Содержание

Глава 1

Методы геометрического считывания информации

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

1.1. Идентификация человека посредством электроники

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

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

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

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

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

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

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

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

1.1.1. Сравнение с шаблоном и технические ошибки

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

1.1.2. Верификация и ошибки верификации

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

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

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

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

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

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

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

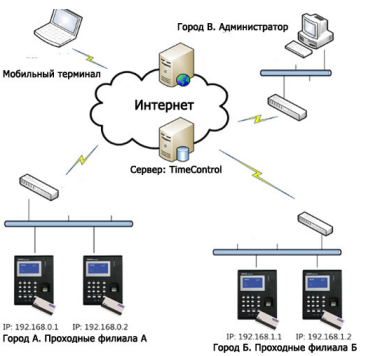

Рис. 1.2. Блок-схема контроля и администрирования в системе идентификации, действующей посредством интернета

1.2. Методы считывания информации для анализа в системе кодового доступа

1.2.1. Отпечаток пальца

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

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

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

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

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

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

Оптический метод

Для получения оптического изображения отпечатка пальца может быть использовано устройство, подобное цифровой камере. Кончик пальца прикладывается к стеклянной пластине, освещенной должным образом. Необходим 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 разработками и внедрением. Для определения выступов и впадин отпечатка пальца в лабораториях разработана матрица микромеханических датчиков, но пока еще нет уверенности в их устойчивости. Таким методом также невозможно отличить настоящий палец от имитации.

1.2.2. Геометрия лица человека

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

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

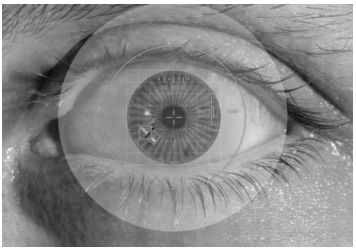

Рис. 1.3. Иллюстрация сканирования по геометрии лица человека

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

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

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

1.2.3. Радужная оболочка и сетчатка глаза

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

На рис. 1.4 представлена иллюстрация этого метода.

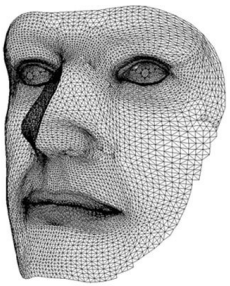

Рис. 1.4. Иллюстрация метода сканирования по оболочке и сетчатке глаза

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

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

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

1.2.4. Идентификация по рисунку вен ладони и ее геометрии

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

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

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

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

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

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

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

1.2.5. Дополнительная идентификация по штрих-коду

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

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

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

1.3. Устройства считывания информации. Взаимодействие со СКУД

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

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

В СКУД поддерживаются оба варианта подключения:

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

1.3.1. Идентификация по бесконтактным картам

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

Ниже рассмотрены основные особенности такого типа идентификаторов.

Физическое исполнение

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

Таблица 1.1. Различные современные идентификаторы и их особенности

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

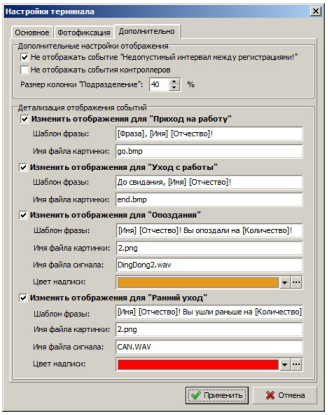

Рис. 1.6. Иллюстрация окна программы Бюро пропусков

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 выполнятся 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 Timex 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.

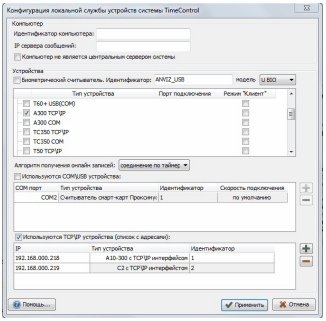

Рис. 1.7. Иллюстрация работы с кодами

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: