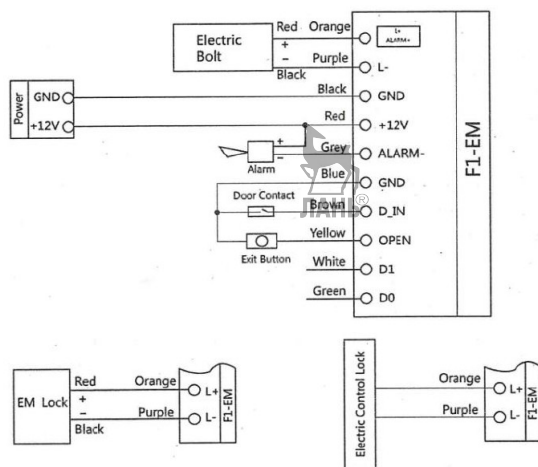


Рис. 2.10. Схема подключения СКУД

Схема подключения СКУД со специальным источником питания изображена на рис. 2.11.

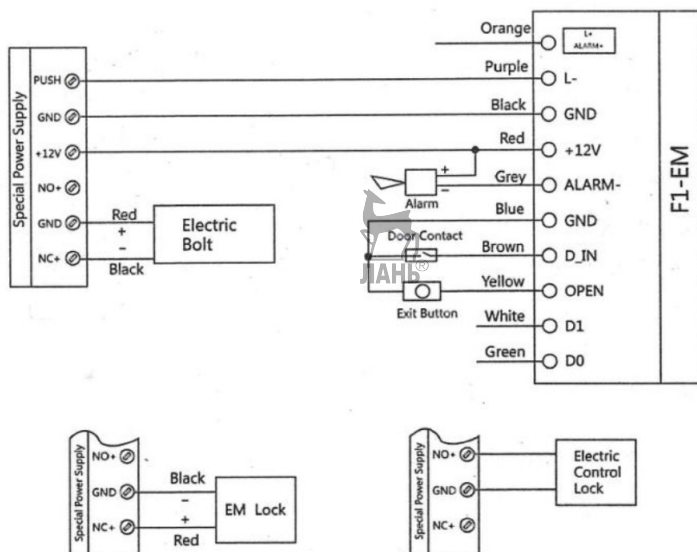


Рис. 2.11. Схема подключения СКУД со специальным источником питания

Функционал устройства в режиме «Мастер»

Существуют 3 способа добавления и удаления пользователей: с помощью мастер-карты, с помощью пульта ДУ, с помощью мастер-пальца.

Действия с помощью мастер-карты предполагают добавление отпечатков пальцев (пользователей) и добавление карт пользователей. Разберем последовательно оба этих случая.

Для добавления по мастер-карте приложите палец пользователя «1» дважды и затем приложите палец пользователя 2 дважды, нажмите на кнопку **Мастер-карта добавления**.

! Внимание, важно!

При добавлении отпечатка пальца пользователя необходимо введение отпечатка дважды, в это время индикатор включает красный, затем зеленый цвет, что означает успешную регистрацию отпечатка. При удалении отпечатка пользователя палец подносится 1 раз.

При добавлении карт пользователей нажмите кнопку **Мастер-карта добавления**, приложите **Карта 1** пользователя и затем **Карта 2** пользователя. Затем снова нажмите **Мастер-карта добавления**.

! Внимание, важно!

Номера отпечатков пальцев пользователей могут быть в диапазоне 3–1000. Номера карт пользователей занимают диапазон 1001–3000. При добавлении отпечатков пальцев или карт в режиме мастер-карты номера пользователей генерируются автоматически для диапазонов 3–1000 и 1001–3000. Номера пользователей 1 и 2 зарезервированы за мастер-пальцами.

Удаление пользователей

Последовательность действий такова: **Мастер-карта удаления**, затем **Карта пользователя** или (вариативно) приложите палец 1 раз. В заключение процедуры нажимаем кнопку **Мастер-карта удаления**.

! Внимание, важно!

Для удаления более чем одной карты или отпечатка пальца просто подносите карты или пальцы к считывателю последовательно. При удалении отпечатка пальца пользователя палец подносится один раз.

Действия с помощью пульта ДУ и добавление пользователей

Вход в режим программирования осуществляется с помощью комбинации:

* Мастер-код # Заводская установка Мастер-кода: 888888

Примечание. Все шаги, описанные ниже, производятся после входа в режим программирования.

Добавление пользователей осуществляется в следующей последовательности.

А. Автогенерация номеров пользователей

Для добавления отпечатка пальца (пользователя) 1 приложите палец дважды, затем нажмите «#» (для добавления более одного отпечатка пальца прикладывайте пальцы последовательно).

Для добавления карты пользователя 1 поднесите карту и затем нажмите «#» или вместо карты пользователя 1 введите номер карты (8 цифр) и потом «#» (для добавления более одной карты просто подносите карты последовательно).

Примечание. При добавлении карт пользователей заносится только номер карты, но не сама карта. Номер карты из 8 цифр напечатан на карте.

Аналогично, при удалении карт достаточно ввести номер карты для удаления, нет необходимости подносить карту, если она утеряна.

Б. Ручной ввод номеров пользователей

Для добавления отпечатка пальца (пользователя):

1 Номер пользователя # приложите палец # (номер пользователя для отпечатка пальца может быть любым в диапазоне 3–1000, для каждого пользователя должен быть свой уникальный номер).

Для добавления отпечатков пальцев (пользователей) последовательно:

1 3 # приложите палец первого пользователя 4 # приложите палец второго пользователя ... N # приложите палец пользователя N #.

Для добавления карты пользователя: 1 Номер пользователя # поднесите карту # или 1 Номер пользователя # введите номер карты (8 цифр) # (номер пользователя карт может быть любым в диапазоне 1001–3000, для каждого пользователя должен быть свой уникальный номер).

Для добавления карт пользователей последовательно:

1 1001 # поднесите карту пользователя 1 1002 # поднесите карту пользователя 2 # ... N # поднесите карту пользователя N # или 1 1001 # введите номер карты пользователя 1 1002 # введите номер карты пользователя 2 ... N # введите номер карты пользователя N #.

Удаление пользователей с помощью пальца и по ID

Удаление отпечатка пальца пользователя: пользователь – приложите палец один раз – кнопка «#».

Для удаления карты пользователя: поднесите карту, затем нажмите «#» или введите номер карты и завершите нажатием «#».

Для удаления более чем одной карты или отпечатка пальца просто поднесите карты или пальцы к считывателю последовательно.

Удаление пользователей по номеру – используйте рекомендацию: ввод ID пользователя и затем кнопка «#».

Примечание. При удалении пользователей удаляется пользователь по его номеру, и не нужно прикладывать его палец или подносить его карту. Это удобно, если пользователь отсутствует или карта потеряна.

Сохранение изменений и выход из режима программирования

Действия с помощью мастер-пальца осуществляются через вход в режим программирования по следующему алгоритму:

* «Мастер-код» # «Заводская установка Мастер-кода»: 888888

Примечание. Шаги, описанные ниже, производятся после входа в режим программирования.

Добавление мастер-пальца

Приложите мастер-палец первого пользователя дважды, нажмите #, приложите мастер-палец второго пользователя дважды.

Пользователь 1: мастер-палец 1 – для добавления пользователей.

Пользователь 2: мастер-палец 2 – для удаления пользователей.

Добавление отпечатков пальцев: нажмите «Мастер-палец» добавления, затем приложите палец пользователя дважды и снова нажмите «Мастер-палец добавления».

Добавление карт: «Мастер-палец добавления» – поднесите карту пользователя – «Мастер-палец добавления».

Добавление пользователей последовательно

Добавление отпечатков пальцев осуществляется в следующей последовательности: нажмите «Мастер-палец добавления» – приложите палец первого пользователя – приложите палец второго пользователя и т. д. (если пользователей несколько) – приложите палец пользователя N и завершите нажатием кнопки «Мастер-палец добавления».

Добавление карт: кнопка «Мастер-палец добавления» – поднесите карту пользователя 1, поднесите карту пользователя 2, поднесите карту пользователя N и завершите нажатием «Мастер-палец добавления».

Удаление отпечатков пальцев и карт

«Мастер-палец удаления» приложите палец пользователя 1 – приложите палец пользователя 2 ... приложите палец пользователя N – «Мастер-палец удаления».

«Мастер-палец удаления» поднесите карту пользователя 1 – поднесите карту пользователя 2 ... поднесите карту пользователя N – «Мастер-палец удаления».

Удаление всех пользователей

Последовательно нажать: *Мастер код # 20000 # *



Внимание, важно!

Эта операция удаляет все отпечатки пальцев и все карты, включая мастер-пальцы, но оставляет мастер-карты. Перед удалением всех пользователей предлагается убедиться в неактуальности всех удаляемых данных.

Установка группового кода

Установка группового кода осуществляется последовательно: 30–255 #

Это действие может потребоваться, если контроллер TS-RDR-Bio1 используется как считыватель с выходом Wiegand-26 и подключается к стороннему контроллеру.

Установка типа замка и времени переключения реле двери

Замок открывается при подаче питания (электромеханический замок), и время его открывания связано с последовательностью: * Мастер-код # 40–99 #

Замок открывается при снятии питания (электромагнитный замок), и время его открывания связано с последовательностью: * Мастер-код # 50–99 #

Примечание. Заводская установка – замок, открывающийся при снятии питания, время реле 5 с.

Установка контроля состояния двери

* Мастер-код # 60 # – отключение контроля состояния двери (заводская установка) 61 # – включение контроля состояния двери.

