Министерство внутренних дел Российской Федерации
Федеральное казенное учреждение
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА»

АНАЛИТИЧЕСКИЙ ОБЗОР
«Исследование современных методов персональной идентификации в целях применения в системах централизованного наблюдения»

Москва 2015

Содержание

Введение

Широкое внедрение систем контроля и управления доступом (СКУД) становится все более актуальной задачей вследствие повышения террористических угроз и роста уровня преступности. Ограничение доступа в опасные помещения, контроль за перемещением персонала по объекту позволяет повысить технику безопасности и снизить риск технологических аварий. Кроме того, контроль над перемещением персонала по объекту может быть использован как средство повышения дисциплины и автоматизации учета рабочего времени, а также обеспечения охраны технологических и коммерческих секретов от промышленного шпионажа и предотвращения правонарушений на рабочих местах и т. д.

В основе работы системы контроля и управления доступом заложен принцип принятия решения о допуске субъектов (сотрудников) и о санкционировании перемещения объектов (транспортных средств, грузов и т. д.) в отдельные зоны на основании анализа идентификационных признаков, принадлежащих конкретному субъекту или объекту с информацией, заложенной в памяти системы. Одними из основных компонентов систем контроля и управления доступом являются устройства идентификации, предназначенные для осуществления процедуры опознавания субъекта (объекта) при пересечении им границ охраняемой территории в точке доступа, по определенным (идентификационным) признакам.

Каждый из субъектов (объектов) обладает присвоенным или присущим ему изначально индивидуальным идентификационным признаком. В качестве носителя присваиваемого признака может выступать пароль (кодовое число) или некоторый предмет, в который или на который с помощью специальной технологии занесены идентификационные данные.

Наиболее перспективными направлениями в системах идентификации в настоящее время являются технологии бесконтактной идентификации, основанные на радиочастотных методах и биометрической идентификации.

Метод дистанционного считывания является наиболее быстро развивающейся технологией для систем контроля и управления доступом. Считывание кода с идентификатора происходит на определенном расстоянии от считывателя без непосредственного контакта. Существует несколько технологий записи идентификационного кода на носителях-идентификаторах, например, на эффекте поверхностной акустической волны. Однако наиболее широкое распространение получили идентификаторы с установленной внутри интегральной микросхемой, которая представляет собой устройство, содержащее в общем случае приемник, передатчик и процессор с памятью, в которой хранится идентификационный код. Также внутри идентификатора расположена антенна, с помощью которой происходит обмен данными между считывателем и идентификатором в радиочастотном диапазоне электромагнитных волн.

В качестве идентификационных признаков могут также использоваться биометрические данные человека (отпечатки пальцев, геометрия кисти руки, голос, радужная оболочка глаза и т.п.).

Устройства биометрической идентификации в системах контроля и управления доступом до недавнего времени были достаточно редкими элементами этих систем из-за своей сложности и высокой цены. Развитие современных технических средств привело к появлению на рынке относительно недорогих и качественных средств биометрического контроля доступа.

При идентификации по индивидуальным биометрическим признакам определяется именно человек – носитель этих признаков, а не выданный ему документ – карта, код, ключ и.т.п. Это является основным отличием данных систем от любых других идентифицирующих устройств.

Современные методы персональной идентификации базируются на следующих основных принципах:

1) Принцип индивидуальности идентифицируемых объектов. "Устойчивость к подделке" – эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор. Под индивидуальностью понимается безусловное отличие объекта

идентификации от любых других. Для практической реализации этого принципа необходимо выявление специфических отличительных свойств, присущих идентифицируемому объекту. Эти отличительные свойства называют идентифицирующими признаками.

Данный принцип предполагает разграничение понятий "сходство" и "тождество". Выявление идентифицирующих признаков лежит в основе идентификации.

2) Принцип "устойчивости к окружающей среде" – характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях, таких как изменение освещения или температуры помещения.

3) Принцип относительной устойчивости идентифицируемых объектов – способность сохранять относительно неизменными свои существенные индивидуальные свойства. Степень устойчивости объектов может быть различной. Если к моменту исследования существенные для идентификации свойства претерпели сильные изменения, проведение идентификации осложняется или становится невозможным.

4) Принцип достаточности и оптимальности при выборе показателей идентификации и методов их определения – выбор необходимых и достаточных для надежного подтверждения тождества показателей, характеризующих различные свойства объекта.

5) Принцип надежности, воспроизводимости и сопоставимости результатов идентификации (принцип эффективности). В качестве двух основных характеристик любой биометрической системы можно принять ошибки первого и второго рода (FAR (False Acceptance Rate) и FRR(False Rejection Rate)). Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей. Второе – вероятность отказа доступа человеку, имеющего допуск. Система тем лучше, чем меньше значение FRR при одинаковых значениях FAR. Иногда используется и сравнительная характеристика EER, определяющая точку в которой графики FRR и FAR пересекаются. Но она далеко не всегда репрезентативна.

При повторных испытаниях, независимо от субъектов, средств и условий проведения идентификации, должны быть получены одни и те же результаты.

6) Принцип "простоты использования" – показывает насколько сложно воспользоваться биометрическим сканером, время проведения процедуры идентификации.

7) "Скорость работы" и "качество системы – стоимость системы" – одни из основных принципов, которые должны соответствовать требованиям к современным методам идентификации.

Системы контроля и управления доступом, использующие методы идентификации на основе приведенных выше принципов, начали внедряться с середины 70-х годов 20 века. Поскольку стоимость подобных систем в то время была весьма велика, они применялись лишь в тех местах, где необходимо было обеспечить наивысшую степень защиты. Однако в последние годы с появлением недорогих и мощных микропроцессорных устройств, развитием компьютерных методов анализа образов, подобные системы стали применяться чаще, в связи с уменьшением их стоимости.

Целью настоящего аналитического обзора является выявление наиболее перспективных методов персональной идентификации для применения их в системах централизованного наблюдения путем проведения многокритериальной оценки характеристик современных методов персональной идентификации.

1 Термины и определения

активный идентификатор (active tag): Идентификатор, обладающий способностью генерировать сигнал.

алгоритм (algorithm): Последовательность действий биометрической системы, направленных на решение поставленной задачи, имеющая конечное число шагов и обычно использующаяся биометрическим ядром (биометрическим системным программным обеспечением) для того, чтобы определить, соответствуют ли друг другу биометрический образец и шаблон.

аутентификация (Authentication): Метод проверки подлинности, позволяющий достоверно убедиться в том, что субъект действительно является тем, за кого он себя выдает. Различные системы аутентификации можно разделить на три класса в соответствии с тем, что именно должен предъявлять системе субъект:

– то, что он знает;

– то, чем он владеет;

– то, что является частью его самого.

Первый класс использует различного рода шифры, набираемые человеком (например, PIN-коды, криптографические коды и т.п.).

Второй класс использует шифры, передаваемые при помощи физических носителей информации (пластиковые карты с магнитной полосой, электронные таблетки "touch memory", электронные token-устройства, proximity-карты и т.д.).

Третий (биометрический) класс принципиально отличается тем, что аутентификации подвергается собственно личность человека – его индивидуальные характеристики (рисунок папиллярного узора, радужная оболочка глаза и т.д.), которые невозможно потерять, передать другому человеку и достаточно трудно подделать.

база данных (database): Любое хранилище биометрических шаблонов и связанной с ними информации о конечном пользователе.

бесконтактный способ (contactless manner): Способ обмена сигналами и подачи питания на карту без применения гальванических элементов (т.е. при отсутствии омического пути от внешнего интерфейсного оборудования к интегральной(ым) схеме(ам), содержащейся(имся) в карте).

бесконтактный(ая): Имеющий(ая) отношение к способу обмена сигналами и подачи питания на карту без применения гальванических элементов (т. е. при отсутствии омического пути от внешнего интерфейсного оборудования к интегральной(ым) схеме(ам), содержащейся(имся) в карте).

биометрическая верификация (biometric verification): Автоматический (автоматизированный) процесс установления принадлежности полученного биометрического образца и имеющегося биометрического шаблона одной личности.

биометрическая идентификация (biometric identification): Процесс сравнения представленного биометрического образца с контрольной выборкой шаблонов (схема "один ко многим") с целью определения соответствия образца какому-либо из контрольных шаблонов в данной контрольной выборке для установления соответствующей шаблону личности.

биометрическая система (biometric system): Автоматизированная система, обеспечивающая:

– получение биометрического образца от конечного пользователя;

– извлечение биометрических данных из биометрического образца;

– сравнение биометрических данных с данными, содержащимися в шаблонах баз данных,

– идентификацию или верификацию полученных данных (определение степени схожести полученных и имеющихся в базе данных данных);

– проведение действия, в зависимости от результатов идентификации или верификации.

биометрические данные (biometric data): Любые данные, характеризующие какую-либо биометрическую характеристику.

биометрические технологии (Biometric Technologies): Совокупность методов,

используемых при создании биометрических систем.

биометрический (biometric): Имеющий отношение к биометрии.

биометрический тип (biometric type): Тип биометрической технологии.

Пример - Биометрическая технология на основе отпечатка пальца.

биометрия (biometrics): Автоматизированное распознавание личности, основанное на определении поведенческих и биологических (анатомических и физиологических) характеристик.

верификация (Verification): Режим идентификации, в котором предварительно (например, при помощи ввода PIN-кода или предъявления физического носителя информации) субъект называет себя. В этом случае вместо многократного сравнения по всему списку зарегистрированных пользователей осуществляется только единственное сравнение (действительно ли предъявленная биометрическая характеристика соответствует "названной" записи в списке).

дальность считывания (read range): Максимальное расстояние, с которого система идентификации может гарантированно считывать информацию с заданных индификаторов в соответствии с установленными критериями.

емкость памяти (memory capacity): Объем данных, выраженный в битах или байтах, который может храниться в памяти идентификатора.

заводское программирование (factory programming): Запись данных на идентификатор в процессе ее производства, которые будут доступны только для считывания.

защита от записи (write protection): Техническое решение, позволяющее обеспечить защиту всей или части памяти идентификатора от изменения, перезаписи или стирания находящейся в ней информации.

идентификационная карта (identification card): Карта, которая содержит данные о ее держателе и эмитенте и может содержать сведения, необходимые в качестве входных данных для применения карты в соответствии с ее назначением и выполнения основанных на них транзакций.

идентификационный признак идентификатора (tag ID): Признак изготовителя и/или пользователя назначенный для конкретного идентификатора.

идентификация (Identification): Проверка наличия субъекта в списке зарегистрированных пользователей и выявление того, кто он, осуществляется многократным сравнением по всему списку зарегистрированных пользователей (иногда называется режимом распознавания "один ко многим"). Существуют также режимы "один к одному" (см. Верификация) или "один к нескольким", когда субъект предварительно называет свой класс, в который может входить несколько субъектов.

ключ (key): Последовательность символов управления криптографической операцией (например, шифровка, расшифровка, закрытая или общедоступная операция в динамической аутентификации, подписи производства, верификация подписи).

кодирование данных (data coding): Представление битов данных в канале прямой передачи или преобразование логических битов данных в физические сигналы.

коллизия (collision): Состояние, которое возникает в результате одновременной передачи информации от различных источников по одному каналу передачи.

нарушение прав личности (Privacy Violation): Хранение в некоторых биометрических системах непосредственно изображений (пусть даже небольшой его части) папиллярных узоров. В основном присуще применению корреляционных алгоритмов распознавания.

несанкционированный доступ (penetration): Несанкционированное обращение к системе обработки данных.

оптическая зона (accessible optical area): Область на карте с оптической памятью, пригодная для доступа пучка считывания и/или записи с применяемой оптической системы.

ориентация (машиносчитываемый носитель данных) (orientation): Расположение машиносчитываемого носителя данных относительно устройства считывания, выражаемое в виде трех пространственных углов в некотором диапазоне изменений, представляемых через крен, перекос и разворот.

отпечаток пальца (Fingerprint): Термин, присущий красковому методу съема изобра-

жения папиллярного узора, иногда жаргонное выражение для папиллярного узора, полученного любым способом, например, в результате сканирования на дактилоскопическом сканере.

ошибки распознавания (Recognition Errors): Любые неправильно принятые биометрической системой решения. Различают ошибки трех родов:

– ошибка первого рода – "не узнать своего", т.е. принимается решение "чужой", хотя на самом деле субъект присутствует в списке зарегистрированных пользователей (для вероятности ложного отказа используется термин FRR – от английского False Rejection Rate;

– ошибка второго рода – "пропустить чужого", т.е. принимается решение "свой", хотя, на самом деле, субъект отсутствует в списке зарегистрированных пользователей (для вероятности ложного доступа используется термин FAR – от английского False Acceptance Rate.

– ошибка третьего рода – принимается решение "чужой", но не по результату сравнения, а по причине невозможности получить наблюдение выбранной биометрической характеристики (например, устройство ввода папиллярного рисунка – дактилоскопический сканер – не может снять изображение из-за каких-либо недостатков кожи).

папиллярный узор (Papillar Tracery): Складки эпидермиса, повторяющие строение внешнего слоя дермы. Кожа человека состоит из двух слоев. Наружный слой называется эпидермисом, а второй, более глубокий, – дермой. Поверхность дермы, прилегающая к эпидермису, образует многочисленные выступы – так называемые дермальные сосочки. На большей части тела сосочки располагаются беспорядочно, а на ладонных поверхностях кистей и, в частности, пальцев дермальные сосочки складываются в ряды. Поэтому эпидермис, повторяющий строение внешнего слоя дермы, на этих участках тела образует небольшие складки, отображающие и повторяющие ход рядов дермальных сосочков. Эти складки, видимые на поверхности кожи невооруженным глазом, называются папиллярными линиями (лат. papillae – сосочки) и отделяются друг от друга неглубокими бороздками. На вершинах складок – гребнях папиллярных линий имеются многочисленные мельчайшие поры – наружные отверстия выводных протоков потовых желез кожи. Папиллярные линии, особенно на поверхностях пальцев кисти, образуют различные узоры, называемые папиллярными узорами. Рисунок папиллярного узора формируется в окончательном виде в процессе внутриутробного развития и с момента рождения до смерти человека остается неизменным. После любых повреждений эпидермиса, не затрагивающих сосочков дермы, папиллярный узор в процессе заживления восстанавливается в прежнем виде. Если повреждены сосочки дермы, то образуется рубец, в определенной мере деформирующий в этом месте узор, но не изменяющий его первоначального общего рисунка и деталей строения в других местах.

пассивный идентификатор (passive tag): Идентификатор, обладающий способностью отражать и модулировать несущий сигнал, полученный от устройства считывания опроса.

повторяемость биометрической характеристики (Biometric Parameter Repeatability): Устойчивость значений биометрической характеристики для данного человека. "Повторяемость" исключает ошибку "неузнавания" зарегистрированного пользователя.

радиочастотная идентификация RFID (radio frequency identification): Технология автоматической идентификации и сбора данных, которая использует электромагнитную или индуктивную связь, осуществляемую посредством радиоволн, для взаимодействия с радиочастотной идентификаторой и однозначного считывания ее идентификационных данных путем применения различных видов модуляции сигнала и кодирования данных.

скорость передачи данных (data transfer rate): Величина, измеряемая средним числом битов, знаков или блоков, передаваемых в единицу времени между двумя пунктами.

считывание (read (noun)): Процесс поиска и извлечения данных с какого-либо машиносчитываемого носителя, сопровождающийся, при необходимости, управлением разрешения конфликтов и защитой от ошибок, а также декодированием в канале передачи данных и в источнике данных, требуемым для восстановления и передачи данных, записанных в их источнике.

считывать (read (verb)): Получать данные от устройства ввода, устройства хранения данных или с носителя данных.

считывающее устройство (reader): Функциональный блок, который используют для

сбора или анализа данных, вводимых из запоминающего устройства, носителя данных или иного источника.

уникальность биометрической характеристики (Biometric Parameter Uniqueness): Точное соответствие биометрической характеристики только одному человеку.

функциональная совместимость (interoperability): Способность систем различных изготовителей выполнять взаимный обмен данными, позволяющая осуществлять их эффективное совместное использование.

чувствительность к пространственной ориентации (orientation sensitivity): Зависимость уровня сигнала ответа идентификатора от ее угловой ориентации в пространстве по отношению к антенне устройства считывания/опроса.

шифровать/шифрование (encrypt/encryption): Обратимое преобразование данных с помощью криптографического алгоритма для создания зашифрованного текста с целью защиты информации (обеспечения конфиденциальности).

2 Основные типы идентификации

Существует всего три основных типа персональной идентификации:
– идентификация по запоминаемому коду;
– идентификация по вещественному коду;
– идентификация по биометрическому признаку.

Как видно из названия, идентификация по запоминаемому коду предполагает запоминание кода (пароля) пользователем. Запомненный пользователем код и является идентификатором. В качестве устройств ввода кода (считывателей) в этом случае используется цифровая или алфавитно-цифровая клавиатура, а также различные кодовые переключатели, панели или другие подобные устройства.

Достоинством идентификации по запоминаемому коду является то, что для нее не требуется вещественный носитель кода. Соответственно запоминаемый код невозможно потерять, он не может быть украден, отсутствуют затраты на его изготовление.

Однако, процесс идентификации, основанный на запоминании кода пользователем, имеет ряд недостатков. Так, для повышения надежности, код должен иметь как можно большее количество разрядов (знаков). Например, коды доступа многих сейфовых замков высокой секретности имеют не менее 12 разрядов. Запомнить такое количество цифр или знаков большинству людей достаточно трудно. Это приводит к тому, что код записывают на бумаге, секретность кода после этого практически теряется. Уязвимым местом идентификации по запоминаемому коду является возможность (как визуально, так и при помощи специальных технических средств) "подсмотреть" код в процессе его ввода на клавиатурном считывателе. Еще одна проблема связана с пропускной способностью систем, использующих идентификацию такого типа. При большом потоке людей через проходную, ошибки, связанные с неправильным набором кода, резко снижают пропускную способность и порождают множество конфликтов со службой охраны.

Справедливости ради следует отметить, что клавиатурные считыватели имеют определенные достоинства. Например, разрядность кода, может быть выбрана произвольно, код может устанавливаться самим пользователем и произвольно им изменяться, и быть неизвестным оператору системы, также имеется возможность ввода дополнительных кодов, например, кода "тихой" тревоги при нападении, кодов управления.

В настоящее время идентификация по запоминаемому коду применяется в простых автономных устройствах доступа или в качестве дополнительной наряду с другими типами идентификации.

В основе идеи идентификации по вещественному коду лежит применение в качестве идентификаторов материальных носителей кода. Существует великое множество, как видов материальных носителей, так и используемых технологий записи/чтения и хранения кода. В современных автоматизированных системах идентификации в качестве идентификаторов используются пластиковые карты, брелоки, браслеты, механические или электронные ключи, и другие подобные устройства.

Несмотря на великое разнообразие видов вещественных идентификаторов, все они обладают общими достоинствами и общими недостатками.

К достоинствам идентификации по вещественному носителю можно отнести стабильно высокую скорость считывания кода, и как следствие, повышенную пропускную способность систем, использующих данный тип идентификации. В отличие от идентификации по запоминаемому коду, при идентификации по вещественному носителю, пользователю не требуется запоминать код, а достаточно иметь навык использования идентификатора, что в силу неоднородности возрастных и интеллектуально-психологических качеств пользователей может оказаться огромным достоинством. Так, люди, находящиеся в состоянии стресса, дети и люди пожилого возраста с большой долей вероятности могут забыть код, но навык использования идентификатора, закрепленный на уровне условных рефлексов, забыть практически невозможно.

Главным недостатком идентификации по вещественному коду является то, что идентификатор не имеет однозначной привязки к конкретному пользователю, а, следовательно, любой человек, завладев идентификатором, будет признан системой, использующей иденти-

фикацию по вещественному коду, санкционированным пользователем. И наоборот, санкционированный пользователь, утративший идентификатор (потерял или случайно не захватил его с собой) не будет признан системой, использующей идентификацию по вещественному коду.

Идентификация по биометрическому признаку – идентификация, основанная на использовании индивидуальных физических признаков человека. Суть идентификации по биометрическому признаку заключается в том, что каждый человек обладает индивидуальными неповторимыми свойствами. Например, код ДНК, папиллярный рисунок пальцев и ладони, радужная оболочка глаза, геометрия лица и прочее. Эти параметры могут являться надежным идентификационным признаком, который нельзя потерять, подделать передать другому лицу.

Запоминаемый и вещественный код относятся к так называемому присвоенному типу кода. При этом идентифицируется не сам человек (пользователь), а код, который ему присвоен. В этом состоит основной недостаток подобного вида идентификации. Код и пароль могут стать известными постороннему лицу случайно или преднамеренно. Идентификатор с вещественным кодом может быть потерян, украден или передан другому человеку по сговору. Если система работает в автоматическом режиме, то от подобных угроз она не защищена. Частично эта проблема решается применением многорубежной идентификации, например, по карточке и по запоминаемому коду. Однако это только несколько усложняет задачу для нарушителя. В этом случае ему нужно, например, украсть карточку и узнать код, что конечно сложнее, но принципиально метод многорубежной идентификации не решает задачу защиты от подобных угроз.

Кардинальным решением этой задачи является биометрическая идентификация, которая более эффективна, так как опознание производится не по присвоенным человеку идентификационным признакам, а по физиологическим свойствам или особенностям самого человека.

Наряду с неоспоримыми преимуществами идентификации по биометрическому признаку, она обладает и недостатками. Основное отличие идентификации по биометрическому признаку от других состоит в том, что идентификация данного типа носит принципиально вероятностный характер. Для систем, использующих идентификацию по запоминаемому или вещественному коду, решение о допуске принимается детерминировано. Ошибки здесь возможны только при аппаратных неисправностях или программных сбоях. Для систем, использующих идентификацию по биометрическому признаку, решения принимаются на основе вероятностного характера полученной информации. В этом случае ошибки принятия решений неизбежны, и можно говорить только о снижении вероятности появления ошибок. Уровень этих ошибок будет являться критерием качества системы и, в общем случае, должен быть указан в руководстве по эксплуатации или, по крайней мере, известен пользователю системы на основании эмпирических данных. Этот критерий определяется двумя техническими характеристиками: вероятностью несанкционированного допуска (ошибка первого рода – FAR) и вероятностью ложного задержания (ошибка второго рода – FRR). Вероятность несанкционированного допуска – выраженное в процентах число допусков системой неавторизованных лиц. Вероятность ложного задержания – выраженное в процентах число отказов в допуске системой авторизованных пользователей. Очевидно, что величину этих ошибок хотелось бы уменьшить. Эти две характеристики можно изменять, уменьшая или увеличивая чувствительность анализирующих приборов. Однако, уменьшая таким способом одну величину, одновременно увеличиваем другую. В данной ситуации, безусловно, необходимо найти оптимальное значение, когда величина суммарных ошибок системы минимальна. Еще одним общим недостатком систем, использующих идентификацию по биометрическому признаку, является значительно более высокая сложность аппаратной составляющей системы (хранилища баз данных, биометрических считывателей, устройств позиционирования и т.д.). Сложность системы влечет за собой снижение ее надежности и повышение стоимости. Кроме того, у подавляющего числа людей возникает чисто психологический барьер при использовании идентификации по биометрическому признаку (от нежелания вносить свои биометрические параметры в базу данных, до страха процесса сканирования биометрического признака).

3 Идентификация по запоминаемому коду

3.1 Кодонаборные панели

Идентификация по запоминаемому коду осуществляется посредством ввода заведомо известного только пользователю кода (последовательность цифр или иных символов) на клавиатуре кодонаборной панели. Для ввода цифровой последовательности кода обычно используются кодонаборные панели с клавиатурой, содержащей десять цифровых клавиш и несколько служебных. Количество и расположение клавиш на панели варьируется в зависимости от их назначения и иных требований к исполнению (информативность, эстетические требования, и другие). Пример изображения кодонаборной панели приведен на рисунке 3.1.

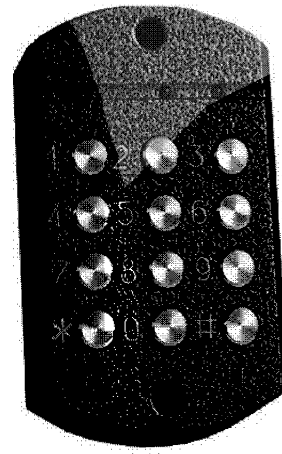
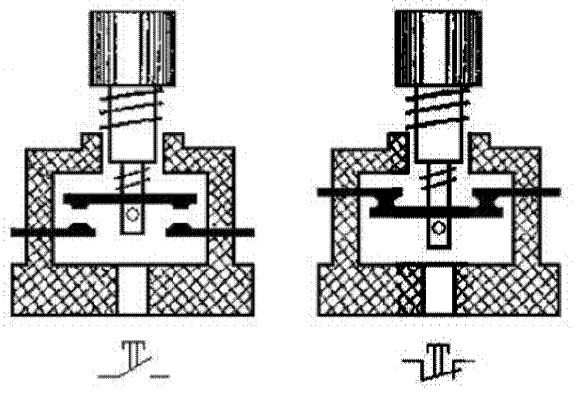


Рисунок 3.1 – Кодонаборная панель, предназначенная для ввода цифровой последовательности, в антивандальном исполнении

Ввод цифровой последовательности кода осуществляется посредством физического нажатия на клавиши или прикосновения к областям наборного поля. Клавиатуры различаются методом регистрации факта ввода необходимой цифры (символа). Наибольшее распространение получили механические, сенсорные и клавиатуры на оптопарах.

Принцип работы механической клавиатуры основан на механическом переключении (замыкании или размыкании) электрических контактов соответствующей клавиши при нажатии на нее. На рисунке 3.2 а) приведено изображение нормально разомкнутой клавиши механической клавиатуры, а на рисунке 3.2 б) нормально замкнутой клавиши.



а) *б)*

Рисунок 3.2

С целью повышения надежности электрического контакта токоведущих частей переключателей клавиш и уменьшения явления "дребезга", в его конструкцию может быть введен механизм быстрого переключения (см. рисунок 3.3).

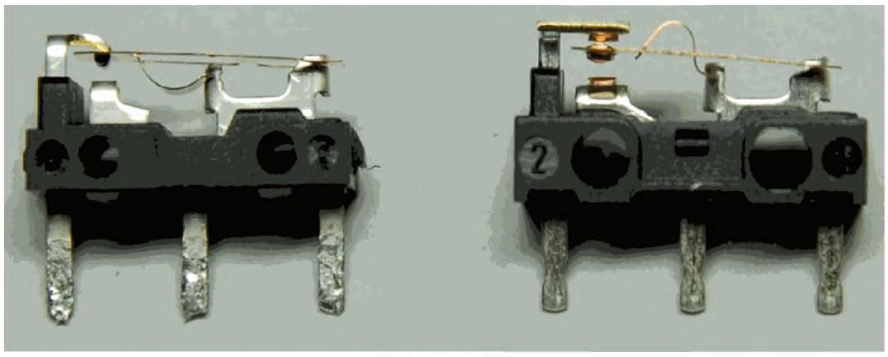


Рисунок 3.3

В составе клавиатуры несколько переключателей могут иметь электрическое соединение, выполненное по матричной схеме (см. рисунок 3.4). Данное схемотехническое решение позволяет сократить количество электрических проводников для передачи сигналов о нажатых клавишах от клавиатуры до исполнительного устройства.

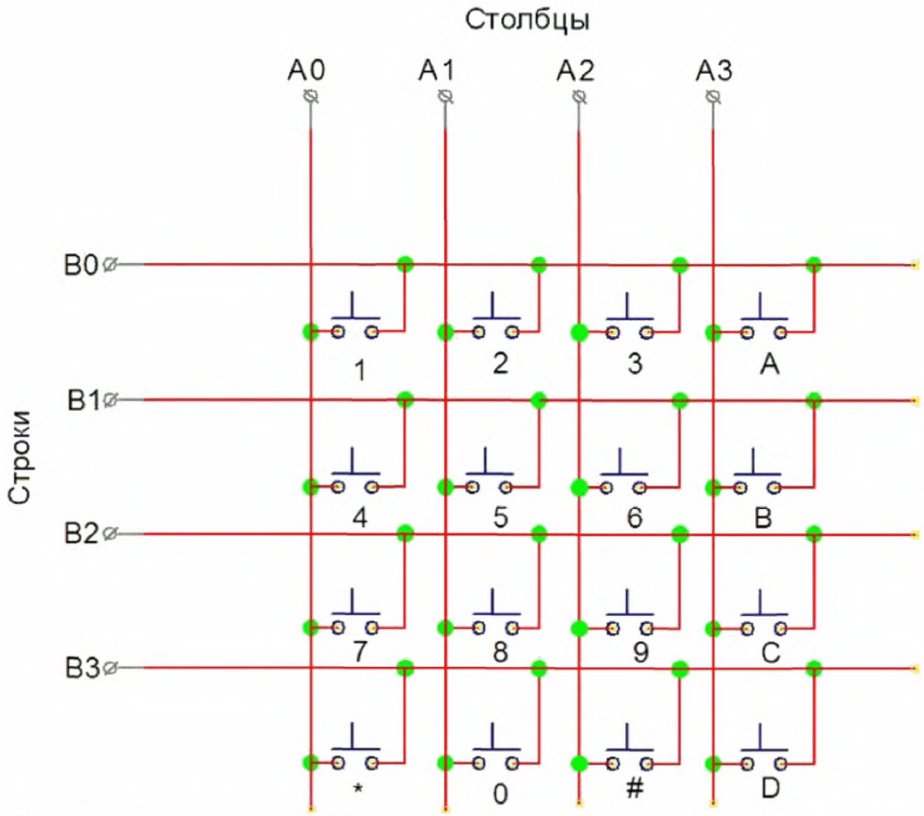


Рисунок 3.4 – Схема электрических соединений матричной клавиатуры

В независимости от конструктивного исполнения, наличие подвижных элементов конструкции и механически коммутируемых контактов переключателей в значительной мере ограничивает их рабочий ресурс.

Отсутствие необходимости внесения дополнительных конструктивных и схемотехнических решений для регистрации изменения состояния механических переключателей при нажатии на соответствующую клавишу, ввиду высокого сопротивления разомкнутых контактов

и низкого замкнутых, позволяют сопрягать клавиатуры данного типа с широким спектром исполнительных устройств.

В основе работы сенсорной клавиатуры лежит принцип регистрации изменения электрического потенциала электронной схемы ввиду изменения сопротивления или тока утечки на "землю" между неподвижными или малоподвижными областями клавиатуры, закрепленными за соответствующими цифрами (символами). Изображение сенсорной клавиатуры приведено на рисунке 3.5.

Рисунок 3.5

Наибольшее распространение получили клавиатуры на базе сенсоров с резистивным и емкостным методами регистрации касания. Резистивный метод регистрации касания заключается в отслеживании электронной схемой клавиатуры сопротивления между двумя токопроводящими слоями (см. рисунок 3.6).

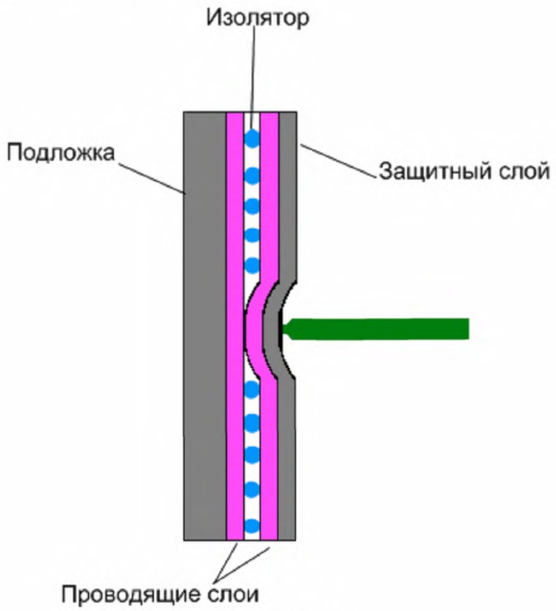


Рисунок 3.6

В исходном состоянии два проводящих слоя разделены слоем эластичного изолятора. При касании внешнего слоя происходит его упругая деформация, в результате которой слой эластичного изолятора продавливается и в точке касания между слоями возникает электрический контакт, регистрируемый электронной схемой.

Клавиатура может состоять либо из нескольких отдельных сенсоров, либо быть выполненной в виде единого модуля, в котором проводники двух проводящих слоев выполнены в виде взаимно перпендикулярных полос (горизонтальных на одном слое и вертикальных на другом), имеющих область пересечения, соответствующую области каждой цифры (символа) клавиатуры. Полосы также имеют электрическое соединение по матричной схеме.

Отсутствие механически подвижных элементов предполагает более долгий срок службы клавиатур, построенных на резистивных сенсорах, по сравнению с клавиатурами на механических переключателях.

Периодическая деформация в результате нажатий в процессе эксплуатации токопроводящего и изоляционного слоев ограничивает срок службы клавиатуры ввиду постепенной утраты упругости между этими слоями.

Ввиду относительно большого сопротивления между контактными областями резистивных сенсоров в замкнутом состоянии, сенсорные клавиатуры, как правило, выполнены в виде завершенного модуля, содержащего электрическую схему, обеспечивающую гарантию точного определения состояния каждого сенсора, и кодирующее устройство, выдающее сигналы во внешние электрические цепи.

Емкостный метод регистрации касания заключается в отслеживании электронной схемой клавиатуры области возникновения тока утечки на землю через емкость человеческого тела в месте касания пользователем емкостного сенсора (см. рисунок 3.7). Клавиатуры данного типа традиционно выполняются в виде единого модуля, содержащего электрическую схему преобразования сигналов, поступающих от сенсоров. В исходном состоянии на внешний электропроводящий слой подается электрический потенциал. Внутренний электропроводящий слой разделен на области в местах расположения отдельных клавиш (областей касания). При отсутствии касания какого-либо сенсора, электрический потенциал на всей площади внешнего электропроводящего слоя одинаков. Касание сенсора пользователем приводит к внесению в электрическую цепь емкости тела человека и передачи ему части электрического потенциала. Вследствие этого уменьшается потенциал внешнего слоя в месте касания и внутреннего электропроводящего слоя, составляющего с внешним слоем электрическую емкость. Это изменение потенциала на внутреннем слое регистрируется электрической схемой и выдается во внешние электрические цепи в виде электрических сигналов.

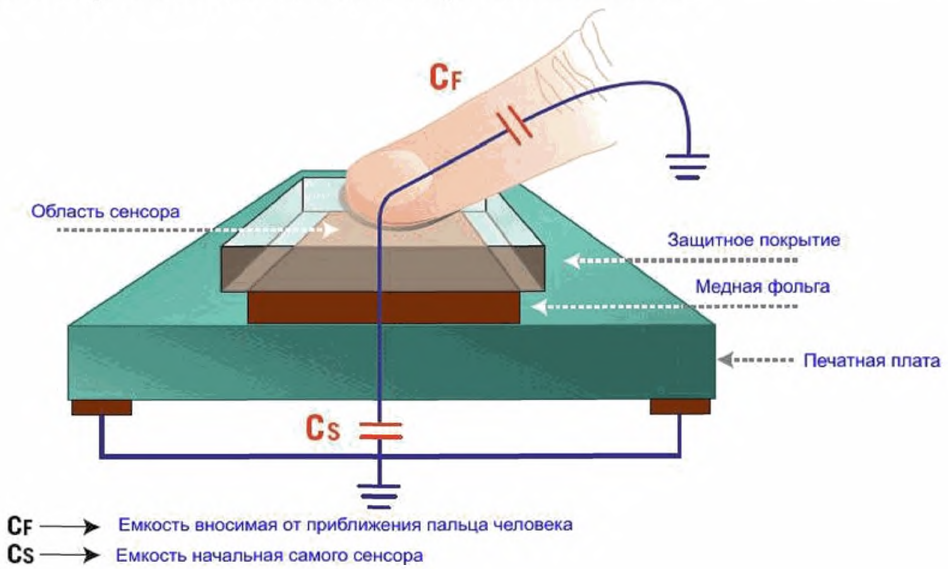


Рисунок 3.7

Отсутствие подвижных элементов в клавиатурах, построенных на базе емкостных сенсоров, повышает ее срок службы относительно механических переключателей с точки зрения механического износа.

Наличие открытых участков электрических цепей для передачи электрического потенциала, делает клавиатуру на базе емкостных сенсоров чувствительной к потенциалам статического напряжения тела человека и помехам, вызванным изменением управляющего электрического потенциала в результате увлажнения.

Для повышения вандалоустойчивости кодонаборных панелей используются методы регистрации ввода цифровой последовательности (касания кодонаборного поля), исключающие наличие в конструкции панели подвижных или механически уязвимых элементов. Наиболее распространенной является конструкция кодонаборного поля на оптопарах, использующих световые лучи инфракрасного диапазона, как более устойчивого к оптическим помехам, вызванным загрязнением (см. рисунок 3.8).

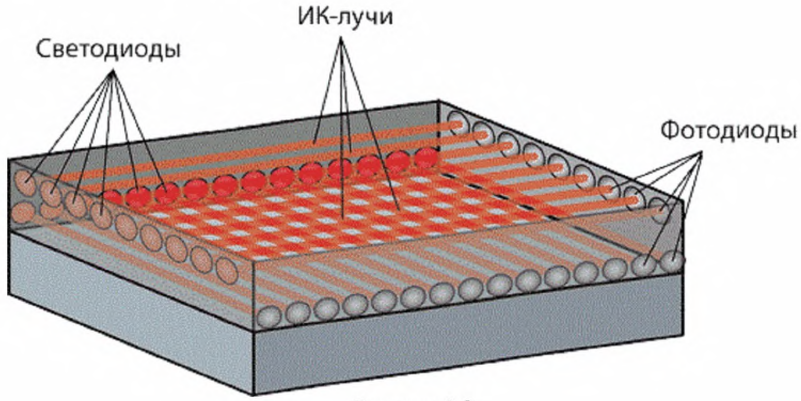


Рисунок 3.8

Символы кодонаборного поля нанесены на его заднюю стенку, не содержащую каких-либо электронных элементов или цепей. По периметру кодонаборной панели установлены свето- и фотодиоды, образующие оптопары. Каждая пара свето- и фотодиода устанавливается соответственно каждой строке и каждому столбцу кодонаборной панели так, что перед каждым символом образуется пересечение двух взаимно перпендикулярных световых лучей (см. рисунок 3.9).

Рисунок 3.9

При работе кодонаборной панели светодиоды излучают узконаправленные световые лучи, которые, при отсутствии касания областей символов, попадают на фотодиоды, формируя сигналы, обрабатываемые электрической схемой. При касании области символа пальцем или иным предметом происходит перекрытие двух лучей, пересекающихся над этой областью, вследствие чего они не попадают на соответствующие фотодиоды. Прерывание сигналов с двух фотодиодов позволяет электронной схеме произвести однозначную регистрацию факта касания области одного определенного символа и сформировать соответствующий сигнал во внешние цепи.

Наличие жестко закрепленных за определенными цифрами (символами) областей благоприятно сказывается на возможности определения цифр (символов), наиболее часто используемых в кодовых комбинациях, или их непосредственного наблюдения с целью последующего несанкционированного использования. Данное обстоятельство наиболее актуально для механических клавиатур, где наиболее часто используемым цифрам (символам) соответствуют клавиши с более выраженным механическим износом, загрязнением, или наоборот его отсутствием, по сравнению с остальными клавишами. Данное обстоятельство снижает имитостойкость метода идентификации по запоминаемому коду и позволяет подбор кодовой последовательности, ограниченной цифрами (символами), соответствующими наиболее часто используемым клавишам.

С целью исключения указанных факторов в устройстве идентификации по запоминаемому коду может быть введена визуальная обратная связь. Наличие в кодонаборном устройстве обратной визуальной связи позволяет пользователю при вводе кода обойтись всего одной клавишей. Изображение кодонаборной панели с обратной визуальной связью приведено на рисунке 3.10.

Рисунок 3.10

При проведении процедуры идентификации, устройство ввода кодовой последовательности псевдослучайным образом генерирует и по очереди выводит на дисплей цифры (символы). Для ввода кодовой последовательности необходимо производить нажатие клавиши в период индикации символа, соответствующего очередному символу требуемой кодовой последовательности.

Данный метод ввода кодовой последовательности исключает возможность определения кодовой последовательности по степени механического износа клавиш и затрудняет визуальное наблюдение вводимой кодовой последовательности.

К достоинствам метода идентификации при помощи использования кодонаборных панелей можно отнести:

1) Низкая стоимость модулей клавиатур, обладающих ограниченными функциональными возможностями и предназначенными исключительно для приема вводимой кодовой последовательности;

2) Возможность санкционированной дистанционной передачи кодовой последовательности;

3) Отсутствие затрат на изготовление, хранение и копирование идентификатора;

4) Отсутствие аналого-цифрового преобразования, способствующего возникновению ошибок при проведении процедуры идентификации (для кодонаборных панелей, обладающих ограниченными функциональными возможностями и предназначенными исключительно для приема вводимой кодовой последовательности).

К недостаткам метода идентификации при помощи использования кодонаборных панелей можно отнести:

1) Необходимость запоминания кодовой последовательности;

2) Возможность подбора или визуального наблюдения вводимой кодовой последовательности (за исключением идентификатора, использующего визуальную обратную связь);

3) Низкий рабочий ресурс (для клавиатур на механических переключателях и резистивных сенсорах);

4) Подверженность кодонаборных панелей, предназначенных для размещения на открытом воздухе, к внешним механическим и климатическим воздействиям.

Метод идентификации, основанный на применении кодонаборных панелей, аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования. Так как каждая система из "Списка технических средств..." имеет собственный протокол обмена данными, существуют трудности при сопряжении с ними кодонаборных панелей сторонних предприятий-изготовителей.

В настоящее время в "Списке технических средств..." представлены следующие системы и технические средства охраны, имеющие в своем составе, или имеющие возможность подключения кодонаборных панелей:

Автоматизированная система передачи извещений "Приток-А" (производство ООО "Охранное бюро Сократ", г. Иркутск)

– "Приток-А-КОП-01(8)";
– "Приток-А-КОП-01(16)";
– "Приток-А-КОП-02";
– "Приток-А-КОП-02.1";
– "Приток-А-КОП-02.2";
– "ППКОП 011-8-1-01К Приток-А-4(8)";
– "ППКОП 011-8-1-01К Приток-А-4(16)".

Автоматизированная система передачи извещений КЦНОП049-2/2/240/7680-1 "Альтаир" (производство ЗАО "ПК ЦНИТИ, г. Ногинск, Московская область; ОАО "Радий", г. Касли Челябинская область)

– "Набат ЛПП-2АК";
– УОО "А-401";
– УОО "А-402";
– УОО "А-801";
– УОО "А-802".

Автоматизированная система передачи извещений "Ахтуба" (производство "НПО Ахтуба-Плюс", г. Волжский, Волгоградская область)

– КВР.

Автоматизированная система передачи извещений "Юпитер" (производство ООО "Элеста", г. Санкт-Петербург)

– АК "Юпитер";
– УВС-ТМ;
– ППКОП "Юпитер 24к".

Автоматизированная система передачи извещений "Заря" (производство ЗАО "Риэлта", г. Санкт-Петербург)

– УОО "Заря – ГК-IP-МО"*;
– УОО "Заря – ГК-IP-М1"*;
– УОО "Заря – ГК-IP-М2"*;
– ППКО "Заря-ИО"*;
– ППКО "Заря-УО"*;
– ППКОП "Заря-УО-М1"*;
– ППКОП "Заря-УО-М2"*;
– ППКОП "Заря-УО-IP"*;
– ППКОП "Заря-УО-IP-GPRS"*;
* – имеется возможность подключения выносной кодонаборной панели "ВУПС-К".

Автоматизированная система передачи извещений «Лагуна» (производство ООО "КВАЗАР", г. Ногинск, Московская область)

– ППКО "Редут-NET-GSM";
– УО "Лагуна IP/GSM".

Автоматизированная система передачи извещений по радиоканалу "Иртыш-3Р" (производство ООО НТК "Интекс", г. Омск)

– "Иртыш-Ш1".

Автоматизи-рованная система передачи извещений по радиока-налу "Струна-5" (производство ЗАО НПФ "Интеграл+", г. Казань)

– "БПО-1";
– "БПО-2";
– "БПО-4";
– "ПУУ";
– "ПУ";
– "БРР".

ППКОП "Ладога-А" (производство ЗАО "Риэлта", г. Санкт-Петербург)

– "Ладога КВ-А" (2 исп.);
– "Ладога КВ-РК".

ППКОП01059-42/126-1 "Кодос А-20" (производство ОАО "Бауманн", г. Москва)

– ППК "КОДОС А-20";
– КОДОС "АКП".

Интегрированный комплекс технических средств охраны "Пахра" (производство ООО АСБ "Рекорд", г. Александров, Владимирская область)

– "СЛЗ".

Комплекс, состоящий из прибора приемно-контрольного охранно-пожарного и управления ППКОПУ 01059-1000-3 "Р-08" ("Рубеж-08") и его модификаций, программного обеспечения и дополнительного оборудования (производства ООО "СИГМА-ИС", г. Москва)

– "ПУО-02";
– "ПУО-03";
– "УСК-02К";
– "УСК-02КС".

Интегрированная система безопасности "Стрелец-Интеграл" (производство ЗАО "Аргус-Спектр", г. Санкт-Петербург)

– "ПС-И".

Интегрированная система охраны (ИСО) "Орион" (производство ЗАО НВП "Болид", г. Королев Московская область)

– "С2000";
– "С2000-К";
– "С2000-КС".

Система беспроводной охранно-пожарной сигнализации "Астра-Zитадель" (производство ЗАО НТЦ "ТЕКО", г. Казань)

– ППКОП "Астра-Z 812 М";

– ППКОП "Астра-Z 8945";

– ПКУ "Астра-814".

Устройство беспроводной охранно-пожарной сигнализации "Астра-РИ-М" (производство ЗАО НТЦ "ТЕКО", г. Казань)

– ППКОП "Астра-812";

– ППКОП "Астра-812М".

Внутриобъектовая радиосистема охранно-пожарной сигнализации "Стрелец" (производство ЗАО "Аргус-Спектр", г. Санкт-Петербург)

– "ПУ-Р";

– "ПУЛ-Р".

Система охранной сигнализации с функцией домофона СОС "Спрут-100" (производства ОАО "Радий", г. Касли Челябинская область)

– "Спрут-100";

– "Спрут-100М".

Прибор приемно-контрольный охранно-пожарный ППКОП 0312149-1024-1 «Форпост» производства ООО "Элтис-Техника", г. Санкт-Петербург).

Стоимость кодонаборных панелей варьируется в достаточно широком диапазоне и зависит от принципа работы, функциональных возможностей, эстетико-эргономических показателей, степени устойчивости к внешним воздействиям, популярность торговой марки предприятия-изготовителя. Так, по состоянию на 11.08.2015 г., цена кодонаборной панели модели "ПОЛИС 52" (производитель "Витек") составляет 1521,00 руб., цена кодонаборной панели марки TS-KBD-EM Metal (производитель "TANTOS") составляет 3804,00 руб., цена кодонаборной панели модели "SC-TP16" (производитель "Parsec") составляет 5894,00 руб.

(Материалы взяты с интернет-страницы http://kodsb.ru/skud/kod_panel).

4 Идентификация по вещественному коду

4.1 Идентификаторы с перфорационным кодированием

Идентификаторы с перфорационным кодированием обычно выполняются в виде ключей или брелоков. Специально выделенная область идентификатора предназначается для размещения сквозных отверстий (перфораций), количество и расположение которых определяет код идентификатора. Примеры идентификаторов с перфорационным кодированием, выполненных в виде ключа и карты приведены на рисунках 4.1 и 4.2 соответственно.

Рисунок 4.1 – Идентификатор с перфорационным кодированием, выполненный в виде ключа

Рисунок 4.2 – Идентификатор с перфорационным кодированием, выполненный в виде карты

Для чтения индивидуального кода чаще всего применяются считыватели, использующие оптический метод считывания. Вместе с тем, ранее существовали идентификаторы с перфорацией, код которых читался считывателями, использующими электромеханический метод считывания.

При использовании оптического метода считывания, над перфорированной областью идентификатора, помещенного в считыватель, размещается источник (источники) светового излучения (видимого или инфракрасного диапазона). Под перфорированной областью идентификатора размещаются приемники излучения (фотоэлементы), чувствительные к используемому диапазону светового излучения. Материал, из которого изготовлена перфорированная область идентификатора, полностью непрозрачен для применяемого диапазона светового излучения. На фотоэлементы считывателя, расположенные непосредственно под отверстиями перфорации идентификатора, световое излучение попадает, что позволяет считывателю распознать код идентификатора. Принцип оптического чтения кода идентификатора с перфорационным кодированием приведен на рисунке 4.3.

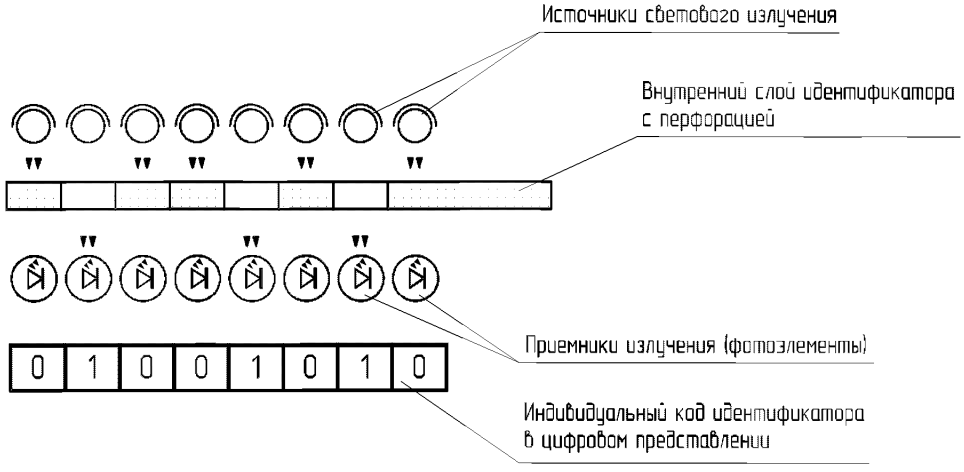


Рисунок 4.3

Применение инфракрасного диапазона светового излучения позволяет значительно повысить защищенность идентификатора от несанкционированного копирования. Достигается это за счет использования специальной трехслойной структуры перфорированной области идентификатора. Внешние слои идентификатора не имеют перфораций, являются прозрачными для инфракрасного диапазона светового излучения, но в то же время, полностью непрозрачными для видимого диапазона. Внутренний слой содержит перфорации и является полностью непрозрачным для инфракрасного диапазона. Наличие у идентификатора внешних непрозрачных для видимого диапазона светового излучения слоев исключает возможность "подсмотреть" или сфотографировать взаимное местоположение перфорационных отверстий. Принцип оптического чтения кода трехслойного идентификатора с перфорационным кодированием приведен на рисунке 4.4.

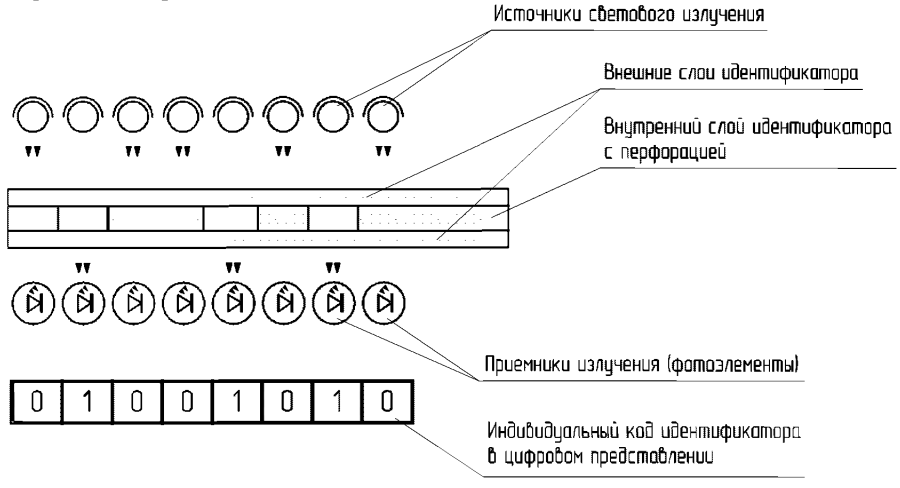


Рисунок 4.4

Принцип действия электромеханического метода считывания аналогичен оптическому методу, с той лишь разницей, что вместо светового излучения используются подпружиненные токопроводящие штыри, а вместо фотоэлементов – контактные площадки. Кроме того, материал из которого изготовлена перфорированная область идентификатора, является диэлектриком. Принцип электромеханического чтения кода идентификатора с перфорационным кодированием, приведен на рисунке 4.5.

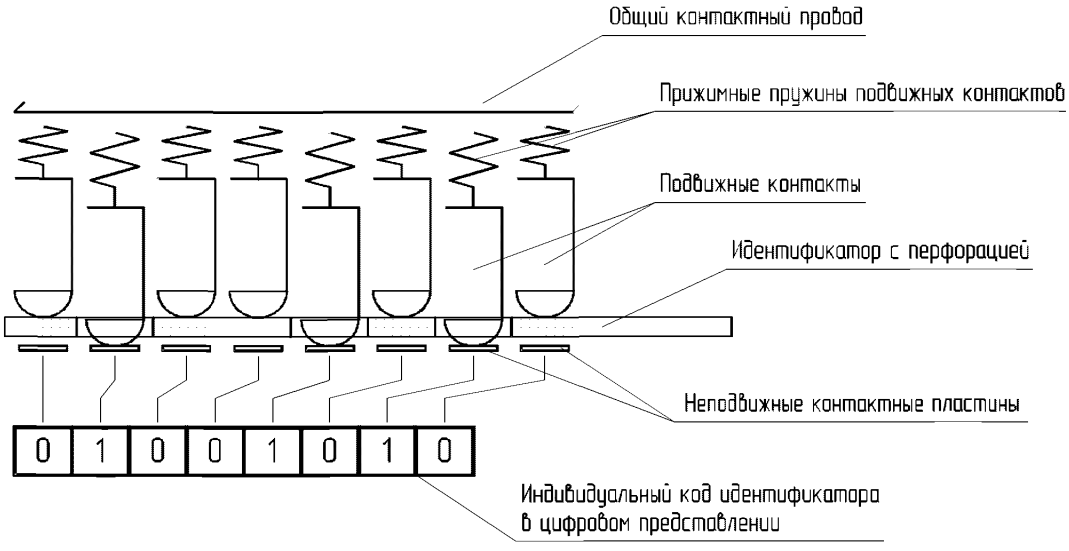


Рисунок 4.5

К достоинствам метода идентификации, использующего перфорационное кодирование можно отнести:

1) Простоту (а, следовательно, и дешевизну) изготовления идентификаторов;

2) Повышенную устойчивость к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);

3) Сравнительно небольшие массогабаритные характеристики идентификаторов.

К недостаткам метода, использующего перфорационное кодирование можно отнести:

1) Ограниченное число возможных комбинаций кодов, обусловленное соотношением геометрических параметров самого идентификатора и его перфорационных отверстий;

2) Механический контакт идентификатора со считывателем приводит к разрушению (истиранию) как самого идентификатора, так и считывателя, тем самым, ограничивая срок их службы;

3) Простоту изготовления идентификатора (с однослойной структурой перфорированной области) оборачивающуюся простотой его имитации;

4) Подверженность считывателей, предназначенных для размещения на открытом воздухе, к внешним механическим и климатическим воздействиям;

5) Перфорационные отверстия идентификатора (с однослойной структурой перфорированной области) подвержены загрязнению, что может привести к неправильному считыванию его кода.

Метод идентификации, основанный на применении перфорационного кодирования, потенциально совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но, в силу присущих ему недостатков, не отвечает требованиям, предъявляемым к техническим средствам охраны, стоящим на вооружении вневедомственной охраны МВД России.

В текущей редакции "Списка технических средств..." систем и технических средств, использующих метод идентификации, основанный на применении перфорационного кодирования, не представлено.

Сведений о наличии на Российском рынке технических средств охраны современных систем, использующих метод перфорационного кодирования, в открытых источниках не представлено, в связи с чем не представляется возможным приведение ценовых показателей.

4.2 Идентификаторы со встроенными пассивными радиоэлементами или магнитом

Идентификаторы данного типа изготавливаются в виде ключей (см. рисунок 4.6) или брелоков (см. рисунок 4.7). Корпус идентификаторов выполняется из диэлектрического материала (как правило, из пластмасс). Внутрь корпуса помещается пассивный радиоэлемент (чаще всего резистор) или магнит. Значение электрического параметра пассивного элемента (или магнита) идентификатора является его кодом. В случае использования пассивных радиоэлементов на корпус идентификатора выводятся электрически соединенные с ними контактные площадки. При использовании магнита контактные площадки не требуются.

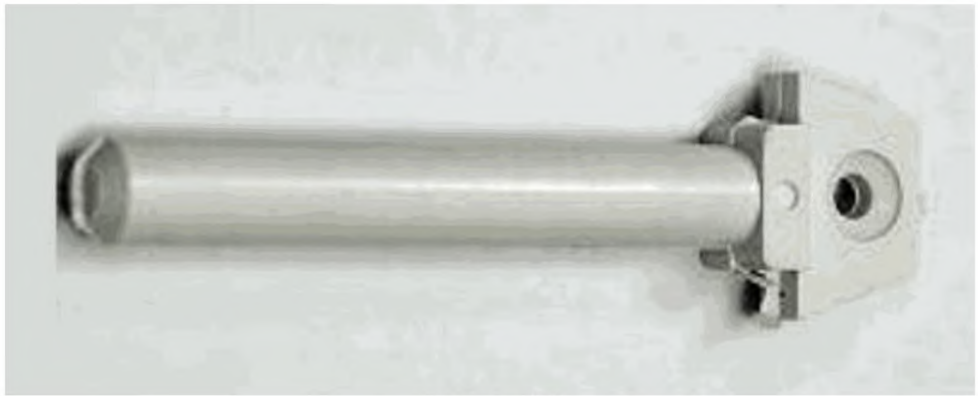


Рисунок 4.6

Рисунок 4.7

Для чтения кода идентификаторов со встроенными пассивными элементами применяются считыватели, использующие электро-контактный метод считывания.

Контактные площадки идентификатора, помещенного в считыватель, обеспечивают электрическое подключение пассивного радиоэлемента идентификатора в измерительную цепь считывателя. Считыватель производит измерение электрического параметра пассивного элемента и сравнивает его значения со значением (значениями), хранящимся в его памяти. Наряду с резистором в качестве пассивного радиоэлемента считывателя могут применяться конденсаторы, диоды и др., а так же их сочетание. В простейшем случае, вместо пассивного радиоэлемента используется электропроводная вставка. Принцип чтения кода идентификатора со встроенными пассивными радиоэлементами приведен на рисунке 4.8.

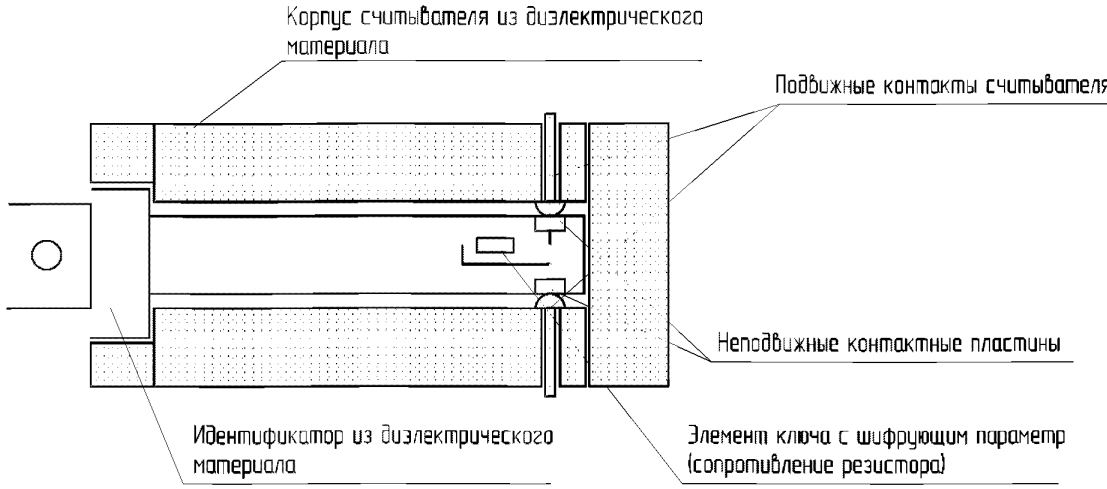


Рисунок 4.8

Для чтения кода идентификаторов со встроенным магнитом применяются считыватели, использующие магнито-контактный метод считывания. Магнитное поле (встроенного магнита) идентификатора, помещенного в считыватель, воздействует на чувствительный к магнитному полю элемент – геркон (герметичный контакт), тем самым, изменяя параметры электрических цепей считывателя. Принцип чтения кода идентификатора со встроенным магнитом приведен на рисунке 4.9.

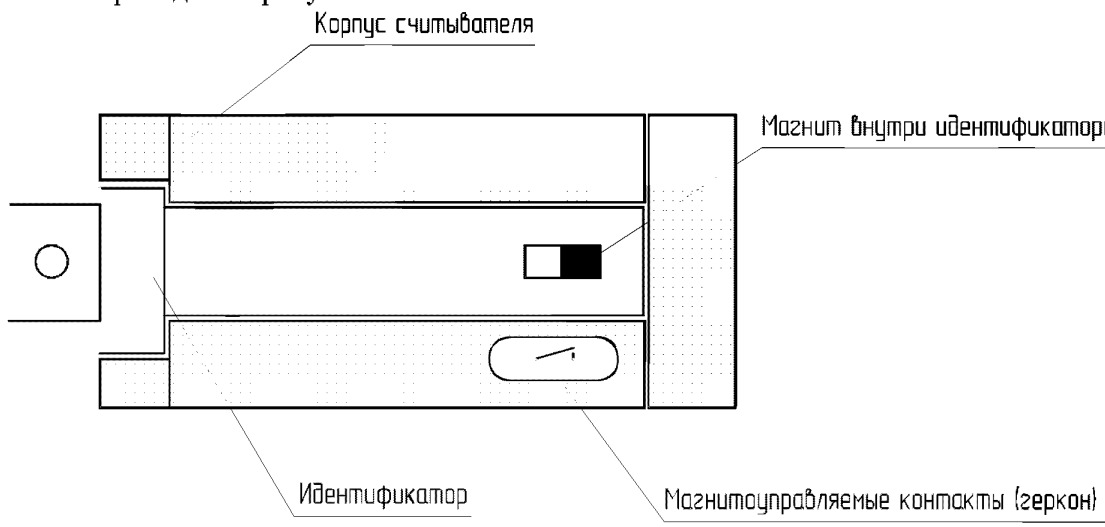


Рисунок 4.9

К достоинствам метода идентификации, использующие встроенные в идентификатор пассивные радиоэлементы или магниты, можно отнести:

1) Относительную простоту (а, следовательно, и дешевизну) изготовления идентификатора;

2) Устойчивость к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);

3) Сравнительно небольшие массогабаритные характеристики идентификатора;

4) Простота технической реализации процесса считывания кода идентификатора считывателем.

К недостаткам метода идентификации, использующего встроенные в идентификатор пассивные радиоэлементы или магниты, можно отнести:

1) Единый для всех идентификаторов код, либо сильно ограниченное число возмож-

ных комбинаций кодов у идентификаторов, используемых в одной системе;

2) Механический контакт идентификатора со считывателем приводит к разрушению (истиранию) как самого идентификатора, так и считывателя, тем самым, ограничивая срок их службы;

3) Подверженность считывателей, предназначенных для размещения на открытом воздухе, к внешним механическим и климатическим воздействиям;

4) Контактные площадки идентификатора и считывателя подвержены загрязнению и окислению, что может привести к невозможности считывания кода, либо к неправильному распознаванию кода;

5) Технические параметры пассивных радиоэлементов и магнитов со временем или под действием нестабильности условий внешней среды могут изменяться, таким образом, что при их измерении считывателем, может повлечь к неправильному распознаванию кода;

6) Использование в идентификаторе пассивных радиоэлементов с нестабильными характеристиками резко снижает имитостойкость.

Метод идентификации, основанный на применении пассивных радиоэлементов или магнитов, потенциально совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, однако, как и метод идентификации, основанный на применении перфорационного кодирования, не отвечает требованиям, предъявляемым к техническим средствам охраны, стоящим на вооружении вневедомственной охраны МВД России.

В текущей редакции "Списка технических средств..." систем и технических средств, использующих метод идентификации, основанный на применении пассивных радиоэлементов или магнитов, не представлено.

Метод идентификации, основанный на применении пассивных радиоэлементов или магнитов, был широко распространен в домофонах первого поколения, в настоящее время снятых с производства по причине морального устаревания.

Сведений о наличии на Российском рынке технических средств охраны современных систем, использующих метод идентификации, основанный на применении пассивных радиоэлементов или магнитов, в открытых источниках не представлено, в связи с чем не представляется возможным приведение ценовых показателей.

4.3 Идентификационные карты с линейным и двухмерным штриховым кодированием

Линейный штриховой код представляет собой нанесенный на поверхность идентификационной карты рисунок, содержащий последовательность параллельных линий, отличающихся цветом и шириной. Количество, ширина и взаимное расположение полосок определяют код идентификационной карты. Пример изображения элементов линейного штрихового кодирования приведен на рисунке 4.10. В настоящее время разработано множество типов линейного штрихового кодирования, наиболее распространенными из которых являются: EAN (EAN-8 состоит из 8 цифр, EAN-13 состоит из 13 цифр), UPC (UPC-A, UPC-E), Code56, Code128 (UPC/EAN-128), Codabar, "Interleaved 2 of 5".

Рисунок 4.10

Двухмерные штриховые коды были разработаны для кодирования большого объема информации. Расшифровка такого кода проводится в двух измерениях (по горизонтали и по вертикали).

Двухмерные штриховые коды подразделяются на многоуровневые – stacked (см. рисунок 4.11) и матричные – matrix (см. рисунок 4.12). Многоуровневые штриховые коды появились исторически ранее, и представляют собой поставленные друг на друга несколько обычных линейных штриховых кодов. Матричные же коды более плотно упаковывают информационные элементы по вертикали.

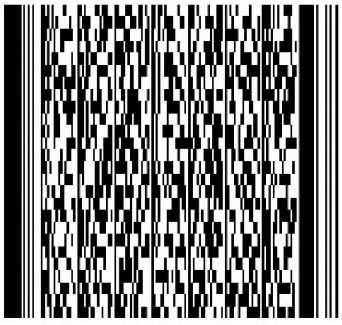


Рисунок 4.11

Рисунок 4.12

В настоящее время разработано множество двумерных штриховых кодов, применяемых с той или иной широтой распространения, наиболее распространенными из которых являются: Aztec Code, Data Matrix, MaxiCode, PDF417, QR код, Microsoft Tag.

Пример изображения идентификационной карты с линейным штриховым кодированием приведен на рисунке 4.13.

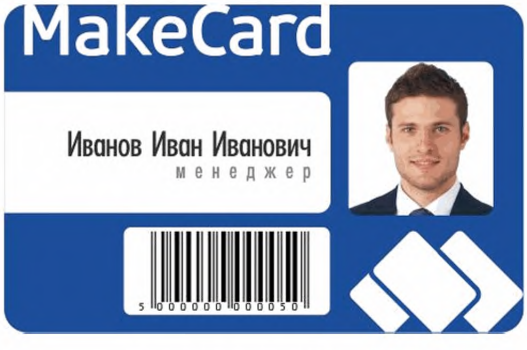


Рисунок 4.13

Для чтения кода идентификационных карт со штриховым кодированием применяются считыватели, использующие оптический метод считывания.

Большинство типов считывателей способно считывать код идентификационной карты дистанционно (при поднесении ее к оптическому устройству), вместе с тем, при использовании некоторых типов считывателей, перед чтением индивидуального кода идентификационной карты требуется осуществить ее позиционирование.

Для повышения защищенности от несанкционированного копирования идентификационных карт со штриховым кодированием используются специальные непрозрачные покрытия. Чтение кода в этом случае производится в инфракрасном оптическом диапазоне. Из всех идентификационных карт со штриховым кодированием наибольшей степенью защиты обладают карты со скрытым штриховым кодом. Невидимый для глаз штриховой код впечатывается в основу карты и считывается с помощью излучения в инфракрасном оптическом диапазоне. Индивидуальный код образуется за счет конфигурации теней при прохождении инфракрасного излучения через карту.

К достоинствам метода идентификации, использующего линейное и двухмерное штриховое кодирование, можно отнести:

1) Простоту изготовления идентификационной карты;

2) Сравнительно высокую устойчивость к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация).

3) Большой объем кодируемой информации (для карт с двухмерным кодированием) позволяет обеспечить значительное число возможных комбинаций кодов.

К недостаткам метода идентификации, использующего линейное и двухмерное штриховое кодирование, можно отнести:

1) Легкость повторения идентификационного признака при имитации идентификационной карты;

2) Поверхность идентификационной карты подвержена загрязнению и истиранию, что может сказаться на правильности считывания ее кода.

3) Механический контакт идентификационной карты со считывателем (при позиционировании) приводит к разрушению (истиранию) как самой идентификационной карты, так и считывателя, тем самым, ограничивая срок их службы;

4) Непродолжительный срок службы, составляющий от 18 до 30 месяцев;

5) Оптическая система считывателя требует бережного обращения и квалифицированного обслуживания.

Метод идентификации, основанный на применении идентификационных карт с линейным и двухмерным штриховым кодированием, аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но, как и в случае кодонаборных панелей, для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В текущей редакции "Списка технических средств..." систем и технических средств, использующих метод идентификации, основанный на применении идентификационных карт с линейным и двухмерным штриховым кодированием, не представлено.

Стоимость идентификационных карт с линейным и двухмерным штриховым кодированием зависит от закупаемой партии, используемых для изготовления карт материалов, наличия дополнительных функций. По состоянию на 11.08.2015 г. цена идентификационной карты с линейным (двухмерным) штриховым кодированием (габаритные размеры 86×54×0,76 мм, производитель "MyCard") составляет 6,20 руб. (при тираже от 5000 шт.) и 18,00 руб. (при тираже от 100 шт.).

(Материалы взяты с интернет-страницы http://mycard.su).

В зависимости от особенностей исполнения корпуса, считыватели штрихового кода могут иметь исполнение для ручного удержания или стационарного размещения. По состоя-

нию на 11.08.2015 г. цена ручного светодиодного сканера штриховых кодов "Zebex Z-3080" (производитель "Zebex") составляет 3430,00 руб., цена ручного светодиодного сканера штрих кодов марки "Proton ICS-7100" (производитель "Proton") составляет 4350,00 руб., цена ручного светодиодного сканера штрих кодов марки "Argox AS-8312" (производитель "Argox") составляет 7288,00 руб. Цена ручного лазерного сканера модели "XL-6000" (производитель "XL-6000") составляет 2490,00 руб., цена ручного лазерного сканера штриховых кодов модели "Motorola LS-1203" (производитель "Motorola") составляет 6901,00 руб., цена ручного лазерного сканера штриховых кодов марки "Opticon OPR-3001" (производитель "Opticon") составляет 12190,00 руб. Цена стационарного сканера штриховых кодов марки "CINO FM480" (производитель "CINO") составляет 9610,00 руб., цена стационарного сканера штриховых кодов марки "Metrologic MS7120 Orbit" (производитель "Honeywell (Metrologic)") составляет 18188,00 руб., цена стационарного сканера штриховых кодов марки "Metrologic MS7625 Horizon" (производитель "Honeywell (Metrologic)") составляет 30507,00 руб. Цена сканера двухмерных штриховых кодов марки "Motorola DS 4208" (производитель "Motorola") составляет 9490,00 руб., цена сканера двухмерных штриховых кодов марки "Metrologic MS1690 Focus" (производитель "Honeywell (Metrologic)") составляет 12370,00 руб., цена сканера двухмерных штриховых кодов марки "Motorola DS-6707" (производитель "Motorola") составляет 26666,00 руб.

(Материалы взяты с интернет-страницы http://www.pos-shop.ru).

4.4 Идентификационные карты с магнитным кодированием

Идентификационные карты с магнитным кодированием (магнитной полосой) достаточно широко используются в банковских и кредитных системах. До недавнего времени наиболее массовое применение они находили в системах контроля и управления доступом.

Идентификационная карта с магнитной полосой состоит из пластикового основания прямоугольной формы, на верхнюю поверхность которого нанесена чувствительная к магнитному полю полоса (магнитная полоса), способная хранить записанную на нее информацию на протяжении продолжительного времени. Помимо магнитной полосы, в качестве вспомогательной информации, на идентификационной карте могут быть нанесены текст, последовательность цифр, знаки, фотографии и т.п. Пример изображения идентификационной карты с магнитной полосой приведен на рисунке 4.14.

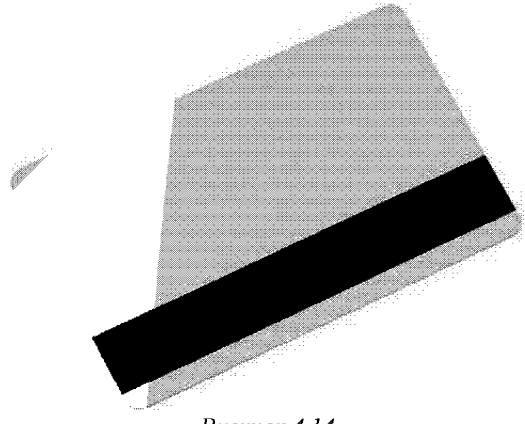


Рисунок 4.14

Для чтения (записи) кода идентификационной карты с магнитной полосой применяются считыватели, использующие магнитно-контактный метод считывания. Чтение индивидуального кода производится при протягивании магнитной полосы идентификационной карты по магнитной головке считывателя. Для надежного чтения кода должно быть обеспечено плотное прилегание магнитной полосы к магнитной головке считывателя.

В последнее время ведутся разработки новых технологий, позволяющих улучшить свойства идентификационных карт с магнитной полосой. Например, идентификационная карта "Watemark Magnetics" состоит из организованной структуры слоев оксида, которые размещаются в виде двух полос разной ширины, при этом толщина каждой из полос не превышает три четверти миллиметра. Изготовление таких полос может производиться только в производственных условиях, в результате каждая идентификационная карта имеет уникальный шестнадцатеричный индивидуальный код размером до 12 знаков. Индивидуальный код идентификационной карты "Watemark Magnetics" не может быть ни разрушен, ни изменен никаким внешним магнитным полем. Среди идентификационных карт с магнитной полосой, карта "Watermark Magnetics" является одной из наиболее имитостойких и защищенных от несанкционированного копирования.

К достоинствам метода идентификации при помощи использования идентификационных карт с магнитным кодированием можно отнести:

1) Сравнительную дешевизну изготовления идентификаторов;

2) Возможность многократной перезаписи индивидуального кода способствует повышению имитостойкость идентификационной карты и увеличению срока ее использования;

3) Простота процесса перезаписи кода позволяет в случае необходимости оперативно его поменять;

4) Совместимость алгоритмов кодирования идентификационных карт с магнитной полосой делает возможным использование уже имеющихся у пользователя карт (например, банковских) для применения их в системе централизованного наблюдения;

5) Большой объем кодируемой информации позволяет обеспечить значительное число возможных комбинаций кодов;

6) Высокая имитостойкость и устойчивость к несанкционированному копированию идентификационных карт "Watemark Magnetics", обеспечиваемые особенностями технологии ее производства;

К недостаткам метода идентификации при помощи использования идентификационных карт с магнитным кодированием можно отнести:

1) Магнитно-контактный метод считывания приводит к износу как идентификационной карты, так и магнитной головки считывателя, тем самым ограничивая срок их службы;

2) Непродолжительный срок службы, составляющий от 12 до 18 месяцев;

3) Низкую устойчивость идентификационных карт (кроме карт "Watemark Magnetics") к воздействию внешнего магнитного поля, что может привести к повреждению (уничтожению) кода;

4) Низкую устойчивость идентификационных карт (кроме карт "Watemark Magnetics") к несанкционированному копированию (при наличии у злоумышленников необходимых знаний и относительно несложного оборудования);

5) Магнитная головка считывателя подвержена загрязнению, что может привести к неправильному чтению индивидуального кода идентификационной карты, и требует постоянного квалифицированного обслуживания;

6) Пользователь должен иметь навык, необходимый для правильного обращения с идентификационной картой и считывателем.

Метод идентификации, основанный на применении идентификационных карт с магнитным кодированием, может работать совместно с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием; как и в случае с кодона борными панелями, для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В текущей редакции "Списка технических средств..." систем и технических средств, использующих метод идентификации, основанный на применении идентификационных карт с магнитным кодированием, не представлено.

Стоимость идентификационных карт с магнитным кодированием, как и карт с линейным и двухмерным штриховым кодированием, зависит от закупаемой партии, используемых для изготовления карт материалов, наличия дополнительных функций. По состоянию

на 11.08.2015 г. цена идентификационной карты с магнитным кодированием стандартными габаритными размерами 86×54×0,76 мм (производитель "PartnerCard") зависит от тиража и составляет 4,00 руб. (при тираже от 10000 шт.) и 10,00 руб. (при тираже от 100 шт.) Цена щелевого считывателя идентификационных карт с магнитным кодированием модели "Champtek MR 312" (производитель "Champtek") составляет 5095,00 руб., цена щелевого считывателя идентификационных карт с магнитным кодированием модели "Cipher 1023-123" (производитель "Cipher") составляет 7095,00 руб., цена щелевого считывателя идентификационных карт с магнитным кодированием модели "MSR Mini 400" (производитель "MSR") составляет 17350,00 руб.

(Информация взята с интернет-страниц http://partner-card.ru, http://www.scancode.ru).

4.5 Идентификационные карты Виганда (Wiegand)

Данная технология идентификационных карт была разработана для создания карт, не чувствительных к внешним магнитным полям. Она основана на физическом эффекте, обнаруженным в 1975 году американским исследователем Джоном Вигандом. (John R. Weigand). Действие этого эффекта проявляется в том, что при движении сверхкоротких металлических проводников, строго определенного состава, в магнитном поле возникает индукционный отклик в катушке считывателя.

В структуру пластиковой карты при производстве впрессовываются полоски проводников, расположенных в строго определенной последовательности (различной для разных карт), которая и определяет индивидуальный код карты. Изображение идентификационной карты Виганда приведено на рисунке 4.15.

Рисунок 4.15

Считыватель карты Виганда представляет собой индукционную катушку с двумя магнитами противоположной полярности. При движении идентификационной карты в магнитном поле в индукционной катушке возникают выбросы тока, которые воспринимаются схемой считывателя. Причем индукционная катушка и магниты находятся в пластиковом или металлическом корпусе и для полной герметичности залиты специальным изоляционным материалом, а считывание не требует плотного контакта. Изображение считывателя идентификационной карты Виганда приведено на 4.16.

Рисунок 4.16

К достоинствам метода идентификации при помощи использования идентификационных карт Виганда можно отнести:

1) Высокую надежность идентификационных карт вследствие простоты их конструкции;

2) Высочайшую степень защиты от несанкционированного копирования (копирование не возможно) вследствие использования засекреченной технологии изготовления;

3) Высокую устойчивость к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);

4) Отсутствие плотного контакта идентификационной карты со считывателем при чтении индивидуального кода, что минимизирует их износ.

К недостаткам метода идентификации при помощи использования идентификационных карт Виганда можно отнести:

1) Высокую стоимость идентификационных карт и считывателей;

2) Узкий круг производителей не может гарантировать стабильность поставки идентификационных карт вне зависимости от экономической и политической ситуации в мире;

3) Необходимость поднесения идентификационной карты для считывания ее кода к считывателю.

Метод идентификации, основанный на применении идентификационных карт Виганда, может найти применение в совместной работе с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но, как и в предыдущих случаях, потребуется обеспечить совместимость с протоколом обмена данными объектового оборудования.

В текущей редакции "Списка технических средств..." систем и технических средств, использующих метод идентификации, основанный на применении идентификационных карт Виганда, не представлено.

Стоимость идентификационных карт Виганда, главным образом, определяется уникальностью технологии их производства, кроме того, она зависит от закупаемой партии и наличия дополнительных функций. По состоянию на 11.08.2015 г. цена идентификационной карты Виганда марки "HID SensorCard ISO" (производитель "HID") составляет 374,00 руб., цена идентификационной карты Виганда марки "HID SensorCard II" (производитель "HID") составляет 411,00 руб., цена идентификационной карты Виганда марки "HID SensorCard Extra Duty" (производитель "HID") составляет 433,00 руб. Цена считывателя карт Виганда модели "HID Classic Swipe" (производитель "HID") составляет 40788,00 руб., цена считывателя карт Виганда модели "HID Epic" (производитель "HID") составляет 43749,00 руб., цена встроенного считывателя карт Виганда модели "HID Insertion" (производитель "HID") составляет 48683,00 руб.

(Информация взята с интернет-страниц http://www.kvantum.spb.ru, http://videoglaz.ru).

4.6 Идентификационные карты с оптической памятью

Идентификационная карта с оптической памятью состоит из пластикового основания прямоугольной формы, на верхней поверхности которого имеется область, предназначенная для записи/чтения данных (включая код идентификационной карты) оптическим методом. Изображение идентификационной карты с оптической памятью и ее считывателя приведено на рисунке 4.17.

Рисунок 4.17

Способ записи (чтения) данных для идентификационных карт такого типа схож со способом, применяемым для записи данных на оптические CD-диски. Чтение считывателем индивидуального кода карты производится при помощи установленного в нем лазера. Современная технология обеспечивает очень высокую плотность записи, поэтому объем памяти идентификационных карт такого типа исчисляется мегабайтами. Это позволяет хранить не только буквенно-цифровые данные, но и видео (аудио) файлы.

К достоинствам метода идентификации при помощи использования идентификационных карт с оптической памятью можно отнести:

1) Относительно невысокую стоимость изготовления идентификационных карт;

2) Высокую устойчивость к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация).

3) Большой объем памяти данных, записываемых на идентификационную карту, позволяет использовать многоразрядные коды, что значительно увеличивает число комбинаций кодов;

4) Большой объем памяти данных позволяет записывать на идентификационную карту не только ее код, но и разнообразную дополнительную информацию о пользователе – носителе идентификатора (личная фотография, образец подписи и т.п.);

5) Высокие имитостойкость и степень защищенности от несанкционированного копирования, обеспечиваемые особенностями технологии ее изготовления.

К недостаткам метода идентификации при помощи использования идентификационных карт с оптической памятью можно отнести:

1) Критичность идентификационной карты к прозрачности защитного слоя области данных, загрязнение или повреждение которого могут привести к невозможности считывания кода и прочих данных с карты;

2) Оптическая система считывателя (особенно лазерного) требует бережного отношения, чувствительна к загрязнению, требует квалифицированного обслуживания;

3) Однократность, либо ограниченное число процедур перезаписи индивидуального кода идентификационной карты;

4) Сравнительно высокую стоимость считывателя.

Метод идентификации, основанный на применении идентификационных карт с оптической памятью, аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования, как и в предыдущих случаях, требуется совместимость с протоколом обмена данными объектового оборудования.

В текущей редакции "Списка технических средств..." систем и технических средств, использующих метод идентификации, основанный на применении идентификационных карт с оптической памятью, не представлено.

В настоящее время идентификационные карты с оптической памятью представлены крайне ограниченным рядом предприятий изготовителей, ведущим из которых является "LaserCard".

Стоимость идентификационных карт с оптической памятью, определяется преимущественно устойчивостью материала карты к внешним механическим и иного рода воздействиям, а также от закупаемой партии и наличия дополнительных функций. По состоянию на 11.08.2015 г. цена идентификационной карты с оптической памятью стандартных габаритных размеров предприятия-изготовителя "LaserCard" зависит от тиража, объема памяти, вида печати, и составляет от 52,00 руб. (для карт объемом памяти 1,1 Мбайт при тираже от 1000 шт.), и 247,00 руб (для карт объемом памяти 2,8 Мбайт при тираже 5000 шт.).

Цена считывателя карт с оптической памятью марки " Intermec LaserCards Mercury 600Q Optical Memory Card Reader Writer" (предприятие-изготовитель "LaserCard") составляет 8040,00 руб.

(Материалы взяты с интернет-страниц http://by.inttorg.ru).

4.7 Электронные ключи iButton (Touch-Memory)

Технология

Электронный ключ iButton – это микросхема, заключённая в круглый герметичный корпус диаметром 16,3 мм, выполненный из нержавеющей стали. Прочный корпус обладает повышенной устойчивостью к воздействию различных внешних неблагоприятных факторов. Диаметр iButton MicroCan (название стандарта корпуса) составляет 16,3 мм. Корпус имеет два исполнения, отличающихся по толщине: 3,1 мм (версия F3) и 5,89 мм (версия F5). На рисунках 4.18 и 4.19 представлены чертежи корпусов обеих версий.

Поскольку крышки у всех версий одинаковы, то для всех применяется одна и та же считывающая чашка. Кромка корпуса MicroCan позволяет удобно его закреплять в держателях разнообразной конструкции. Примеры различных держателей ключа iButton приведены на рисунках 4.20 – 4.22.

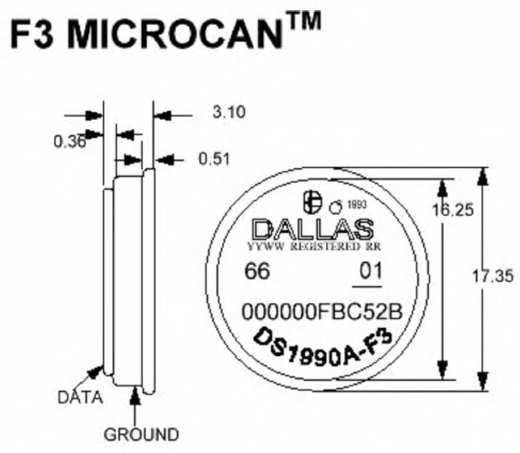


Рисунок 4.18 – Чертеж ключа iButton исполнения версии F3

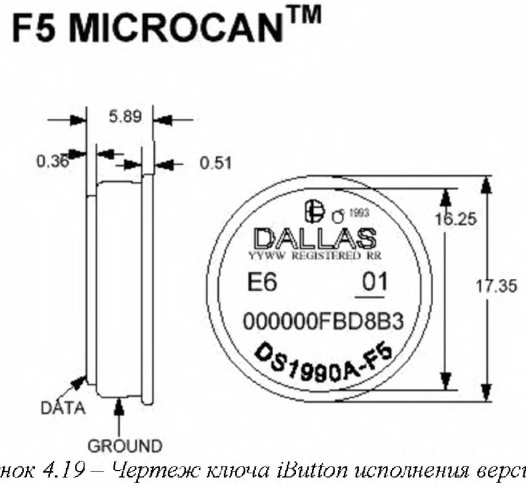


Рисунок 4.19 – Чертеж ключа iButton исполнения версии F5

Рисунок 4.20 – Держатель ключа iButton, выполненный в виде брелока

Рисунок 4.21 – Держатель ключа iButton, объединенный с механическим ключом

Рисунок 4.22 – Держатель ключа iButton, выполненный в виде перстня

Корпус состоит из двух электрически изолированных друг от друга частей, являющихся контактами, через которые микросхема соединяется со считывателем. Таким образом, получается очень недорогой (в смысле использования аппаратных ресурсов считывающей аппаратуры) и надёжный интерфейс – один провод данных и один общий провод. Энергия, необходимая для обмена информацией и работы микросхемы в корпусе, берётся от провода данных. На рисунке 4.23 приведена схема внутреннего устройства ключа iButton.

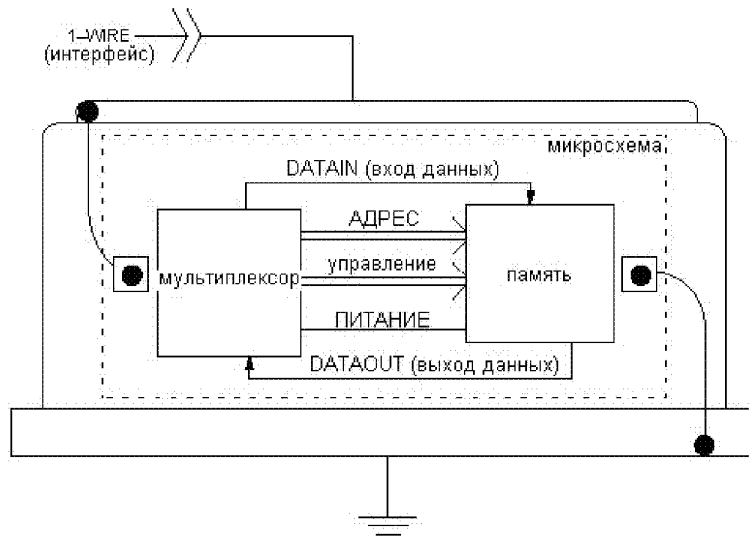


Рисунок 4.23

Внутренняя микросхема изготовлена по технологии CMOS (КМОП), и в состоянии ожидания основной ток потребления – только ток утечки (который для CMOS очень мал), что позволяет использовать для хранения перезаписываемых данных внутри iButton собственный маломощный элемент питания. Для сохранения энергопотребления на предельно низком уровне во время состояний активности (чтение данных, например), а также для совместимости с существующими сериями микросхем логики и микропроцессорами, линия данных в iButton выполнена как в выход с открытым стоком (см. рисунок. 4.24).

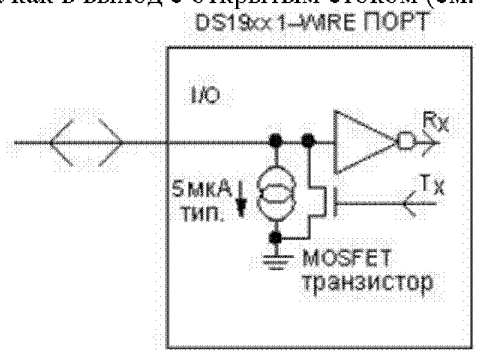


Рисунок 4.24

Для нормальной работы с внешней логикой типа CMOS нужен только нагрузочный резистор 5 кОм, подсоединённый к плюсу питания VDD (5 В) и к выходу обычного двунаправленного порта с открытым стоком (см. рисунок 4.25).

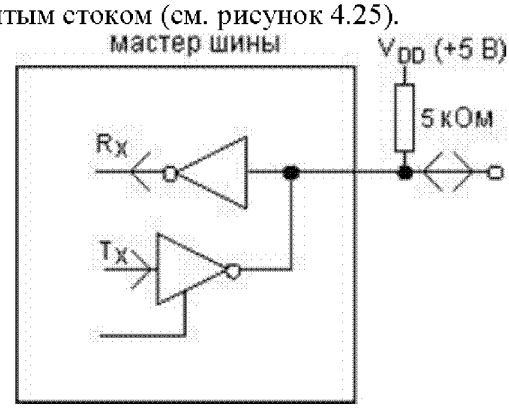


Рисунок 4.25

Если вход и выход процессора используют разные выводы, то их подключают, как показано на рисунке 4.26. Выход, подключенный на рисунке к базе транзистора, должен быть обычным двухтактным, либо с внутренним нагрузочным резистором.

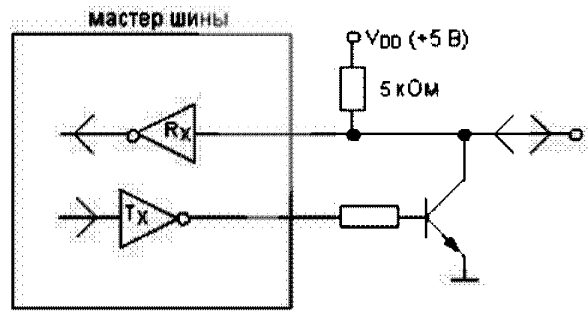


Рисунок 4.26

Протокол

Для простого аппаратного исполнения iButton, описанного выше, используется специальный, оптимизированный протокол, позволяющий осуществлять двунаправленный обмен данными. Протокол носит название 1-Wire. Последовательная передача осуществляется в полудуплексном режиме (т. е. либо приём, либо передача), внутри дискретно определённых временных интервалов, называемых тайм-слотами. Микроконтроллер (master - устройство), подключенный к считывающей чашке, всегда инициирует передачу с помощью посылки командного слова на прикладываемый к чашке электронный ключ iButton (он играет роль подчинённого, или slave - устройства). К шине может быть подключено несколько slave-устройств. Подобно электрическим вилке и розетке, которые определяют потребитель и источник электричества, контактное считывающее устройство в виде чашки является атрибутом master-устройства (которое, кстати, во многих случаях служит источником энергии для iButton), а круглая металлическая "таблетка" iButton является признаком slave-устройства. Такое точное разделение позволяет автоматически избежать конфликтов типа соединения двух master-устройств.

Команды и данные посылаются бит за битом и собираются в байты, причём вначале передаётся наименее значащий бит LSB (Least Significant Bit). Синхронизация master и slave происходит по спадающему срезу сигнала, когда master замыкает стоком выходного транзистора порта линию данных на провод земли. Через определённое время после среза сигнала происходит анализ (выборка) состояния данных на линии (лог. 0 или лог. 1) для получения одного бита информации. В зависимости от направления передачи информации в данный момент эту выборку делает либо устройство master, либо устройство slave. Этот метод обмена информацией называют передачей данных в тайм-слотах. Каждый тайм-слот отсчитывается независимо от другого. В обмене данными могут иметь место паузы без возникновения ошибок. На рисунке 4.27 представлены основные характеристики описанного выше обмена данными.

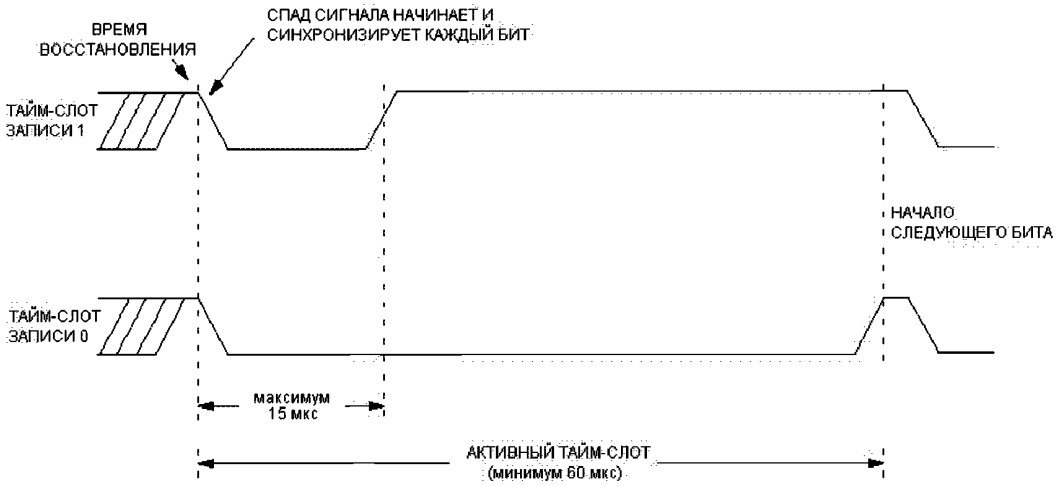


Рисунок 4.27

Синхронизация

Почти сразу после присоединения к считывающему устройству (через несколько микросекунд) slave - устройство iButton выдаёт на линию импульс низкого уровня, чтобы сказать устройству master, что оно на линии и ожидаёт получения команды. Этот сигнал называется presence pulse (импульс присутствия, далее просто presence). Master может также давать запрос на iButton с целью получения presence, путём выдачи на iButton специального импульса, называемого импульсом сброса (reset pulse, далее просто reset). Если iButton принял reset или если он был отсоединён от считывающего устройства, он будет анализировать линию данных, и как только линия снова достигнет высокого уровня, iButton сгенерирует presence. Полная последовательность импульсов reset и presence приведена на рисунке 4.28.

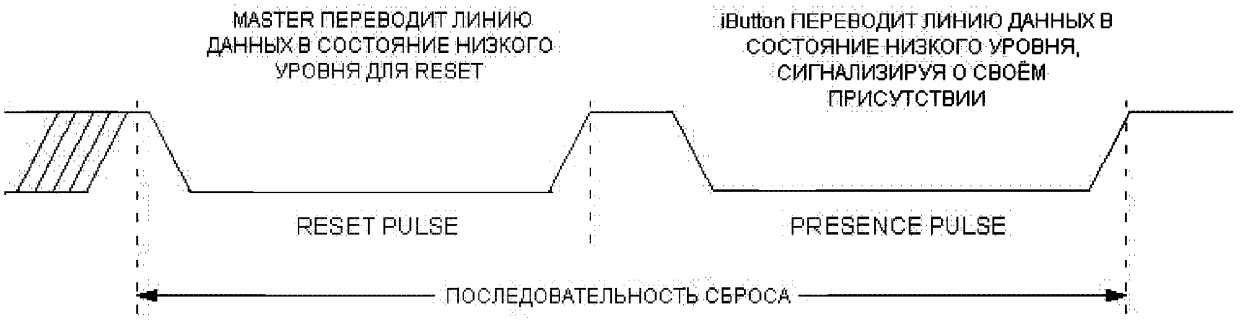


Рисунок 4.28

Передача данных

После выдачи presence, iButton ожидает получения команды. Любая команда записывается в iButton с помощью последовательности тайм-слотов, записывающих в iButton биты 1 и 0. Такая последовательность создаёт полный байт команды.

Передача данных в обратном направлении (чтение iButton) использует те же самые временные правила для представления 0 или 1. Поскольку iButton разработано как slave - устройство, то оно оставляет устройству master определять начало каждого тайм-слота. Чтобы произвести чтение iButton, master для чтения одного бита данных просто генерирует тайм-слот записи лог. 1 (именно тайм-слот записи, а не чтения). Если бит, который посылает iButton, равен 1, то iButton просто ожидает появления следующего тайм-слота, пропуская текущий. При этом с линии данных master считывает 1. Если бит, который посылает iButton, равен 0, то iButton удерживает линию данных в состоянии лог. 0 определённое время, и master считывает с линии данных 0. Пример полной последовательности выполнения команды приведен на рисунке 4.29. Активность устройства master изображена толстыми линиями. Серой линией показан ответ iButton. Тонкая линия показывает, что не активно ни одно из

устройств. Линия, через которую происходит обмен данными, подключена к положительному полюсу источника питания (обычно +5 В) через специальный нагрузочный резистор.

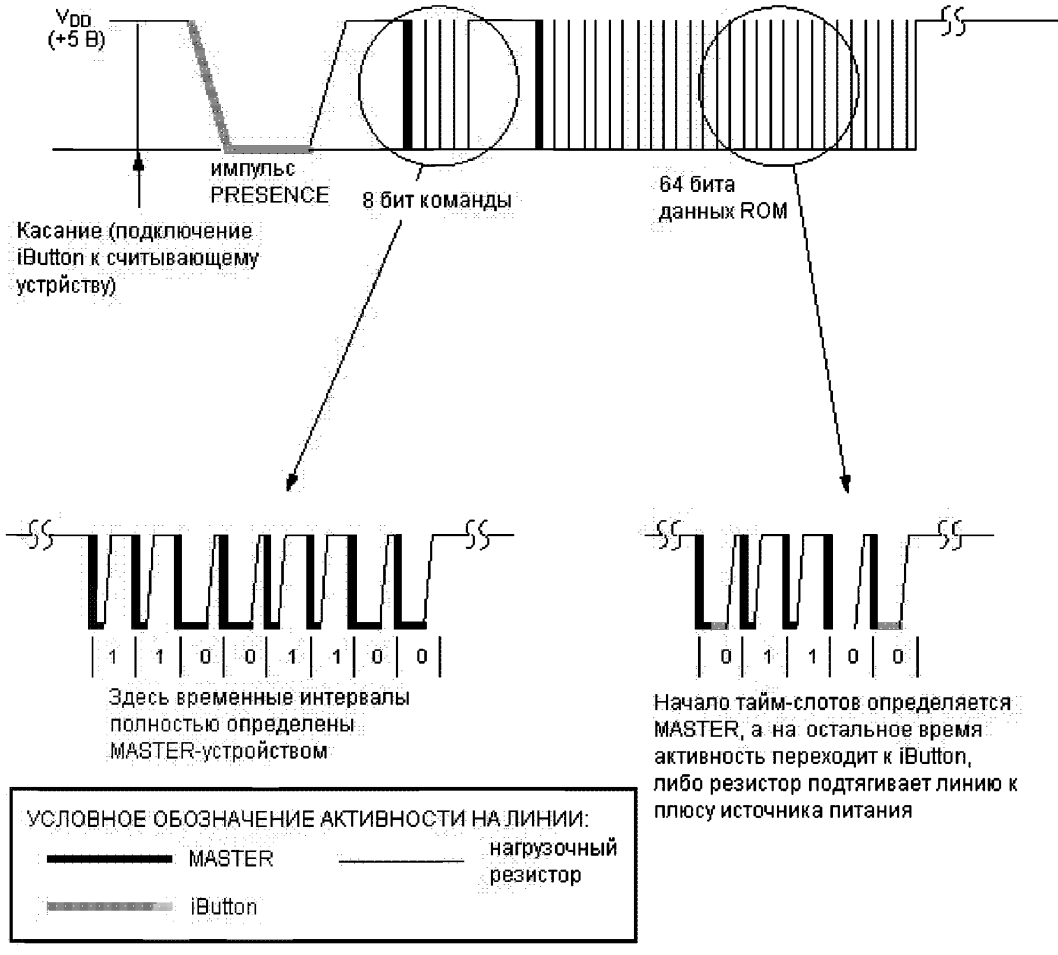


Рисунок 4.29

Регистрационный номер, записанный в ПЗУ (ROM)

Запрограммированная лазерным лучом ROM-секция содержит 6-байтное, уникальное для каждого устройства iButton число – серийный номер. Кроме того, во всех iButton записан в одном байте код типа устройства (family code), а также проверочный байт CRC. Младшие 7 бит family code указывают на тип устройства. Старший бит family code используется в качестве флага для версий, предназначенных для особых покупателей. Таким образом, можно закодировать 128 стандартных разновидностей устройств. 48-битный (6-байтный) серийный номер может представить любое десятичное число до $2{,}81 \times 10^{14}$. Если выпускать в год 1000 биллионов (10^{12}) устройств одного и того же типа, то этого числа хватит на 281 год. Кроме того, можно выпускать 128 типов различных устройств. Если старший бит family code установлен в 1, то устройство функционирует так же, как и стандартное, однако серийный номер устанавливается по специальным правилам – часть серийного номера резервируется для обозначения конкретного покупателя (заказчика).

Электронные ключи iButton имеют множество вариантов исполнений.

Типы устройств iButton

В таблице 4.1 представлен полный обзор разновидностей ключей iButton.

Таблица 4.1

Тип устройства	Family Code	Серийный номер	Количество бит, тип памяти	Защищённые биты NV RAM	Часы реального времени	Таймер интервалов времени	Счётчик циклов
DS1990A	01H	есть	–	–	–	–	–
DS1991	02H	есть	512, NVRAM	3×384	–	–	–
DS1992	08H	есть	1K, NVRAM	–	–	–	–
DS1993	06H	есть	4K, NVRAM	–	–	–	–
DS1994	04H	есть	4K, NVRAM	–	есть	есть	есть
DS1995	0AH	есть	16K, NVRAM	–	–	–	–
DS1996	0CH	есть	64K, NVRAM	–	–	–	–
DS1982	09H	есть	1K, EEPROM	–	–	–	–
DS1985	0BH	есть	16K, EEPROM	–	–	–	–
DS1986	0FH	есть	64K, EEPROM	–	–	–	–
DS1920	10H	есть	16, EEPROM	температурный iButton			

Примечания:

1. NVRAM (NonVolatile Random Access Memory) – память с произвольным доступом на чтение и запись, с энергонезависимым хранением информации;

2. EEPROM (Electrically Erasable, Programmable Read Only Memory) – электрически стираемая (не всегда) память с произвольным доступом на чтение.

Краткое описание iButton

DS1990A

Этот iButton является устройством – серийным номером, который может служить уникальным электронным идентификатором чего-либо или кого-либо. Это самый простейший из всех типов iButton. DS1990A содержит только ROM, запрограммированную на заводе. Поскольку информация сохранена на перерезаемых лазером связях в полисиликоне (нет зарядных элементов памяти или статических триггеров), DS1990A не нуждается в энергии для сохранения данных. Кроме того, для функционирования также почти не требуется энергия. DS1990A использует напряжение на линии данных для работы и сохраняет минимальный внутренний заряд для обеспечения работоспособности во время генерирования presence и в течение небольшого времени в любом из тайм-слотов, когда происходит операция чтения. На рисунке 4.30 показано, как организованы данные внутри DS1990A.

Рис. 4.30 – Структура данных ключа DS1990A

Первый байт, передаваемый из ROM, является кодом типа устройства – family code. После него идёт гарантированно уникальный серийный номер (6 байт), у которого наименее значащий байт передаётся первым. Последний байт несёт информацию Cyclic Redundancy Check (CRC), что означает проверочный циклический избыточный код. CRC специальным образом вычисляется от первых семи байт. Процесс позволяет быстро проверить правильность передачи информации. Если CRC, вычисленный устройством master от первых 7 байт, совпадает с принятым от iButton, то чтение было полностью верным. Этот метод – одна из причин, по которой iButton не требует стабильного электрического контакта со считывающим устройством.

DS1991, MultiKey iButton

Так же, как и DS1990A, DS1991 содержит серийный номер, family code и CRC. Кроме того, DS1991 содержит 64 байта энергонезависимой памяти scratchpad (необходимой для корректной операции записи в условиях ненадёжного контакта со считывающим устройством) и три независимые, защищённые паролем области памяти по 48 байт каждая, которые называются субключами (отсюда, похоже, и пошло название DS1991 – MultiKey iButton). Для каждой защищённой области имеется поле пароля из 8 байт и открытое для свободного чтения поле из 8 байт. Таким образом, каждая защищённая область занимает 64 байта.

DS1991 разработан как электронный ключ с высокой степенью защиты, который позволяет получать доступ к различным защищённым областям с помощью только одного устройства. Каждый из трёх ключей можно рассматривать как защищённый файл, для доступа к которому надо знать пароль. Открытое поле такого ключа содержит имя защищённого файла. Таким образом, разные люди могут использовать даже один и тот же пароль, хотя они и пользуются разными экземплярами DS1991.

DS1991 имеет защиту от взлома. Если для чтения данных используется неверный пароль, то устройство будет выдавать случайные числа. Если запрограммирован новый пароль, то все данные субключа будут автоматически стёрты. Несмотря на то, что возможна прямая запись в защищённые субключи, незащищённая область памяти scratchpad должна использоваться как временное хранилище для проверки данных перед тем, как они будут скопированы в свое положенное место (субключ). Это даёт гарантию, что будут записаны неискажённые данные, даже если во время соединения прервётся контакт. В зависимости от применения, незащищённая область памяти scratchpad может альтернативно использоваться как простая память общего назначения, работающая на чтение и запись.

DS1992, iButton с энергонезависимой памятью на 1 Кбит

Как и все iButton, DS1992 содержит уникальный серийный номер. Внутренние 128 байт энергонезависимой памяти организованы как 4 области памяти (страницы) по 32 байта. Имеется также память scratchpad размером 32 байта (её назначение то же самое, что и у DS1991). Начать чтение RAM можно с любой байтовой позиции и на любой странице. Запись возможна только через scratchpad. После того, как записанные в scratchpad данные проверены на соответствие оригиналу, выполняется команда копирования данных из scratchpad в конечное место назначения данных, чем предотвращаются ошибки записи из-за возможного непостоянного контакта со считывающим устройством.

DS1993, iButton с энергонезависимой памятью на 4 Кбит

DS1993 является версией DS1992 с увеличенным объёмом памяти – в четыре раза больше. Вместо 4-х имеется 16 страниц памяти по 32 байта. Конечно, DS1993 имеет собственный family code, размещённый в ROM.

DS1992 и DS1993 разработаны как уникальное идентификационное устройство и мобильный носитель данных. С использованием специальных структур данных эти устройства могут сохранять многочисленные независимые файлы разного назначения. Кроме того, для защищённого доступа легкодоступный серийный номер может использоваться как исходная величина совместно с секретным ключевым словом для кодирования приватных файлов данных. Несмотря на то, что закодированные данные можно прочитать, невозможно их продублировать из-за того, что два серийных номера не могут быть одинаковыми.

DS1994, iButton с таймером и энергонезависимой памятью на 4 Кбит

DS1994 добавляет к DS1993 часы реального времени, таймер временных интервалов и счётчик циклов. За исключением family code, DS1994 полностью совместим с DS1993. Дополнительные регистры для часов и управляющие регистры размещены в верхней, последней странице памяти.

Что касается представления времени, часы DS1994 имеют отличительные особенности по сравнению с обычными часами реального времени на рынке. Часы в DS1994 – это двоичный счётчик с дискретностью 1/256 секунды. Минута, час, день, месяц и год вычисляются от количества секунд, прошедших относительно произвольно выбранной "нулевой даты" (обыч-

но 1-е января 1970 года, 00 часов, 00 минут, 00 секунд). Таким образом, любое изменение в правилах отображения времени, зависящее от страны, перелагается на внешнее программное обеспечение, с которым работает DS1994. Кроме того, это представление времени упрощает вычисление интервалов времени между событиями и увеличивают точность настройки часов.

Таймер интервалов времени можно использовать как секундомер с остановом для подсчёта времени между некоторыми событиями, или как инструмент для контроля времени использования приборов, поскольку DS1994 включает в себя свойство для генерирования прерываний. Для получения статистики работы счётчик циклов запоминает, как часто прибор (например, машина или компьютер) был включен. Таймер интервалов добавляет в память время функционирования прибора. Однако, для этого применения DS1994 должен быть встроен в контролируемый прибор. К тому же, когда устройство DS1994 используется в процедурах касания со считывающим устройством, оно даёт полную информацию о частоте использования и среднее время каждого касания. RTC (Real Time Clock – часы реального времени) с регистрами тревоги обеспечивают функцию доступа с ограничением по времени. При достижении определённого времени доступ к устройству будет запрещён с помощью управляющего компьютера.

Возможность защиты от записи счётчиков и закрытие доступа к внутренним регистрам тревоги переводят устройство DS1994 на уровень не сбрасываемого контроллера истекающего времени. Все эти дополнительные особенности и связанные с ними регистры и управляющие флаги размещены на последней странице памяти (с номером 16). Доступ к содержимому этой страницы тот же самый, как и к обычным страницам памяти. Несмотря на то, что для операции записи обычно используют scratchpad, структура команд позволяет записать один или несколько байт.

DS1995, iButton с энергонезависимой памятью на 16 Кбит

Для применений, требующих сохранения нескольких файлов различного размера, ёмкость DS1993 может оказаться недостаточной. DS1995 учетверяет доступную ёмкость предыдущих версий iButton до 16 Кбит (до 64 страниц по 32 байта каждая). Поскольку DS1995 имеет ту же самую логическую структуру и понимает тот же самый набор команд, что и другие версии iButton с энергонезависимой памятью, устройство DS1995 полностью совместимо с существующим прикладным программным обеспечением. Новое уникальное значение family code указывает на наличие дополнительной ёмкости памяти.

DS1996, iButton с энергонезависимой памятью на 64 Кбит

DS1996 учетверяет ёмкость DS1995 до 64 Кбит (до 256 страниц по 32 байта каждая). С теми же самыми командами, как и у других iButton с энергонезависимой памятью, DS1996 позволяет легко провести апгрейд существующих систем. Как и все iButton, это устройство имеет уникальное значение family code.

DS1995 и DS1996 значительно превосходят по ёмкости существующие мобильные носители данных, как, например, серийные чип-карты или магнитные полосы. Использование серийного номера как исходной величины совместно с секретным ключевым словом позволяет сохранять как закодированные, так и незащищённые файлы данных в одном устройстве.

DS1982, Add-Only iButton с однократно программируемой памятью на 1 Кбит

Серии DS198x используют технологию EEPROM, которая не требует встроенного источника энергии для поддержания сохранности данных. Так же как и у DS1990A, энергия для работы берётся непосредственно с линии данных. Как и все iButton, DS1982 содержит секцию ROM с серийным номером и family code. Память организована как 4 страницы по 32 байта каждая.

Чтение DS1982 происходит так же, как и чтение других iButton со встроенной памятью, однако, запись происходит по-другому. Перед тем как байт данных попадёт на своё место назначения в памяти, он сначала записывается в scratchpad размером в 1 байт. Далее происходит самопроверка команды записи – адреса назначения и записываемых данных - с помощью 8-битного CRC. Если проверка прошла успешно, импульс длительностью 1 мс и напряжением 12 В сделает копию байта scratchpad в место назначения байта. Эта процедура предотвращает некорректную запись в случае пропадания контакта с устройством.

Такая изощрённая проверка перед записью необходима для устройств, основанных на технологии EEPROM, поскольку однажды записанные неверные данные уже невозможно исправить. Когда данные нуждаются в обновлении, старые данные "переназначаются" и добавляется новый набор данных. Этот режим функционирования объясняет имя Add-Only iButton (iButton только для добавления данных) для этой группы. Устройства Add-Only iButton невозможно стереть. Каждая страница памяти аппаратно защищена от последующих попыток записи. Таким образом, каждое обновление будет оставлять для контроля постоянный след. Такое свойство памяти используется, например, в кассовых аппаратах (фискальная память).

Флаги, показывающие состояние страницы данных (запрещена она для записи и т. п.), помещены в 8-ми байтах статуса памяти устройства. Запись в данные статуса применяет ту же самую интегрированную процедуру, как и для страниц данных. Когда читаются информация статуса или просто данные, встроенный генератор CRC защищает поток данных от потенциальных ошибок.

DS1985, Add-Only iButton с однократно программируемой памятью на 16 Кбит

С 16-кратной ёмкостью по сравнению с DS1982, DS1985 является наименьшим устройством типа Add-Only, полностью поддерживающим сохранение и обновление нескольких файлов приложений. Память приложений организована как 64 страницы по 32 байта каждая. В дополнение к памяти приложений, имеется 88 байт памяти статуса, выделенной для байт переназначения, флагов и бит защиты от записи. Специальная команда сигнализирует о перенаправлении данных для предотвращения потерь времени и чтения неверных данных. Другие функции у DS1985 те же самые, что и у DS1982.

DS1986, Add-Only iButton с однократно программируемой памятью на 64 Кбит

DS1986 является 64 Кбитным апгрейдом DS1985. Память организована как 256 страниц по 32 байта каждая. Расширенная область памяти потребовала увеличения памяти статуса до 352 байт. Все другие особенности DS1986 те же, что и у DS1985.

Выдающаяся особенность iButton типа Add-Only - невозможность удаления данных. Если данные нуждаются в обновлении, то это происходит путём изменения пути на другую страницу, что оставляет постоянный след изменений. Это позволяет реконструировать оригинальные и промежуточные версии данных. Благодаря аппаратной защите от записи такие устройства устойчивы к вмешательству в содержимое данных. Если запрограммирован бит защиты от записи, нет никаких шансов изменить хотя бы один бит соответствующей страницы или перенаправить байт.

DS1920, Temperature iButton

Как показывает название, это устройство содержит термометр в корпусе MicroCan. Вместо памяти пользователь получает доступ к 9-битному преобразователю (дающему точность 0,5 градуса по Цельсию), как если бы это была бы память, и к управляющим регистрам. Уникальная секция ROM тоже является стандартной для этих устройств, что позволяет создать цепочку из термометров и считывать их значения из одного места. Точность измерения температуры составляет 0,5 градуса Цельсия в диапазоне температур от 0 до +70 градусов. В диапазонах от минус 40 до 0 градусов и от +70 до +85 градусов по Цельсию точность ухудшается до 1 градуса. Время определения температуры составляет около одной секунды.

Описанные выше устройства поставляются в корпусе MicroCan. Кроме того, имеются некоторые другие устройства в других корпусах, имеющие некоторые общие особенности вышеописанных iButton. Например, продукты, предназначенные для пайки – адресуемый электронный ключ DS2407 и двухинтерфейсная память с таймером DS2404S-C01.

На рисунке 4.31 приведено изображение считывателя электронных ключей iButton.

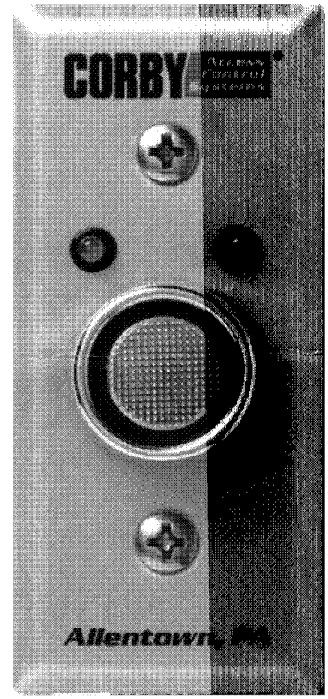


Рисунок 4.31

К достоинствам метода идентификации с использованием электронных ключей iButton можно отнести:

1) Сравнительно низкую стоимость самого электронного ключа, его считывателя;

2) Высокую степень устойчивости к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);

3) Корпус ключа, выполненный из нержавеющей стали, обладает повышенной устойчивостью к воздействию коррозии и агрессивных сред;

4) Высокие имитостойкость и степень защищенности от несанкционированного копирования (за исключением электронного ключа DS1990A), обеспечиваемые наличием кодированных областей памяти ключа;

5) Большой объем памяти данных, записываемых в электронный ключ, позволяет использовать многоразрядные индивидуальные коды, что значительно увеличивает число комбинаций кодов;

6) Большой объем памяти данных позволяет записывать в электронный ключ не только его код, но и разнообразную дополнительную информацию о пользователе – носителе идентификатора;

7) Продолжительный срок службы ключа;

8) Отсутствие в электронном ключе источника электропитания повышает удобство его использования (нет необходимости в периодической замене источников электропитания);

9) Низковольтный двухпроводный интерфейс способствует упрощению монтажа и снижению затрат на него.

К недостаткам метода идентификации с использованием электронных ключей iButton можно отнести:

1) Открытость протокола обмена данными создает реальную угрозу создания устройств, полностью имитирующих тактику работы электронных ключей iButton (устройства, имитирующие тактику работы электронного ключа DS1990A, уже созданы);

2) Особенности конструктивного исполнения электронного ключа и его считывателя допускают возможность разрыва электрического соединения в процессе обмена данными, что приводит к появлению ошибок при чтении индивидуального кода;

3) Контактные поверхности электронного ключа и его считывателя подвержены загрязнению, что может привести к ненадежности электрического соединения, и, как следствие, к неправильному считыванию индивидуального кода;

4) Считывающие чашки некоторых конструктивных исполнений не обеспечивают надежного электрического контакта при одновременном использовании ключей iButton, исполненных в версиях F3 и F5.

Метод идентификации, основанный на применении электронных ключей iButton, аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием.

В настоящее время в "Списке технических средств..." представлены следующие системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения считывателей электронных ключей iButton:

ППКОП "Ладога-А" (производство ЗАО "Риэлта", г. Санкт-Петербург)

Устройство постановки/снятия "Ладога УПС-А";

Устройство постановки/снятия "Ладога УПС-А исп. 1."

Автоматизированная система передачи извещений "Приток-А" (производство ООО "Охранное бюро Сократ", г. Иркутск)

Приток-С-20;

ППКОП 011-8-1-01К Приток-А-4(8);

ППКОП 011-8-1-01К Приток-А-4(16);

Приток-СКД-02*;

Бортовой комплект.

* – имеется возможность подключения считывателей, производящих обмен данными по протоколу iButton, сторонних предприятий-изготовителей.

Автоматизированная система передачи извещений КЦНОП049-2/2/240/7680-1 "Альтаир" (производство ЗАО "ПК ЦНИТИ, г. Ногинск, Московская область; ОАО "Радий", г. Касли Челябинская область)

– "Набат ЛПП-2АТ";

– УОО "А-401";

– УОО "А-402";

– УОО "А-801";

– УОО "А-802".

Автоматизированная система передачи извещений "Ахтуба" (производство "НПО Ахтуба-Плюс", г. Волжский, Волгоградская область)

– УО "6ША";

– УО "3Ш";

– УО "1ША-02";

– УО "1Ш".

Автоматизированная система передачи извещений "Юпитер" (производство ООО "Элеста", г. Санкт-Петербург)

– АК "Юпитер";

– ППКОП "Юпитер 24";

– ППКОП "Юпитер 24к";

– "Юпитер 3GSM";

– "Юпитер 5GPRS";

– "РИО Т";

– УОО "Юпитер 5 IP".

Автоматизированная система передачи извещений "Заря" (производство ЗАО "Риэлта", г. Санкт-Петербург)

– УОО "Заря – ГК-IP-МО"*;

– УОО "Заря – ГК-IP-М1"*;

– УОО "Заря – ГК-IP-М2"*;

– ППКО "Заря-ИО"*;
– ППКО "Заря-УО"*;
– ППКОП "Заря-УО-М1"*;
– ППКОП "Заря-УО-М2"*;
– ППКОП "Заря-УО-IP"*;
– ППКОП "Заря-УО-IP-GPRS"*;

* – имеется возможность подключения выносного считывателя электронных ключей iButton "ВУПС".

Автоматизированная система передачи извещений «Лагуна» (производство ООО "КВАЗАР", г. Ногинск, Московская область)

– ППКО "Редут-NET-GSM";
– УО "Лагуна IP/GSM".

Автоматизированная система передачи извещений по радиоканалу "Иртыш-3Р" (производство ООО НТК "Интекс", г. Омск)

– ППКОП "Иртыш-214";
– УООР "Иртыш-424";
– ППКОП "Иртыш-113";
– ППКОП "Иртыш-244".

Автоматизи-рованная система передачи извещений по радиока-налу "Струна-5" (производство ЗАО НПФ "Интеграл+", г. Казань)

– "БРО-1";
– БР/Р "Интеграл 433/2400";
– "БПО-1";
– "БПО-2";
– "БПО-4";
– "БПО-8";
– "БПО-16";
– "ПУУ";
– "ПУ";
– "БРО-5 GSM".

ППКОП "Ладога-А" (производство ЗАО "Риэлта", г. Санкт-Петербург)

– "Ладога УПС-А" (2 исп.).

Комплекс, состоящий из прибора приемно-контрольного охранно-пожарного и управления ППКОПУ 01059-1000-3 "Р-08" ("Рубеж-08") и его модификаций, программного обеспечения и дополнительного оборудования (производства ООО "СИГМА-ИС", г. Москва)

– "СКУ-01";
– "ППКОП Р-020".

Интегрированная система безопасности "Стрелец-Интеграл" (производство ЗАО "Аргус-Спектр", г. Санкт-Петербург)

– "БШС8-И".

Интегрированная система охраны (ИСО) "Орион" (производство ЗАО НВП "Болид", г. Королев Московская область)

– ППКОП "С2000-4";
– "С2000-КДЛ";
– "С2000-2";
– "Считыватель-2".

Система беспроводной охранно-пожарной сигнализации "Астра-Zитадель" (производство ЗАО НТЦ "ТЕКО", г. Казань)

– ППКОП "Астра-Z 812 М";
– ППКОП "Астра-Z 8945";
– ПКУ "Астра-814".

Устройство беспроводной охранно-пожарной сигнализации "Астра-РИ-М" (производство ЗАО НТЦ "ТЕКО", г. Казань)

– ППКОП "Астра-812";

– ППКОП "Астра-812М".

Система охранной сигнализации с функцией домофона СОС "Спрут-100" (производства ОАО "Радий", г. Касли Челябинская область)

– "Спрут-100";

– "Спрут-100М".

Прибор приемно-контрольный охранно-пожарный ППКОП 0312149-1024-1 «Форпост» производства ООО "Элтис-Техника", г. Санкт-Петербург).

Стоимость электронных ключей iButton определяется типом ключа, его исполнением и закупаемой партией. По состоянию на 11.08.2015 г. цена электронного ключа iButton (Touch-Memory) типа DS-1990A (поставщик НПО "Сибирский Арсенал") составляет 63,00 руб, цена электронного ключа iButton (Touch-Memory) типа DS-1990A (производитель "Maxim") составляет 103,20 руб., цена электронного ключа iButton (Touch-Memory) типа DS-1992 (производитель "Maxim") составляет 432,00 руб., цена электронного ключа iButton (Touch-Memory) типа DS-1904 (производитель "Maxim") составляет 805,90 руб.

Цена считывателя электронных ключей iButton (Touch-Memory) Порт ТМ вар. 3 (поставщик НПО "Сибирский Арсенал") составляет 125,00 руб. Цена считывателя электронных ключей iButton (Touch-Memory) модели RDS-04 (производитель "Maxim") составляет 322,40 руб., цена типового считывателя электронных ключей iButton (Touch-Memory) модели RDS-01 (производитель "Maxim") составляет 612,50 руб., цена типового считывателя электронных ключей iButton (Touch-Memory) модели RDS-12 (производитель "Maxim") составляет 1212,10 руб.

(Информация взята с интернет-сайтов: http://www.aladdin-rd.ru/catalog/ibutton, http://www.aladdin-rd.ru/catalog/ibutton, http://www.shop.arsenalnpo.ru).

4.8 Идентификационная карта с голографической памятью

Идентификационные карты с голографической памятью являются одним из видов идентификационных карт с оптической памятью, но, из-за уникальности технологии записи и считывания данных, целесообразно рассматривать их как отдельный вид идентификационных карт.

Используемые при изготовлении таких идентификационных карт трехмерные голограммы формируются на основе интерференции двух или нескольких когерентных волн. Применение голограммы обеспечивает плотность записи информации до 10 бит на 1 мм^2. Пример голографического изображения приведен на рисунке 4.32. Чтение считывателем индивидуального кода карты производится при помощи установленного в нем лазера. Конструкция и принцип работы считывателя идентификационных карт с голографической памятью практически полностью повторяют считыватель идентификационных карт с оптической памятью.

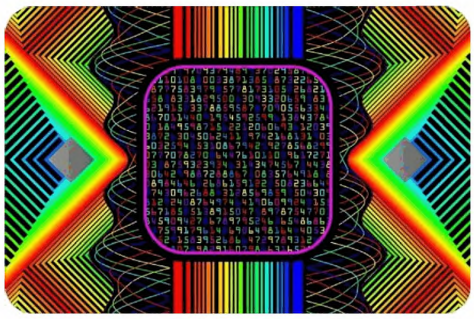


Рисунок 4.32

Изображение идентификационной карты с голографической памятью приведено на рисунке 4.33.

Рисунок 4.33

Повышенная защищенность идентификационной карты обусловлена тем, что техническая реализация методов голографии отличается достаточной сложностью и требует применения специализированной аппаратуры.

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

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

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

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

При необходимости голограммы могут применяться и для хранения биометрических данных (например, отпечатков пальцев). Для обеспечения надежной защиты от попыток фальсификации или копирования идентификационных карт фирма применила еще и шифрование данных.

К достоинствам метода идентификации, основанном на использовании идентификационных карт с голографической памятью можно отнести:

1) Высокую устойчивость идентификационной карты к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);

2) Высокие имитостойкость и степень защищенности от несанкционированного копирования, обеспечиваемые особенностями технологии изготовления идентификационной карты.

3) Большой объем памяти данных позволяет записывать на идентификационную карту не только ее код, но и разнообразную дополнительную информацию о пользователе – носителе идентификатора;

К недостаткам метода идентификации, основанном на использовании идентификационных карт с голографической памятью можно отнести:

1) Критичность идентификационной карты к прозрачности защитного слоя области данных, загрязнение или повреждение которого могут привести к невозможности считывания индивидуального кода и прочих данных с карты;

2) Оптическая система считывателя чувствительна к загрязнению, требует квалифицированного обслуживания и особенно бережного отношения;

Метод идентификации, основанный на применении идентификационных карт с голографической памятью, потенциально совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но, как и в случае прочих методов идентификации, для его использования требуется совместимость с протоколом обмена данными объектового оборудования

В текущей редакции "Списка технических средств..." систем и технических средств, использующих метод идентификации, основанный на применении идентификационных карт с голографической памятью, не представлено.

В настоящее время в России отсутствую предприятия-изготовители, производящие идентификационные карты с голографической памятью. Сведений о наличии на Российском рынке технических средств охраны зарубежных предприятий-изготовителей современных систем, использующих идентификационные карты с голографической памятью, в открытых источниках не представлено, в связи с чем не представляется возможным приведение ценовых показателей.

4.9 Идентификационные смарт-карты (карты с искусственным интеллектом)

Идентификационные карты данного типа содержат вмонтированные в основу миниатюрные интегральные микросхемы – запоминающее устройство и микропроцессор. Одно из преимуществ карточек этого типа – возможность регистрации значительного объема идентификационных данных. Идентификационные карты данного типа иногда еще называют "разумными" или "интеллектуальными". Изображения идентификационной смарт-карты и ее считывателя приведены на рисунках 4.34 и 4.35 соответственно.

Рисунок 4.34

Рисунок 4.35

Вычислительный микроблок идентификационной карты содержит три типа запоминающих устройств (ЗУ). Для хранения программного обеспечения предназначена память типа ПЗУ (постоянное запоминающее устройство). В ПЗУ информация заносится фирмой-изготовителем на этапе выпуска карты в обращение, не допускается внесения каких-либо изменений в хранящейся инструкции.

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

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

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

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

В секретной зоне записывается идентифицирующая информация, например, личный номер или код-пароль. Кроме того, здесь же обычно хранятся временные и территориальные полномочия пользователя по доступу к охраняемым объектам и помещениям. Информация секретной зоны может быть считана только терминалом системы контроля доступа, для которого предназначена данная карточка. Изменения также вносятся только по команде этой системы. Хранимые здесь данные не раскрываются никакой посторонней считывающей аппаратурой, в том числе фирме-изготовителю. Секретная информация заносится в эту зону при регистрации пользователя контрольно-пропускной системой. До недавнего времени в качестве такой памяти применялись запоминающие устройства СППЗУ (стираемое программируемое постоянное ЗУ). Внесенная информация могла быть стерта только с помощью ультрафиолетового излучения и спецоборудования. Более современным типом памяти является ЭСППЗУ – электрически стираемое программируемое постоянное ЗУ, которое, в отличие от предыдущего, более долговечно (срок службы – до нескольких лет) и обладает большей гибкостью.

Некоторые идентификационные смарт-карты позволяют хранить цифровые образы биометрических характеристик пользователя (динамику росписи, отпечатка пальца, ладони, геометрических параметров кисти, рисунка глазного дна, портретного изображения). В целях защиты от несанкционированного использования идентификационных карточек, применяемых пользователями таких систем, электронный "портрет" хранится в памяти в цифровом, зашифрованном виде, что значительно затрудняет восстановление записанной информации и ее подделку злоумышленниками.

К достоинствам метода идентификации, основанном на использовании идентификационных смарт-карт можно отнести:

1) Сравнительно невысокая стоимость изготовления идентификационной карты и считывателя;

2) Высокая устойчивость идентификационной карты к воздействию внешним факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, вибрация);

3) Большой объем памяти данных идентификационной карты;

4) Наличие процессора, управляемого встроенной операционной системой, позволяет идентификационной карте не только хранить записанные на нее данные, но и производить их математическую, логическую и крипто обработку;

5) Предусмотрена возможность санкционированной замены программного обеспечения идентификационной карты, а, следовательно, и алгоритмов обработки и шифрования данных.

6) Большой объем памяти данных позволяет записывать на идентификационную карту не только ее индивидуальный код, но и разнообразную дополнительную информацию о носителе идентификатора (личная фотография, образец подписи и т.п.);

7) Высокие имитостойкость и степень защищенности от несанкционированного копирования идентификационной карты, обеспечиваемые применением специальных аппаратных и программных методов защиты;

К недостаткам метода идентификации, основанном на использовании идентификационных смарт-карт можно отнести:

1) Критичность идентификационной карты к воздействию статического электричества, переменного электромагнитного поля;

2) Изгибание пластиковой основы идентификационной карты, возникающее в процессе внешних механических воздействий, может привести к повреждению процессорного модуля,

модуля памяти или контактных площадок;

3) Электро-контактный метод считывания приводит к износу контактов как самой идентификационный карты, так и контактных площадок считывателя, тем самым, ограничивая срок их службы;

4) Необходимость помещения идентификационной карты в считыватель в процессе чтения ее кода снижает удобство ее использования и увеличивает время ее обработки.

Метод идентификации, основанный на применении идентификационных смарт-карт, аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения считывателей идентификационных смарт-карт не представлено.

Цена идентификационных смарт-карт находится в зависимости от объема памяти, вида операционной системы, материала основы идентификационной карты, наличию дополнительных функций.

По состоянию на 12.08.2015 г. цена смарт-карты модели SLE4442/5542 с объемом памяти 256 байт (производитель Smart Card ISBC) зависит от тиража и составляет 59,06 руб. (при тираже 500 шт.), цена смарт-карты модели ACOS3-24K с объемом памяти 72 Кбайт (производитель Smart Card ISBC) зависит от тиража и составляет 267,18 руб. (при тираже 500 шт.), цена криптопроцессорной карты модели Siemens CardOS v.4.3B объемом памяти 64 Кбайт (производитель Siemens) зависит от тиража и составляет 728,00 руб. (при тираже 1 шт.).

Цена считывателя смарт-карт фирмы "ACS" марки "ACR38U-I1" составляет 1229,00 руб., цена считывателя смарт-карт фирмы "ACS" марки "ACR39U-I1" составляет 1372,00 руб., цена считывателя смарт-карт фирмы "ACS" марки "ACR3901U-H3" составляет 1970,00 руб.

(Материалы взяты с интернет-сайта http://www.smartcardreader.ru/).

4.10 Бесконтактные идентификаторы RFID (технология Proximity)

Дистанционный принцип идентификации (технология Proximity) широко применяется в системах контроля и управления доступом. Способ дистанционного (бесконтактного) считывания, называемый в английской транскрипции "Proximity", что в буквальном переводе означает "дистанционный", наиболее быстро развивающаяся технология идентификации. Чтение кода идентификатора происходит на определенном расстоянии от считывателя без непосредственного контакта. Существует несколько технологий записи идентификационного кода на идентификаторы, например, на эффекте поверхностной акустической волны. Однако, наиболее широкое распространение получили идентификаторы с установленной внутри интегральной микросхемой, которая представляет собой достаточно сложное электронное устройство, содержащее в общем случае приемник, передатчик и процессор с памятью, в которой храниться идентификационный код. Внутри идентификатора расположена также антенна, с помощью которой происходит обмен данными между считывателем и идентификатором в радиочастотном диапазоне электромагнитных волн. Именно такой тип дистанционного идентификатора и получил название RFID (Radio Frequency IDentification, радиочастотная идентификация). Изображение идентификационной RFID карты приведено на рисунке 4.36.

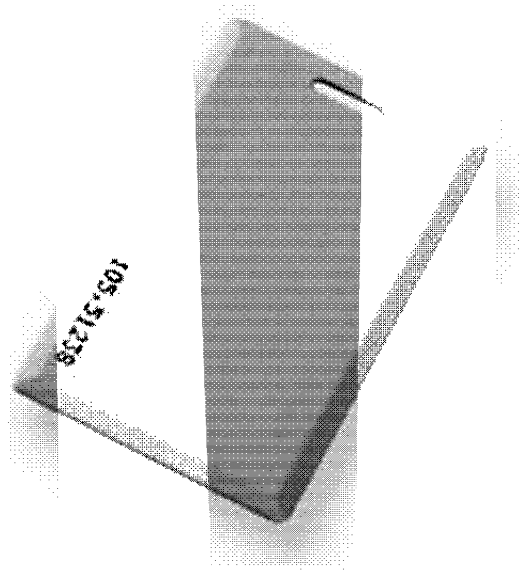


Рисунок 4.36

По способу обеспечения электропитания RFID идентификаторы подразделяются на:

– пассивные;

– активные;

– полупассивные.

Пассивные RFID идентификаторы не имеют встроенного источника энергии. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования кремниевого чипа, размещённого в метке и передачи ответного сигнала.

Активные RFID идентификаторы обладают собственным источником электропитания и не зависят от энергии считывателя, вследствие чего они читаются на дальнем расстоянии, имеют большие размеры и могут быть оснащены дополнительной электроникой. Активные RFID идентификаторы обычно имеют гораздо больший радиус считывания и объём памяти, чем пассивные, и способны хранить больший объём информации для отправки приемопередатчиком.

Полупассивные RFID идентификаторы, также называемые полуактивными, очень похожи на пассивные метки, но оснащены батареей, которая обеспечивает чип энергопитанием.

По типу используемой памяти RFID, идентификаторы подразделяются на:

RO (англ. Read Only) – данные записываются только один раз, сразу при изготовлении. Такие RFID идентификаторы пригодны только для идентификации. Никакую новую информацию в них записать нельзя, и их практически невозможно подделать;

WORM (англ. Write Once Read Many) – кроме уникального идентификатора такие метки содержат блок однократно записываемой памяти, которую в дальнейшем можно многократно читать;

RW (англ. Read and Write) – такие RFID идентификаторы содержат идентификатор и блок памяти для чтения/записи информации. Данные в них могут быть перезаписаны многократно.

Принцип работы пассивных RFID идентификаторов показан на структурной схеме, приведенной на рисунке 4.37. Считыватель излучает электромагнитное поле от своей антенны. RFID идентификатор, попадая в это поле, с помощью своей антенны за счет индуктивной связи получает питание встроенной микросхемы, и затем передает обратно на считыватель свой код с помощью модуляции радиочастоты.

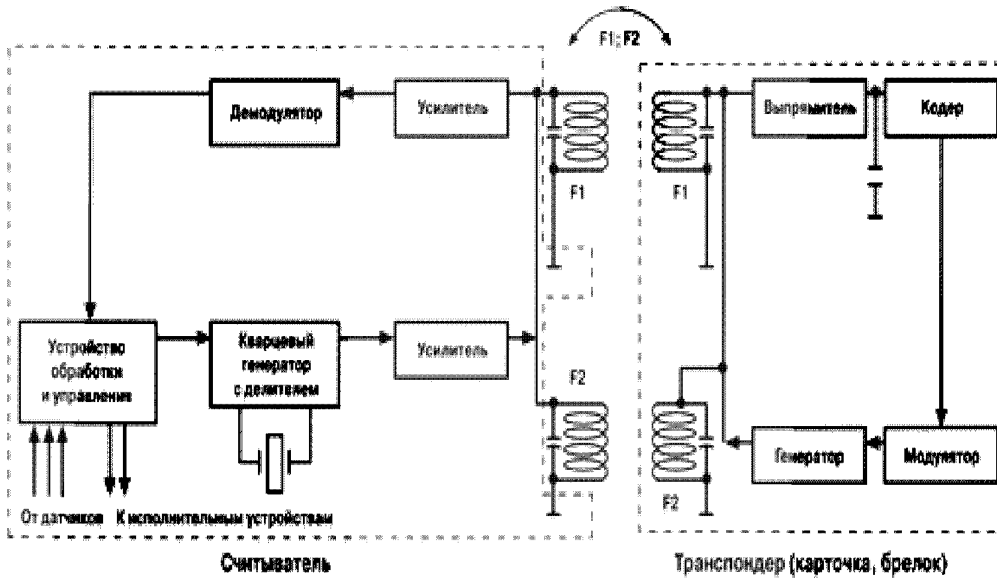


Рисунок 4.37

Существует четыре диапазона рабочих частот, которые наиболее широко применяются RFID идентификаторами: 125 кГц; 13,56 МГц; 860 – 928 МГц; 2,45 ГГц. Основные технические параметры, характеризующие RFID идентификаторы, использующие каждый из частотных диапазонов, приведены в таблицах 4.2 – 4.5.

Таблица 4.2

156 кГц (LF)	
Расстояние считывания	от 3 до 70 см
Скорость передачи данных	до 9600 бит/сек
Наличие антиколлизии	есть, но не у всех
Объем памяти	32 – 1024 байта
Существующие типы считывателей	Стационарные, стационарные с выносной антенной, настенные, ручные, модули
Сфера использования	Применяются в системах контроля доступа, для идентификации животных, автомобильных иммобилайзерах

Таблица 4.3

13,56 МГц (HF)	
Расстояние считывания	от 3 до 100 см
Скорость передачи данных	до 64 кбит/сек
Наличие антиколлизии	есть
Объем памяти	8 – 16384 байта
Сфера использования	Применяются в системах контроля доступа, платежных системах, для идентификации товаров на складах и книг в библиотечных системах

Таблица 4.4

860 – 928 МГц (UHF)	
Расстояние считывания	от 10 см до 10 м
Скорость передачи данных	от 128 и более кбит/сек
Наличие антиколлизии	есть, до 150 идентификаторов/сек
Объем памяти	64 – 1024 бит (ISO), 64 или 96 бит (EPC)
Сфера использования	Применяются в системах логистики и учета движения транспорта. Отличительной особенностью является повышенная дальность и высокая скорость чтения

Таблица 4.5

2,45 ГГц (UHF)	
Расстояние считывания	от 2 до 10 м
Скорость передачи данных	до 128 и более кбит/сек
Наличие антиколлизии	есть
Объем памяти	от 64 бит до 32 кбайт
Сфера использования	Применяются в системах логистики и учета движения транспорта. Отличительной особенностью является повышенная дальность и высокая скорость чтения

Изображение считывателя бесконтактной идентификационной Proximity-карты приведено на рисунке 4.38.

Рисунок 4.38

Помимо RFID карт, идентификаторы данного типа выполняются в виде браслетов, брелоков, ключей и т.п. Примеры RFID идентификаторов, выполненных в различных исполнениях, приведены на рисунках 4.39 – 4.44.

Рисунок 4.39 – RFID идентификатор, выполненный в виде брелока

Рисунок 4.40 – RFID идентификатор, выполненный в виде браслета

Рисунок 4.41 – RFID идентификатор, выполненный в виде одноразового браслета

Рисунок 4.42 – RFID идентификаторы, выполненные в виде болта и винта

Рисунок 4.43 – RFID идентификаторы, выполненные в виде герметичных капсул

Рисунок 4.44 – RFID идентификатор, выполненный в защищенном исполнении, для установки на транспортные средства

Расстояние считывания зависит от мощности электромагнитного поля считывателя и от габаритов антенны. Некоторые модели считывателей имеют выносную антенну, которая выполняется в виде нескольких витков провода, и может быть расположена, например, в дверной коробке или под полотном асфальтового покрытия дороги, для идентификации автомобилей.

Необычное применение RFID идентификаторам найдено в системе "Стрелец-ПРО" (производство ЗАО "Аргус-Спектр", г. Санкт-Петербург). В данной системе RFID-идентификаторы используются совместно с другими системами определения местоположения, что позволяет производить определение местоположения пользователей, находящихся как вне, так и внутри помещений.

Система "Стрелец-ПРО" предназначена для обеспечения физической защиты объектов и выполняет следующие функции:

1. Контроль охраны:

– Датчик неподвижности (функция "Не спать");

– Автоматический мониторинг обхода периметра (GPS, Глонасс).

2. Передача тревожного сигнала на пульт (тревожная кнопка).

3. Оперативное персональное оповещение по событиям "Проникновение", "Тревога" "Пожар" (получение текстовых сообщений).

Характеристики системы:

– емкость до 2000 браслетов;

– дальность до 50 км (при применении ретрансляторов);

– поддержка стандартов спутниковых навигационных систем GPS и Глонасс;

– датчик неподвижности;

– наличие вибровызова в браслете;

– степень защиты браслетов IP67 (водонепроницаемый корпус).

К достоинствам метода идентификации на основе использования бесконтактных идентификаторов RFID можно отнести:

1) Низкую стоимость идентификаторов и считывателей;

2) Бесконтактный, дистанционный обмен данными между идентификатором и считывателем, обеспечивает наибольшую пропускную способность и является наиболее удобным для пользователей;

3) Бесконтактное считывание идентификатора позволяет применить скрытую установку считывателя, что значительно повышает устойчивость системы к криминальным воздействиям, вандалоустойчивость и устойчивость к неблагоприятным природным факторам;

4) Высокая степень устойчивости идентификаторов к воздействию внешних факторов (повышенная/пониженная температура окружающей среды, повышенная влажность воздуха, сильные электрические и магнитные поля, статическое напряжение, вибрация);

5) Высокие имитостойкость и степень защищенности от несанкционированного копирования, обеспечиваемые наличием кодированного обмена данными;

6) Большой объем памяти данных, записываемых на идентификатор, позволяет использовать многоразрядные коды, что значительно увеличивает число комбинаций кодов;

7) Продолжительный срок службы идентификаторов;

8) Отсутствие в пассивных идентификаторах источника электропитания повышает удобство их использования (нет необходимости в периодической замене источников электропитания); в тоже время, наличие в активных идентификаторах встроенного источника электропитания обеспечивает увеличение дальности считывания;

9) Взаимная ориентация идентификатора и считывателя не имеет принципиального значения;

10) Бытовые радиопередающие устройства, электронные ключи или брелоки, находящиеся в контакте с идентификатором, не мешают его обмену данными со считывателем.

К недостаткам метода идентификации на основе использования бесконтактных идентификаторов RFID можно отнести:

1) Из-за использования передачи данных по радиоканалу становится возможным их несанкционированное дистанционное считывание, что при отсутствии криптозащиты протокола обмена данными позволяет злоумышленникам, используя сравнительно несложную аппаратуру, имитировать работу идентификатора;

2) Одновременное внесение в чувствительную зону считывателя сразу нескольких идентификаторов (возникновение коллизии) может привести к неправильной работе системы.

Метод идентификации, основанный на применении бесконтактных идентификаторов RFID аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." представлены следующие системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения считывателей, бесконтактных идентификаторов RFID:

ППКОП01059-42/126-1 "Кодос А-20" (производство ОАО "Бауманн", г. Москва)

– 1100УЛ -1040УЛ;
– КОДОС RC-102E;
– КОДОС RC-102H;
– КОДОС RC-103E;
– КОДОС RC-103H;
– КОДОС EC-202;
– КОДОС EC -202Ш;
– КОДОС EC -202 (исп.К);
– КОДОС EC-30–4;
– КОДОС EC-502;
– КОДОС EC-602;
– КОДОС RD-1030;
– КОДОС RD -1030 (исп.К);
– КОДОС RD-1040;
– КОДОС RD -1040 (исп.К);
– КОДОС RD -1100;
– КОДОС RD -1100 (исп.К);
– КОДОС RD -1030USB;
– КОДОС RD -1040USB;
– КОДОС RD -1100USB;
– КОДОС RDM-20;

– КОДОС К-30;
– КОДОС К -40;
– КОДОС К -100.

Комплекс, состоящий из прибора приемно-контрольного охранно-пожарного и управления ППКОПУ 01059-1000-3 "Р-08" ("Рубеж-08") и его модификаций, программного обеспечения и дополнительного оборудования (производства ООО "СИГМА-ИС", г. Москва)

– СКУ-01;
– УСК-02Н;
– УСК-02С;
– УСК-02АВ;
– СКУСК-01Р.

Интегрированная система безопасности "Стрелец-Интеграл" (производство ЗАО "Аргус-Спектр", г. Санкт-Петербург)

– БПС8-И.

Интегрированная система охраны (ИСО) "Орион" (производство ЗАО НВП "Болид", г. Королев Московская область)

– С2000-КДЛ;
– С2000-2;
– С2000-Proxy.

Цена бесконтактных идентификаторов RFID находится в зависимости от типа идентификатора (активный или пассивный), диапазона его рабочих частот, конструктивного исполнения и наличия дополнительных функций. По состоянию на 11.08.2015 г. цена бесконтактного идентификатора RFID марки "Farpointe Data Standard Light PSC-1" (производитель "Farpointe Data Inc".) составляет 138,00 руб., цена бесконтактного идентификатора RFID марки "Farpointe Data Multi Technology PSM-2" (производитель "Farpointe Data Inc".) составляет 167,00 руб., цена бесконтактного идентификатора RFID типа proximity-брелок марки "Farpointe Data Key Ring Tag PSK-3" (производитель "Farpointe Data Inc".) составляет 182,00 руб.

Цена считывателя бесконтактной идентификационной Proximity-карты марки "Микро-R" (производитель "Прокс") составляет 1432,33 руб., цена считывателя бесконтактной идентификационной Proximity-карты марки "PR-P05" (производитель "Релвест") составляет 12710,00 руб., цена считывателя бесконтактной идентификационной Proximity-карты марки "Em-Reader-LR жесть" (производитель "Прокс") составляет 31250,93 руб.

(Материалы взяты с интернет-страниц http://www.tosb.ru/catalog/identifikatory, http://prox.ru).

5 Идентификация по биометрическому признаку

5.1 Идентификация по отпечатку пальца

Впервые идентификация личности по отпечатку пальца была использована в криминалистике. Возникла целая наука – дактилоскопия, которая занимается вопросами идентификации личности человека по отпечаткам пальцев. Отпечатки пальцев человека являются носителями уникальных индивидуальных признаков. Они обеспечивают возможность однозначной идентификации личности человека (узор папиллярных линий каждого пальца человека является строго индивидуальным и в течение всей жизни остается постоянным, и не изменяется по размеру с 18 – 20-летнего возраста). Дактилоскопия построена на двух основных качествах, присущих узорам папиллярных линий пальцев:

– стабильность рисунка узора на протяжении всей жизни человека;

– уникальность рисунка, что означает отсутствие двух индивидуумов с одинаковыми дактилоскопическими отпечатками.

Созданы современные компьютерные криминалистические системы для сравнения отпечатков пальцев с хранящимися в архиве баз данных изображениями отпечатков пальцев. Пример изображения отпечатка пальца человека приведен на рисунке 5.1.

Рисунок 5.1

Практическое использование работ по дактилоскопическим технологиям для организации систем контроля доступа долгое время казалось нереальным из-за высокой стоимости и сложности подобных систем. В настоящее время – это бурно развивающаяся область. Дактилоскопические технологии переживают сегодня настоящий бум. Это связано с появлением малогабаритных недорогих сканирующих считывателей для ввода отпечатков пальцев, развитием микропроцессорной техники, разработкой компьютерных методов анализа изображений.

Весь процесс идентификации занимает не более нескольких секунд и не требует усилий от тех, кто использует данную систему. В настоящее время уже производятся подобные системы размером меньше колоды карт. Пример исполнения считывателя отпечатка пальцев приведен на рисунке 5.2.

Рисунок 5.2 – Считыватель отпечатков пальцев производства фирмы Microsoft

Определенным недостатком, сдерживающим развитие данного метода, является предубеждение части людей, которые не желают оставлять информацию о своих отпечатках пальцев. При этом контраргументом разработчиков аппаратуры является заверение в том, что информация о папиллярном узоре пальца не хранится – хранится лишь короткий идентификационный код, построенный на базе характерных особенностей отпечатка вашего пальца. По данному коду нельзя воссоздать узор папиллярных линий и сравнить его с отпечатками пальцев, оставленными, допустим, на месте преступления.

Существует два основных алгоритма сравнения полученного кода с имеющимся в базе шаблоном: по характерным точкам и по рельефу всей поверхности пальца. В первом случае выявляются характерные участки и запоминается их взаиморасположение. Во втором случае запоминается вся "картина" в целом. В современных системах используется также комбинация обоих алгоритмов, что позволяет повысить уровень надежности системы.

С целью идентификации личности по отпечаткам пальцев, проверяемый набирает на клавиатуре свой идентификационный номер и помещает указательный палец на окошко сканирующего устройства. При совпадении получаемых признаков с эталонными, предварительно заложенными в память и активизированными при наборе идентификационного номера, подается команда исполнительному устройству. Хотя узор папиллярных линий пальцев индивидуален, использование полного набора их признаков чрезмерно усложняет устройство идентификации. Поэтому с целью его удешевления применяют признаки, наиболее легко измеряемые автоматом. Выпускают сравнительно недорогие устройства идентификации по отпечаткам пальцев, действие которых основано на измерении расстояния между основными дактилоскопическими признаками. На величину вероятности ошибки опознания влияют также различные факторы, в том числе температура пальцев.

Обычно алгоритмы используют характерные точки узора папиллярных линий пальцев: окончание линии узора, разветвлении линии, одиночные точки. Дополнительно привлекается информация о морфологической структуре отпечатка папиллярных линий пальца: относительное положение замкнутых линий папиллярного узора, "арочных" и спиральных линий. Особенности папиллярного узора преобразовываются в уникальный код (образ), который сохраняет информативность изображения отпечатка. И именно "коды отпечатков пальцев" хранятся в базе данных, используемой для поиска и сравнения. Время перевода изображения отпечатка пальца в код и его идентификация обычно не превышает 1 с, в зависимости от размера базы. Время, затраченное на поднесение руки – не учитывается.

Распознавание отпечатка пальца основано на анализе распределения особых точек (концевых точек и точек разветвления папиллярных линий), местоположение которых задается в декартовой системе координат. Для снятия отпечатков в режиме реального времени применяются специальные контактные датчики различных типов.

Говоря о надежности аутентификационной процедуры по отпечаткам пальцев, необходимо рассмотреть также вопрос о возможности их копирования и использования другими лицами для получения несанкционированного доступа. В качестве одной из возможностей по обману терминала специалисты называют изготовление искусственной кисти с требуемыми отпечатками пальцев (или изъятия "подлинника" у законного владельца). Но существует и способ борьбы с такой фальсификацией. Для этого в состав терминального оборудования должны быть включены:

– инфракрасный детектор, который позволит зафиксировать тепловое излучение от руки (или пальца);

– фотоплетизмограф, который определяет наличие изменений отражения света от поверхности потока крови;

– измеритель электрического сопротивления кожи, который позволит контролировать изменение сопротивления организма при различных воздействиях на человека и, соответственно, различном психофизическом состоянии.

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

Известны три основных подхода к реализации систем идентификации по отпечаткам пальцев. Самый распространенный на сегодня способ строится на использовании оптики – призмы и нескольких линз со встроенным источником света. Свет, падающий на призму, отражается от поверхности, соприкасающейся с пальцем пользователя, и выходит через другую сторону призмы, попадая на оптический сенсор (обычно, монохромная видеокамера на основе ПЗС-матрицы), где формируется изображение (см. рисунок 5.3).

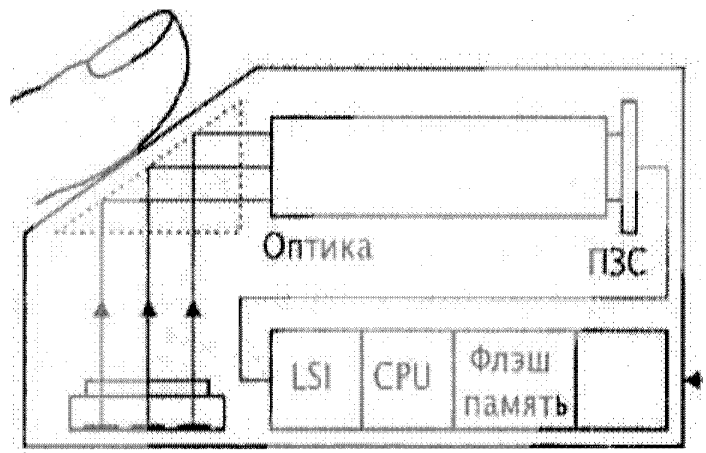


Рисунок 5.3 – Структурная схема оптического сканера отпечатка пальца

Другой способ использует методику измерения электрического поля пальца с применением полупроводниковой пластины. Когда пользователь устанавливает палец в сенсор, он выступает в качестве одной из пластин конденсатора (см. рисунок 5.4). Другая пластина конденсатора – это поверхность сенсора, которая состоит из кремниевого чипа, содержащего 90 тысяч конденсаторных пластин с шагом считывания 500 точек на дюйм. В результате получается 8-битовое растровое изображение гребней и впадин пальца.

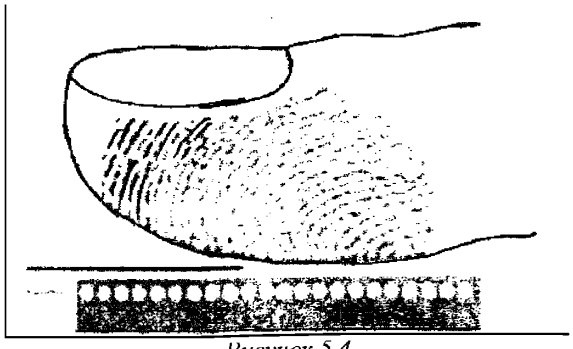


Рисунок 5.4

Существует еще один метод реализации таких систем. Его разработала компания "Who Vision Systems". В основе их системы TactileSense – электрооптический полимер. Этот материал чувствителен к разности электрического поля между гребнями и впадинами кожи. Градиент электрического поля конвертируется в оптическое изображение высокого разрешения, которое затем переводится в цифровой формат, который уже можно передавать в ПК по параллельному порту или USB-интерфейсу.

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

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

Более сложные алгоритмы обработки соединяют характерные точки изображения векторами и описывают их свойства и взаимоположение (см. рисунок 5.5). Алгоритм обработки позволяет хранить не само изображение, а его "образ" (набор характерных данных).

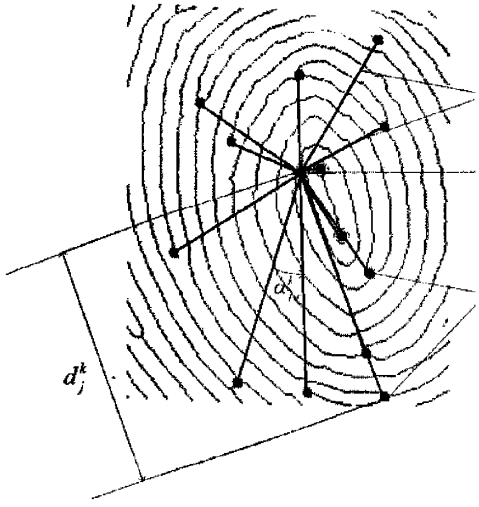


Рисунок 5.5

В таблице 5.1 приведено соотношение статистических показателей FAR и FRR, характеризующих степень достоверности идентификации по отпечатку пальца.

Таблица 5.1

FAR	FRR
0,10 %	0,30 %
0,01 %	0,40 %
0,005 %	0,60 %
0,00 %	0,90 %

Характерное значение FAR для метода идентификации по отпечатку пальца – 0,001 %.

К достоинствам метода идентификации по отпечатку пальца можно отнести:

1) Относительно высокую достоверность, статистические показатели метода (FAR и FRR) лучше показателей способов идентификации по форме лица, голосу, динамике подписи и др.;

2) Низкую стоимость считывателей, сканирующих изображение отпечатка пальца с использованием оптического и электрооптического методов сканирования;

3) Простоту и удобство для пользователя процедуры сканирования отпечатков пальцев;

4) Методика идентификации по отпечаткам пальцев лишена психологических барьеров, которые имеются, например, у систем, требующих воздействия на глаз световым пучком.

К недостаткам метода идентификации по отпечатку пальца можно отнести:

1) Поверхность кожного покрова пальцев часто повреждается из-за оказываемых на руки внешних механических и химических воздействий, что может привести к искажению считываемого биометрического признака – узора папиллярных линий;

2) В системах, использующих полупроводниковый и электронно-оптический методы сканирования отпечатка пальцев, возникают проблемы при сканировании пальцев людей пожилого возраста и людей, обладающих сухой кожей;

3) Высокую стоимость считывателей, сканирующих изображение отпечатка пальца с использованием полупроводникового метода сканирования;

4) Кремниевый чип, применяемый при сканировании изображения пальца с использованием метода полупроводникового сканирования, требует эксплуатации в герметичной оболочке, а дополнительные покрытия уменьшают его чувствительность;

5) Низкую имитостойкость систем, не оснащенных дополнительными средствами распознавания признаков, присущих пальцам живого человека;

6) Определенным недостатком является исторически сложившееся предубеждение в сознании людей, что снятие отпечатков папиллярных линий пальцев ассоциируется с криминальными целями, а также с вторжением в частную жизнь и это вызывает негативный оттенок в реакции на сканирование отпечатков папиллярных линий пальцев;

7) Критичность метода идентификации к чистоте сканирующей поверхности считывателя и кожного покрова пальцев.

Метод идентификации, основанный на применении бесконтактных идентификаторов RFID аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." имеется единственное устройство, использующее метод идентификации по отпечатку пальца – ШУ024-2, входящее в состав **комплекса, состоящего из прибора приемно-контрольного охранно-пожарного и управления ППКОПУ 01059-1000-3 "Р-08" ("Рубеж-08") и его модификаций, программного обеспечения и дополнительного оборудования (производства ООО "СИГМА-ИС", г. Москва)**.

Цена считывателя отпечатков пальцев зависит от метода снятия отпечатков, наличия в считывателе дополнительных методов распознавания имитации признаков, присущих живому человеку, статистических показателей FAR и FRR, характеризующих степень достоверности идентификации, обусловленных заложенным алгоритмом обработки данных программным обеспечением.

По состоянию на 12.08.2015 г цена считывателя отпечатка пальца модель "Smartec ST-FE700" (производитель "Smartec") составляет 5852,00 руб., цена считывателя отпечатка пальца модель "BioSmart FS-80" (производитель "BioSmart") составляет 6555,00 руб., цена считывателя отпечатка пальца модель "ZKTeco ZK7500" (производитель "ZKTeco") составляет 6957,00 руб.

(Информация взята с интернет-страницы http://cctv-optom.ru).

5.2 Идентификация по радужной оболочке глаза

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

С помощью этих алгоритмов необработанные видеоизображения глаза преобразуются в уникальный идентификационный двоичный поток Iris-код, полученный в результате определения позиции радужки, ее границы и выполнения других математических операций для описания текстуры радужной оболочки в виде последовательности чередования фаз, похожих на штрих-код. Пример изображения радужной оболочки глаза приведен на рисунке 5.6.

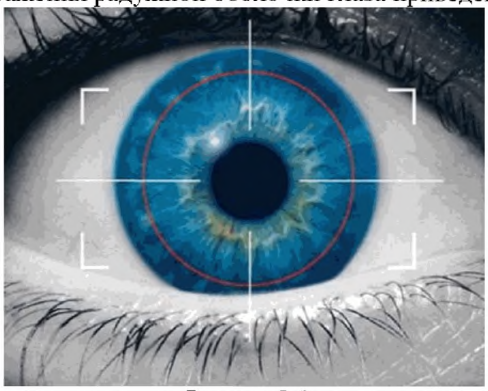


Рисунок 5.6

Полученный таким образом Iris-код используется для поиска совпадений в базах данных (скорость поиска – около 1 миллиона сравнения Iris-кодов в 1 с) и для подтверждения или не подтверждения идентифицируемой личности.

Различают активные и пассивные системы распознавания радужной оболочки глаза. В системах первого типа пользователь должен сам настроить камеру, передвигая ее для более точной наводки. Пассивные системы проще в использовании, поскольку камера в них настраивается автоматически. Пример изображения считывателя радужной оболочки глаза приведен на рисунке 5.7.

Рисунок 5.7

В качестве примера современной системы идентификации на основе анализа радужной оболочки глаза рассмотрим решение, предложенное компанией LG. Система IrisAccess позволяет менее чем за 1 с отсканировать рисунок радужной оболочки глаза, обработать и сравнить с 4 тыс. других записей, которые она хранит в своей памяти, а затем послать соответствующий сигнал в охранную систему. Технология – полностью бесконтактная. На основе изображения радужной оболочки глаза строится компактный цифровой код размером 512 байт. Устройство имеет высокую надежность по сравнению с большинством известных систем биометрического контроля.

Характеристики FAR и FRR для радужной оболочки глаза наилучшие в классе современных биометрических систем (за исключением, возможно, метода распознавания по сетчатке глаза).

В таблице 5.2 приведено соотношение статистических показателей FAR и FRR, характеризующих степень достоверности идентификации по радужной оболочке глаза.

Таблица 5.2

FAR	FRR
0,10 %	0,08 %
0,01 %	0,09 %
0,00 %	0,10 %
0,00 %	0,17 %
0,00 %	0,19 %

Характерное значение FAR для метода идентификации по радужной оболочке глаза – 0,00001 %. Здесь стоит отметить немаловажную особенность, отличающую систему распознавания по радужной оболочке от других систем. В случае использования камеры с разрешением от 1,3 Мп., можно захватывать два глаза на одном кадре. Так как вероятности FAR и FRR являются статистически независимыми вероятностями, то при распознавании по двум глазам значение FAR будет приблизительно равняться квадрату значения FAR для одного глаза. Например, для FAR 0,001 % при использовании двух глаз вероятность ложного допуска будет равна 10 – 8 %, при FRR всего в два раза выше, чем соответствующее значение FRR для одного глаза при FAR равном 0,001%.

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

К достоинствам метода идентификации по радужной оболочке глаза можно отнести:

1) Процесс сканирования радужной оболочки, как правило, не требует от пользователя фокусировки взгляда на какой-либо цели, так как рисунок радужной оболочки находится на поверхности глаза;

2) Высокую достоверность, статистические показатели метода (FAR и FRR) лучше показателей способов идентификации по отпечатку пальца, форме лица, голосу, динамики подписи и др.;

3) Сканирование изображения радужной оболочки глаз можно производить на расстоянии от нескольких сантиметров до нескольких метров, при этом физический контакт человека с устройством отсутствует;

4) Глаза являются одним из самых оберегаемых от повреждения органов человека, что является дополнительной гарантией сохранности и неизменности во времени радужной оболочки глаз.

5) При использовании в считывателях камер высокой четкости возможно одновременное сканирование радужных оболочек сразу двух глаз, что при небольшом увеличении продолжительности обработки данных, значительно повышает достоверность идентификации.

К недостаткам метода идентификации по радужной оболочке глаза можно отнести:

1) Высокую сложность и стоимость считывателей;

2) Считыватели требуют бережного отношения и квалифицированного обслуживания;

3) Камера, используемая в считывателях чувствительна к загрязнению, из-за чего считыватели и их применение вне помещения имеют жесткие ограничения.

Метод идентификации по радужной оболочке глаза аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения считывателей радужной оболочке глаза не представлено.

Цена считывателей радужной оболочке глаза зависит от статистических показателей FAR и FRR, характеризующих степень достоверности идентификации, обусловленных заложенным алгоритмом обработки данных программным обеспечением.

По состоянию на 11.08.2015 г. цена биометрического считывателя радужной оболочки глаза модели "EyeLock EyeSwype Nano" (производитель "EyeLock") составляет 325085,00 руб., цена биометрического считывателя радужной оболочки глаза модели "EyeLock EyeSwype Nano-TS" (производитель "EyeLock") составляет 455118,00 руб.

(Информация взята с интернет-страницы http://videoglaz.ru/catalog).

5.3 Идентификация по сетчатке глаза

При идентификации по сетчатке глаза измеряется угловое распределение кровеносных сосудов на поверхности сетчатки относительно слепого пятна глаза и другие признаки. Капиллярный рисунок сетчатки глаз различается даже у близнецов и может быть с большим успехом использован для идентификации личности. Изображение капилляров сетчатки глаза человека представлено на рисунке 5.8.

Рисунок 5.8

Всего насчитывают около 250 признаков. Такие биометрические терминалы обеспечивают высокую достоверность идентификации, сопоставимую с дактилоскопией, но требуют от проверяемого лица фиксации взгляда на объективе сканера.

Сканирование сетчатки происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Сканеры сетчатки глаза получили широкое распространение в СКУД особо секретных объектов, так как у них один из самых низких процентов отказа в доступе зарегистрированных пользователей (FAR) и практически не бывает ошибочного разрешения доступа (FRR). Однако изображение радужной оболочки должно быть четким, поэтому катаракта может отрицательно воздействовать на качество идентификации личности. Пример сканера сетчатки глаз приведен на рисунке 5.9.

Рисунок 5.9

Начало разработок этого направления идентификации относится к 1976 г., когда в США была образована компания Eye Dentify, которая до настоящего времени сохраняет монополию на производство коммерческих систем аутентификации по ретине. Основным устройством для системы такого типа является бинокулярный объектив. При осуществлении процедуры аутентификации пользователь должен прильнуть глазами к окулярам и, глядя вовнутрь, сфокусировать взгляд на изображении красного цвета. Затем, ему следует дождаться смены цвета на зеленый (что указывает на правильную фокусировку) и нажать на стартовую кнопку. Сканирование глазного дна выполняется источником инфракрасного излучения, безопасного для глаз. Достаточно смотреть в глазок камеры менее минуты. За это время система успевает подсветить сетчатку и получить отраженный сигнал. Для сканирования сетчатки используется инфракрасное излучение низкой интенсивности, направленное через зрачок к кровеносным сосудам на задней стенке глаза. Отраженное от ретины излучение фиксируется специальной чувствительной камерой.

Замеры ведутся по 320 точкам фотодатчиками и результирующий аналоговый сигнал с помощью микропроцессора преобразуется в цифровой код. При этом используется алгоритм быстрого преобразования Фурье. Полученный цифровой вектор, состоящий из коэффициентов Фурье, сравнивается с зарегистрированным эталоном, хранящимся в памяти системы. Благодаря такому методу преобразования и представления изображения глазного дна, для хранения каждого эталона расходуется по 40 байт. Память терминала Eye Dentification System 7.5, реализующего этот алгоритм, рассчитана на запоминание до 1200 эталонов. Время регистрации составляет примерно 30 с, время аутентификации – 1,5 с. При этом, значение FAR составляет 0,01 %, а FRR – 0,0001 %.

С точки зрения безопасности данная система выгодно отличается от всех других, использующих биометрические терминалы, не только малым значением FAR и FRR, но и использованием специфического аутентификационного атрибута, который практически невозможно подменить для обмана системы при проверке.

К достоинствам метода идентификации по сетчатке глаза можно отнести:

1) Высокую достоверность, статистические показатели метода (FAR и FRR) сопоставимы с аналогичными показателями идентификации по радужной оболочке глаза;

2) Глаза являются одним из самых оберегаемых от повреждения органов человека, что является дополнительной гарантией сохранности и неизменности во времени сетчатки глаз.

К недостаткам метода идентификации по сетчатке глаза можно отнести:

1) Высокая сложность и стоимость считывателей;

2) Сложность и сравнительно большая продолжительность процесса распознавания идентификационного признака;

3) Низкая пропускная способность систем, использующих данный метод идентификации;

4) Возникновение у большинства людей психологического барьера, причиной которого является подсознательное желание уберечь глаза от какого-либо воздействия (инфракрасная подсветка).

Метод идентификации по сетчатке глаза аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения сканеров сетчатки глаза не представлено.

Цена сканеров сетчатке глаза зависит от типа используемых сканеров (монокулярный, бинокулярный), статистических показателей FAR и FRR, характеризующих степень достоверности идентификации, обусловленных заложенным алгоритмом обработки данных программным обеспечением.

По состоянию на 11.08.2015 г. цена сканера сетчатки глаза фирмы "Myris" модели "eyeLock" составляет 19506,00 руб., цена сканера сетчатки глаза модели "Fujitsu-siemens scananap SV600" (производитель "Fujitsu-siemens") составляет 44990,0 руб.

(Информация взята с интернет-страницы http://e-go-shop.ru/skanjer-sjetchatki-glaza).

5.4 Идентификация по геометрии лица

Существует множество методов распознавания по геометрии лица. Все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны. Эта область биометрии достаточно перспективна, потому что мы узнаем друг друга в первую очередь по лицу. Данная область делится на два направления: 2-D распознавание и 3-D распознавание. У каждого из них есть достоинства и недостатки, однако многое зависит еще и от области применения и требований, предъявленных к конкретному алгоритму.

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

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

2-D распознавание лица – один из самых статистически неэффективных методов биометрии. Появился он довольно давно и применялся, в основном, в криминалистике, что и способствовало его развитию. В последствие появились компьютерные интерпретации метода, в результате чего он стал более надёжным, но, безусловно, уступал и с каждым годом все больше уступает другим биометрическим методам идентификации личности. В настоящее время из-за плохих статистических показателей он применяется, в мультимодальной или, как ее еще называют, перекрестной биометрии, или в социальных сетях.

Пример 2-D образа лица человека, созданного на основе его характерных точек приведен на рисунке 5.10.

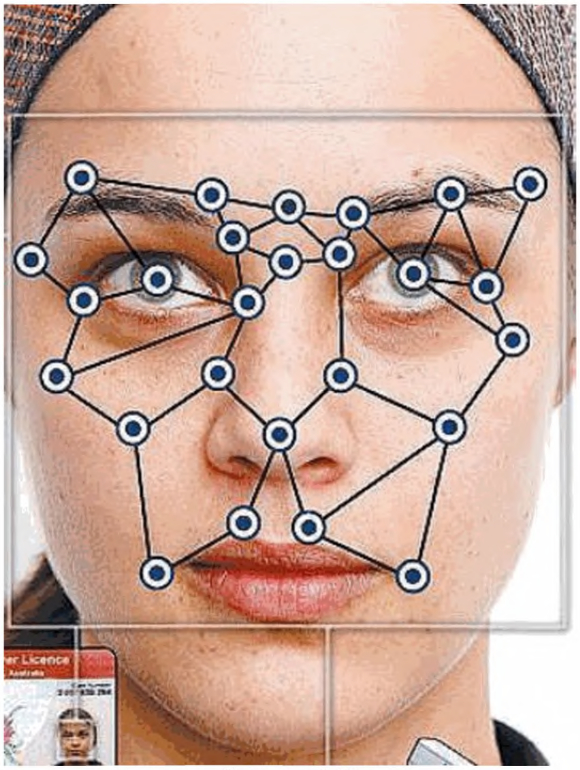


Рисунок 5.10

В таблице 5.3 приведено соотношение статистических показателей FAR и FRR, характеризующих степень достоверности идентификации по 2-D геометрии лица.

Таблица 5.3

FAR	FRR
0,10 %	2,50 %
0,01 %	5,00 %
0,00 %	6,00 %
0,00 %	9,00 %

Характерное значение FAR для метода идентификации по 2-D геометрии лица – 0,1 %.

Реализация метода идентификации по 3-D геометрии лица представляет собой довольно сложную задачу. Несмотря на это, в настоящее время существует множество методов по 3-D распознаванию лица. Методы невозможно сравнить друг с другом, так как они используют различные сканеры и базы. Далеко не все из них выдают FAR и FRR, используются абсолютно различные подходы. Переходным от 2-D к 3-D методом является метод, реализующий накопления информации по лицу. Этот метод имеет лучшие характеристики, чем 2-D метод, но так же, как и он использует всего одну камеру. При занесении субъекта в базу, субъект поворачивает голову, и алгоритм соединяет изображение воедино, создавая 3-D образ. Пример 3-D образа лица человека приведен на рисунке 5.11.

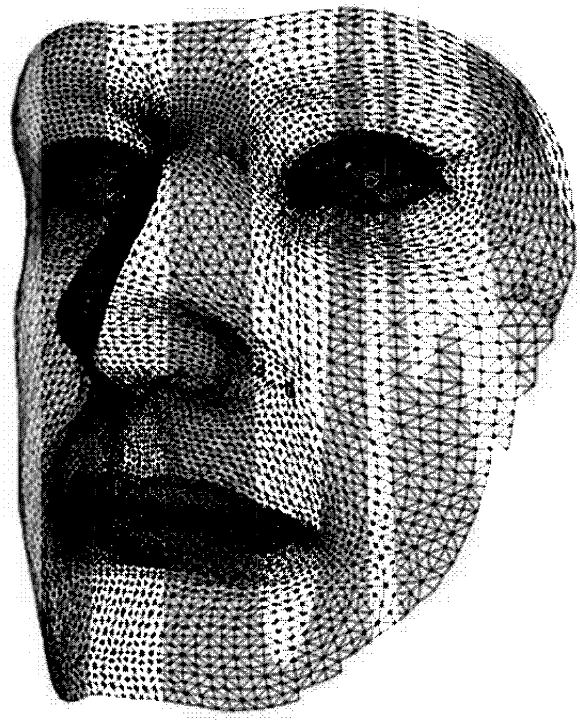


Рисунок 5.11

А при распознавании используется несколько кадров видеопотока. Наиболее классическим методом является метод проецирования шаблона. Он состоит в том, что на объект (лицо) проецируется сетка. Далее камера делает снимки со скоростью десятки кадров в секунду, и полученные изображения обрабатываются специальной программой. Луч, падающий на искривленную поверхность, изгибается – чем больше кривизна поверхности, тем сильнее изгиб луча. Изначально при этом применялся источник видимого света, подаваемого через "жалюзи". Затем видимый свет был заменен на инфракрасный, который обладает рядом преимуществ. Обычно на первом этапе обработки отбрасываются изображения, на котором лица не видно вообще или присутствуют посторонние предметы, мешающие идентификации. По полученным снимкам восстанавливается 3-D модель лица, на которой выделяются и удаляются ненужные помехи (прическа, борода, усы и очки). Затем производится анализ модели – выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносящийся в базу данных. Время захвата и обработки изображения составляет 1 – 2 секунды для лучших моделей. Так же набирает популярность метод 3-D распознавания по изображению, получаемому с нескольких камер. Этот метод даёт точность позиционирования, согласно уверениям разработчиков, выше метода проецирования шаблона.

Статистическая надежность метода идентификации по 3-D геометрии лица сравнима с надежностью метода идентификации по отпечаткам пальцев. Характерное значение FAR для метода идентификации по 3-D геометрии лица – 0,0047 %, а FRR – 0,103 %.

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

В настоящее время существует четыре основных метода распознавания лица, различающихся сложностью реализации и целью применения:

– "eigenfaces";

– анализ "отличительных черт";

– анализ на основе "нейронных сетей";

– метод "автоматической обработки изображения лица".

"Eigenface" можно перевести как "собственное лицо". Эта технология использует двумерные изображения в градациях серого, которые представляют отличительные характеристики изображения лица. Метод "eigenface" часто используется в качестве основы для других методов распознавания лица. Комбинируя характеристики 100 – 120 "eigenface", можно восстановить большое число лиц. В момент регистрации "eigenface" каждого конкретного человека представляется в виде ряда коэффициентов. Для режима установления подлинности, в котором изображение используется для проверки идентичности, "живой" шаблон сравнивается с уже зарегистрированным шаблоном с целью определения коэффициента различия. Степень различия между шаблонами определяет факт идентификации. Технология "eigenface" оптимальна при использовании в хорошо освещенных помещениях, когда есть возможность сканирования лица в фас.

Метод анализа "отличительных черт" – наиболее широко используемая технология идентификации. Она подобна методу "Eigenface", но в большей степени адаптирована к изменению внешности или мимики человека (улыбающееся или хмурящееся лицо). В технологии "отличительных черт" используются десятки характерных особенностей различных областей лица, причем с учетом их относительного местоположения. Индивидуальная комбинация этих параметров определяет особенности каждого конкретного лица. Лицо человека уникально, но достаточно динамично, так как человек может улыбаться, отпускать бороду и усы, надевать очки – все это увеличивает сложность процедуры идентификации. Например, при улыбке наблюдается некоторое смещение частей лица, расположенных около рта, что в свою очередь будет вызывать подобное движение смежных частей. Учитывая такие смещения, можно однозначно идентифицировать человека и при различных мимических изменениях лица. Так как этот анализ рассматривает локальные участки лица, допустимые отклонения могут находиться в пределах до 25° в горизонтальной плоскости, и приблизительно до 15° в вертикальной плоскости и требует достаточно мощной и дорогой аппаратуры, что соответственно снижает возможности распространения данного метода.

В методе, основанном на нейронной сети, характерные особенности обоих лиц – зарегистрированного и проверяемого, сравниваются на совпадение. "Нейронные сети" используют алгоритм, устанавливающий соответствие уникальных параметров лица проверяемого человека и параметров шаблона, находящегося в базе данных, при этом применяется максимально возможное число параметров. По мере сравнения определяются несоответствия между лицом проверяемого и шаблоном из базы данных, затем запускается механизм, который с помощью соответствующих весовых коэффициентов определяет степень соответствия проверяемого лица шаблону из базы данных. Этот метод увеличивает качество идентификации лица в сложных условиях.

Метод автоматической обработки изображения лица – наиболее простая технология, использующая расстояния и отношение расстояний между легко определяемыми точками лица, такими, как глаза, конец носа, уголки рта. Хотя данный метод не столь мощный, как "eigenfaces" или "нейронная сеть", он может быть достаточно эффективно использован в условиях слабой освещенности.

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

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

2) Определение положения головы. Определение положения головы человека является важным этапом и позволяет внести поправки при дальнейшем распознавании. На этом этапе

созданная компанией трехмерная модель головы сопоставляется с изображением головы в кадре. При этом оцениваются такие параметры, как угол поворота головы по осям X, Y, Z, точный замер и смещение изображения в кадре.

3) Отслеживание перемещения лица от кадра к кадру. При идентификации движущегося в поле зрения камеры человека необходимо отслеживать перемещение лица от кадра к кадру. Имея несколько изображений одного и того же человека в разных ракурсах, программа выбирает наиболее удачный с ее точки зрения кадр и сохраняет его в базе данных. Обрабатывая несколько изображений одного и того же человека в разных ракурсах, можно добиться очень высокой точности распознавания.

4) Сравнение изображения с данными базы.

Этот этап является логическим завершением в цепочке алгоритма идентификации личности по видеоизображению.

Оценочные характеристики при проверке эффективности различных вариантов таких устройств приведены в таблице 5.4.

Таблица 5.4. Проверка эффективности распознавания черт лица

Условия оценки эффективности	FAR, %	FRR, %
Один и тот же день, одно и то же освещение	2	0,4
Один и тот же день, разное освещение	2	9
Разные дни	2	11
Разные дни в течение 1,5 лет	2	43

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

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

Путем сканирования изображения лица в инфракрасном свете создается уникальная температурная карта лица – термограмма. Идентификация по термограмме обеспечивает показатели, сравнимые с показателями идентификации по отпечаткам пальцев.

К достоинствам метода идентификации по геометрии лица можно отнести:

1) Высокую достоверность, статистические показатели метода (FAR и FRR) сопоставимы с аналогичными показателями идентификации по отпечатку пальца (идентификация по 3-D геометрии лица);

2) Сравнительно низкую стоимость оборудования (идентификация по 2-D геометрии лица);

3) Отсутствие необходимости физического контакта пользователя со сканером;

4) Высокую устойчивость к воздействию дестабилизирующих факторов как в облике распознаваемого человека (наличие бороды, очков, изменение прически и т.п.), так и в условиях процесса идентификации (поворот головы, низкая освещенность) (идентификация по 3-D геометрии лица);

К недостаткам метода идентификации по геометрии лица можно отнести:

1) Низкую статистическую достоверность (идентификация по 2-D геометрии лица);

2) Слабую устойчивость к воздействию дестабилизирующих факторов (идентификация по 2-D геометрии лица);

3) Обязательно фронтальное расположение идентифицируемого лица (идентификация по 2-D геометрии лица);

4) Высокую стоимость оборудования (идентификация по 3-D геометрии лица).

Метод идентификации по геометрии лица аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения сканеров геометрии лица не представлено.

Цена сканеров геометрии лица зависит от метода регистрации (2-D, 3-D), статистических показателей FAR и FRR, характеризующих степень достоверности идентификации, обусловленных заложенным алгоритмом обработки данных программным обеспечением.

По состоянию на 11.08.2015 г. цена сканера геометрии лица марки "BRAVO VF-380" (производитель "Bravo") составляет 16958,00 руб, цена сканера по геометрии лица марки "Smartec ST-FR040EM" (производитель "Smartec") составляет 24872,00 руб., цена сканера по геометрии лица марки "L1 Bioscrypt 3D Face Reader" (производитель "L1") составляет 534432,00 руб.

(Информация взята с интернет-страницы http://cctv-optom.ru).

5.5 Идентификация по почерку и динамике подписи

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

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

Подпись – такой же уникальный атрибут человека, как и его физиологические характеристики. Кроме того, это и более привычный для любого человека метод идентификации, поскольку он, в отличие от снятия отпечатков пальцев, не ассоциируется с криминальной сферой.

Одна из перспективных технологий аутентификации основана на уникальности биометрических характеристик движения человеческой руки во время письма. Обычно выделяют два способа обработки данных по подписи: простое сравнение с образцом и динамическую верификацию.

Первый весьма ненадежен, так как основан на обычном сравнении введенной подписи с хранящимися в базе данных графическими образцами. Из-за того, что подпись не может быть всегда одинаковой, этот метод дает большой процент ошибок.

Способ динамической верификации требует намного более сложных вычислений и позволяет в реальном времени фиксировать параметры процесса подписи, такие, как скорость движения руки на разных участках, сила давления и длительность различных этапов подписи. Это дает гарантии того, что подпись не сможет подделать даже опытный графолог, поскольку никто не в состоянии в точности скопировать поведение руки владельца подписи. Пользователь имитирует свою обычную подпись, а система считывает параметры движения и сверяет их с теми, что были заранее введены в базу данных. При совпадении образа подписи

с эталоном, система прикрепляет к подписываемому документу информацию, включающую имя пользователя, адрес его электронной почты, должность, текущее время и дату, параметры подписи, содержащие несколько десятков характеристик динамики движения (направление, скорость, ускорение) и другие. Эти данные шифруются, затем для них вычисляется контрольная сумма, и далее все это шифруется еще раз, образуя так называемую биометрическую метку. Для настройки системы вновь зарегистрированный пользователь от пяти до десяти раз выполняет процедуру подписания документа, что позволяет получить усредненные показатели и доверительный интервал.

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

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

Пороговое значение коэффициентов ошибок может изменяться в зависимости от требуемой степени безопасности. Подпись выполняется обычной шариковой ручкой или карандашом на специальной сенсорной панели, входящей в состав терминала.

К достоинствам метода идентификации по почерку и динамике подписи можно отнести:

1) Высокую имитостойкость, обусловленную сложностью точного воспроизводства индивидуальных параметров динамики написания текста;

2) Метод не вызывает "технологического дискомфорта", как бывает в случае снятия отпечатков пальцев, что ассоциируется с деятельностью правоохранительных органов.

К недостаткам метода идентификации по почерку и динамике подписи можно отнести:

1) Низкую производительность (пропускная способность);

2) Сравнительно невысокую статистическую достоверность;

3) Сложность и высокая стоимость оборудования считывателя.

Метод идентификации по почерку и динамике подписи аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения устройств идентификации по почерку и динамике подписи, не представлено.

Цена устройств идентификации по почерку и динамике подписи зависит от статистических показателей FAR и FRR, характеризующих степень достоверности идентификации, обусловленных заложенным алгоритмом обработки данных программным обеспечением.

По состоянию на 11.08.2015 г. цена считывателя характеристик почерка и динамики подписи CS-170S-X фирмы Wacom составляет 2335,80 руб., модели KP-300E-01 - 9312,60 руб.

(Информация взята с интернет-страницы http://dic.academic.ru)

5.6 Идентификация по геометрии кисти рук

Метод идентификации пользователей по геометрии руки по своей технологической структуре и уровню надежности сопоставим с методом идентификации по отпечатку пальца. Статистическая вероятность существования двух кистей рук с одинаковой геометрией чрезвычайно мала. Однако, следует учитывать, что признаки руки меняются с возрастом, а биометрический считыватель имеет сравнительно большие размеры. Пример считывателя геометрии руки приведен на рисунке 5.12.

Рисунок 5.12

Существующие в настоящее время устройства идентификации по геометрии кисти рук используют математическую модель идентификации по данному параметру, имеющую объем, не превышающий 9 байт. Это позволяет хранить большой объем записей и быстро осуществлять процесс идентификации. При этом устройство сканирует как внутреннюю, так и боковую сторону ладони, используя для этого встроенную видеокамеру и различные алгоритмы сжатия изображения. В процессе построения идентификационного оцифрованного образа оценивается более 90 различных характеристик, включая размеры самой ладони в трех плоскостях, длину и ширину пальцев, очертания суставов и иных параметров. Для повышения достоверности идентификации в идентификаторы могут быть введены элементы сканирования иных параметров руки. В системах идентификации считывание геометрических размеров силуэта кисти руки может производиться как с разведенными, так и со сведенными пальцами.

Для проведения процедуры считывания геометрических характеристик кисти, ее кладут ладонью вниз на оптическую сенсорную панель. Через прорези в ее поверхности оптические сенсорные ячейки сканируют кисть по опорным точкам ладони и фаланг пальцев (см. рисунок 5.13).

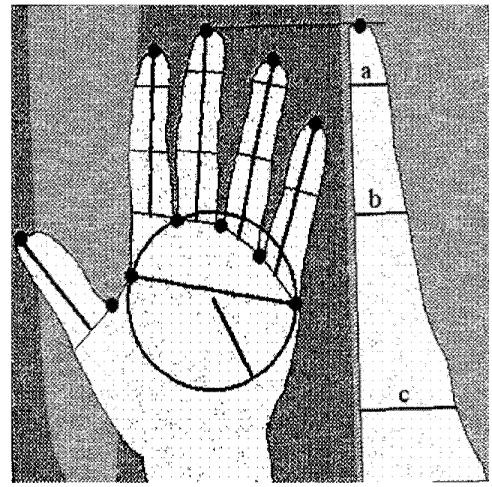


Рисунок 5.13

Идентификатор определяет стартовые точки по оцифрованным моделям двух пар пальцев – указательному и среднему, безымянному и мизинцу. Каждый палец сканируется по всей длине, при этом замеряется длина, изгиб и расстояние до соседнего пальца. Если каждое измерение соответствует допустимому диапазону зарегистрированного опорного образа, то результат аутентификации считается положительным. Оцифрованный образ может храниться либо в базе данных, либо в памяти идентификационной карточки пользователя. С целью обеспечения дополнительной защиты от копирования и имитации, данные подвергаются дополнительному шифрованию.

Для повышения корректности результата идентификации, в цифровой образ включается дополнительные данные, несущие информацию о допустимых отклонениях в образе, зависящих от качества отсканированного изображения кисти. Указанные меры обеспечивают вероятность ошибок FAR – 1 %, FRR – 1,5 %.

К достоинствам идентификации по геометрии кисти рук можно отнести:

1) Высокую достоверность, статистические показатели метода (FAR и FRR) выше показателей способов идентификации по голосу, динамике росписи и др.;

2) Простоту и удобство для пользователя процедуры сканирования кисти рук;

3) Методика идентификации по кисти рук лишена психологических барьеров, которые имеются, например, у систем, требующих воздействия на глаз световым пучком.

4) Отсутствие чувствительности к повреждениям кожного покрова.

К недостаткам идентификации по геометрии кисти рук следует отнести:

1) Высокую стоимость считывателей, сканирующих изображение кисти рук с использованием оптического и электрооптического методов;

2) Низкую имитостойкость систем, не оснащенных дополнительными средствами распознавания признаков присущих кистям рук живого человека;

3) Критичность метода идентификации к чистоте сканирующей поверхности считывателя и кожного покрова пальцев.

Метод идентификации по геометрии кисти рук аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения устройств идентификации по геометрии кисти рук, не представлено.

Цена устройств идентификации по геометрии кисти рук зависит от метода, статистических показателей FAR и FRR, характеризующих степень достоверности идентификации, обусловленных заложенным алгоритмом обработки данных программным обеспечением.

По состоянию на 11.08.2015 г. цена считывателя геометрии кисти рук "HandKey

ID3D-R" (производитель "Recognition Systems") складывается из стоимости самого сканера и программного обеспечения к нему и составляет в зависимости от количества встраиваемых считывателей от 208614.69 руб. до 297071.94 руб.

(Информация взята с интернет-страницы http:// www.aamsystems).

5.7 Идентификация по голосу

Метод идентификации пользователей по голосу по своему принципу очень удобен ввиду отсутствия необходимости производить какие-либо действия со стороны пользователя. Однако данный метод имеет низкую точность идентификации ввиду природного искажения голоса под действием естественных факторов: времени суток, степени усталости, сытости, наличия заболеваний носоглотки у пользователя и иных факторов.

Также помехи могут быть внесены аудиотрактом или в процессе формирования эталонного образа. Следует учитывать, что отрицательное влияние на процесс идентификации оказывают ошибки при произнесении, различное эмоциональное состояние проверяемого в момент регистрации эталона при каждой идентификации, использование разных устройств регистрации при записи эталонов и идентификации, помехи в низкокачественных каналах передачи данных, внешний акустический шум и т. п.

Основными факторами, снижающими имитостойкость метода идентификации по голосу, являются возможность использования несанкционированно произведенных магнитофонных записей или возможность имитации голоса.

Данные особенности метода идентификации вытекают из его принципа работы. Система записывает парольную фразу в спектрально-временном представлении (см. рисунок 5.14) и формирует эталонный образ из оцифрованного представления рисунка гармонического ряда голосовых формант и его изменения во времени. Ошибки и допуски при проведении каждой из операций в процессе формирования эталонного образа или при каждой процедуре идентификации отрицательно сказываются на показателе имитостойкости метода и являются неизбежными, поскольку система идентификации производит оценку конкретных параметров речевого сигнала.

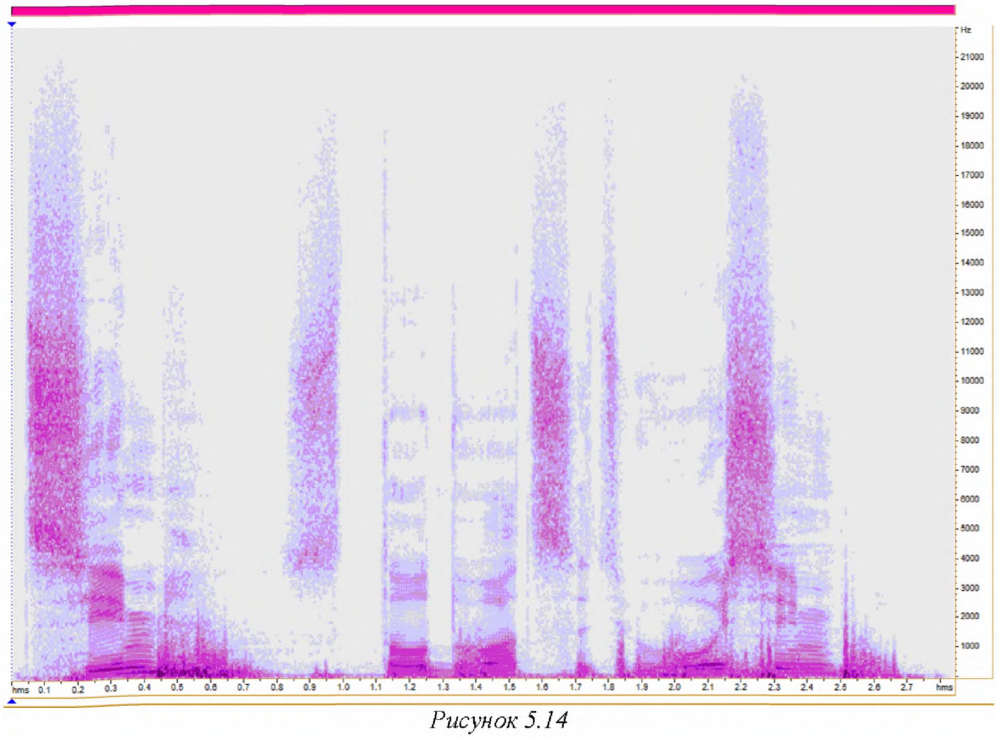


Рисунок 5.14

Ввиду того, что человек оценивает воспринимаемый голос по характерным качествам, не обращая внимания на количественную сторону отдельных компонент речевого сигнала, максимально точная имитация голоса возможна только при наличии у имитируемой речи ярко выраженных особенностей произношения или тембра. Поэтому, увеличение количества анализируемых признаков голоса и усложнение алгоритмов анализа способствует уменьшению вероятности положительного результата распознавания имитируемого голоса. Также для повышения имитостойкости метода идентификации по голосу может применяться метод генерации системой псевдослучайных паролей, которые необходимо проговаривать пользователю при идентификации или при применении дополнительных методов идентификации (по запоминаемому коду или вещественному идентификатору).

Задача повышения надежности распознавания может быть решена за счет привлечения грамматической и семантической информации в системах распознавания речи. Для решения этой задачи разработана модель входного языка, учитывающая особенности грамматического и семантического поведения языка. Лингвистический процессор, построенный на основе учитывающей особенности языка лингвистической базы, работающий под управлением программы синтактико-семантического анализа, обеспечивает:

– отсеивание маловероятных вариантов распознавания;

– учет обнаруженных при анализе грамматических событий, характеризующих регулярность грамматической структуры;

– степень грамотности предложения в целом.

Указанные особенности позволяют повысить надежность акустического и фонетического распознавания до 95 – 97 % при среднем времени одного цикла идентификации до 15 с при фразах из трех – четырех слов. Соответствующая указанным показателям вероятность ошибок составляет: FAR – 0,3 %, FRR – 1 %.

К достоинствам метода идентификации по голосу можно отнести:

1) Удобство использования, обусловленное дистанционностью процесса идентификации, не подразумевающего позиционирования и физического контакта пользователя со считывающей системой.

2) Возможность скрытой установки считывающей системы повышает ее вандалоустойчивость.

К недостаткам метода идентификации по голосу следует отнести:

1) Высокую стоимость программного обеспечения, включающего в себя лингвистический процессор, модули синтактико-семантического анализа и лингвистическую базу.

2) Низкую имитостойкость в случае отсутствия дополнительных методов идентификации;

3) Высокую вероятность возникновения ошибок второго рода (FRR) по причине изменения характеристик голоса под воздействием физиологических причин.

Метод идентификации по голосу аппаратно совместим с применяемым в подразделениях вневедомственной охраны МВД России объектовым оборудованием, но для его использования требуется совместимость с протоколом обмена данными объектового оборудования.

В настоящее время в "Списке технических средств..." системы или технические средства охраны, имеющие в своем составе, или имеющие возможность подключения устройств идентификации по голосу, не представлено.

Цена устройств идентификации по голосу зависит от метода, статистических показателей FAR и FRR, характеризующих степень достоверности идентификации, обусловленных заложенным алгоритмом обработки данных программным обеспечением.

Для метода идентификации по голосу, не требуется дорогостоящая аппаратура, достаточно микрофона и звуковой платы, подключенных к компьютеру. По состоянию на 11.08.2015 г. цена микрофона для ПК фирмы Philips SBCMD650/00 составляет 620,00 руб., цена микрофона для ПК фирмы Philips SBCME570/00 составляет 740 руб., цена микрофона фирмы Sven MK-200 составляет 1350,00 руб. Цена звуковой платы Creative Labs Sound Blaster Live составляет 2346,00 руб., цена звуковой платы Adlib 598,55 руб.

(Информация взята с интернет-страницы http://www.sotmarket.ru/category/microfony).

6 Сравнительный анализ методов персональной идентификации

6.1 Достоверность считывания

Достоверность считывания – степень соответствия кода или образа (оцифрованного представления) идентификационного признака, распознанного считывателем, его опорному представлению, имеющемуся в базе данных системы идентификации.

Наименьшей достоверностью считывания обладают системы, использующие методы идентификации по вещественному коду, процесс распознавания которого сопряжен с преобразованием нецифрового представления кода в цифровой формат.

В указанных системах используются следующие типы идентификаторов:

– идентификаторы с перфорационным кодированием;

– идентификаторы со встроенными пассивными радиоэлементами или магнитами;

– идентификаторы с линейным и двухмерным штриховым кодированием;

– идентификационные карты с магнитным кодированием;

– идентификационные карты с оптической памятью;

– идентификационная карта с голографической памятью.

Низкая достоверность перечисленных идентификаторов обусловлена низкой устойчивостью нецифровых носителей кода к влиянию внешних воздействий. Идентификационные карты с перфорационным и штриховым кодированием критичны к загрязнению области, содержащей индивидуальный код. Идентификационные карты с оптической и голографической памятью обеспечивают корректное считывание при выполнении условия прозрачности защитного слоя области данных. Идентификаторы со встроенными пассивными радиоэлементами или магнитами подвержены изменению их технических параметров со временем или под действием меняющихся условий внешней среды. Корректность считывания идентификационных карт с магнитным кодированием находится в зависимости от скорости протягивания магнитной полосы вдоль считывающей магнитной головки.

Наивысшей достоверностью считывания обладают системы, использующие методы идентификации по запоминаемому коду и по вещественному коду, в основу процесса считывания которого положен цифровой обмен данными.

К таким вещественным идентификаторам относятся:

– идентификационная карта Виганда (Wiegand);

– электронные ключи iButton (Touch Memory);

– идентификационная смарт-карта;

– бесконтактные идентификаторы RFID.

Столь высокая достоверность считывания указанных идентификаторов является следствием устойчивости носителей идентификационных признаков к воздействию внешних неблагоприятных факторов и повышенной надежности процесса считывания.

Наивысшая достоверность считывания запоминаемого кода обусловлена простотой и высокой степенью повторяемости процесса введения кодовой последовательности.

Достоверность считывания системы, использующей методы идентификации по биометрическим признакам, зависит от многообразия характеристик идентифицируемой части человеческого тела и алгоритмов преобразования их физических параметров в цифровое представление образа. Сложность части человеческого тела, используемой для идентификации, как и задание большого числа опорных точек, используемых для создания ее образа, способствует повышению достоверности считывания. В настоящее время существуют системы, использующие методы идентификации по биометрическим признакам, обладающие низкой, средней и высокой степенью достоверности.

6.2 Устойчивость к копированию

Устойчивость к копированию – способность идентификатора обеспечивать защиту области идентификационных данных от несанкционированного копирования.

В принципы идентификации по запоминаемому коду и по биометрическому признаку изначально заложено отсутствие вещественного носителя кода, в связи с чем, копирование идентификационного признака невозможно.

Наименьшей устойчивостью к копированию кода обладают:

– идентификаторы с перфорационным кодированием;

– идентификаторы с линейным и двухмерным штриховым кодированием.

Низкая устойчивость к копированию указанных идентификаторов обусловлена простотой получения визуального образа идентификационных признаков без применения специализированного оборудования. Снимок кодового поля, сделанный на бытовой фотографический аппарат, достаточен для успешного создания копии идентификатора.

Для следующих идентификаторов проведение несанкционированного копирования кода возможно, но требует применения специализированного оборудования:

– идентификаторы со встроенными пассивными радиоэлементами или магнитами;

– идентификационные карты с магнитным кодированием;

– электронные ключи iButton (Touch Memory);

– бесконтактные идентификаторы.

Несанкционированное копирование данных, осуществленное в процессе защищенного обмена кодовыми посылками между идентификатором и считывателем, не позволят раскрыть алгоритм шифрования, а, следовательно, будет бесполезным в попытке создания имитации идентификатора.

В настоящее время существуют системы, использующие бесконтактные идентификаторы, обладающие различной степенью криптозащищенности канала передачи данных и устойчивостью к их копированию.

Наиболее устойчивыми к копированию кода являются следующие типы идентификаторов:

– идентификационные карты с оптической памятью;

– идентификационная карта с голографической памятью.

– идентификационная карта Виганда (Wiegand);

– идентификационная смарт-карта.

В идентификационных картах с оптической и голографической памятью кодовая информация представлена в виде последовательности питов или интерференционного оттиска, размеры элементов которых не позволяют произвести копирование содержащихся данных без специализированного промышленного оборудования.

Каждая идентификационная карта Виганда имеет впрессованный в объем карты набор полосок проводников, состав материала которых является интеллектуальной собственностью фирмы-изготовителя и не поддается повторению.

Идентификационная смарт-карта оснащена миниатюрной интегральной микросхемой (запоминающим устройством и микропроцессором), обеспечивающей реализацию процессов логической, математической и криптообработки данных, исключающих возможность их копирования.

6.3 Имитостойкость

Имитостойкость – свойство идентификатора, характеризующееся устойчивостью к имитации его идентификационного признака.

В принцип идентификации по запоминаемому коду изначально заложено отсутствие вещественного носителя кода, в связи с чем, имитация идентификатора как такового невозможна.

Наименьшей имитостойкостью обладают системы, использующие следующие типы идентификаторов:

– идентификаторы с перфорационным кодированием;

– идентификаторы со встроенными пассивными радиоэлементами или магнитами;

– идентификаторы с линейным и двухмерным штриховым кодированием;

– идентификационные карты с магнитным кодированием;

– электронные ключи iButton (Touch Memory) типа DS1990A.

Электронные ключи iButton всех других типов содержат программные методы защиты области данных, что обеспечивает их высокую имитостойкость. Вместе с тем, открытость протокола обмена данными создает угрозу изготовления устройств, полностью имитирующих работу электронных ключей iButton.

Наилучшую имитостойкость демонстрируют системы, использующие следующие типы

идентификаторов (идентификационных признаков):

– идентификационные карты с оптической памятью;

– идентификационная карта с голографической памятью;

– идентификационная карта Виганда (Wiegand);

– электронные ключи iButton (Touch Memory), за исключением типа DS1990A;

– идентификационная смарт-карта;

– идентификация по биометрическому признаку.

Высокая имитостойкость систем, использующих указанные типы идентификаторов, обусловлена следующими факторами:

– наличием защищенного протокола обмена данными (электронные ключи iButton, за исключением ключа типа DS1990A; идентификационная смарт-карта);

– использованием уникального состава материала полосок проводников (идентификационная карта Виганда);

– невозможность повторения идентификатора без специализированного промышленного оборудования (идентификационные карты с оптической и голографической памятью);

– сложность повторения совокупности индивидуального биометрического признака и иных признаков, присущих живому человеку, при наличии дополнительных методов распознавания их имитации.

Системы, использующие бесконтактные идентификаторы, имеют имитостойкость, зависящую от наличия в протоколе обмена данными между идентификатором и считывателем алгоритмов защиты передачи данных.

6.4 Производительность (пропускная способность)

Производительность (пропускная способность) – свойство системы идентификации, характеризуемое максимально возможным количеством проведенных циклов идентификации в единицу времени.

Наименьшей производительностью обладают системы, использующие метод идентификации по биометрическому признаку и по запоминаемому коду.

Для систем идентификации по биометрическому признаку длительность цикла идентификации складывается из времени, затрачиваемого на:

– позиционирование носителя идентификационного признака (требуется не для всех видов биометрической идентификации);

– считывание (сканирование) идентификационного признака;

– аналого-цифровое преобразование идентификационного признака;

– формирование образа идентификационного признака;

– аутентификация образа;

– выполнение действий по результатам проведенной аутентификации.

Основное время цикла идентификации затрачивается на проведение позиционирования носителя и считывания биометрического признака, – процедур, отсутствующих при проведении идентификации по запоминаемому и вещественному коду.

Для систем идентификации по запоминаемому коду длительность цикла идентификации зависит от:

– индивидуальных психомоторных качеств живого человека, осуществляющего ввод кодовой последовательности;

– влияния человеческого фактора на правильность действий при вводе кодовой последовательности;

– эргономических свойств устройств ввода кодовой последовательности;

– длительности кодовой последовательности.

Длительность цикла идентификации по вещественному коду в большей степени определяется быстродействием цифровой обработки считанного кода, и в меньшей степени зависит от действий пользователя, практически исключая влияние человеческого фактора. Эта особенность идентификации по вещественному коду позволяет ей иметь наибольший показатель производительности, по сравнению с другими типами идентификации.

6.5 Устойчивость к внешним воздействиям

Устойчивость к внешним воздействиям – свойство системы сохранять работоспособное состояние при влиянии неблагоприятных факторов внешних воздействий.

Для устройств считывания (сканирования) идентификационных признаков устойчивость к воздействиям естественного и техногенного характера определяется особенностями его конструктивного исполнения. Наименьшей устойчивостью к внешним воздействиям обладают считыватели (сканеры) систем, применяющих оптический метод считывания (сканирования) идентификационного признака, что характерно для систем идентификации по:

– перфорационному кодированию;
– линейному и двухмерному штриховому кодированию;
– карте с оптической памятью;
– карте с голографической памятью.
– биометрическому признаку.

Считыватели иных идентификационных признаков имеют чувствительность к воздействиям определенного типа:

– для идентификаторов со встроенными пассивными радиоэлементами или магнитами, электронных ключей iButton (Touch Memory) и идентификационных смарт-карт – загрязнение и воздействие агрессивной среды и повышенной влажности, приводящее к возникновению оксидной пленки на поверхностях контактных площадок;

– для идентификационных карт с магнитным кодированием и смарт-карт – загрязнение образивосодержащими частицами считывающих головок (только для карт с магнитным кодированием) и поверхности протягивающих роликов, приводящее к выходу их из строя.

Наибольшей устойчивостью к воздействию внешних факторов обладают считыватели бесконтактных идентификаторов, имеющие закрытое исполнение корпуса, не требующие доступа к внутренним элементам, и не имеющие в своем составе контактов, оптических модулей и движущихся частей. Считыватели бесконтактных идентификаторов, предназначенные для скрытого размещения, обладают большей устойчивостью к воздействию внешних факторов.

6.6 Удобство использования

Удобство использования – характеристика метода персональной идентификации, определяющаяся эргономическими показателями идентификаторов и считывателей, временными затратами при пользовании, возможностью оперативного занесения и изменения идентификационного кода, и требуемым уровнем технической грамотности пользователя.

Для идентификации по запоминаемому коду и по биометрическому признаку не требуется наличие вещественного носителя кода, что исключает возможность его утраты, повреждения, кражи, и обеспечивает постоянную готовность к его применению. Вместе с тем, данные методы идентификации требуют от пользователя специальных навыков обращения и знания особенностей работы устройств считывания для проведения правильного сканирования биометрических признаков, или необходимость постоянного удержания в памяти кодовой последовательности и принятия мер, исключающих ее визуальный контроль при вводе со стороны посторонних лиц. Также следует учитывать, что отдельные биометрические признаки могут подвергаться повреждениям или изменениям со временем.

Для методов идентификации, использующих вещественный носитель кода, обмен данными со считывателем в процессе идентификации происходит в полуавтоматическом режиме, что практически исключает влияние человеческого фактора, требуя от пользователя только правильного позиционирования идентификатора относительно считывателя.

Идентификационный код большинства идентификаторов, имеющих вещественный носитель кода, прописывается однократно на предприятии-изготовителе и в дальнейшем не подлежит изменению. Электронные ключи iButton, за исключением типа DS1990A, смарт-карты и бесконтактные идентификаторы позволяют производить перезапись идентификационного кода, что предоставляет дополнительные удобства для пользователя в случае необходимости оперативного изменения кодов системы.

С точки зрения эргономики, все имеющиеся варианты исполнения вещественных носи-

телей кода имеют примерно равные показатели удобства, и предпочтение какого-либо варианта есть субъективное мнение каждого из пользователей.

Следует отдельно отметить повышенное удобство использования бесконтактных идентификаторов, ввиду отсутствия необходимости их точного позиционирования относительно считывателя, возможности дистанционного проведения процедуры идентификации, полностью закрытого исполнения носителя кода, затрудняющего его повреждение, а также широкой номенклатуры исполнения идентификаторов.

6.7 Стоимость производства и эксплуатации

Стоимость производства и эксплуатации устройств, входящих в системы персональной идентификации является одним из основных факторов, определяющим их выбор.

Как правило, стоимость производства определяется следующими факторами:

– рыночным спросом на конкретный тип продукции;

– стоимостью используемого при производстве сырья;

– сложностью технологического процесса производства;

– промышленным потенциалом предприятия-изготовителя;

– коэффициентом накладных расходов;

– процентом прибыли, закладываемым предприятием-изготовителем.

При массовом автоматизированном производстве основная составляющая стоимости изготавливаемых устройств практически не зависит от сложности технологического процесса и определяется преимущественно стоимостью затрачиваемого сырья и остальными факторами. В стоимостных параметрах оборудования систем идентификации часто наблюдается дисбаланс между стоимостью идентификатора и стоимостью считывателя в одну или другую сторону. Так, стоимость считывателя ключей iButton гораздо ниже стоимости самих ключей, но ситуация с идентификационной картой с оптической памятью и ее считывателем диаметрально противоположная. Именно поэтому стоимость системы идентификации следует оценивать как совокупность стоимостей идентификатора и считывателя.

По стоимостным характеристикам идентификаторы (идентификационные карты) и считыватели (сканеры) условно можно подразделить на три категории:

– низкой стоимости – идентификация по запоминаемому коду, по перфорационному кодированию, по встроенным пассивным радиоэлементам или магнитам, с линейным и двухмерным штриховым кодированием, – в силу относительной технологической простоты конструкции идентификаторов и считывателей, отсутствия особых требований к материалам, за исключением случаев антивандального исполнения и исполнения с повышенной устойчивостью к внешним воздействиям;

– высокой стоимости – идентификация по биометрическому признаку, – по причине применения в системах идентификации высокотехнологичных устройств считывания биометрических признаков, специализированного программного обеспечения и базы данных образов, а также высокой стоимости обслуживания;

– средней стоимости – все остальные методы идентификации, не отнесенные к первым двум категориям, характеризуемые сочетанием сравнительно высокой технической сложности и низкой стоимости производственных затрат при массовом производстве.

6.8 Обобщение результатов сравнительного анализа методов персональной идентификации

Результаты сравнительного анализа методов персональной идентификации, с указанием весового значения критериев сравнения, приведены в таблице 6.1. В нижней строке таблицы приведена суммарная оценка методов персональной идентификации выраженная численной характеристикой, отражающая степень пригодности метода персональной идентификации при использовании его в объектовом оборудовании, применяемом подразделения вневедомственной охраны МВД России.

Сравнительный анализ методов персональной идентификации.

Таблица 6.1

Методы идентификации / Критерии	Идентификация по запоминаемому коду	Идентификация по вещественному коду										Идентификация по биометрическому признаку						
	Кодонаборная панель	Идентификатор с перфорационным кодированием	Идентификатор со встроенным пассивным радиоэлементом или магнитом	Идентификационные карты с линейным или штриховым кодированием	Карты с магнитным кодированием	Карты Виганда	Карты с оптической памятью	Электронные ключи iButton	Идентификационная карта с голографической памятью	Идентификационная смарт-карта	Бесконтактный идентификатор RFID	Идентификация по отпечатку пальца	Идентификация по радужной оболочке глаза	Идентификация по сетчатке глаза	Идентификация по геометрии лица	Идентификация по подписи	Идентификация по геометрии кисти рук	Идентификация по голосу
Достоверность считывания	+++	+	+	+	+	+++	+	+++	+	+++	+++	++	+++	+++	+++	+	+++	+
Устойчивость к копированию	+++	+	++	+	++	+++	+++	+	+++	+++	++	+++	+++	+++	+++	+++	+++	+++
Имитостойкость	++	+	+	+	+	+++	+++	+	+++	+++	+++	+* (+++)	+++	+++	++	+++	+* (++)	+
Производительность (пропускная способность)	+	++	++	++	++	++	++	+++	++	++	+++	++	++	+	+	+	+	+
Устойчивость к внешним воздействиям	++	+	+++	++	++	+++	+	+++	++	++	+++	+	++	++	++	++	++	++
Удобство использования	++	++	++	++	+	++	+	++	+	++	+++	++	++	+	+	+	++	+++
Стоимость производства и эксплуатации	+++	+++	+++	++	+++	+	++	+++	++	+++	+++	++	+	+	++	+	+	+
Суммарная оценка	16	11	14	11	12	17	13	16	14	18	20	13 (15)	16	14	14	12	13 (14)	12

Примечания:

1) В таблице используются следующие обозначения соответствующих критериев оценки:

" + " – удовлетворительно;

" + + " – хорошо;

" + + + " – отлично.

2) * – при отсутствии дополнительных методов распознавания имитации иных признаков, присущих живому человеку.

6.9 Выводы

Результаты проведенного анализа методов персональной идентификации позволяют сделать следующие выводы:

1) В настоящее время в "Списке технических средств..." представлены технические средства охраны, использующие следующие методы персональной идентификации:

а) идентификация по запоминаемому коду;

– кодонаборная панель;

б) идентификация по вещественному коду:

– электронные ключи iButton,

– бесконтактные идентификаторы RFID;

в) идентификация по биометрическому признаку:

– отпечатки пальцев.

Наибольшее распространение получили методы идентификации, использующие электронные ключи iButton и кодонаборные панели. Данное обстоятельство обусловлено относительно низкой стоимостью их производства и эксплуатации. Метод идентификации, использующий бесконтактные идентификаторы RFID, получил меньшее распространение, несмотря на его удобство. Метод идентификации по отпечаткам пальцев представлен только в одной системе, что свидетельствует о его невостребованности при организации охраны подавляющего большинства объектов, защищаемых подразделениями вневедомственной охраны МВД России. Большое число технических средств охраны совмещают в себе методы идентификации, использующие электронные ключи iButton и кодонаборные панели.

2) Все рассмотренные методы персональной идентификации, в соответствии с результатами, представленными в таблице 6.1, можно разделить на три категории по степени пригодности метода при использовании его в объектовом оборудовании, применяемом подразделения вневедомственной охраны МВД России. К первой категории относятся методы персональной идентификации, наиболее полно удовлетворяющие требованиям, предъявляемым к объектовому оборудованию системы централизованного наблюдения. Ко второй категории относятся методы персональной идентификации, применение которых в объектовом оборудовании системы централизованного наблюдения целесообразно только при защите объектов особой важности. Главным критерием оценки методов персональной идентификации второй категории является надежность; цена системы идентификации является второстепенным критерием. К третьей категории относятся методы персональной идентификации, применение которых в объектовом оборудовании системы централизованного наблюдения не целесообразно по причинам, указанным пп. 6.1 – 6.7.

К первой категории методов персональной идентификации относятся (методы расположены в порядке убывания степени пригодности):

а) идентификация с использованием бесконтактных идентификаторов RFID;

б) идентификация с использованием смарт-карт;

в) идентификация с использованием кодонаборных панелей;

г) идентификация с использованием магнитного кодирования;

д) идентификация с использованием электронных ключей iButton.

Ко второй категории методов персональной идентификации относятся (методы расположены в порядке убывания степени пригодности):

а) идентификация по сетчатке глаза;

б) идентификация по радужной оболочке глаза;

в) идентификация с использованием карт Виганда;

г) идентификация по отпечатку пальца;

д) идентификация с использованием карт с голографической памятью;

е) идентификация с использованием карт с оптической памятью;

ж) идентификация по геометрии лица.

К третьей категории методов персональной идентификации относятся (методы расположены в порядке убывания степени пригодности):

а) идентификация с использованием линейного или штрихового кодирования;

б) идентификация с использованием перфорационного кодирования;

в) идентификация с использованием идентификаторов со встроенным пассивным радиоэлементом или магнитом;

г) идентификация по геометрии кисти руки;

д) идентификация по подписи;

е) идентификация по голосу.

4) Разработка проекта технических требований на технические средства, обеспечивающие возможность применения рассмотренных методов идентификации в подразделениях вневедомственной охраны МВД России с учетом категории защищаемых объектов, будет проведена в соответствии с планом научно-исследовательских и опытно-конструкторских работ ФКУ НИЦ «Охрана» МВД России на 2015 год.

7 Список использованных источников

ГОСТ Р ИСО/МЭК 10536-1 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты поверхностного действия. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 11693 Карты идентификационные. Карты с оптической памятью. Общие характеристики

ГОСТ Р ИСО/МЭК 11695-1 Карты идентификационные. Карты с оптической памятью. Метод голографической записи данных. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 11695-2 Карты идентификационные. Карты с оптической памятью. Метод голографической записи данных. Часть 2. Размеры и расположение оптической зоны

ГОСТ Р ИСО/МЭК 15693-1 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 15963 Информационные технологии. Радиочастотная идентификация для управления предметами. Уникальная идентификация радиочастотных меток

ГОСТ Р ИСО/МЭК 19762-1 Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь. Часть 1. Общие термины в области АИСД

ГОСТ Р ИСО/МЭК 19762-2 Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь. Часть 2. Оптические носители данных (ОНД)

ГОСТ Р ИСО/МЭК 19762-3 Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь. Часть 3. Радиочастотная идентификация (РЧИ)

ГОСТ Р ИСО/МЭК 19762-4 Информационные технологии. Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь. Часть 4. Общие термины в области радиосвязи

ГОСТ Р ИСО/МЭК 19785-1 Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных

ГОСТ Р ИСО/МЭК 19794-10 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки

ГОСТ Р ИСО/МЭК 19794-2 Автоматическая идентификация. Идентификация биометрическая. Формы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки

ГОСТ Р ИСО/МЭК 19794-3 Автоматическая идентификация. Идентификация биометрическая. Формы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца

ГОСТ Р ИСО/МЭК 19794-4 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

ГОСТ Р ИСО/МЭК 19794-5 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными". Часть 5. Данные изображения лица

ГОСТ Р ИСО/МЭК 19794-6 Автоматическая идентификация. Идентификация биометрическая. Формы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

ГОСТ Р ИСО/МЭК 19794-9 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла

ГОСТ ISO/IEC 24724 Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода GS1 DataBar

ГОСТ 30721 Автоматическая идентификация. Кодирование штриховое. Термины и определения

ГОСТ Р 51241 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 51294.9 Автоматическая идентификация. Кодирование штриховое. Спецификации символики PDF417 (ПДФ417)

ГОСТ ИСО/МЭК 7810 Карты идентификационные. Физические характеристики

205 ТР 205 – 09 "Технические рекомендации по проектированию систем антитеррористической защищенности и комплексной безопасности высотных и уникальных зданий"

25 РД 25.03.001 – 2002 "Системы охраны и безопасности объектов. Термины и определения"

78 Р 78.36.005 – 2011 "Выбор и применение систем контроля и управления доступом"

78 Р 78.36.018 – 2011 "Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности"