

## 6. Протоколы аутентификации (идентификации)

6.1. Общие сведения.

6.2. Парольная идентификация/аутентификация.

6.3. Протокол идентификации/аутентификации с использованием хеш-функции.

6.4. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.

6.5. Сервер аутентификации Kerberos.

6.6. Идентификация/аутентификация с помощью биометрических данных.

6.7. Идентификационные карты и электронные ключи.

6.7.1. Общие сведения.

6.7.2. Карты с магнитной полосой.

6.7.3. Контактные смарт-карты и USB-ключи.

6.7.4. Бесконтактные RFID-карты.

6.7.5. Зарубежный опыт.

Вопросы для самопроверки.

### 6.1. Общие сведения

**Идентификация** (англ. identification) - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов).

**Аутентификация** (англ. authentication) - проверка соответствия (подлинности) сущности предъявленному ею идентификатору. (Заметим, что происхождение русскоязычного термина «аутентификация» не совсем понятно. Английское «authentication» скорее можно прочесть как «аутентикация»; трудно сказать, откуда в середине взялось еще «фи» – может, из идентификации? Тем не менее, термин устоялся и закреплен в РД Гостехкомиссии РФ).

Для полноты картины приведем определение термина авторизация, который не следует путать с двумя вышеприведенными. **Авторизация** (англ. authorization) - предоставление сущности возможностей в соответствии с положенными ей правами или проверка наличия прав при попытке выполнить какое-либо действие.

Идентификация и аутентификация – это первая линия обороны, «входная дверь» в информационное пространство организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.

Идентификация сродни присвоению имени ребенку (не совсем точное сравнение, но все же). В любой ИС должны быть определены все субъекты, участвующие в информационном обмене. Часть из них может быть сгруппирована, если они наделены одинаковыми (схожими) правами и обладают одинаковыми (схожими) характеристиками. Каждый субъект (группа субъектов) должен обладать уникальным именем (обозначением).

Аутентификация бывает **односторонней** (обычно клиент доказывает свою подлинность серверу) и **двусторонней** (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

Субъект может подтвердить свою подлинность, предъявив один из следующих **аутентификаторов**:

- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (паспорт, личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев, образец ДНК и т.п.).

В том случае, если в ходе процедуры аутентификации клиент должен предъявить сразу несколько аутентификаторов, аутентификация называется **многофакторной**. Например, в ходе двухфакторной аутентификации клиент должен знать пароль и воспользоваться личной карточкой.

Рассмотрим основные программно-технические способы реализации идентификации и аутентификации:

- пароли;
- с использованием хеш-функции;
- на основе шифрования с открытым ключом;
- сервер аутентификации Kerberos;
- биометрия;
- идентификационные карты и электронные ключи.

## 6.2. Парольная идентификация/аутентификация

Введенный пользователем пароль сравнивается с паролем, имеющимся в БД, хранящейся в защищаемой ИС, и если они совпадают, то дается разрешение на использование защищаемых ресурсов.

Главное **достоинство** парольной аутентификации – простота и привычность. Пароли давно встроены в ОС, СУБД и программные продукты. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Парольная аутентификация имеет массу **недостатков**:

- как правило, пароль генерируется в одном месте (например, на сервере) и должен быть передан во второе (например, клиенту). При передаче пароль может быть перехвачен злоумышленником;
- многие ОС и приложения имеют пароли, указанные производителем по умолчанию. После установки такой системы очень часто забывают их удалить. БД стандартных паролей можно найти в Интернете;
- злоумышленник может получить БД паролей, хранящихся в зашифрованном виде, и воспользоваться ей:
  - в Windows NT/2000/XP учетные записи (пользователи и пароли) хранятся в файле «%System Root% \ System32 \ Config \ sam». При работающем ОС пользователь не может выполнять операции чтения/записи с данным файлом (блокируется процессом lsass.exe, «убить» который невозможно). Получить доступ к файлу можно, загрузив ОС с другого носителя. Другой вариант заключается в использовании файла «%System Root% \ Repair \ sam». Он доступен для чтения/записи, но, как правило, содержит пароли «стоletней» давности;

- в ранних версиях Unix файл с учетными записями «/etc/passwd» был доступен для чтения любым желающим. В современных разновидностях Unix файл с паролями «/etc/shadow» или «etc/secure» доступен только с привилегиями супервизора. Другой способ получения доступа к паролям – обрушения процесса, обращающегося к файлу с паролями. При этом Unix создает файл «core dump», содержащий дампы памяти (с паролями);

- после получения файла с зашифрованными паролями можно воспользоваться многочисленными программами-взломщиками. Одними из самых популярных взломщиков являются: для Windows – L0phtCrack, для Unix – John the Ripper. Время, требуемое для взлома пароля, зависит от его качества. Так, например, взлом пароля для L0phtCrack на компьютере с процессором Xeon 400 МГц при использовании:

- цифр и латиницы – 5,5 часов;

- всех символов – 480 часов.

- кроме перечисленных выше приемов взлома паролей, их можно подсмотреть (например, с помощью оптических приборов), сообщить другу/подруге (если секрет знают двое – это уже не секрет), записать на бумажке и приклеить на клавиатуру или монитор и т.п.

Тем не менее, так как парольная защита используется во многих продуктах и системах, можно порекомендовать следующие **меры, позволяющие повысить надежность парольной защиты**:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.). Еще лучше воспользоваться программами генераторами паролей (ключей);

- ограничение доступа к файлу с паролями;

- удаление резервных копий файлов с паролями («%System Root% \ Repair \ sam»);

- использование защищенных протоколов обмена ключами (например, основанные на протоколе обмена ключами Диффи-Хеллмана);

- ограничение числа неудачных попыток входа в систему (это затруднит применение «метода грубой силы»). В Windows 2000 и XP этот параметр устанавливается по пути «Администрирование / Локальная политика безопасности / Политики учетных записей / Политика блокировки учетной записи / Пороговое значение блокировки». Там же («Политики учетных записей») можно настроить срок блокировки учетной записи, минимальную длину пароля, сроки его действия и т.п.;

- управление сроком действия паролей, их периодическая смена, использование сеансовых ключей;

- удаление паролей уволенных или лишенных полномочий пользователей.

### **6.3. Протокол идентификации/аутентификации с использованием хеш-функции**

Напомним, что хеш-функция – легко вычисляемая функция, преобразующая исходное сообщения произвольной длины (прообраз) в сообщение фиксированной длины (хеш-образ), для которой не существует эффективного алгоритма поиска коллизий.

При идентификации/аутентификации пользователь вводит пароль, а по каналу связи высылается его хеш-образ. Проверяющая система сравнивает введенный хеш-образ с образом, хранящимся в ИС для этого пользователя и в случае их совпадения разрешает доступ. Т.о. система не хранит паролей, что повышает ее защищенность (**достоинство**).

**Недостаток** приведенной схемы заключается в том, что все равно необходимо как-то передавать хеш-образ для хранения в системе или для аутентификации и на этом пути его может перехватить злоумышленник, а затем воспользоваться им.

#### 6.4. Протокол идентификации/аутентификации на основе шифрования с открытым ключом

Широкое распространение при идентификации и аутентификации получили протоколы на базе ассиметричного шифрования. Существует десятки разновидностей таких протоколов, наиболее известными из которых являются протоколы на основе алгоритмов RSA, схемы Фейге-Фиата-Шамира, Эль-Гамала, Шнорра и т.д.

##### Протокол на основе алгоритма RSA.

Этап 1. Генерация ключей.

1. **A** генерирует открытый и закрытый ключи ( $e=5$ ,  $n=91$ ) и  $d=29$ ).

2. **A** передает открытый ключ **B**.

Этап 2. Аутентификация.

Таблица 6.1. Аутентификация на основе алгоритма RSA

№ п/п	Описание операции	Пример
1	<b>B</b> выбирает случайное число $k \in \{1, \dots, n-1\}$ , вычисляет $r = k^e \bmod n$ и посылает <b>r</b> <b>A</b> .	$k = 23$ $r = 23^5 \bmod 91 = 4$
2	<b>A</b> вычисляет $k' = r^d \bmod n$ и посылает <b>k'</b> <b>B</b> .	$k' = 4^{29} \bmod 91 = 23$
3	<b>B</b> проверяет соотношение $k = k'$ и, если оно истинно, принимает доказательство, в противном случае - отвергает.	$k = 23$ $k' = 23$

##### Схема Клауса Шнорра.

Этап 1. Генерация ключей (выполняет **A**).

Таблица 6.2. Генерация ключей по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	Выбираются два простых числа <b>p</b> и <b>q</b> такие, что $(p-1) \bmod q = 0$ .	$p = 23, q = 11$
2	Выбирается секретный ключ $x \in \{1, \dots, q-1\}$ .	$x = 8$
3	Выбирается <b>g</b> такое, что $g^q \bmod p = 1$ .	$g=3$ $3^{11} \bmod 23 = 1$
4	Вычисляется открытый ключ <b>y</b> такой, что $(g^x * y) \bmod p = 1$ .	$y = 4$ $(3^8 * 4) \bmod 23 = 26244 \bmod 23 = 1$
5	Публикация открытого ключа <b>y</b> .	

## Этап 2. Аутентификация.

Таблица 6.3. Аутентификация по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	<b>А</b> выбирает случайное число $k \in \{1, \dots, q-1\}$ , вычисляет $r = g^k \bmod p$ и посылает <b>р</b> <b>Б</b> .	$k = 6$ $r = 3^6 \bmod 23 = 16$
2	<b>Б</b> выбирает случайное число $e \in \{0, \dots, 2^t-1\}$ , где $t$ - некоторый параметр, и посылает <b>е</b> <b>А</b> .	$e = 4$
3	<b>А</b> вычисляет $s = (k + x * e) \bmod q$ и посылает <b>s</b> <b>Б</b> .	$s = (6 + 8 * 4) \bmod 11 = 5$
4	<b>Б</b> проверяет соотношение $r = (g^s * y^e) \bmod p$ и, если оно выполняется, принимает доказательство, в противном случае - отвергает.	$16 = (3^5 * 4^4) \bmod 23$

Для обеспечения стойкости протокола в 1989 г. Шнорр рекомендовал использовать **p** длиной 512 бит, **q** длиной 140 бит и **t** = 52.