Если контроль состояния двери включен:

а) если дверь открыта по команде контроллера, но не закрыта в течение 1 мин, включается встроенный зуммер (выключается через 1 мин после включения);

б) если дверь принудительно открыта или дверь не открыта в течение 120 с после срабатывания замка, включаются встроенный зуммер и выход тревоги (внешняя сирена).

Установка блокировки двери

Осуществляется последовательностью нажатий: * Мастер-код #

Обычный режим 70 # – отключение блокировки двери (заводская установка).

Режим блокировки 71 # – включение блокировки двери на 10 мин, если 10 раз поднесена недействующая карта или введен неверный пароль.

Режим тревоги 72 # – включение тревоги на 10 мин, если 10 раз поднесена недействующая карта или введен неверный пароль.

Установка режима шлюза

* Мастер-код # 80 # – режим шлюза выключен (заводская установка); 81 # – режим шлюза включен.

Установка времени выхода тревоги

* Мастер-код # 90–3 #

Время выхода тревоги задается в интервале 0–3 мин, заводская установка 1 мин.

Действия пользователя на открывание двери и отключение тревоги

Открывание двери картой: поднесите карту. Открывание двери по отпечатку пальца: приложите палец.

Если контроллер переходит в режим тревоги (встроенный зуммер, внешняя сирена), для отключения сигнала тревоги поднесите действующую карту, или приложите действующий палец, или поднесите мастер-карту, или приложите мастер-палец, или введите мастер-код #.

Любой из описанных методов выключает сигнал тревоги.

На рис. 2.12 представлена иллюстрация практического монтажа устройства.

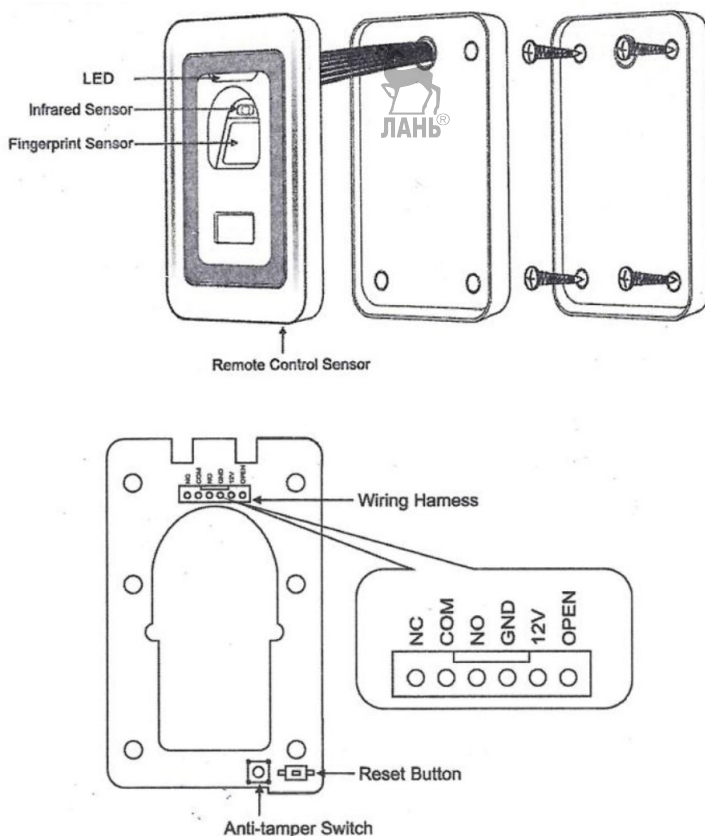


Рис. 2.12. Иллюстрация практического монтажа устройства

2.10.2. Другие способы применения контроллера

Как вариант рассмотрим ситуацию, в которой контроллер HN-F1ME работает как считыватель, подключаемый к другому контроллеру.

Контроллер HN-F1ME имеет выход Wiegand-26 и может подключаться к контроллеру с входом Wiegand-26 как дополнительный считыватель, схема подключения приведена на рис. 2.13.

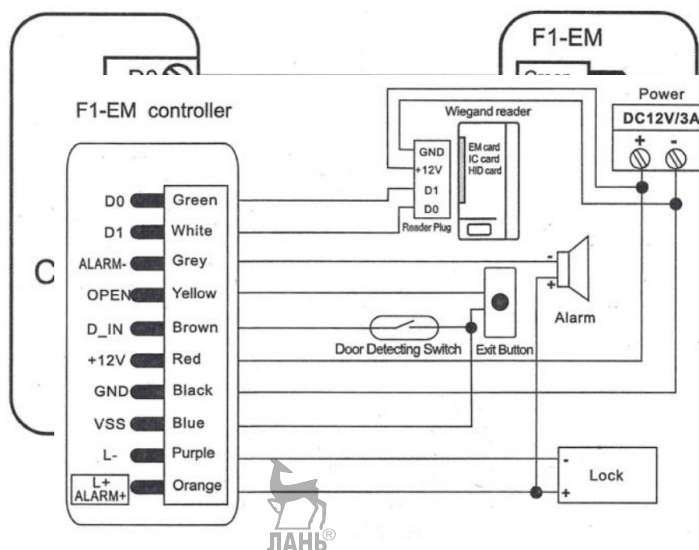


Рис. 2.13. Схема подключения дополнительного считывателя

Подключение дополнительного считывателя к контроллеру HN-F1ME

Контроллер HN-F1ME имеет порт Wiegand-26, к которому можно подключить любой дополнительный считыватель с интерфейсом Wiegand-26, для любого типа карт. Схема подключения приведена ниже. При добавлении карт особенных типов их следует прикладывать к дополнительному считывателю, а не к считывателю в контроллере (кроме карт EM Marine, которые можно прикладывать как к дополнительному считывателю, так и к считывателю в контроллере).

Установка двух контроллеров HN-F1ME на одну дверь

Для двухсторонней точки прохода соедините порты Wiegand-26 двух контроллеров, схема подключения приведена на рис. 2.14.

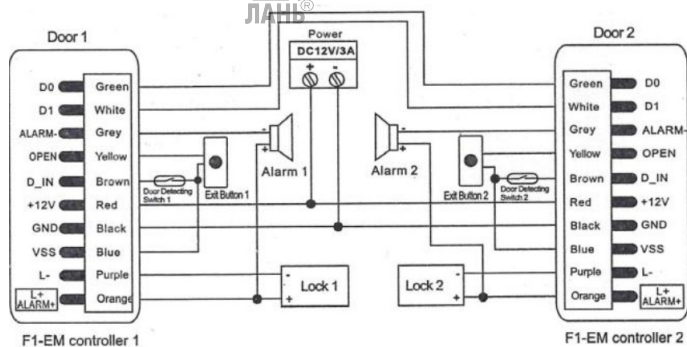


Рис. 2.14. Схема подключения для двухсторонней точки прохода

Один контроллер HN-F1ME устанавливается внутри, второй контроллер устанавливается снаружи, контроллеры подключаются друг к другу. Каждый автономный контроллер работает как считыватель. Такая комбинация обладает следующими особенностями.

Регистрацию пользователей можно производить на любом из контроллеров. Оба контроллера обмениваются информацией, поэтому емкость памяти для такой системы составляет 6000 пользователей. Каждый пользователь может использовать карту или отпечаток пальца для доступа.

Настройки двух контроллеров HN-F1ME должны быть одинаковыми. Если мастер-код разный, пользователь, зарегистрированный на контроллере снаружи, не сможет проходить через контроллер внутри.

Организация шлюза на двух контроллерах TS-RDR-Bio1

Схема подключения приведена на рис. 2.15, она используется для двух дверей, на каждую из которых установлены один контроллер и один электрозамок.

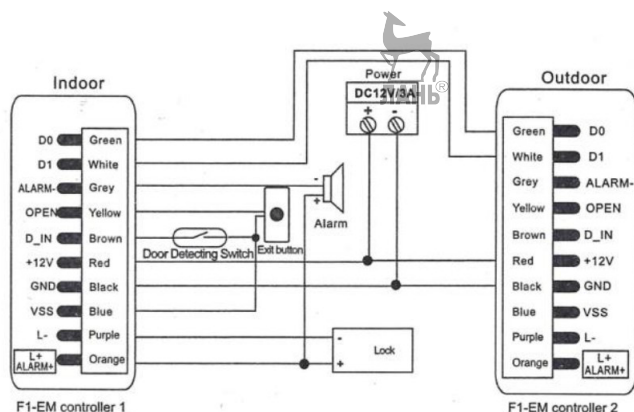


Рис. 2.15. Схема подключения с использованием двух контроллеров

Функция шлюза заключается в следующем: если любая из дверей открыта, другую открыть нельзя, пока не закроется открытая дверь. Включите функцию шлюза в настройках контроллеров. Шлюзы используются преимущественно в банках, тюрьмах и других местах, где требуется повышенный уровень безопасности. Шлюз можно считать одной точкой прохода.

Если пользователь подносит карту или прикладывает палец для считывания на контроллере 1, открывается дверь 1, пользователь должен войти и закрыть за собой дверь 1, только после этого он может открыть дверь 2, поднося карту или прикладывая палец для считывания на контроллере 2.

Сброс контроллера на заводские установки

Выключите питание, нажмите кнопку **RESET** (SW14) на плате контроллера, удерживайте ее и включите питание, отпустите кнопку после двух коротких звуковых сигналов, индикатор замигает оранжевым. После этого поднесите по очереди две EM Marine-карты, индикатор переключится на красный, показывая, что сброс на заводские установки выполнен успешно. Первая из поднесенных карт будет мастер-картой добавления, вторая – мастер-картой удаления.

Примечание. Сброс на заводские установки не удаляет информацию о пользователях. При выполнении сброса на заводские установки нужно занести в контроллер две мастер-карты.

В табл. 2.3 приведена техническая спецификация на устройство HN-F1ME.

Таблица 2.3. Техническая спецификация HN-F1ME

Напряжение питания	12 В DC + 10 %
Потребление в режиме ожидания	Не более 20 мА
Потребление в рабочем режиме	Не более 80 мА
Емкость памяти	Отпечатки пальцев: 1000 Карты: 2000
Совместимые карты	EM–MARINE, 125 кГц
Дальность считывания карт	3–6 см
Рабочая температура	–20 +50 °C
Рабочая влажность	20–95 %
Разрешающая способность сканера отпечатков пальцев	450 DPI
Время чтения отпечатков пальцев	Не более 1 с
Время идентификации	Не более 1 с
FAR	Не более 0,0000256 %
FRR	Не более 0,0198 %
Размеры	115×70×35 мм

В табл. 2.4 представлены сведения о звуковых сигналах и индикации устройства.

Таблица 2.4. Звуковые сигналы и индикация

Режим работы	Индикатор	Считыватель отпечатков	Зуммер
Сброс на заводские установки	Оранжевый	–	2 коротких сигнала
Режим «засыпания»	Медленно мигает красным	–	–
Режим ожидания	Медленно мигает красным	Мигает	–
Вход в режим программирования	Красный	–	Длинный сигнал
Выход из режима программирования	–	–	Длинный сигнал
Неверные действия	–	–	3 коротких сигнала
Открытие двери	Зеленый	–	Длинный сигнал
Тревога	Быстро мигает красным	–	Тревога

В табл. 2.5 представлены сведения по комплектации устройства.

Таблица 2.5. Комплектация устройства

Описание	Кол-во	Примечание
HN-F1ME	1	–
Дистанционный пульт управления	1	–
Карта менеджера	2	Карты добавления и удаления польз.
Инструкция	1	–
Винты	1	Для крепления к задней панели
Отвертка	1	Для установки
Саморезы	4	Для установки
Диод	1	IN4004

2.11. Выводы

Биометрические считыватели, конфигуративно объединенные в ЕБС (единые биометрические системы) как современные электронные системы контроля доступа и идентификации среди других систем кодового доступа, являются наиболее безошибочным решением для различных служб и организаций, которые могут сегодня предложить разработчики и специалисты РЭА. Это мнение основано на точности определения компонент индивидуального рисунка линий на пальцах людей, чем всегда славилась и дактилоскопия как метод, имеющий ничтожно малые риски ошибок идентификации.

Современные ЕБС, о компонентах и конфигурациях которых мы поговорили выше, являются электронным аналогом того же метода безошибочной идентификации личности, как и дактилоскопия. ЕБС может работать как самостоятельно (автономно), так и в комплексе интегрированной системы как составляющая часть – ступень проверочных мероприятий в системе доступа, учета, контроля рабочего времени и в других случаях.

В качестве периферийных исполнительных устройств в ЕБС применяют как электромагнитные замки, электронные «инвертированные» защелки и различные системы сигнализации (звуковой и световой) самого факта доступа. С пониманием работы элементов ЕБС у разработчиков совершенствуются возможности замены отдельных электронных узлов различных производителей в общей системе контроля доступа без потери ее функций.

Устройства электронной идентификации и контроля доступа совершенствуются во всех сферах и на разных профессиональных уровнях, для защиты объектов и секретной информации разработаны и другие методы, такие как контроль с помощью биометрии лица человека, сканирование зрачка (глазного яблока), идентификация рисунка вен на ладони и др. Все они позволяют с помощью современной электроники усилить охрану объекта и снизить риски ошибки при идентификации конкретных людей – как для стационарных, так и для движимых объектов, когда передача сигнала осуществляется моментально по телекоммуникационным сетям открытого и закрытого доступа, что позволяет оперативно решать актуальные задачи безопасности.

Глава 3

.....

Практическое подключение к единой биометрической системе (ЕБС)



https://t.me/it_boooks/2

В этой главе мы продолжим разговор о биометрических системах считывания информации и подробно остановимся на функционале современных считывателей, их отличительных особенностях и практическом применении.

3.1. Обоснование создания и особенности ЕБС

Важность создания «единой биометрической системы» трудно переоценить. Это взаимное удобство для компаний и частных лиц. Федеральный закон № 482-ФЗ от 31.12.2017 позволяет финансовым структурам идентифицировать человека удаленно. То есть банк имеет право без личного присутствия клиента совершать операции с его счетом (в том числе открывать/закрывать) по оцифрованному заявлению, подтвержденному цифровой подписью.

Актуален такой сервис и на малонаселенных и отдаленных территориях России, где зачастую до офиса нужно проделать немалый путь. Чтобы привлечь новых клиентов, кредитным организациям больше не нужно нести расходы на аренду и содержание здания, зарплату работнику и т. д. Человеку всего один раз нужно прийти в банк, где сотрудник сделает фото и запись голоса, при необходимости зарегистрирует клиента на портале государственных услуг. Информация имеет высокую степень защиты от утечки и кражи данных. Обязанности оператора системы доверены ПАО «Ростелеком». Банк России будет строго контролировать выполнение финансовыми учреждениями сохранности конфиденциальных данных клиентов.

Как мы говорили в первых двух главах книги, для идентификации граждан в биометрических системах контроля доступа используются параметры, уникальные для каждого человека. Проблема исключения подделки и кражи

идентификаторов решается путем использования индивидуальных признаков человека – биометрических идентификаторов:

- отпечатков пальцев;
- геометрии кисти руки;
- рисунка радужной оболочки и кровеносных сосудов сетчатки глаза;
- теплового изображения лица;
- динамики подписи;
- спектральных характеристик речи.

Диапазон проблем, решение которых может быть найдено с использованием современных технологий, широк:

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

Все биометрические технологии имеют общие подходы к решению задачи идентификации, хотя все они различаются удобством применения и точностью результатов.

Биометрическая технология применяется поэтапно:

- сканирование объекта;
- извлечение индивидуальной информации;
- формирование шаблона;
- сравнение текущего шаблона с базой данных;
- запись информации в память и (или) команда исполнительному устройству.

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

Строение ЕБС

Чтобы понять, насколько хорошо работает единая биометрическая система, нужно разобраться, как она действует. ЕБС имеет качественные отличительные признаки, а именно:

- мультимодальность. Проверку проходят два параметра личности – голос и лицо, это позволяет с точностью на 100 % определить, что перед вами настоящий человек;
- мультивендерность. Алгоритмы разрабатываются несколькими участниками проекта, лучшее из технологий включается в единую биометрическую систему идентификации личности;
- Liveness. Биосистема распознает имитацию и покушение на мошенническую сделку, схемы сценария проверок метрики клиента постоянно меняются;
- определение аномального поведения, не присущего ранее человеку. Программа позволяет пресекать действия злоумышленников, исходя из поведенческого фактора, усиливая защиту от фрода.

3.2. БИОМЕТРИЧЕСКИЕ КОНТРОЛЛЕРЫ И ИХ ХАРАКТЕРИСТИКИ

3.2.1. HN-F1ME

HN-F1ME – биометрический считыватель со встроенным контроллером на 1000 отпечатков и на 2000 карт формата Em-Marine, представлен на рис. 2.9 и 3.1.



Рис. 3.1. Биометрический считыватель HN-F1ME со встроенным контроллером на 1000 отпечатков

Программирование отпечатков и карт осуществляется с помощью ИК-пульта, входящего в комплект поставки, либо с помощью мастер-карт/мастер-отпечатков.

Особенности биометрического считывателя HN-F1ME:

- встроенный контроллер с памятью 1000 отпечатков или 2000 карт;
- возможно использование мастер-карт или мастер-пальцев для быстрого занесения/удаления отпечатков или карт;
- возможно подключение 2 контроллеров в режиме шлюза;
- возможно подключение к внешним контроллерам, имеющим вход Wiegand-26;
- настройка времени открытия двери;
- подключение электрозамка;
- антивандальный корпус.

Электрические и технические характеристики

Вендор: Hunter

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: Em-marine

Емкость памяти биометрических данных: 1000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: нет

Материал: металл

Температура эксплуатации: -20...+50 °C

Габаритные размеры: 115×70×35 мм

3.2.2. Биометрический считыватель F16 MIFARE ZKTECO

Биометрический считыватель F16 MIFARE ZKTECO представлен на рис. 3.2.





Рис. 3.2. Внешний вид биометрического считывателя F16 MIFARE

Технические характеристики устройства:

Вендор: ZKTeco
 LCD-дисплей: нет
 Встроенный контроллер: нет
 Тип биометрического сенсора: оптический
 Идентификация по венам: нет
 Идентификация по коду: нет
 Идентификация по лицу: нет
 Дополнительный считыватель: mifare
 Дополнительные интерфейсы: Ethernet, RS485
 Емкость памяти биометрических данных: 3000 шаблонов
 Интерфейс подключения: Wiegand-26
 Релейный выход: да
 Материал: пластик
 Температура эксплуатации: 0...+45 °C
 Габаритные размеры: 62×185×41 мм

3.2.3. Биометрический считыватель ST-SC110EKF SMARTEC

Устройство, внешний вид которого представлен на рис. 3.3, имеет следующие технические характеристики:

Вендор: Smartec
 LCD-дисплей: нет
 Встроенный контроллер: да
 Тип биометрического сенсора: оптический
 Идентификация по венам: нет

Идентификация по коду: да

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Емкость памяти биометрических данных: 200 шаблонов

Релейный выход: да

Материал: пластик

Температура эксплуатации: 0...+50 °C

Габаритные размеры: 88×88×34 мм



Рис. 3.3. Внешний вид биометрического считывателя ST-SC110EKF

3.2.4. Биометрический считыватель FR1200 ZKTECO

FR1200 – биометрический считыватель с интерфейсом RS-458 для использования с биометрическими контроллерами доступа, включая серию inBIO, F8 и др. Внешний вид устройства представлен на рис. 3.4.



Рис. 3.4. Внешний вид FR1200 – биометрического считывателя с интерфейсом RS-458

Считыватель позволяет захватить и передать отпечатки пальцев контроллеру доступа для дальнейшего сравнения отпечатка в нем. Корпус класса защищенности от внешних воздействий IP65 даёт возможность использовать ZK-FR1200 в любых погодных условиях, в том числе и вне помещений.

Особенности считывателя FR1200 и его технические характеристики:

- влагозащищенный корпус IP65;
- компактные габаритные размеры;
- считывание отпечатков и карт EM;
- передача кодированных данных по RS-485.

Вендор: ZKTeco

LCD-дисплей: нет

Встроенный контроллер: нет

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Емкость памяти биометрических данных: 500 шаблонов

Интерфейс подключения: RS485

Релейный выход: нет

Материал: пластик

Температура эксплуатации: 0...+45 °C

Габаритные размеры: 102×50×37 мм

Того же формфактора (соответствие рис. 3.4) устройство FR1200 Mifare – биометрический считыватель с интерфейсом RS-458 для использования с биометрическими контроллерами доступа, включая серию inBIO, F8 и т. д. Считыватель позволяет захватить и передать отпечатки пальцев контроллеру доступа для дальнейшего сравнения отпечатка в нем. Корпус класса защищенности от внешних воздействий IP65 дает возможность использовать ZK-FR1200 в любых погодных условиях, в том числе и вне помещений.

Особенности считывателя FR1200 Mifare:

- влагозащищенный корпус IP65;
- компактные габаритные размеры;
- считывание отпечатков и карт Mifare;
- передача кодированных данных по RS-485.

3.2.5. Биометрический считыватель ST-FR015EM SMARTEC

Технические характеристики

Вендор: Smartec
 LCD-дисплей: нет
 Встроенный контроллер: нет
 Тип биометрического сенсора: оптический
 Идентификация по венам: нет
 Идентификация по коду: нет
 Идентификация по лицу: нет
 Дополнительный считыватель: em-marine
 Интерфейс подключения: RS485
 Релейный выход: нет
 Материал: металл
 Температура эксплуатации: –10...+50 °С
 Габаритные размеры: 77×121×38 мм



3.2.6. Биометрический считыватель MA300 EM ZKTeco

ZK-MA300 – инновационный биометрический считыватель для систем контроля и управления доступом. Устройство использует самый быстрый алгоритм распознавания отпечатков пальца, а также ZK-высокопроизводительный оптический сенсор, обеспечивающий высокое качество изображения. Наличие интерфейсов Ethernet и RS-232/485 позволяет использовать устройства в сетях различного типа. Протокол TCP/IP гарантирует кратчайшее время обмена информацией между устройством и компьютером.

Особенности считывателя ZK-MA300 и технические характеристики:

- распознавание пользователя за 1 с;
- 1500 шаблонов, 10 000 карт, 100 000 событий;
- регистрация по отпечатку пальца или карте EM;
- защита от вскрытия/демонтажа, функция тревоги;
- возможность подключения кнопки EXIT и тревожной сигнализации;
- звуковое сопровождение при добавлении и удалении пользователя;
- аудиовизуальная индикация состояния и результатов распознавания;
- встроенный USB-порт для переноса данных вручную.

Вендор: ZKTeco
 LCD дисплей: нет
 Встроенный контроллер: нет
 Тип биометрического сенсора: оптический
 Идентификация по венам: нет
 Идентификация по коду: нет
 Идентификация по лицу: нет



Дополнительный считыватель: em-marine
 Дополнительные интерфейсы: Ethernet, RS485, USB
 Емкость памяти биометрических данных: 1500 шаблонов
 Интерфейс подключения: Wiegand-26
 Релейный выход: да
 Материал: металл
 Температура эксплуатации: $-10...+60\text{ }^{\circ}\text{C}$
 Габаритные размеры: $148\times 73\times 34,5\text{ мм}$

3.2.7. Биометрический считыватель BIOSMART 5M-E-EM

BioSmart 5M-E-EM – контроллер биометрический для идентификации пользователей по отпечаткам пальцев или RFID-картам. Позволяет управлять замком, турникетом (в одну сторону), другими исполнительными устройствами. Отличительной особенностью контроллера является возможность работы при отрицательных температурах. Контроллер оснащен емкостным сканером отпечатков пальцев, позволяющим обеспечить защиту от муляжей.

Внутренние элементы контроллера покрыты лаком для обеспечения защиты от коррозии и конденсата в условиях уличного применения. Сканер отпечатков пальцев оборудован специальной схемой подогрева, обеспечивающей комфортное сканирование отпечатков пальцев при температурах до $-40\text{ }^{\circ}\text{C}$.

Особенности контроллера 5M-E-EM и технические характеристики:

- наличие Ethernet и USB для связи с компьютером;
- веб-интерфейс для конфигурирования сетевых параметров;
- встроенный считыватель пластиковых карт формата Em-marine;
- конструктивное исполнение в алюминиевом корпусе;
- работа при отрицательных температурах до $-40\text{ }^{\circ}\text{C}$;
- максимальное количество пользователей – 1000;
- автономная память – 25000 событий;
- накладной алюминиевый корпус.

Вендор: BioSmart

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: ёмкостной

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet, USB

Емкость памяти биометрических данных: 1000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: нет



Материал: металл

Температура эксплуатации: $-40...+50\text{ }^{\circ}\text{C}$

Габаритные размеры: $50 \times 160 \times 43\text{ мм}$

3.2.8. Биометрический считыватель BIOSMART 4-O-EM-N-L

BioSmart 4-O-EM-N-L – контроллер для идентификации пользователей по отпечаткам пальцев или RFID-картам. Позволяет управлять замком, турникетом (в одну сторону), другими исполнительными устройствами.

В контроллере используется оптический сканер отпечатков пальцев, имеющий надежную защиту от царапин и сколов, что дает возможность установки оборудования на объектах с большой численностью пользователей.

Особенности контроллера и технические характеристики:

- возможность работы в режиме серверной идентификации;
- встроенный считыватель карт Em-marine;
- поддержка режима идентификации «отпечаток пальца на смарт-карте»;
- наличие интерфейса Wiegand-вход, выход;
- возможность подключения БУР BioSmart;
- количество отпечатков: до 4500 в локальном режиме, до 3000 в серверном;
- количество пользователей 3000, событий в памяти – до 40 000;
- питание 12 В, 300 мА.

Вендор: BioSmart

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet, RS485

Емкость памяти биометрических данных: 4500 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: нет

Материал: пластик

Температура эксплуатации: $0...+50\text{ }^{\circ}\text{C}$

Габаритные размеры: $75 \times 175 \times 54\text{ мм}$

3.2.9. Биометрический считыватель ST-FR040EM SMARTEC

Технические характеристики

Вендор: Smartec

LCD-дисплей: да

Встроенный контроллер: да

Тип биометрического сенсора: фото
Идентификация по венам: нет
Идентификация по коду: да
Идентификация по лицу: да
Дополнительный считыватель: em-marine
Дополнительные интерфейсы: Ethernet, RS485, USB
Емкость памяти биометрических данных: 500 шаблонов
Интерфейс подключения: Wiegand-26
Релейный выход: да
Материал: пластик
Температура эксплуатации: 0...+ 50 °С
Габаритные размеры: 86×210×86 мм

3.2.10. Биометрический считыватель ST-FR032ЕК SMARTEC

Внешний вид устройства представлен на рис. 3.5.



Рис. 3.5. Внешний вид устройства

Технические характеристики

Вендор: Smartec
LCD-дисплей: да
Встроенный контроллер: да
Тип биометрического сенсора: оптический
Идентификация по венам: нет

Идентификация по коду: да

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet, RS485, USB

Емкость памяти биометрических данных: 5000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: пластик

Температура эксплуатации: $-10...+50\text{ }^{\circ}\text{C}$

Габаритные размеры: 62×185×41 мм

3.2.11. Биометрический считыватель BIOSMART MINI-O-EM

Внешний вид контроллера представлен на рис. 3.6.



Рис. 3.6. Внешний вид устройства

BioSmart Mini-O-EM – считыватель предназначен для идентификации пользователей по отпечаткам пальцев или RFID-картам при совместной работе с контроллерами BioSmart Prox-E (EX) и BS-P1. Считыватель не предназначен для самостоятельного управления исполнительными устройствами. В считывателе используется оптический сканер отпечатков пальцев, имеющий надежную защиту от царапин и сколов, что дает возможность установки оборудования на объектах с большой численностью пользователей.

Особенности считывателя и технические характеристики:

- накладной пластиковый корпус;
- память 4500 отпечатков пальцев в локальном режиме;
- встроенный считыватель карт;
- поддержка режима верификации «карта+отпечаток»;
- питание DC12В/0.2А.

Вендор: BioSmart

LCD-дисплей: нет

Встроенный контроллер: нет

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Емкость памяти биометрических данных: 4500 шаблонов

Интерфейс подключения: RS485

Релейный выход: нет

Материал: пластик

Температура эксплуатации: 0...+50 °C

Габаритные размеры: 50×155×40 мм

3.2.12. Биометрический считыватель ST-FR030EMW SMARTEC

Внешний вид устройства представлен на рис. 3.7.



Рис. 3.7. Внешний вид устройства

Технические характеристики

Вендор: Smartec

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet, RS485

Емкость памяти биометрических данных: 5000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: пластик

Температура эксплуатации: –40...+50 °С

Габаритные размеры: 62×185×41 мм

3.2.13. Биометрический считыватель C2000-BIOACCESS-F18 БОЛИД

Внешний вид контроллера представлен на рис. 3.8.



Рис. 3.8. Внешний вид устройства

C2000-BioAccess-F18 – биометрический контроллер доступа, предназначен для совместной работы с АРМ «Орион Про» и организации системы контроля

и управления доступом по биометрическим идентификаторам – отпечаткам пальцев. Контроллеры объединяются в сеть по интерфейсу Ethernet (TCP/IP).

Особенности считывателя *BOLID* и технические характеристики:

- защищенный режим работы с контроллером C2000–2 по интерфейсу Wiegand, который предотвращает возможность несанкционированного доступа в помещение путем отрыва контроллера от стены и замыкания контактов замка;
- входы для подключения датчика положения двери и кнопки ВЫХОД;
- предусмотрены контакты для управления сиреной и дверным звонком;
- цветной графический TFT ЖК-дисплей диагональю 2.4 дюйма с меню на русском и английском языках;
- встроенный считыватель Proximity-карт EM–Marine;
- цифровая клавиатура для настройки прибора через меню и ввода паролей;
- поддерживается режим доступа по комбинации двух идентификаторов: отпечаток пальца, карточка, пароль;
- отображение имени пользователя на дисплее при проходе;
- голосовое оповещение на русском и английском языках.

Вендор: Bolid

LCD-дисплей: да

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: да

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet

Емкость памяти биометрических данных: 3000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: пластик

Температура эксплуатации: 0...+45 °C

Габаритные размеры: 183×80×42 мм

3.2.14. Биометрический считыватель TF1600 ZKTECO

Внешний вид контроллера представлен на рис. 3.9.



Рис. 3.9. Внешний вид устройства

ZK-TF1600 – один из компактных терминалов для идентификации человека по отпечатку пальца, который к тому же обладает водонепроницаемым корпусом со степенью защиты IP65. Устройство разработано специально для автономного использования – в квартире, офисе, магазине, гараже, на фабрике и т. д. Важной особенностью данной модели является наличие встроенного обогревателя, который позволяет поддерживать рабочую температуру от $-40...+45\text{ }^{\circ}\text{C}$.

Особенности считывателя ZK-TF1600 и технические характеристики:

- компактный влагозащищенный корпус IP65;
- идентификация отпечатков пальцев за 1 с;
- 3000 шаблонов, 10 000 карт, 100 000 событий;
- работа при $-40\text{ }^{\circ}\text{C}$ (встроенный обогрев).

Вендор: ZKTeco

LCD-дисплей: нет

Встроенный контроллер: нет

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: нет

Дополнительные интерфейсы: Ethernet, RS485

Емкость памяти биометрических данных: 3000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: пластик

Температура эксплуатации: $-40...+45^{\circ}\text{C}$

Габаритные размеры: $185 \times 62 \times 41$ мм

3.2.15. Биометрический считыватель TF1700 ZKTeco

Внешний вид контроллера представлен на рис. 3.10.



Рис. 3.10. Внешний вид устройства

TF1700 – один из самых компактных терминалов для идентификации человека по отпечатку пальца, который к тому же обладает водонепроницаемым корпусом со степенью защиты IP65. Устройство разработано специально для автономного использования – в квартире, офисе, магазине, гараже, на фабрике и т. д. Для большей информативности предусмотрен дисплей с разрешением 128×64 пикселя.

Особенности считывателя TF1700 и технические характеристики:

- компактный влагозащищенный корпус;
- гладкий и тонкий дизайн для узких участков;
- идентификация отпечатков пальцев за 1 с;
- 3000 шаблонов, 10 000 карт, 50 000 событий;
- настройки против повторного прохода;
- контроль датчика двери, кнопка **EXIT**, режима тревоги;
- дисплей с разрешением 128×64 рх.

Вендор: ZKTeco

LCD-дисплей: да

Встроенный контроллер: нет

Тип биометрического сенсора: оптический

Идентификация по венам: нет
 Идентификация по коду: да
 Идентификация по лицу: нет
 Дополнительный считыватель: em-marine
 Дополнительные интерфейсы: Ethernet, RS485
 Емкость памяти биометрических данных: 3000 шаблонов
 Интерфейс подключения: Wiegand-26
 Релейный выход: да
 Материал: пластик
 Температура эксплуатации: $-10...+50\text{ }^{\circ}\text{C}$
 Габаритные размеры: 185×62×41 мм



3.2.16. FE-MA300 биометрический считыватель Falcon Eye

Внешний вид контроллера представлен на рис. 3.11.



Рис. 3.11. Внешний вид контроллера FE-MA300

FE-MA300 – биометрический контроллер-считыватель. Интерфейсы контроля доступа: замок, датчик двери, кнопка **EXIT**, тревожная сигнализация.

Особенности контроллера-считывателя и технические характеристики

- количество шаблонов отпечатка пальца: 1500;
- количество карт: 10 000;
- количество записей в журнале событий: 100 000;
- коммуникации: RS232/485, TCP/IP, USB-хост;
- интерфейс Wiegand-26: вход/выход.

Вендор: Falcon Eye

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет



Идентификация по лицу: нет
 Дополнительный считыватель: ем-marine
 Дополнительные интерфейсы: Ethernet, RS232, RS485, USB
 Емкость памяти биометрических данных: 1500 шаблонов
 Интерфейс подключения: Wiegand-26
 Релейный выход: нет
 Материал: металл
 Температура эксплуатации: –10...+60 °C
 Габаритные размеры: 73×148×34,5 мм

3.2.17. Биометрический считыватель C2000-BIOAccess-MA300 Болид

Внешний вид контроллера представлен на рис. 3.12.



Рис. 3.12. Внешний вид устройства

C2000-BIOAccess-MA300 – биометрический контроллер доступа. Предназначен для совместной работы с АРМ «Орион Про» и организации системы контроля и управления доступом (СКУД) по биометрическим идентификаторам – отпечаткам пальцев. Контроллеры объединяются в сеть по интерфейсу Ethernet (TCP/IP).

Особенности считывателя BOLID и технические характеристики:

- защищенный режим работы с контроллером C2000–2 по интерфейсу Wiegand, который предотвращает возможность несанкционированного доступа в помещение путем отрыва контроллера от стены и замыкания контактов замка;
- входы для подключения датчика положения двери и кнопки **Выход**;
- предусмотрены контакты для управления сиреной и дверным звонком;
- встроенный считыватель Proximity-карт EM–Marine;

- поддерживается режим доступа по комбинации двух идентификаторов: отпечаток пальца + карточка;
- голосовое оповещение.

Вендор: Bolid

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet

Емкость памяти биометрических данных: 1500 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: металл

Температура эксплуатации: $-10...+60\text{ }^{\circ}\text{C}$

Габаритные размеры: $148 \times 73 \times 34,5\text{ мм}$

3.2.18. Биометрический считыватель ST-FR031EM Smartec

Внешний вид контроллера представлен на рис. 3.13.



Рис. 3.13. Внешний вид устройства

ST-FR031EM – биометрический считыватель для ограничения доступа в помещение путем идентификации персонала по отпечаткам пальцев и картам стандарта Em-Marine. Этот считыватель снабжен контроллером СКУД и имеет релейный выход для управления замком двери. Позволяет подключить кнопку запроса на выход и датчик положения двери. Благодаря Wiegand-интерфейсу

может быть интегрирован в СКУД любых производителей. Устройство способно работать под управлением программного обеспечения Timex.

Особенности считывателя и технические характеристики:

- биометрический считыватель отпечатков: сенсор со стеклянной призмой;
- типы идентификации: биометрический доступ по отпечатку пальца; по карте; по отпечатку + карта;
- поддержка расписания работы считывателя или разблокировки двери;
- общий тревожный выход;
- датчик вскрытия;
- класс защиты IP65;
- возможность хранения до 3000 отпечатков пальцев;
- время идентификации одного отпечатка пальца – менее 1 секунды.

Вендор: Smartec

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet, RS485

Емкость памяти биометрических данных: 3000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: пластик

Температура эксплуатации: 0...+50 °C

Габаритные размеры: 185×62×41 мм

3.3. Автономные контроллеры-считыватели биометрических данных



3.3.1. TS-RDR-Bio 2 контроллер-считыватель Tantos

На рис. 3.14 представлен внешний вид контроллера TS-RDR-Bio 2.



Рис. 3.14. Внешний вид контроллера TS-RDR-Bio 2

TS-RDR-Bio 2 – автономный контроллер доступа предназначен для организации точки доступа для одной двери, может непосредственно управлять электророзамком и позволяет подключить к нему кнопку запроса на выход. Он может использоваться как считыватель и подключаться к сторонним контроллерам. Емкость памяти 998 пользовательских отпечатков + 2 мастер-пальца. Все настройки функций и пользователей могут выполняться с помощью инфракрасного пульта дистанционного управления (ДУ) или с помощью мастер-пальцев. Использование современных технологий идентификации отпечатков пальцев обеспечивает надежность работы контроллера и высокий уровень безопасности управления доступом. Контроллер может эффективно использоваться для контроля доступа людей в таких областях, как бизнес, офисы, производство, частный сектор и др.

Особенности контроллера-считывателя и технические характеристики:

- металлический корпус;
- использует современную технологию для считывания отпечатка пальца, высокая адаптивность;
- 998 пользователей, может использоваться для офисов, в жилом секторе и т. д.;
- контроллер может использоваться как автономно, так и в составе сетевых СКУД;
- добавление и удаление пользователей с помощью инфракрасного пульта ДУ или мастер-пальцев;
- очень простое подключение, совместим со всеми видами электророзамков;

- отпечаток пальца может преобразовываться в номер виртуальной карты и передаваться по протоколу Wiegand-26 на сторонний контроллер;
- имеет функцию тревоги при вскрытии корпуса;
- широкий диапазон питающих напряжений.

Вендор: Tantos

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: нет

Емкость памяти биометрических данных: 1000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: металл

Температура эксплуатации: -20...+50 °C

Габаритные размеры: 120×72×35 мм



3.3.2. TS-RDR-Bio 1 контроллер-считыватель Tantos

На рис. 3.15 представлен внешний вид контроллера.



Рис. 3.15. Внешний вид контроллера TS-RDR-Bio 1

TS-RDR-Bio 1 – автономный биометрический контроллер на 1000 отпечатков. Встроенный считыватель карт Em-marine с контроллером на 2000 карт. Программирование отпечатков и карт осуществляется с помощью ИК-пульта, входящего в комплект поставки.



Особенности контроллера-считывателя:

- возможно использование мастер-карт или мастер-пальцев для быстрого занесения/удаления отпечатков или карт;
- возможно подключение 2 контроллеров в режиме шлюза или использование в качестве внешнего считывателя;
- возможно подключение к сетевым контроллерам, имеющим вход Wiegand-26.

Технические характеристики

Вендор: Tantos

LCD-дисплей: нет

Встроенный контроллер: да

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Емкость памяти биометрических данных: 1000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: металл

Температура эксплуатации: -10...+50 °C

Габаритные размеры: 115×70×35 мм

3.4. Многофункциональные считыватели

3.4.1. Контроллер F16 ZKTeco

Внешний вид устройства представлен на рис. 3.16.



Рис. 3.16. Внешний вид считывателя F16 ZKTeco

F16 – эргономичный биометрический терминал для систем контроля и управления доступом со сканером отпечатков пальцев, считывателем карт и подключением по Ethernet. Пыле-, влагозащищенный корпус IP65. Встроенный считыватель отпечатков пальцев и карт Em-Marine. Встроенное реле для управления замком, инфракрасный датчик пальца, светодиодная подсветка, звуковая сигнализация.

Особенности считывателя F16:

- память: ID card 10 000, 100 000 событий;
- Master-Slave;
- датчик двери, кнопка выхода, тревога, звонок;
- может быть ведущим для FR1200 с функцией Antipassback;
- алгоритм ZK Finger 10.0;
- веб-сервер;
- питание 12 В, 3 А;
- бесплатное русифицированное ПО ZK Access в комплекте с функциями учета рабочего времени.

Технические характеристики

Вендор: ZKTeco

LCD-дисплей: нет

Встроенный контроллер: нет

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: em-marine

Дополнительные интерфейсы: Ethernet, RS485

Емкость памяти биометрических данных: 3000 шаблонов

Интерфейс подключения: Wiegand-26

Релейный выход: да

Материал: пластик

Температура эксплуатации: 0...+45 °C

Габаритные размеры: 62×185×41 мм

3.4.2. Инновационный контроллер MA300 Mifare ZKTeco

Внешний вид контроллера представлен на рис. 3.17.



Рис. 3.17. Внешний вид контроллера MA300 Mifare ZKTeco

ZK MA300 Mifare – инновационный биометрический считыватель для систем контроля и управления доступом. Устройство использует самый быстрый алгоритм распознавания отпечатков пальца, а также ZK-высокопроизводительный оптический сенсор, обеспечивающий высокое качество изображения. Наличие интерфейсов Ethernet и RS-232/485 позволяет использовать устройства в сетях различного типа. Протокол TCP/IP гарантирует простоту и кратчайшее время обмена информацией между устройством и компьютером.

Особенности считывателя ZK MA300 Mifare:

- распознавание пользователя за 1 с;
- 1500 шаблонов, 10 000 карт, 100 000 событий;
- регистрация по отпечатку пальца или карте Mifare;
- защита от вскрытия/демонтажа, функция тревоги;
- возможность подключения кнопки **EXIT** и тревожной сигнализации;
- звуковое сопровождение при добавлении и удалении пользователя;
- аудиовизуальная индикация состояния и результатов распознавания;
- встроенный USB-порт для переноса данных вручную.

Технические характеристики

Вендор: ZKTeco

LCD-дисплей: нет

Встроенный контроллер: нет

Тип биометрического сенсора: оптический

Идентификация по венам: нет

Идентификация по коду: нет

Идентификация по лицу: нет

Дополнительный считыватель: mifare
Дополнительные интерфейсы: Ethernet, RS485, USB
Емкость памяти биометрических данных: 1500 шаблонов
Интерфейс подключения: Wiegand-26
Релейный выход: да
Материал: металл
Температура эксплуатации: –10...+60 °С
Габаритные размеры: 148×73×34,5 мм

3.4.3. Контроллер Optimus SKF-010

Optimus SKF-010 – биометрический контроллер со встроенными считывателями отпечатка пальцев, считывателем карт и «кодонаборной» клавиатурой. Предназначен для организации автономной системы контроля доступа для одной точки прохода, при этом программирование выполняется локально с помощью встроенной клавиатуры. Память до 500 пользователей. Имеется возможность подключения НО и НЗ типов замков. Имеет выход Wiegand для подключения к сторонним контроллерам.

Технические характеристики Optimus SKF-010

Количество отпечатков: 500
Количество кодов 500
Количество карт 500
Сканер отпечатков пальцев Оптический, режим работы 1: N
Дисплей Нет
Площадь сканирования 22×18
Разрешение 500 DPI (точек на дюйм)
Скорость считывания менее 1 с
FRR (ошибка распознавания 1-го рода) 0.1 %
FAR (ошибка распознавания 2-го рода) 0.00001 %
Встроенный считыватель карт EM–MARINE есть
Дальность считывания 1–5 см
Клавиатура есть
Длина кода 4–6 символов
Подсветка клавиатуры есть
Алгоритм работы: отпечаток; карта; код
Выбор режимов доступа нет
Встроенное меню нет (кодовые комбинации)
Администрирование прав доступа нет
USB-вход есть
Реле управления исполнительными устройствами есть
Тип контактов реле Н.О./Н.З.
Коммутируемый ток/напряжение до 2 А 30 В пост. напр.
Регулировка времени задержки реле есть (1–99 с)

Внешние интерфейсы звонок, реле Н.О./Н.З., выход Wiegand-26, кнопка выхода, датчик двери, тревога вскрытия

Тампер вскрытия есть

Корпус, класс защиты пластик, IP20

Рабочая температура от –10 до +50 °С

Питание DC12 В (ток потребления 200 мА)

Размеры 88×88×33 мм

Внешний вид устройства представлен на рис. 3.18.



Рис. 3.18. Внешний вид контроллера

3.4.4. Контроллер ST-FR015E Smartec

Биометрический считыватель обеспечивает работу под управлением ST-NC120F, ST-NC240F, ST-NC440F и ПО Timex. Невозможно использовать для ввода ОП в базу данных. Интерфес RS-485, встроенный считыватель ЕМ. Питание 12 В, ток потребления 0.14 А. Размеры 121×77×38 мм. Температурный режим –10...+50 °С, класс защиты IP65.

Биометрический считыватель ST-FR015ЕМ предназначен для использования в системах контроля доступа совместно с контроллерами ST-NC120F, ST-NC240F и ST-NC440F. Устройство обеспечивает идентификацию пользователей по отпечаткам пальцев и по проксимити-картам стандарта ЕМ и поддерживает следующие режимы распознавания: ОП, карта, ОП и/или карта.

Особенности ST-FR015ЕМ:

- фронтальная панель из нержавеющей стали;
- герметичный корпус с IP65;
- сенсор со стеклянной призмой;
- защита от поддельных отпечатков пальцев;

- обеспечивает сканирование сухих, влажных и грубых пальцев;
- встроенный считыватель карт EM;
- типы идентификации: ОП, карта, ОП и/или карта;
- трехцветный LED-индикатор и зуммер.

Технические характеристики устройства представлены в табл. 3.1.

Таблица 3.1. Технические характеристики

Модель	ST-FR015EM
Алгоритмы	ОП версия 10
Разрешение сканера	500 dpi
Время идентификации	< 2 с
FAR	< 0.0001 %
FRR	< 0.01 %
Считыватель	ЕМ, встроенный, 125 кГц
Интерфейсы	RS485
Питание	12 В пост. тока, не более 140 мА
Диапазон рабочих температур	от –10 до +50 °С без конденсации
Диапазон рабочей влажности	10–90 %
Класс защиты	IP65
Габариты	121×77×38 мм

3.5. ПОРТАТИВНЫЕ И ПЕРЕНОСНЫЕ СЧИТЫВАТЕЛИ

3.5.1. Настольный контроллер Hikvision DS-K1F820-F

Hikvision DS-K1F820-F – устройство ввода отпечатков пальцев предназначено для работы с персональным компьютером по USB-интерфейсу. Используется для сканирования отпечатков пальцев, создания базы шаблонов отпечатков, загрузки данных о характеристиках отпечатков пальцев и изображения в контроллер. Он поддерживает функцию проверки полноты зарегистрированных шаблонов отпечатков пальцев. Используются в том числе для контроля потоков лиц при пересечении границы.

Особенности и технические характеристики

- Разрешение 508 DPI
- Поддерживает функцию PnP (plug and play)
- Оптический датчик отпечатков пальцев, разработанный с устойчивым к царапинам материалом
- Поддерживаемые операционные системы: Windows XP, Windows7 и Windows 10
- Работает от ПК с подключением через USB2.0 без установки дополнительных драйверов
- Габариты (мм): 100×48×35

- ЦПУ 32 бит
 - Режим идентификации Оптический модуль, красная подсветка
 - Разрешение 508 dpi
 - Шаблон пальца для распознавания 256×288 пикселей
 - Питание DC5 В
 - Рабочий ток 200 мА
 - Рабочие условия –30...+70 °С, влажность 20...80 %
- Внешний вид устройства представлен на рис. 3.19.



Рис. 3.19. Внешний вид контроллера Hikvision DS-K1F820-F

3.5.2. Контроллер Smartec ST-FE800

Биометрический USB-сканер Smartec ST-FE800 может использоваться совместно с различными программными приложениями для ввода в базу данных шаблонов отпечатков пальцев, при этом для интеграции с ПО сторонних производителей можно использовать SDK.

Благодаря тому что сканер Smartec ST-FE800 совместим со всеми биометрическими считывателями и терминалами учета рабочего времени марки Smartec, поддерживающими алгоритм распознавания версии 10, а также с программным обеспечением «Таймекс», это устройство может использоваться для централизованного ввода отпечатков пальцев пользователей.

Особенности Smartec ST-FE800

- Высокое качество сканирования
- Небольшие размеры
- Стабильная работа в условиях сильного освещения
- Защита от поддельных отпечатков пальцев
- Обеспечивает сканирование сухих, влажных и грубых пальцев
- SDK для интеграции USB-сканера в любые приложения
- Совместим с устройствами Smartec и программным обеспечением «Таймекс»
- Совместим с Windows® 7, 8, 10 и Windows Server 2012, 2016

Технические характеристики Smartec ST-FE800

Алгоритмы: ОП версия 10, ISO19794–2, ANSI-378

Разрешение: 500–1000 dpi

Глубина цвета: 8 бит (256 уровней серого)

Рабочая область сканера: 15×20 мм

Защита от электростатики: > 15 кВ

Интерфейсы: USB2.0 / USB1.1

Питание: 5 В пост. тока, через USB-порт

Потребляемый ток, ожидание: 60 мА

Потребляемый ток, сканирование: 200 мА

Диапазон рабочих температур: от –20 до +50 °С без конденсации

Диапазон рабочей влажности: 20–90 %

Габариты: 49×44×20 мм

**3.5.3. Контроллер Smartec ST-FR015EM**

Биометрический считыватель Smartec ST-FR015EM предназначен для использования в системах контроля доступа совместно с контроллерами ST-NC120F, ST-NC240F и ST-NC440F. Устройство обеспечивает идентификацию пользователей по отпечаткам пальцев и по проксимити-картам стандарта EM и поддерживает следующие режимы распознавания: ОП, карта, ОП и/или карта.

Считыватель Smartec ST-FR015EM предназначен для врезного монтажа и оснащен прочным корпусом со степенью защиты IP65, что позволяет использовать устройство в условиях повышенной влажности, в диапазоне температур от –10 до +50 °С.

Особенности Smartec ST-FR015EM

- Фронтальная панель из нержавеющей стали
- Герметичный корпус с IP65
- Сенсор со стеклянной призмой
- Защита от поддельных отпечатков пальцев
- Обеспечивает сканирование сухих, влажных и грубых пальцев
- Встроенный считыватель карт EM
- Типы идентификации: ОП, карта, ОП и/или карта
- Трехцветный LED-индикатор
- Зуммер

**Технические характеристики Smartec ST-FR015EM**

Алгоритмы: ОП версия 10

Разрешение сканера: 500 dpi

Время идентификации: < 2 с

FAR: < 0.0001 %

FRR: < 0.01 %

Считыватель: EM, встроенный, 125 кГц

Интерфейсы: RS485

Питание: 12 В пост. тока, не более 140 мА

Диапазон рабочих температур: от –10 до +50 °С без конденсации

Диапазон рабочей влажности: 10–90 %

Класс защиты: IP65

Габариты: 121×77×38 мм

3.5.4. Контроллер Smartec ST-FE700

Биометрический USB-сканер ST-FE700 может использоваться совместно с различными программными приложениями для ввода в базу шаблонов отпечатков пальцев, при этом для интеграции с ПО сторонних производителей можно использовать SDK. В зависимости от необходимой степени интеграции на выбор предлагается одна из трех версий SDK: SDK lite, SDK standard или SDK professional. Поскольку сканер ST-FE700 совместим со всеми биометрическими считывателями и терминалами учета рабочего времени Smartec, а также с программным обеспечением «Таймекс», его можно использовать для централизованного ввода отпечатков пальцев пользователей. Кроме того, аппаратная часть ST-FE700 обеспечивает автоматическую калибровку считывателя и осуществляет шифрование данных при их передаче через USB-интерфейс.

Функциональные возможности Smartec ST-FE700

- Высокое качество сканирования
- Небольшие размеры
- Шифрование отсканированных шаблонов
- Защита от использования поддельных отпечатков пальцев
- Снятие отпечатка независимо от положения пальца на сканере
- Обеспечивает сканирование сухих, влажных и грубых пальцев
- SDK для интеграции USB-сканера в любые приложения
- Совместим со всеми устройствами Smartec и программным обеспечением «Таймекс»
- Совместим с Windows® 7, Vista, XP, 2000, Me, 98, NT®4.0 и Windows Server 2008, 2010

Внешний вид устройства представлен на рис. 3.20.





Рис. 20. Внешний вид устройства Smartec ST-FE700

3.6. ВАРИАНТЫ ИСПОЛНИТЕЛЬНЫХ УСТРОЙСТВ

Биометрический считыватель Мцыри-3 сможет превратить квартиру или офис в сейф. Конструкция запирающей системы состоит из электронного контроллера двери и стальной панели с встроенным сенсором. Технические характеристики модуля:

- Размеры – коробка 120×105×27 мм
- Питание – 4 батарейки типа АА
- Срок службы – 1 год
- Объем памяти биометрического считывателя – 30 отпечатков
- Вероятность ошибки доступа – 0,000001 %
- Работает при температуре от –8 до + 80 °С
- В качестве резервного доступа – цифровой код

Замок с биометрическим считывателем L-9000. Если модель «Мцыри-3» выполнена без привычной ручки, то модуль L-9000 внешне похож на стандартный механический дверной замок с ручкой. Биометрический считыватель и цифровая клавиатура спрятаны под слайдером, что обеспечивает их сохранность.

Интересной особенностью конструкции биометрического замка является наличие «журнала посещений», который фиксирует все прикосновения к двери и способы открытия (ключ, пароль, отпечаток). В аварийном режиме работы замок можно открыть механическим ключом.

- Размеры – как у стандартного механического замка с ручкой
- Питание – 4 батарейки типа АА
- Срок службы – 6 месяцев

- Объем памяти биометрического считывателя – 500 отпечатков пальцев
- Вероятность ошибки доступа – 0,000001 %
- В качестве резервного доступа – ввод PIN-кода на цифровой клавиатуре, механический ключ

Модель биометрического замка «Премиум» напоминает L-9000 – тоже есть наличие обычной дверной ручки, встроенной в замок. Но есть и отличия:

- размеры – цельнометаллический корпус с латунной ручкой;
- питание – 4 батарейки типа АА;
- срок службы – до 18 месяцев;
- объем памяти – 180 отпечатков пальцев;
- вероятность ошибки доступа – 0,000001 %;
- в качестве резервного доступа – механический ключ.

Замок с биометрическим считывателем Samsung Ezon SHS-5230 имеет ручку, в которую вмонтирован идентификатор. Также модуль оснащен сенсорным экраном для ввода пароля и опцией автоматического закрытия двери. Активация функции блокировки исключает возможность открытия двери любым способом.

- Размеры – дверная ручка с дисплеем
- Питание – 4 батарейки типа АА
- Срок службы – 12 месяцев
- Объем памяти – до 100 отпечатков пальцев
- Вероятность ошибки доступа – 0,000001 %
- В качестве резервного доступа – пароль, механический ключ

Считыватель биометрический SSA-R2011 (Samsung) работает по отпечатку пальца, смарт-картам и прокси-картам. Скорость считывания информации – менее двух секунд. Объем памяти – до 1000 отпечатков пальцев. Модуль оснащен световой индикацией и звуковой сигнализацией. Работает при температурном режиме от –20 до +50 °С. Размеры коробки 65.0×128.0×48.5 мм.

Среди исполнительных устройств контроля доступа наиболее распространены следующие запорные или управляемые преграждающие устройства:

- электромеханические замки;
- электронные защелки;
- турникеты (поясные, полноростные, «билетные», раздвижные, вращающиеся 3- или 4-штанговые);
- шлюзовые кабины (тамбурного типа, ротанты, шлагбаумы);
- автоматические ворота (распашные ворота, сдвигающиеся ворота, складывающиеся ворота, рулетные ворота);
- лифты и другое мощное оборудование.

В современных СКУД применяются в основном электромагнитные и электромеханические замки.

Шлюзовые кабины тамбурного типа (2 поворотные двери) имеют пропускную способность от 8 до 12 человек в минуту. Гораздо выше пропускная способность шлюзов-ротантов, в которых используется только одна поворотная дверь.

3.6.1. Дверные замки и защелки

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

Мощные штыревые электромеханические замки сейфового типа при подаче напряжения на специальный электромотор осуществляют «движение» запорных штырей внутрь. Вот почему на важных, в том числе строящихся, объектах целесообразно использовать именно электромеханические замки, а при необходимости быстро установить систему контроля доступа на действующем объекте лучше применять электромеханические защелки, которые позволяют использовать уже существующие механические замки.

Электромагнитные замки состоят из электромагнита, прикрепляющегося к дверной коробке, и ответной металлической пластины, монтируемой на двери.

В дежурном режиме на обмотку электромагнита подается постоянный ток удержания, вызывающий сильное магнитное поле, которое притягивает металлическую пластину двери, удерживая ее в закрытом состоянии. При подаче сигнала на специальный вход устройства магнитное поле исчезает, и дверь может быть открыта. Все электромагнитные замки характеризуются максимальной механической нагрузкой удержания, которая измеряется в килограммах и может достигать до 1000 кг. Вместе с дверными замками используют доводчики, возвращающие дверь в исходное положение.

Преимущество электромагнитных замков:

- небольшой, по сравнению с электромеханическими замками, потребляемый ток;
- отсутствие импульсных выбросов напряжения при открывании.

Отрицательные стороны: большие размеры, шаблонный промышленный дизайн, полная зависимость от наличия электропитания.

Модуль биометрического замка состоит из трех элементов:

- внешняя часть;
- внутренняя часть;
- отсек для батареек.

Во внешнюю часть вмонтирован биометрический считыватель (сканер), который идентифицирует отпечаток пальца. Также внешняя часть может быть оснащена экраном и клавиатурой. Во внутренней части содержится микроконтроллер, в котором хранятся шаблоны отпечатков пальцев. В отсек для батареек вставляются батарейки определенного типа.

По типу монтажа дверные замки с биометрическими считывателями могут быть: врезными, накладными, в форме дверной ручки, встроенными в дверную ручку, ригельными.

Замок с биометрическим считывателем открывается без ключей и магнитных карт. Главный недостаток в том, что биометрический считыватель вас

может «не узнать». Почему такое случается? Потому что папиллярный узор подушечки пальца может стать некорректным для считывания. Это бывает в случае: загрязнения рук, пореза пальца, изменения узора на коже, по иным причинам, частично рассмотренным в главе 1, – когда обладатель отпечатка намеренно искажает узор на пальце.

Чтобы обезопасить себя и биометрический считыватель от ложных срабатываний и некорректной работы, в программное обеспечение вводят несколько вариантов отпечатка пальца.

3.6.2. Варианты применения для сейфовых хранилищ

Сейфовый шкаф можно закрывать на простой ключ, можно установить электронный замок с кодом, а можно пользоваться сейфом вообще без ключа и кода. Это возможно с помощью установки на сейф биометрического замка. Принцип устройства таких сейфов – встроенные дактилоскопические модули. Для аварийного открытия предусмотрен механический ключ или кодовый модуль.

Объем памяти простого биометрического считывателя – до 250–300 отпечатков пальцев. Это позволяет использовать такую систему многим сотрудникам фирмы или офиса одновременно. Сейфы с биометрическими замками в разы дороже аналогов с другими системами замыкания, но они значительно надежнее.

Сетевой контроллер Эра-2000GSM

Эра-2000 GSM – сетевой контроллер с возможностью передачи данных на сервер с применением сетей сотовой связи стандарта GSM, а также функцией управления контролем доступа с использованием номера телефона в качестве идентификатора.

На рис. 3.21 показан внешний вид устройства.



Рис. 3.21. Внешний вид

Устройство предназначено для организации управления доступом на объектах с численностью сотрудников не более 2000 человек. GSM-модель не требует обязательной подводки к сети Ethernet, тем самым рекомендована для

установки там, где нет возможности организации прокладки локальных сетей. Собственная энергонезависимая память хранит информацию о 60 000 событиях. Устройство способно обслуживать одну полноценную точку прохода через интерфейс от Wiegand-4 до Wiegand-64 или две точки через Touch Memory. О методах конфигурации элементов системы и взаимодействия по сети интернет мы говорили в первой главе книги.

Память устройства может содержать сведения о 200 графиках проходов любой сложности. Контроллер поставляется вместе с бесплатным фирменным программным обеспечением «ЭНТ – контроль доступа», которое можно доработать под индивидуальные требования пользователя.

В ПО включены средства автоматизированного формирования отчетов и рассылки авторизованным лицам, программа интеграции с IP-видеосистемами сторонних производителей с возможностью просмотра фрагментов фиксации прохода. Все контроллеры оснащены выходами «открытый коллектор» для управления электромеханическими и электромагнитными замками, кнопкой выхода. Кроме того, он взаимодействует с турникетами, шлагбаумами, приводами ворот, картоприемниками, почтовыми ящиками, лифтами. «Эра-2000 GSM» рекомендован для установки на шлагбаумы с модулем распознавания номеров машин «ЭРА-авто» для организации автотранспортной проходной. Если номер машины в каком-либо случае не идентифицируется камерой, всегда можно будет открыть ворота с использованием номера телефона.

Аппаратный функционал

Входы контроллера

- Считыватель/кодовая панель – 2 шт. (интерфейс Wiegand-26) или 4 шт. (интерфейс Touch Memory)
- Кнопка для открытия замка – 2 шт.
- Датчик открытия прохода – 2 шт.

Выходы (управление) контроллера

- Управление световой индикацией считывателей – 4 шт.
- Управление звуковой индикацией считывателей – 2 шт.

Управление контроллера

- 2 двери – считыватель-кнопка (интерфейс Wiegand-26)
- 2 двери – 2 считывателя (интерфейс Touch Memory)

Технические характеристики

Напряжение питания: 12–24 В

Потребляемая мощность: 1,5 Вт

Габаритные размеры корпуса: 112×125×33 мм

Материал корпуса: пластик

Объем памяти: 60 000 событий (1 точка прохода) / 30 000 событий (2 точки прохода)

Количество пользователей (электронных ключей) 2000 (1 точка прохода) / 1000 (2 точки прохода)

Количество графиков прохода (любой сложности): 200

Количество временных режимов для графиков проходов: 200

Динамическое распределение памяти между электронными ключами и событиями проходов: имеется

Интерфейс работы контроллера: Ethernet (IEEE802.3) / сеть сотовой связи стандарта GSM

Интерфейс связи контроллера со считывателями: Wiegand-4...64, Touch Memory

Рабочий диапазон температур: от -40 до +70 °C

Срок службы изделия: не менее 8 лет

Гарантия на изделие: 5 лет с момента ввода в эксплуатацию (но не более 6 лет с даты производства контроллера)

Количество точек прохода: 2 (Touch Memory) или 1 (Wiegand)

3.7. Выводы

При выборе устройств, в составе которых конфигурированы электронные считыватели отпечатков пальцев, руководствуйтесь правильным назначением конкретной модели; не стоит покупать считыватели с большим объемом памяти для семьи из трех персон. Также различаются и сейфовые замки – есть объемы памяти от 14 до 300 отпечатков пальцев. Приоритетом выбора, как и во всем остальном в жизни, должна быть целесообразность.

Идентификация биометрических параметров значительно упрощает сотрудничество и поможет расширить клиентскую базу. Кроме биометрических характеристик (на которые ориентированы соответствующие считыватели информации), для совершенствования СКУД разработчику необходимо обратить внимание на поведенческие характеристики, такие как клавиатурный почерк, подпись, голос и др. Поведенческие характеристики, в отличие от физиологических особенностей, могут изменяться по прошествии времени. Биометрия, основанная на поведенческих характеристиках, менее точна при идентификации, но тем не менее оба метода имеют более высокий уровень определения личности, нежели пароли и карты.

Опорная литература

Интегрированная автоматизированная система идентификации отпечатков пальцев (IAFIS) ФБР США: <http://www.fbi.gov/hq/cjisd/iafis>.

Кашикаров А. П. Современные ключи и идентификаторы систем кодового доступа // Современная электроника. 2013. № 8. С. 42.

Консорциум по биометрии: <http://www.biometrics.org>.

Консорциум BioAPI: <http://www.bioapi.org>.

Международная ассоциация биометрической промышленности (IBIA): <http://www.ibia.org>.

Смарт-карты и биометрия в системах персональной идентификации, May 2002, Smart Card Alliance: <http://www.smartcardalliance.org/>.

<http://www.smartec-security.ru/news/biometric-reader.htm>.

<http://vzortechology.com>.

http://www.amosystems.ru/system/biometric_system_handkey_II.ahtm.

<http://us.allegion.com/Products/biometrics/handkey2/Pages/default.aspx>.

<http://faceid.ru/index.php?item=f710>.

<http://www.smartec-security.ru/news/face-recognition.htm>.



Книги издательства «ДМК Пресс» можно заказать
в торгово-издательском холдинге «Планета Альянс» наложенным платежом,
выслав открытку или письмо по почтовому адресу:
115487, г. Москва, 2-й Нагатинский пр-д, д. 6А.
При оформлении заказа следует указать адрес (полностью),
по которому должны быть высланы книги;
фамилию, имя и отчество получателя.
Желательно также указать свой телефон и электронный адрес.
Эти книги вы можете заказать и в интернет-магазине: **www.a-planet.ru**.
Оптовые закупки: тел. **(499) 782-38-89**.
Электронный адрес: **books@alians-kniga.ru**.



Антти Суомалайнен

**Биометрическая защита:
обзор технологии**

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com
Корректор *Синяева Г. И.*
Верстка *Арифудин Г. Р.*
Дизайн обложки *Мовчан А. Г.*

Формат 70×90 1/16.
Гарнитура «PT Serif». Печать офсетная.
Усл. печ. л. 7,61. Тираж 200 экз.

Веб-сайт издательства: **www.dmkpress.com**