### Схема на основе протокола с нулевым разглашением.

Суть доказательства с нулевым разглашением очень популярно можно объяснить на примере «пещеры Аладдина» (авторы - Жан-Жак Кискатер и Луи Гийу).

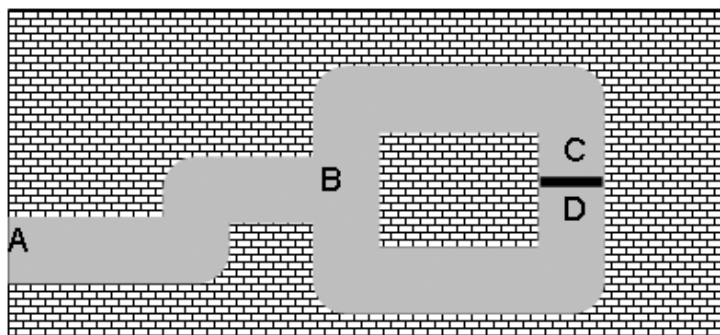


Рис.6.1. Пещера Аладдина

В пещере имеется потайная дверь **C-D**, открыть которую может только тот, кто знает волшебные слова. Алиса хочет доказать Бобу, что знает волшебные слова, но не хочет их раскрыть Бобу. Тогда Алиса может убедить Боба следующим образом.

1. Боб стоит в точке **A**.
2. Алиса проходит к точке **C** или **D**.
3. Боб проходит к точке **B** и предлагает Алисе появиться с левого прохода или с правого.
4. Алиса выполняет просьбу, используя, если необходимо, волшебные слова.
5. Алиса и Боб **n** раз повторяют шаги 1-4.

Если Алиса не знает секрета, то вероятность правильно выйти у нее в каждом раунде 50%:50%. Если шаги повторить **t** раз, то вероятность правильного выхода во всех случаях 1 шанс на  $2^t$ . Например, при  $t=16$  у Алисы всего 1 шанс из 65536.

Практическая реализация протокола рассматривается на примере схемы аутентификации Фейге-Фиата-Шамира.

### Упрощенная схема аутентификации Фейге-Фиата-Шамира.

Этап 1. Генерация ключей (выполняет Посредник).

Таблица 6.4. Генерация ключей по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример
1	Выбирает модуль <b>n</b> , равный произведению двух простых чисел.	$p = 5, q = 7, n = 35$
2	Выбирает число <b>v</b> (открытый ключ), являющееся квадратичным вычетом по модулю <b>n</b> и имеется обратное значение $v^{-1}$ по модулю <b>n</b> . <b>Квадратный вычет</b> – число, удовлетворяющее выражению $x^2 \bmod n = v$ , где $1 \leq x \leq n$ . Для модуля $n = 35$ , квадратными вычетами являются 1 ( $x = 1, 6, 29, 34$ ), 4, 9, 11, 14, 15, 16, 21, 25, 29, 30. Обратное значение вычисляется по формуле $(v * v^{-1}) \bmod n = 1$ . У квадратных вычетов 14, 15, 21, 25 и 30 нет обратных значений по модулю. Таким образом, $v \in \{1, 4, 9, 11, 16, 29\}$ .	$v = 16$ $v^{-1} = 11$ $(16 * 11) \bmod 35 = 176 \bmod 35 = 1$
3	Определяет закрытый ключ <b>s</b> , как наименьшее значение, удовлетворяющее следующему выражению $s^2 \bmod n = v^{-1}$ .	$s = 9$ $9^2 \bmod 35 = 11$
4	Публикация открытого ключа – <b>v</b> и <b>n</b> . Передача закрытого ключа <b>s</b> <b>А</b> .	$16 = (3^5 * 4^4) \bmod 23$

Этап 2. Аутентификация.

Таблица 6.5. Аутентификация по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример	
1	<b>А</b> выбирает случайное число $r \in \{1, \dots, n-1\}$ , вычисляет $z = r^2 \bmod p$ и посылает <b>z</b> <b>Б</b> .	$r = 8$ $z = 8^2 \bmod 35 = 29$	
2	<b>Б</b> посылает <b>А</b> случайный бит <b>b</b> .	$b = 0$	$b = 1$
3	Если $b=0$ , то <b>А</b> посылает <b>Б</b> <b>r</b> , иначе - $y = (r * s) \bmod p$ .	$r = 8$	$y = (8 * 9) \bmod 35 = 2$
4	Если $b=0$ , то <b>Б</b> проверяет, что $z = r^2 \bmod p$ , иначе - $z = (y^2 * v) \bmod p$ .	$29 = 8^2 \bmod 35$	$29 = (2^2 * 16) \bmod 35$

Рассмотренный порядок операций, выполненный 1 раз называется **аккредитацией**. Если первую операцию поменять местами со второй, то **А**, даже не зная закрытого ключа **s**, может подобрать такое значение **r**, которое будет приводить к успешной аккредитации в обоих случаях ( $b=0$  и  $b=1$ ). Подобрать же такое **r**, которое будет приводить к успешной аккредитации в обоих случаях одновременно невозможно. Таким образом, если **А** не знает закрытого ключа **s**, то вероятность успешной аккредитации (подбора **r**) равна  $1/2$ . Аккредитация повторится **t** раз, пока не будет достигнута требуемая вероятность  $1/2^t$ , что **А** не знает закрытого ключа **s**.

## 6.5. Сервер аутентификации Kerberos

Kerberos – программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных ОС.

Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные системы. Каждый субъект обладает секретным ключом. Чтобы субъект **С** мог доказать свою подлинность субъекту **S** (без этого **S** не станет обслуживать **С**), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. **С** не может просто послать **S** свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что **S** не знает (и не должен знать) секретный ключ **С**. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (т.е. сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

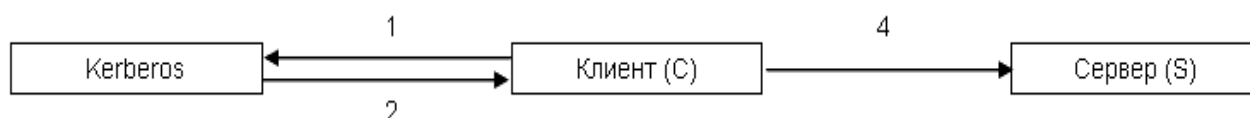


Рис.6.2. Проверка сервером S подлинности клиента С.

Последовательность идентификации/аутентификации с помощью Kerberos версии 5.0 на основе спецификации RFC 1510 в Windows 2000 выглядит следующим образом.

1. Клиент посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге (сервере).
2. Kerberos возвращает клиенту информацию, зашифрованную его секретным ключом.
3. Клиент расшифровывает переданную информацию, получая в результате этой операции так называемый билет, зашифрованный секретным ключом сервера, и временный ключ (ключ сеанса) **K**.
4. Клиент передает свой идентификатор **ID** и билет серверу.
5. Сервер расшифровывает билет, получая идентификатор клиента **ID'** и ключ сеанса **K**.
6. Сервер сравнивает идентификатор клиента, переданный открыто по сети, **ID** с идентификатором, содержащимся в билете **ID'**. Если они совпадают, то аутентификация пройдена успешно.
7. Обмен данными между клиентом и сервером выполняется с помощью ключа сеанса **K**.

Как видно из данного протокола, помимо идентификации/аутентификации, параллельно решается вопрос с обменом сеансовым ключом (симметричное шифрование с использованием доверенного центра).

## 6.6. Идентификация/аутентификация с помощью биометрических данных

Биометрия – древнейший способ идентификации. Собаки различают друг друга по лаю, кошки – по запаху, люди – по лицам, голосу, подписи и т.д.

В общем виде в ИС работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается БД характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в БД.

В дальнейшем для идентификации и аутентификации пользователя процесс снятия и обработки повторяется, после чего производится поиск в БД шаблонов (верификация). В случае успешного поиска личность пользователя и ее подлинность считаются установленными.

Классификация наиболее распространенных биометрических характеристик представлена на следующем рисунке.

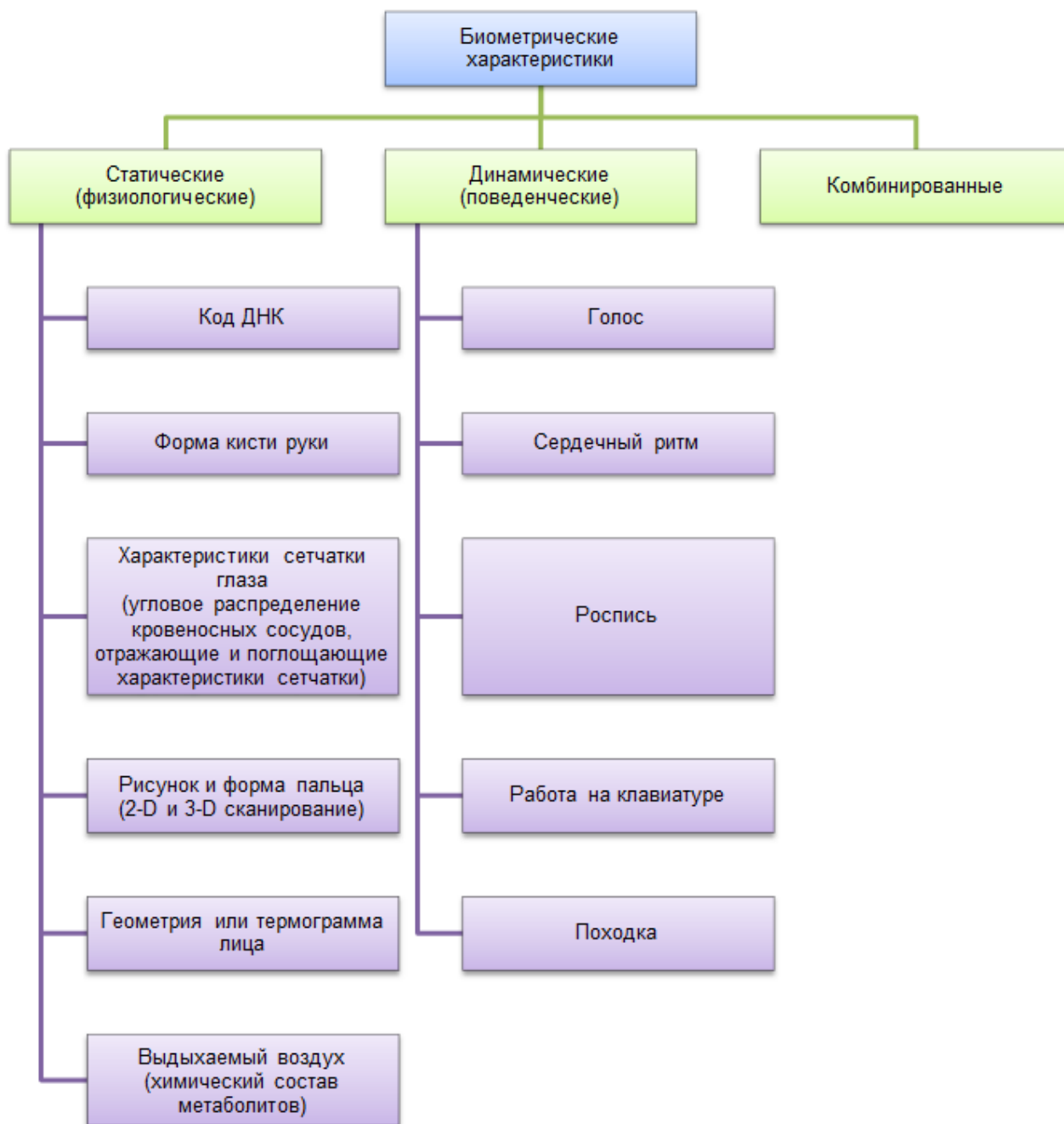


Рис.6.3. Классификация биометрических характеристик

Активность в области биометрии в настоящий момент очень велика. Организован соответствующий консорциум ([www.biometrics.org](http://www.biometrics.org)), активно ведутся работы по стандартизации разных аспектов технологии (формата обмена данными, прикладного программного интерфейса (API) и т.п.), публикуется масса рекламных статей, в которых биометрия преподносится как средство обеспечения сверхбезопасности, ставшее доступным широким массам.

В тоже время **недостатки** биометрических средств отмечаются во многих исследованиях:

- биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути может много чего произойти;
- база шаблонов может быть изменена злоумышленником;



- следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в «полевых» условиях, когда, например, к устройству сканирования могут поднести муляж и т.п.;
- некоторые биометрические данные человека меняются (как в результате старения, так и травм, ожогов, порезов, болезни, ампутации и т.д.), так что база шаблонов нуждается в постоянном сопровождении, а это создает определенные проблемы и для пользователей, и для администраторов;
- если у Вас крадут биометрические данные или их компрометируют, то это, как правило, на всю жизнь. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Палец, глаз или голос сменить нельзя, по крайней мере быстро;
- биометрические характеристики являются уникальными идентификаторами, но их нельзя сохранить в секрете.

До 11 сентября 2001 г., биометрические системы обеспечения безопасности использовались только для защиты государственных секретов и самой важной коммерческой информации. После потрясшего весь мир террористического акта ситуация резко изменилась. Сначала биометрическими системами доступа оборудовали аэропорты, крупные торговые центры и другие места скопления народа. Повышенный спрос спровоцировал исследования в этой области, что, в свою очередь, привело к появлению новых устройств и целых технологий. Естественно, увеличение рынка биометрических устройств привело к увеличению числа компаний, занимающихся ими, создавая конкуренцию послужила причиной к весьма значительному уменьшению цены на биометрические системы обеспечения информационной безопасности.

В рамках безвизовой программы Visa Waiver США подписали с 27 странами соглашение, по которому граждане этих государств смогут въезжать на территорию США сроком до 90 дней без визы при обязательном наличии биометрических паспортов. Начало действия программы - 26 октября 2005 г. Среди государств, участвующих в программе - Австралия, Австрия, Бельгия, Великобритания, Германия, Италия, Лихтенштейн, Люксембург, Монако, Нидерланды, Португалия, Сингапур, Финляндия, Франция, Швейцария, Швеция и Япония. В 2002 г. 118 стран мира (на текущий момент более 200) подписали Новоорлеанское соглашение, признавшее биометрию лица основной технологией идентификации для паспортов и въездных виз следующего поколения.

Стандарты на машиносчитываемые проездные документы (МСПД), к которым относятся и биометрические загранпаспорта граждан РФ, разрабатываются Международной организацией гражданской авиации (англ., International Civil Aviation Organization - ICAO). Скачать стандарты «Doc Series 9303. Machine Readable Travel Documents» можно на сайте организации по адресу [www.icao.int/publications/pages/publication.aspx?docnum=9303](http://www.icao.int/publications/pages/publication.aspx?docnum=9303).

**Первый биометрический загранпаспорт** на территории РФ был выдан 22 мая 2006 г. Это нововведение было ориентировано, в первую очередь, на повышение доверия к документам российских граждан со стороны зарубежных государств, а также для упрощения международных поездок. В России с 2009 г. во всех субъектах РФ действуют пункты выдачи паспортно-визовых документов нового поколения. В пластиковую страницу загранпаспорта встроена бесконтактная пассивная карта RFID (англ. Radio Frequency IDentification - радиочастотная идентификация) ближнего радиуса действия (до 10 см), соответствующая типу А или В стандарта ISO/IEC 14443 «Identification cards. Contactless integrated circuit(s) cards. Proximity cards» (ГОСТ Р ИСО/МЭК 14443 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия»). Данные на карте защищены с помощью технологии контроля доступа BAC (Basic access control), которая позволяет произвести чтение данных только после ввода номера паспорта, даты рождения владельца и даты окончания действия паспорта (обычно осуществляется с помощью распознавания машиносчитываемой зоны паспорта), что исключает несанкционированный доступ к данным на карте. Логическая структура данных (англ. Logical Data Structure - LSD), хранящихся на карте представлена на следующем рисунке.

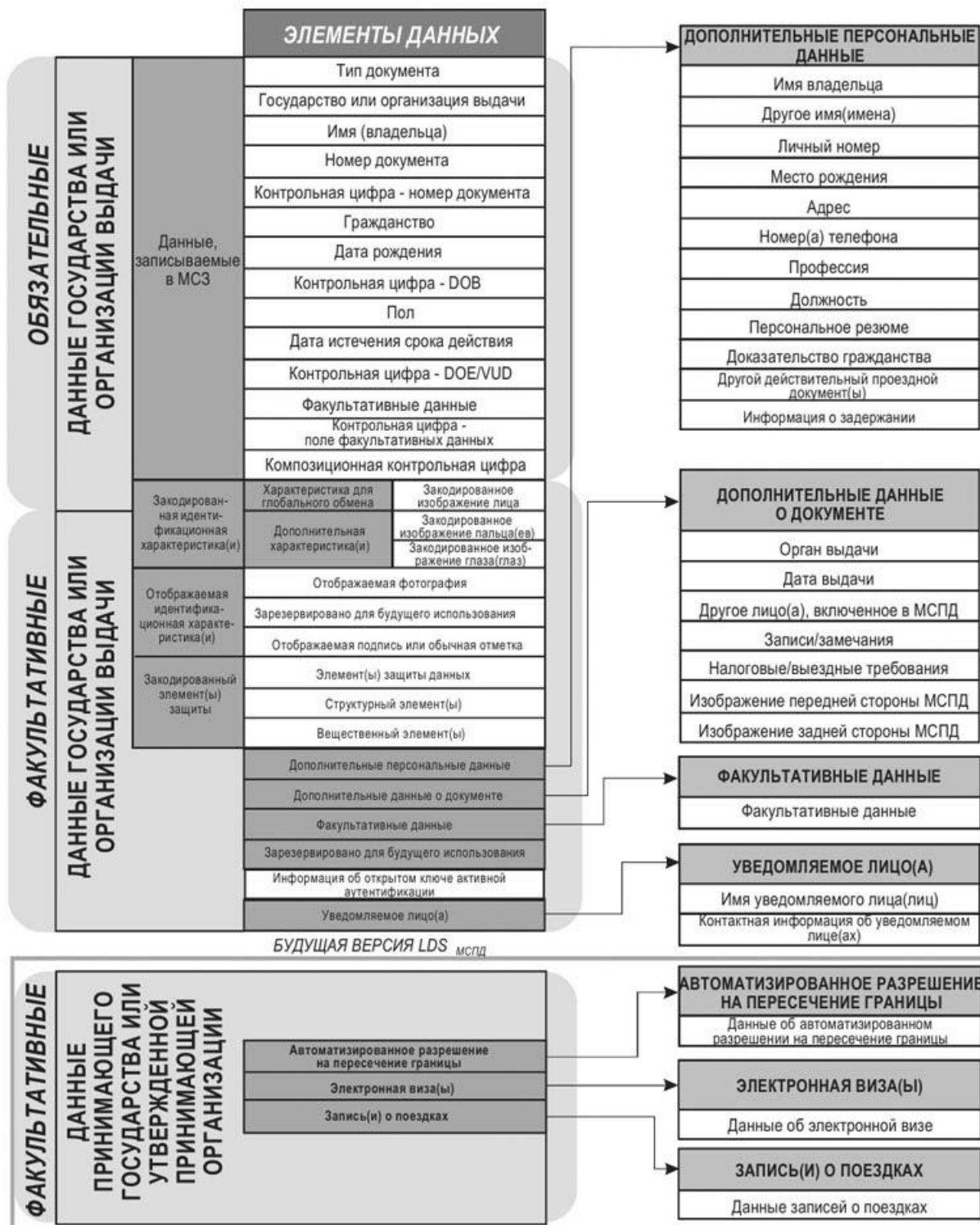


Рис. 6.4. Обязательные и факультативные элементы данных МСПД

Текущий стандарт на МСПД определяют три способа биометрической идентификации - по изображению лица, пальцев и радужной оболочки глаз. При этом обязательным является только изображение лица. На карте российского загранпаспорта содержатся данные следующих групп (англ. Data Group - DG):

- DG1 - данные, записываемые в машиносчитываемую зону;
- DG2 - закодированное изображение лица;
- DG11 - дополнительные персональные данные (дата и место рождения);

- DG12 - дополнительные данные о документе (дата выдачи паспорта и орган, выдающий документ).

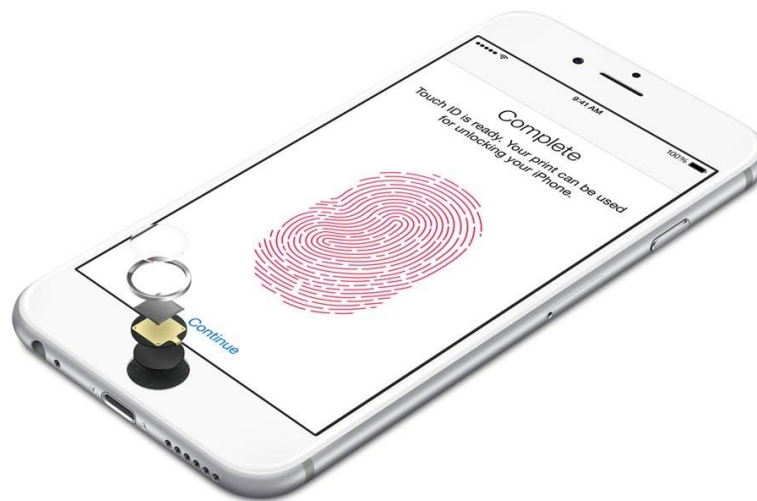
В некоторых странах, помимо изображения лица, на карте в обязательном порядке (согласно местному законодательству) хранится дополнительная биометрическая информация (в частности в Латвии, Молдавии и Эстонии - отпечатки пальцев).

В настоящий момент биометрические средства находят широкое применение и в устройствах личного пользования. В частности ведущие производители сотовых телефонов в 2013-2014 гг. выпустили модели со сканерами отпечатков пальцев.

Таблица 6.6. Сотовые телефоны со сканерами отпечатков пальцев

Наименование модели	iPhone 6	HTC One max	Samsung Galaxy S5
Положение сканера (выделен красной областью)			
Функции	<ol style="list-style-type: none"> <li>1) Разблокирование телефона;</li> <li>2) Покупки в iTunes и App Store;</li> <li>3) API для встраивания биометрической идентификации в приложения.</li> </ol>	<ol style="list-style-type: none"> <li>1) Разблокирование телефона.</li> </ol>	<ol style="list-style-type: none"> <li>1) Разблокирование телефона;</li> <li>2) Покупки в Samsung Apps;</li> <li>3) Покупки с помощью системы электронных платежей PayPal.</li> </ol>

На сайте Apple (<http://www.apple.com/ru/iphone-6/touch-id/>) приведено краткое описание технологии Touch ID, используемой ею в своих мобильных устройствах: «Под поверхностью кнопки «Домой» расположена целая технологическая система. Окружающее кнопку кольцо из нержавеющей стали реагирует на прикосновение и активирует ёмкостный сенсор. Вырезанная лазером из сапфирового стекла поверхность кнопки передаёт изображение пальца на сенсор, который распознаёт его рисунок, позволяя получить детальный отпечаток. Затем программное обеспечение считывает ваш отпечаток и находит соответствие, позволяя разблокировать телефон».



## 6.7. Идентификационные карты и электронные ключи

### 6.7.1. Общие сведения

История персональной идентификации, в частности идентификационных карт (ID-cards), стара и по большей части весьма неприглядна. Еще в Римской империи более 2 тыс. лет назад использовались таблички, так называемые тессера (tesserae), которые должны были иметь при себе граждане, солдаты и рабы. У каждого была своя уникальная табличка. Рабам, правда, чаще выжигали тавро. Карточки вводились и в странах, участвующих в больших войнах, — как дешевое и эффективное средство учета и распределения людских и материальных ресурсов. В Южной Африке во времена апартеида карточки использовались для сегрегации<sup>1</sup> жителей.

Если в ретроспективе материальным носителем идентификатора чаще всего являлся бумажный документ, то сейчас речь идет главным образом об электронных носителях информации, имеющих тот или иной механизм хранения (и, возможно, обработки) персональных данных. Этим механизмом могут быть пластиковые карты с магнитными полосами, смарт-карты, USB-ключи, RFID-метки и т.п. В настоящее время карты (схемы, документы) персональной идентификации в разных формах применяются в более чем ста странах.

Решающим признаком того, наличия или отсутствия в стране системы персональной идентификации, является, по-видимому, следующее обстоятельство: если госслужащий может потребовать от частного лица предъявить некий символ (пластиковую карточку, бумажку и т.п.), на основании которого немедленно будут сделаны выводы относительно качеств этой персоны, система идентификации существует. Если у человека такого символа нет (не важно, по какой причине), то он может быть задержан (ограничен в свободе) до выяснения обстоятельств.

Помимо учета граждан на государственном уровне, персональная идентификация с использованием карт и ключей нашла широкое применение в СКУД (Системах Контроля и Управления Доступом) организаций, а также в финансовой сфере при оплате товаров и услуг.

В настоящее время наиболее распространенными разновидностями карт и ключей являются:

- карты с магнитной полосой;
- контактные смарт-карты и USB-ключи;
- бесконтактные RFID-карты.

---

<sup>1</sup>**Сегрегация** (позднелат. segregatio — отделение) — политика принудительного отделения какой-либо группы населения (обычно упоминается как одна из форм религиозной и расовой дискриминации).

### 6.7.2. Карты с магнитной полосой

**История.**

История создания пластиковых карт с магнитной полосой началась в 1960 г., когда ЦРУ поручило IBM создать автоматизированную компьютерную систему контроля доступа своих сотрудников на подведомственных объектах. Инженеру IBM Форресту Перри (Forrest Parry) пришла идея наклеить кусочек магнитной ленты из ленточного накопителя на пластиковую карту. Он перепробовал несколько десятков разновидностей клея, но результаты оказались неутешительными. Полоски ленты деформировались или их характеристики ухудшались из-за действия клея, делая непригодными к использованию. После очередного дня разочарований Форрест пришел домой и рассказал о своей проблеме жене Дороти, которая в это время гладила его рубашки. Смышленная Дороти попросила его принести образцы карты и магнитной ленты. На следующий день, проделав некоторые манипуляции по настройке утюга, им удалось вплавить ленту в пластик, достигнув достаточно высокой степени сцепления между материалами.



Рис.6.6. Один первых прототипов карты с магнитной полосой на картонной основе

Первая пластиковая карта с магнитной полосой была выпущена в 1970 г. в рамках совместного проекта IBM, American Express и American Airlines для оплаты авиабилетов.

**Стандарты и спецификации.**

Формат записи данных на карты для финансовых операций определяется стандартами ISO/IEC 7811 «Карты идентификационные. Способ записи», ISO/IEC 7813 «Информационные технологии. Карты идентификационные. Карты финансовых операций» и ISO/IEC 4909 «Карты банковские. Карты для финансовых операций. Содержание данных на магнитной полосе для 3-й дорожки».

	Кодировка символов	Максимальное количество символов	Плотность записи
Дорожка 1	7 бит (буквы, цифры и служебные символы)	79	210 bpi
промежуток			
Дорожка 2	5 бит (цифры и служебные символы)	40	75 bpi
промежуток			
Дорожка 3	5 бит (цифры и служебные символы)	107	210 bpi

Рис.6.7. Структура магнитной полосы на пластиковых картах

Кодирование символов выполняется с учетом контроля целостности. Последний бит каждого символа является четным паритетным битом.



Исторически первая дорожка была предназначена для банковских карт, и до конца прошлого века большинство карт имело только одну эту дорожку. Вторая дорожка задействована для хранения исключительно числовых данных, за счет чего она имеет меньшую длину и меньше шансов повреждения данных. Третья дорожка в банковской сфере не используется и предназначена карт прочих систем (например, дисконтные карты). Формат записи данных для первой и второй дорожки банковских карт представлен на следующем рисунке.

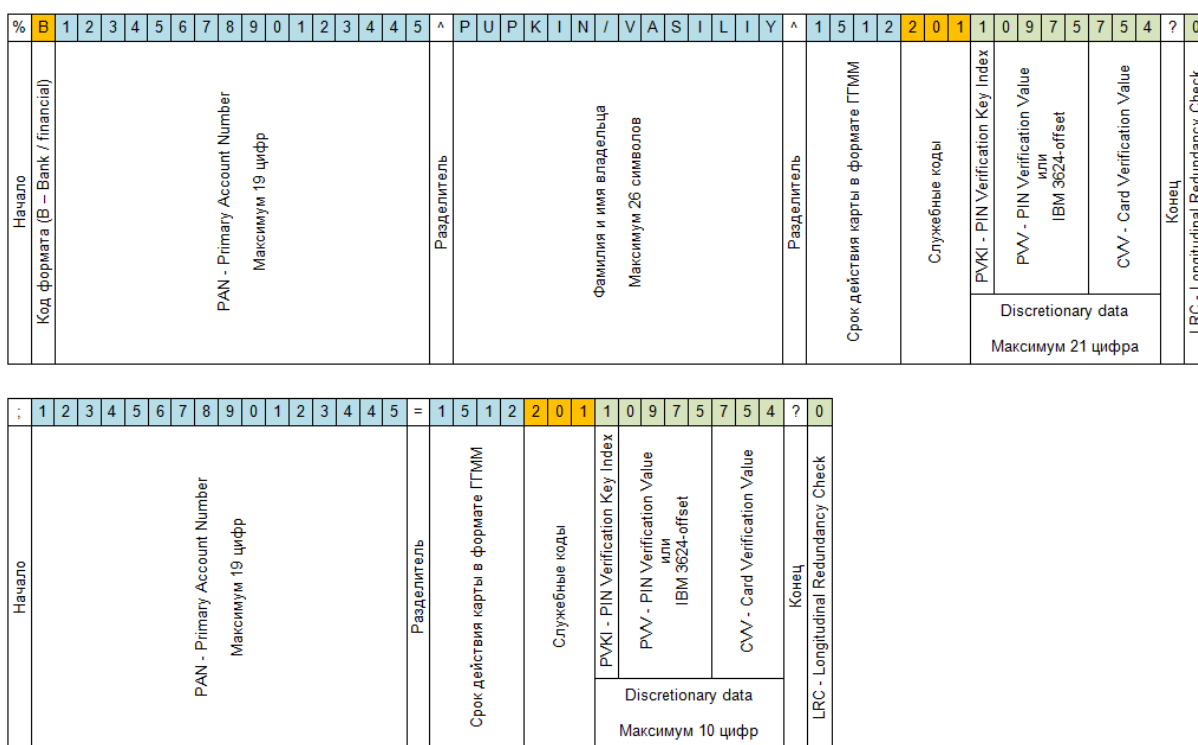


Рис.6.8

**PAN** (номер карточного счета, номер платежной карты) обычно представляет собой 16-значный номер карты, напечатанный на лицевой стороне карты.

**Discretionary data** (дискреционные данные) – данные зарезервированные для карточного эмитента<sup>2</sup> и используемые им по своему усмотрению. Тем не менее, первые 8 символов этого поля стандартизованы и предназначены для подтверждения правильности введенного PIN-кода<sup>3</sup>, выявления ситуаций повреждения магнитной полосы или грубой подделки карты.

**PVKI** (номер ключа проверки PIN-кода) представляет собой значение от 1 до 6 и определяет ключ расшифрования PVV.

**PVV** (значение проверки PIN-кода) и IBM 3624-offset представляют собой зашифрованное значение PIN-кода. В частности, алгоритм VISA PVV представляет собой следующую последовательность операций.

1. Определяется TSP (Transformed Security Parameter – преобразованный параметр безопасности), как последние 12 цифр PAN (за исключением крайней правой цифры) плюс PVKI плюс введенные 4 цифры PIN-кода. Например, PAN = 1234567890123445<sub>10</sub>, PVKI = 1<sub>10</sub>, PIN-код = 9090<sub>10</sub> -> TSP = 56789012344 1 9090<sub>10</sub>.
2. TSP шифруется с помощью банковского ключа, соответствующего PVKI, по алгоритму 3DES (DES-EDE2). Например, DES-EDE2 = 0FAB9CDEFFE7DCBA<sub>16</sub>.
3. Определяется PVV путем сканирования шестнадцатеричной строки DES-EDE2 слева-направо, пока не будет выбрано 4 цифры. Если после первого сканирования будут найдены менее 4 цифр, то при повторном сканировании выбираться будут только шестнадцатеричные цифры, которые конвертируются в цифры путем вычитания из них 10. Например, PVV = 0975 (0, 9, 7, F=5).

**CVV** (значение проверки подлинности карты) определяется по тому же алгоритму, что и PVV, только шифруемая строка (аналог TSP) формируется из следующих данных: 10 цифр PAN (за исключением крайней правой цифры) плюс срок действия карты (в формате ММГГ) плюс служебные коды (для приведенного выше примера, шифруемая строка – 789012344 1215 201<sub>10</sub>). Из-за того, что CVV/CVC слабо защищен от клонирования, в настоящее время он практически не используется и вместо него на картах ставятся нули.

**LRC** (продольный контроль избыточности) предназначен для контроля целостности всей дорожки. Количество единиц в битовом представлении всей дорожки, включая биты символа LRC за исключением четного паритетного бита символа LCR, должно быть четным. Четный паритетный бит символа LCR предназначен для контроля целостности только символа LCR [ISO 7811-2 «Карты идентификационные. Способ записи. Часть 2. Магнитная полоса малой коэрцитивной силы»].

На обратной стороне карты печатается код **CVV2**.



Рис.6.9. CVV2

В отличие от CVV, код CVV2 используется при дистанционных транзакциях (card not present по терминологии платежных систем), например через Интернет. Код CVV2 передается online вместе с другими реквизитами пластиковой карты в процессинговый центр, который уже передает его в банк-эмитент для проверки. Проверка осуществляется также, как и для PVV и CVV - банк заново вычисляет значение CVV2 и сравнивает его с полученным.

Генерация кода CVV2 осуществляется по тому же алгоритму и с использованием тех же ключей, что и обычного CVV. При этом есть следующие особенности шифруемой строки: срок действия карты берется в формате ГГММ, а вместо служебных кодов указываются нули (для приведенного выше примера, шифруемая строка – 789012344 1512 000<sub>10</sub>).

Значения CVV и CVV2 используются для платежных карт VISA. Для других платежных систем используемые коды приведены в следующей таблице.

Таблица 6.7. Коды проверки подлинности карты

Платежная система	Код на магнитной полосе	Код, напечатанный на карте
VISA	CVV - Card Verification Value	CVV2 - Card Verification Value 2
MasterCard	CVC - Card Verification Code	CVC2 - Card Verification Code 2
American Express	CSC - Card Security Code	CID - Card Identification Number*
Discover	CVV - Card Verification Value	CID - Card Identification Number
JBC - Japan Credit Bureau (Японское кредитное бюро)	CAV - Card Authentication Value	CAV2 - Card Authentication Value 2

\* Код CID карт American Express состоит из четырех цифр и печатается на лицевой стороне карты.

### Сферы применения.

Карты с магнитной полосой нашли широкое применение в общественной жизни. Среди них можно отметить карты:

- банковские;
- социальные;
- подарочные;
- дисконтные;
- телефонные;
- проездные;
- визитные (клубные);
- развлекательных центров;
- и т.д.

---

<sup>2</sup> **Эмитент** (англ. issuer) — орган исполнительной власти, местного самоуправления или юридическое лицо, которому в установленном порядке и на определенных условиях предоставлено право эмиссии (выпуска в обращение) денег, ценных бумаг и других финансово-платежных инструментов.

<sup>3</sup> **PIN-код** (англ. Personal Identification Number) – персональный идентификационный номер.

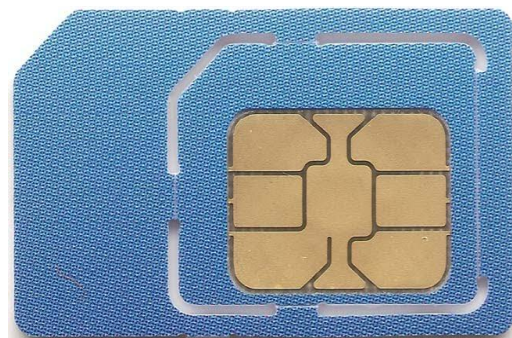
### 6.7.3. Контактные смарт-карты и USB-ключи

#### История.

Первая смарт-карта (карта со встроенной микросхемой, англ. integrated circuit card, ICC - карта с интегрированными электронными цепями) была выпущена в 1983 г. во Франции и использовалась для оплаты телефонных счетов (France Telecom). В 1991 г. немецкой компанией Giesecke & Devrient были выпущены первые SIM-карты<sup>4</sup> (разновидность смарт-карты) для телефонов стандарта GSM<sup>5</sup>. В банковской сфере смарт-карта впервые стала использоваться во французской платежной системе Carte Bleue (русс. «Голубая карта») в 1992 г.



а) банковская карта



б) SIM-карта



Рис.13.10. Контактные смарт-карты

В большинстве случаев смарт-карты, помимо модуля памяти, содержат также микропроцессор и операционную систему. Назначение смарт-карт - одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

Отцом смарт-карты принято считать французского изобретателя Ролана Морено. Его первоначальная патентная заявка предполагала использование микросхемы в перстне, но уже в 1975 г. был подан патент (Data-transfer system, US 4007355) на систему передачи данных (например, при кассовых операциях), в которой портативное устройство с микросхемой памяти предполагалось изготавливать в виде плоской карты. В 1976 г. он продемонстрировал совместную работу считывающего устройства и смарт-карты для проведения финансовых операций. Будучи поклонником фильмов Вуди Аллена, свой проект он назвал кодовым именем TMR – аббревиатура фильма «Take the Money and Run» (русс. «Бери деньги и беги»).

В некоторых источниках отцами смарт-карты называют немецких изобретателей Гельмута Греттрупа и Юргена Деслофа, но в поданном ими в 1968 г. патенте на идентификационный переключатель (Identification switch, US 3678250 / DE 1945777) трудно уловить сходство с современными смарт-картами. А вот в патенте 1970 г. на идентификационную систему (Identification system, US 3641316) речь действительно идет о плоских картах с интегральными схемами. В 1976 г. Юрген Деслоф подал патент на защищенную идентификационную систему (Identification system safeguarded against misuse, US 4105156), предусматривающую наличие на смарт-карте, помимо модуля памяти, еще и микропроцессора.

Различают **контактные** и **бесконтактные** (работающие на некотором расстоянии от считывающего устройства) смарт-карты.

Наиболее распространенными смарт-картами являются следующие:

- контактные смарт-карты с интерфейсом ISO 7816;
- контактные смарт-карты с USB-интерфейсом;
- бесконтактные (RFID) смарт-карты.

## 1. Контактные смарт-карты с интерфейсом ISO 7816.

### Стандарты и спецификации.

Физические параметры смарт-карт, расположение и назначение контактов, протокол обмена, механизм действия команд и т.д. описывается стандартом ISO/IEC 7816 «Карты идентификационные. Карты на интегральных схемах с контактами».

Расположение и назначение контактов приведены во 2-ой части стандарта.


напряжение питания	C1–VCC		C5–GND	заземление
сигнал восстановления	C2–RST		C6–VPP	напряжение программирования
сигнал синхронизации	C3–CLK		C7–I/O	ввод/вывод данных
зарезервировано	C4–		C8–	зарезервировано

Рис.6.11

В 6-ой части стандарта определяются элементы данных (англ. Data element - DE), которые могут храниться на смарт-карте в виде информационных объектов (англ. Data object - DO) и использованы для обмена данными. Под **элементом данных** подразумевается смысловое (содержательное)

описание единицы информации, для которого определены наименование, описание логического содержания, формат и кодирование. **Информационный объект** – информация, состоящая из тега, длины и значения. Тег DO однозначно определяет (идентифицирует) элемент данных.

Различают **простой** и **составной** DO. Например:

- простой DO – «дата истечения срока действия карты» в формате «ГГММ», тег «5916», длина 2 байта;
- составной DO – «имя», тег «5B16», максимальная длина 39 байт. Включает в себя элементы данных:
  - фамилия;
  - имя (имена);
  - уточняющее дополнение к имени (например, младший, номер и т.п.);
  - символ-заполнитель.

На смарт-карте могут содержаться DO различного назначения. Некоторые из них приведены в следующей таблице.

Таблица 6.8. Некоторые теги для смарт-карт стандарта ISO 7816

Тег (hex)	Наименование элемента данных	Примечания
Персональные (идентификационные) данные		
5B	Имя	Имя физического лица
5F2B	Дата рождения	Дата рождения физического лица
5F35	Пол	Пол физического лица
5F42	Адрес	Адрес физического лица
5F2C	Гражданство держателя карты	Держатель карты – владелец счета, к которому привязана карта
Данные для аутентификации		
5F2F	Стратегия использования PIN-кода	Определяет необходимость запроса терминалом введения PIN-кода и при каких условиях
5F3C	Динамическая взаимная аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в процессе взаимной аутентификации
5F3B	Динамическая внешняя аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в команде ВЫПОЛНИТЬ ВНЕШНЮЮ АУТЕНТИФИКАЦИЮ
5F3A	Динамическая внутренняя аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в команде ВЫПОЛНИТЬ ВНУТРЕННЮЮ АУТЕНТИФИКАЦИЮ
6C	Образцы держателя карты	Составной тег, содержащий, по меньшей мере, один из трех DO, указанных ниже

5F2E	Биометрические данные держателя карты	Отпечатки пальцев, ладоней, характеристики голоса, динамические характеристики подписи и т.д.
5F40	Портретное изображение держателя карты	
5F43	Изображение рукописной подписи держателя карты	
Данные для использования ЭЦП		
7F21	Сертификат держателя карты	Составной DO, содержащий открытый ключ держателя карты, дополнительную информацию, подпись органа по сертификации
5F49	Открытый ключ держателя карты	Содержит открытый ключ держателя карты для ЭЦП, использующей асимметричные механизмы
5F48	Секретный ключ держателя карты	Содержит секретный ключ держателя карты для ЭЦП, использующей асимметричные механизмы
5F4A	Открытый ключ органа по сертификации	Содержит открытый ключ органа по сертификации для ЭЦП, используемой для подтверждения подлинности сертификата
Дополнительные данные		
45	Данные эмитента	По ISO/IEC 7816-4
5F34	Порядковый номер карты	
55A	Первичный идентификатор счета (PAN)	
5F28	Код страны	Код для представления названия страны (по ISO 3166)
5F26	Дата активации карты	Дата, начиная с которой карта может использоваться под ответственность ее эмитента
59	Дата истечения срока действия карты	Дата, после которой карта считается недействительной
43	Данные об услугах, предоставляемых картой	По ISO/IEC 7816-4
5F2A	Код валюты	Код для представления валют и денежных средств (по ISO 4217)
5F21	Дорожка 1 (карта)	Информация, закодированная на дорожке 1-ой магнитной полосы (в соответствии с ISO/IEC 7813), включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC (при наличии на пластиковой карте магнитной полосы)
5F22	Дорожка 2 (карта)	Информация, закодированная на дорожке 2-ой магнитной полосы (в соответствии с ISO/IEC 7813), включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC (при наличии на пластиковой карте магнитной полосы)

**Сферы применения и реализуемые механизмы защиты.**

Информационные объекты, хранящиеся на смарт-карте, могут быть использованы для обеспечения следующих механизмов защиты:

- аутентификация участвующей стороны по паролю (проверка введенного PIN-кода);
- аутентификация участвующей стороны по ключу (аутентификация с использованием шифрования с открытым ключом);
- аутентификация данных (обеспечение целостности хранимых или пересылаемых данных с использованием криптографической контрольной суммы или ЭЦП);
- шифрование данных (обеспечение конфиденциальности хранимых или пересылаемых данных).

Смарт-карты с интерфейсом ISO 7816 получили наибольшее распространение в банковской сфере (пластиковые кредитные и дебетовые карты) и мобильной телефонии (SIM-карты).

## **2) Контактные смарт-карты с USB-интерфейсом (USB-ключи).**

### **Стандарты и спецификации.**

Как правило, представляют собой обычную смарт-карту стандарта ISO 7816, совмещенную с микропроцессором и USB-считывателем в одном корпусе.



а) Рутокен

б) eToken

Рис.6.12. USB-ключи

### **Сферы применения и реализуемые механизмы защиты.**

Наличие USB-порта подразумевает подключение данных устройств к компьютеру. Совместная работа USB-ключей и установленного на компьютере специального ПО позволяет решать следующие задачи:

- усовершенствовать процесс аутентификации (двухфакторная аутентификация) на локальном компьютере и в корпоративной сети, а также защищенный доступ к бизнес-приложениям;
- зашифровать данные на серверах, ноутбуках и рабочих станциях;
- обеспечить защиту персональных данных;
- защитить электронную почту и взаимодействие с коллегами в системах электронного документооборота;
- обезопасить финансовые операции в системах дистанционного банковского обслуживания (ДБО);

- внедрить ЭЦП и защитить документы в системах сдачи электронной отчетности через Интернет;
- обеспечить защиту корпоративного сайта в Интернет;
- и т.д.

В частности, рутокены российского производителя ЗАО «Актив-софт» [[www.rutoken.ru](http://www.rutoken.ru)] имеют следующие механизмы защиты данных:

- аутентификация:
    - поддержка 3-х категорий владельцев: Администратор, Пользователь, Гость;
    - поддержка 2-х Глобальных PIN-кодов: Администратора и Пользователя;
    - поддержка Локальных PIN-кодов для защиты конкретных объектов (например, контейнеров сертификатов) в памяти устройства;
    - настраиваемый минимальный размер PIN-кода (для любого PIN-кода настраивается независимо);
    - поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по Глобальным PIN-кодам в сочетании с аутентификацией по Локальным PIN-кодам;
  - шифрование и ЭЦП:
    - поддержка алгоритма ГОСТ 28147-89: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ);
    - поддержка алгоритмов DES (3DES), RC2, RC4, MD4, MD5, SHA-1;
    - выработка сессионных ключей (ключей парной связи) по схемам VKO GOST R 34.10-2001 (RFC4357) и VKO GOST R 34.10-2012;
    - генерация последовательности случайных чисел требуемой длины;
    - поддержка алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001: генерация ключевых пар, формирование и проверка ЭЦП;
    - поддержка алгоритмов ГОСТ Р 34.11-2012 и ГОСТ Р 34.11-94: вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭЦП;
    - поддержка PKCS#11 версии 2.20 (англ. Public Key Cryptography Standards - Стандарты криптографии с открытым ключом, разработанные и опубликованные RSA Laboratories);
    - поддержка алгоритма RSA с ключами до 2048 бит;
    - расшифрование по схеме EC El-Gamal;
    - интеграция с MS Windows посредством интерфейсов Microsoft Crypto API и Microsoft Smartcard API.
-

<sup>4</sup> **SIM-карта** (англ. Subscriber Identification Module - модуль идентификации абонента) - идентификационный модуль абонента, применяемый в мобильной связи стандарта GSM.

<sup>5</sup> **GSM** (англ. Global System for Mobile communications) - глобальный стандарт цифровой мобильной сотовой связи с разделением каналов по времени и частоте.

#### 6.7.4. Бесконтактные RFID-карты

**RFID** (англ. Radio Frequency IDentification, радиочастотная идентификация) - способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах (RFID-метках, RFID-тегах) [17].

Большинство RFID-меток состоит из двух частей. Первая - интегральная схема для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала и некоторых других функций. Вторая - антенна для приема и передачи сигнала.

##### История.

Принято считать, что технология радиочастотной идентификации берет свое начало с изобретения радара перед Второй мировой войны.

В 1904 г. немецкий инженер Кристиан Хюльсмейер продемонстрировал работу радиолокационного устройства для обнаружения корабля в густом тумане. Более совершенное устройство (телемобилоскоп), на которое он получил патент в 1905 г., уже позволяло определять расстояние до корабля. Одно из первых устройств, предназначенных для радиолокации воздушных объектов, продемонстрировал 26 февраля 1935 г. шотландский физик Роберт Ватсон-Ватт, который примерно за год до этого получил патент на изобретение подобной системы.

В Советском Союзе осознание необходимости средств обнаружения авиации, свободных от недостатков звукового и оптического наблюдения, привела к разворачиванию исследований в области радиолокации. Идея, предложенная молодым артиллеристом Павлом Ощепковым, получила одобрение высшего командования: наркома обороны СССР К. Е. Ворошилова и его заместителя - М. Н. Тухачевского.

3 января 1934 г. в СССР был успешно проведен эксперимент по обнаружению самолёта радиолокационным методом. Самолёт, летящий на высоте 150 метров, был обнаружен на дальности 600 метров от радарной установки. Эксперимент был организован представителями Ленинградского Института Электротехники и Центральной Радиолaborатории. Руководил экспериментом военный инженер М. М. Лобанов. В 1934 г. маршал Тухачевский в письме правительству СССР написал: «Опыты по обнаружению самолётов с помощью электромагнитного луча подтвердили правильность положенного в основу принципа». Первая опытная установка «Рapid» была опробована в том же году, в 1936 г. советская сантиметровая радиолокационная станция «Буря» засекала самолёт с расстояния 10 километров. Первые РЛС в СССР, принятые на вооружение РККА и выпускавшиеся серийно были: РУС-1 - с 1939 г. и РУС-2 - с 1940 г.

Технология, наиболее близкая к RFID, - система распознавания «свой-чужой» (англ. Identification Friend or Foe, IFF) была изобретена Исследовательской лабораторией ВМС США в 1937 г. и активно применялась союзниками во время Второй мировой войны. В СССР первые серийные авиационные радиоответчики СЧ-1 были приняты на вооружение РККА и начали поступать в войска с начала 1943 г.

В 1945 г. советский инженер Л.С. Термен изобрёл устройство, которое позволило накладывать аудиоинформацию на случайные радиоволны. Звук вызывал колебание диффузора, которое незначительно изменяло форму резонатора, модулируя отражённую радиочастотную волну. И хотя устройство представляло лишь пассивный передатчик (т.н. «жучок»), это изобретение причисляют к первым предшественникам RFID-технологии.

Развитие радарных и радиочастотных передач продолжалось в 50-е и 60-е гг. Ученые в США, Европе и Японии проводили исследования и представляли отчеты, объясняющие, как радиочастотная энергия могла быть использована для удаленной идентификации объектов.

Первый настоящий предок современных RFID-технологий (активная перезаписываемая метка) был запатентован Марио Кардулло в январе 1973 г. (Transponder apparatus and system, US 3713148 A), хотя устройство, с почти дословным сочетанием слов в аббревиатуре RFID, было запатентовано Чарльзом Уолтоном только в 1983 г. (Portable radio frequency emitting identifier - портативный радиочастотный излучающий идентификатор, US 4384288 A).

В 1970-х годах Национальная Лаборатория в Лос-Аламосе по заданию Департамента энергетики США разработала RFID-систему для отслеживания ядерных материалов (метки размещались на грузовиках, выполняющих перевозку материалов), а по заданию Департамента сельского хозяйства - для отслеживания перемещения коров и контроля получения ими лекарств (метки в стеклянной капсуле вживлялись под кожу).

### **Классификация RFID-систем :**

- по дальности считывания:
  - ближней идентификации (считывание производится на расстоянии до 20 см);
  - идентификации средней дальности (от 20 см до 5 м);
  - дальней идентификации (свыше 5 м);
- по рабочей частоте:
  - диапазона LF (англ. Low Frequency – низкая частота) - 125 .. 134 кГц;
  - диапазона HF (англ. High Frequency – высокая частота) - 13.56 МГц;
  - диапазона UHF (англ. Ultra High Frequency – ультравысокая частота) - 860 .. 960 МГц;
  - диапазона SHF (англ. Super High Frequency – сверхвысокая частота) - 2.4 ГГц;
- по типу используемой памяти:
  - RO (англ. Read Only) - идентификационные данные записываются только один раз, сразу при изготовлении;
  - WORM (англ. Write Once Read Many) - содержат идентификатор и блок однократно записываемой памяти;
  - RW (англ. Read and Write) - содержат идентификатор и блок многократно перезаписываемой памяти;
- по источнику питания:
  - пассивные. Не имеют встроенного источника питания. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования чипа, размещенного в метке, и передачи ответного сигнала. Дальность действия меток составляет 1-200 см (ВЧ-метки) и 1-10 метров (СВЧ-метки);
  - активные. Имеют собственный источник питания. Дальность действия меток до 300 м;
  - полупассивные.

### **Стандарты и спецификации.**

Стандартизацией RFID-систем занимается несколько международных организаций. Ими разработано и опубликовано несколько десятков стандартов, в т.ч. под эгидой ISO:

- ISO 11784 «Идентификация животных радиочастотным кодом. Структура кода»;
- ISO 11785 «Идентификация животных по радиочастотным сигналам. Техническая концепция»;
- ISO 14223 «Радиочастотная идентификация животных. Современные датчики»;
- ISO 10536 «Карты идентификационные. Карты на интегральных схемах бесконтактные»;
- ISO 14443 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия»;
- ISO 15693 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты с радиосвязью через большой зазор»;
- DIN/ISO 69873 «Носители данных для инструмента и зажимных приспособлений»;
- ISO 17363 «Применение радиочастотной идентификации (RFID) в цепи поставок. Контейнеры грузовые»;
- VDI 4470 «Системы охраны товаров»;
- ISO 15961 «Информационные технологии. Распознавание радиочастот для управления элементом. Протокол данных: прикладной интерфейс»;
- ISO 15962 «Информационные технологии. Идентификация радиочастоты для управления элементом данных. Протокол данных: правила кодирования данных и логические функции памяти»;
- ISO 15963 «Информационные технологии. Радиочастотная идентификация для управления предметами. Уникальная идентификация радиочастотных меток»;
- ISO 18000 «Информационные технологии. Идентификация радиочастотная для управления предметами»;
- и др.

Одна из организаций, занимающаяся разработкой и продвижением RFID-технологий в различных секторах экономики является GS1 (англ. Global Standard One). В спецификации этой организации «EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID. Version 2.0.0.0» (EPC Gen2) определена структура памяти RFID-метки для продуктов (товаров), содержащая четыре раздела (банка):

- **Банк 00<sub>2</sub> – RESEVED.** Используется для хранения ACCESS- и KILL-паролей. После производства метки значения паролей нулевые. Их установка возможна с помощью соответствующей команды радиоинтерфейса. Если значение ACCESS-пароля (32 бита) ненулевое, то чтение/запись данных на метку возможны только при знании этого пароля. Если значение KILL-пароля (32 бита) ненулевое, то чтение/запись данных на метку невозможны (метка перестает реагировать на команды без возможности восстановления ее работы);

- **Банк 01<sub>2</sub> – EPC** (англ. Electronic Product Code – электронный код продукта). Используется для хранения уникального идентификатора продукта. Наиболее распространенная длина идентификатора 64 или 96 бит. В настоящий момент разрабатывается спецификация на 256 битовый EPC. В банке хранится также идентификатор протокола обмена информацией с RFID-меткой (StoredPC) и значение циклического контроля кода (StoredCRC). Последний вычисляется по полиному CRC-16-CCITT в целях контроля целостности значений StoredPC и EPC;

- **Банк 10<sub>2</sub> – TID** (Tag ID). Используется для хранения уникального идентификатора метки, указывающего на ее изготовителя. Значение TID в соответствии с ISO 15963 состоит из трех полей: кода категории (AC); регистрационного номера организации (изготовителя метки),



присваивающей TID; серийного номера метки. Если  $AC = 11100000_2 (E0_{16})$ , тогда ID изготовителя и серийный номер устанавливаются в соответствии с ISO 1816-6, если  $AC = 11100010_2 (E2_{16})$  – в соответствии со спецификациями GS1, ISO 18000-6 (для радиочастотных меток типа C) и ISO 18000-3 (для систем радиочастотной идентификации, работающих в режиме 3);

- **Банк 11<sub>2</sub> – User.** Необязательный банк, используемый для хранения произвольной информации. Может отсутствовать в конкретной модели метки.

### Сферы применения.

RFID-системы нашли широкое применение в различных сферах деятельности. В следующей таблице представлены некоторые из них.

Таблица 6.9. Сферы применения RFID-меток

Сфера применения	Примеры
Промышленность	<p>1) RFID-метка с набором конечных требований к изделию может быть помещена на раму или корпус собираемого на конвейере автомобиля и в процессе конвейерного производства на различных участках (сборка, окраска и т.п.) автомобиль может быть автоматически окрашен определённым образом, могут быть установлены другие колёсные диски, изменён цвет обивки и т.п.</p> <p>2) Оператор, имеющий карточку с RFID-меткой может управлять оборудованием в определённой локации.</p>
Транспорт	<p>1) В 2014 г. в Зеленограде (Московская область) начат пилотный проект по оснащению общественного и спецтранспорта RFID-метками для беспрепятственного пропуска на перекрестках, оборудованных светофорами. Светофоры оборудуют считывателями, которые смогут распознавать сигнал от RFID-меток, установленных на спецтранспорте, и максимально быстро (в течение 10-15 секунд) включать зелёный свет.</p> <p>2) В конце марта 2013 г. на общественное обсуждение был вынесен проект национального стандарта для комплексов фотовидеофиксации. Новый ГОСТ подразумевает оснащение RFID-метками регистрационных номеров машин и RFID-считывателями дорожных камер, чтобы они могли распознавать грязные номера.</p> <p>3) С помощью RFID-меток на производстве жевательных резинок Wrigley отслеживается маршрут перевозки сырья.</p> <p>4) Морские контейнерные перевозки. Каждый контейнер оснащается RFID-меткой, содержащей информацию о грузе и скомбинированной с датчиками (например, открытия, содержания кислорода и т. п.) и передающей данные на центральную станцию сбора данных на борту контейнеровоза, которая в свою очередь передаёт данные через спутниковую связь. Т.о. владелец груза получает возможность отслеживать местоположение и сохранность груза.</p> <p>5) Начиная с 2004 г., функция Smart Key/Smart Start стала доступна в Toyota Prius. С тех пор Toyota встроила эту функцию во многие другие модели брендов Toyota и Lexus. Ключ содержит активную RFID-микросхему, позволяющей машине идентифицировать его с расстояния до 1 метра от антенны. Водитель может открыть дверь и завести машину, не вынимая ключ из кармана.</p> <p>6) Ford, Honda и некоторые другие производители используют основанные на RFID ключи зажигания в качестве антиугонной системы.</p>

Транспортные платежи	<p>1) В Гонконге транспортные перевозки оплачиваются в основном с использованием RFID-технологии, названной Octopus Card (англ. Octopus - осьминог). Она была запущена в 1997 г. для сбора оплаты за проезд, но «выросла» до масштабов обычной платежной карты, которая может использоваться в торговых автоматах, фастфудах и супермаркетах. Карта может быть перезаряжена (добавлены наличные) в специальных автоматах или в магазинах и может быть считана на расстоянии в несколько сантиметров от считывателя.</p> <p>2) JR East в Японии ввела Suica (англ. Super Urban Intelligent Card - умная городская суперкарта) для оплаты проезда в железнодорожном транспорте в ноябре 2001 г., используя технологию FeliCa (англ. Felicity Card - карта счастья) фирмы SONY.</p> <p>3) В Самаре с 1 июля 2008 г. введена система оплаты проезда в общественном транспорте с помощью RFID-смарткарт.</p>
Складской учет	<p>1) Немецкий производитель подъемно-погрузочного оборудования Jungheinrich внедрил технологию RFID в систему складской навигации.</p> <p>2) Компания «Марс» запустила систему складского учета упаковок кормов для животных (Pedigree, Whiskas, Chappi) на базе RFID-технологии.</p> <p>3) В 2012 г. сеть магазинов электроники и бытовой техники Media Markt совместно с METRO Group RFID Innovation Center (Германия) внедрила пилотный проект с технологией RFID в одном из отделов в ТЦ «Золотой Вавилон Ростокино» (Москва). RFID-метки применялись для автоматизации приемки и учета товара, а также в торговом зале для контроля за наличием товара на полке.</p>
Торговля	<p>В Германии на экспериментальной площадке сети гипермаркетов METRO проводится эксперимент по внедрению радиочастотных меток во всех магазинах сети, в т.ч. и в России. Планируется, что ручные считыватели у кассиров в ближайшее время перестанут использоваться. В случае, когда товар маркирован радиочастотными метками, покупатель, набрав продукты в тележку, провозит её через своеобразный турникет на расчётно-кассовом узле. Установленные сканеры автоматически считывают по радиоканалу всю информацию о товаре, который лежит в тележке и сразу же печатается чек. Если расчёт покупатель ведет с помощью кредитной карты, то и присутствие кассира в этом случае уже не требуется.</p>
Системы контроля и управления доступом (СКУД)	<p>1) Идентификация и ограничение доступа на заданную территорию.</p> <p>2) Учёт рабочего времени.</p> <p>3) Автоматическое разблокирование эвакуационных выходов и закрывание противопожарных дверей в случае пожарной тревоги.</p>
Медицина	<p>1) RFID-браслеты используют для отождествления младенца с матерью.</p> <p>2) Поиск ушедшего из своей палаты пациента, требующего по состоянию здоровья постоянного присмотра (например, страдающего болезнью Альцгеймера), или срочно разыскиваемого врача.</p> <p>3) Немецкий концерн Siemens AG, совместно с компанией Schweizer electronic разработали RFID-чип со встроенным датчиком температуры, выдерживающий операции стерилизации и пастеризации, а также ускорение до 5000 g, развиваемое на центрифуге. Данный чип предназначен, например, для использования в банках крови.</p>

	4) RFID-метки для идентификации людей использовались после урагана Катрина (август 2005 г.) - все данные о погибших, которые собирали эксперты, записывались в метку, навешиваемую ярлыком на ногу.
Человеческие имплантаты	1) В 2004 г. Министерство юстиции Мексики имплантировало 18 своим сотрудникам VeriChip для контроля за доступом в комнаты с государственными секретами. 2) Ночные клубы в Барселоне и Роттердаме, используют имплантируемую метку для идентификации своих VIP-посетителей, которые, в свою очередь, пользуются ими для оплаты за выпивку.
Маркировка (чипирование) животных	1) Оpozнaвание животных при помощи микрочипов применяется для упрощения их учёта, перемещения через границу, страхования, исключения подмены при разведении. Использование уникального номера позволяет отслеживать животных от фермы до потребителя, проверять своевременность обязательных вакцинаций и лечения. 2) Согласно Регламенту Европейского Парламента № 998/2003, вступившему в силу 3 июля 2004 г., домашние животные (собаки, кошки и хорьки), путешествующие через границы Европейского союза, должны быть идентифицированы микрочипом либо отчетливым клеймом. 3) В Канаде с 2005 г. требуется наличие электронной метки у всех животных, покидающих хозяйство, где они появились.
Библиотеки	1) Учет перемещений книг и документов, защита от краж или случайного выноса. 2) Обустройство пунктов приема и выдачи книг: идентификация книг и читательских билетов. 3) Инвентаризация и поиск книг, контроль правильности размещения книг. 4) Оснащение комплексов и терминалов автоматической выдачи и приема книг, систем автоматической сортировки. 5) Одно из самых крупных библиотечных применений RFID - библиотека Ватикана, насчитывающая в своем фонде более двух миллионов экземпляров книг.
Паспортный контроль	1) Первые RFID-паспорта (е-паспорта) были введены в Малайзии в 1998 г. 2) RFID-метки включены в новые (биометрические) загранпаспорта граждан Украины
Спорт	RFID-браслеты, одеваемые на спортсменов, используются в спортивном ориентировании, триатлоне и некоторых других видах спорта.

На следующих фотографиях показан внешний вид некоторых RFID-меток.



1) ключ для домофона; ISO 14443A



2) ключ для домофона; ISO 14443A



3) браслет; ISO10536/14443/15693



4) браслет; ISO10536/14443/15693



5) ушная клипса для животных; ISO 11784/11785



6) имплантат для животных и людей; ISO14443A



7) паспорт; ISO 14443

8) для забивки в деревянные изделия; ISO 17364; HID



9) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex

10) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex



11) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex



12) на металл; EPC Class1 Gen2 и ISO 18000-6C; Confidex



13) для пластиковых контейнеров и возвратной тары; EPC Class1 Gen2 и ISO 18000-6C; Confidex



14) для пластиковых контейнеров и возвратной тары; EPC Class1 Gen2 и ISO 18000-6C; Confidex



15) для прачечных производств, медицинских учреждений для автоматизированного учета и сортировки изделий из ткани, постельного белья, одежды; ISO 18000-3; HID



16) для прачечных производств, медицинских учреждений для автоматизированного учета и сортировки изделий из ткани, постельного белья, одежды, хирургических инструментов; EPC Class1 Gen2 и ISO 18000-6C; HID



17) для дорогостоящих товаров; ISO 15693/18000-3; HID



18) для крепления на контейнеры с отходами; EPC Class1 Gen2 и ISO 18000-6C; HID



Рис.6.13. Внешний вид RFID-меток

(назначение; стандарты; производитель)

#### 6.7.5. Зарубежный опыт

Система персональной карточной идентификации специфична для каждого государства. Одним из признаков жесткости системы идентификации является объем и степень детализации информации о субъекте, связанной с его уникальным идентификатором. В Малайзии действует одна из самых развитых систем такого рода. Там электронный паспорт на персону включает следующие данные: имя, дата рождения, пол, имена родителей, исповедуемая религия, этническая принадлежность, физические характеристики, фотография, отпечатки пальцев и идентификационный номер. Кроме того, эти карточки разных цветов: синяя — для граждан, красная — для постоянно проживающих, зеленая — для временно проживающих, коричневая — для бывших заключенных или диссидентов.

Системы поголовной идентификации трактовались в «свободном западном мире» как один из порочных атрибутов тоталитарного общества. Теперь же в этом самом мире развернулись дискуссии о введении надежной идентификации собственных граждан, как эффективном инструменте противодействия терроризму, оказания социальных услуг и защиты социальной справедливости в условиях массовой миграции населения.

Южной Корее ИС на основе ID-cards получили наибольшее распространение. К сентябрю 1999 г. все 37 миллионное население Кореи в возрасте до 18 лет получило национальные идентификационные карты. Карта используется для регистрации проживания, в качестве водительского удостоверения, пенсионного и медицинского страхового свидетельства. Она опционально может использоваться при выплате налогов, для оплаты телефонных звонков и в качестве электронного кошелька. Ее использование позволило снизить среднее время оказания различных услуг с 67 до 15 минут, а в области здравоохранения - с 55 до 5 минут.

В 2003г. завершена выдача подобных карт в Тайване (22 млн. населения).

ID-карта гражданина Эстонии является первичным удостоверением личности и действительна в пределах Эстонии. Она признана всеми членами Евросоюза и государствами-членами Шенгенского соглашения, не входящими в Европейский Союз, в качестве официального удостоверения для путешествующего лица. Она используется крупными банками Эстонии в качестве средства аутентификации, может использоваться в качестве проездного билета в общественном транспорте городов Таллина и Тарту, для получения медицинских услуг и электронного голосования на выборах. В феврале 2007 г. Эстония была первой страной в мире, которая ввела электронное голосование на парламентских выборах. Более 30000 человек приняло участие в электронном голосовании.

В России был принят Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», в котором дается определение универсальной электронной карты, целей ее создания и областей применения. **Универсальная электронная карта (УЭК)** — российская пластиковая карта, объединяющая в себе идентификационное и платежное средство.



Кроме этого, планируется использовать карту, как универсальный проездной документ, электронный ключ, электронный кошелек, единую дисконтную и бонусную карту.

Для реализации указанных выше возможностей в «Спецификации универсальной электронной карты» (ред.2.1. от 2014г.) для карт на базе интегральных схем с криптографическими сопроцессорами (смарт-карт) регламентируется поддержка следующих **криптографических алгоритмов**:

- 3DES – время шифрования блока данных длиной 128 байт на ключе длиной 112 бит в режиме CBC-поряд - не более 20 мс;
- RSA (поддерживаемая длина модуля ключей: для проверки электронной подписи – не менее 1984 бит, для вычисления электронной подписи – не менее 1024 бита) – время формирования ЭЦП (при представлении ключей RSA в формате CRT) над данными длиной 1024 бит – не более 250 мс; время проверки ЭЦП (при представлении ключей RSA в формате CRT) над данными длиной 1024 бит - не более 100 мс;
- SHA1 – время формирования проверочного значения (свертки, хеш-образа) сообщения (при длине 18 байт) – не более 30 мс;
- ГОСТ Р 34.10-2001 (действует до окончания срока действия сертификата ФСБ России) – время вычисления электронной подписи не более 250 мс, время проверки электронной подписи не более 500 мс;
- ГОСТ Р 34.10-2012 (начиная с 01.01.2015);
- ГОСТ 28147-89 – время криптографического преобразования (зашифрования/расшифрования) не более 2 мс;
- ГОСТ Р 34.11-94 (до окончания срока действия сертификата ФСБ России) – время формирования проверочного значения (свертки, хеш-образа) сообщения (при длине 32 байта) – не более 30 мс.

Хранение информации для считывания аппаратными средствами осуществляется на следующих **носителях**:

- магнитной полосе (по ГОСТ Р ИСО/МЭК 7811-6–2010);
- контактной смарт-карте (по ГОСТ Р ИСО/МЭК 7816-1–2010);
- бесконтактной (RFID) смарт-карте (по ГОСТ Р ИСО/МЭК 14443-1–2004).

Функции координатора и оператора проекта по внедрению УЭК осуществляет ФУО ОАО «Универсальная электронная карта» (ОАО «УЭК»). На официальном сайте ОАО «УЭК» <http://www.uecard.ru> на конец августа 2014 г. зарегистрировано более 450 000 заявлений от граждан РФ на получение карты.

В Правительстве РФ считают, что в будущем должен произойти плавный переход от УЭК к полноценному электронному паспорту с постепенным отказом от бумажных внутренних паспортов. С началом выдачи электронных паспортов постепенно прекратится выпуск УЭК. Созданная инфраструктура будет использована для электронных паспортов. Выдавать электронный паспорт будет Федеральная миграционная служба, а заниматься услугами и сервисами, подключенными к электронному паспорту, будет по-прежнему ОАО «УЭК».

В заключении следует отметить, что разумное применение ID-cards с ограниченной сферой действия и детализацией персональных данных представляется вполне разумной и оправданной мерой.

### **Вопросы для самопроверки**

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».



2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

## **Практическая работа №2.2**

### **Идентификация и аутентификация (RSA, схемы Шнорра и Фейге-Фиата-Шамира)**

В практической работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:

- на основе алгоритма RSA;
- по схеме Шнорра;
- по схеме Фейге-Фиата\_Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа ( $k$  или  $r$ ) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.