РАЗДЕЛ 16
ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Аннотация. *Выполнен обзор и анализ современных подходов, которые используются сегодня для идентификации пользователей компьютерных систем. Данное исследование является важным в связи с актуальностью проблемы защиты компьютерной информации и ограничению доступа к информационным и техническим ресурсам компьютера. Результаты выполненных исследований и сформулированные выводы могут быть полезные при создании собственных систем защиты компьютерной информации отдельными пользователями.*

Ключевые слова: *защита компьютерной информации, идентификация пользователей ЭВМ.*

Abstract. *A review and analysis of modern approaches which are used today for authentication of users of the computer systems is executed. This research is important in connection with actuality of problem of protection of computer information and access restriction to the informative and technical resources of computer. Results of the executed researches and formulated conclusions can be useful at creation of the own systems of protection of computer information separate users.*

Keywords: *protection of computer information, computer user identification.*

Введение и постановка задачи. В связи с широким распространением компьютерных технологий все более остро встает проблема защиты информации в компьютерных информационных системах. Поэтому актуальными видятся теоретические разработки в области защиты компьютерной информации и практическое их применение непосредственно в определенных конкретных компьютерных системах. Вопрос защиты информации в компьютерных системах решается с целью изолирования нормально функционирующей информационной системы от несанкционированных управляющих действий и доступа сторонних лиц или программ к компьютерным данным, требующим защиты. Создание единой централизованной системы безопасности является необходимым условием существования современной информационной инфраструктуры.

Управление доступом – эффективный метод защиты информации, регулирующий использование ресурсов информационной системы, для которой разрабатывается концепция информационной безопасности. Методы и системы защиты информации, которые опираются на управление доступом, включают следующие функции:

- идентификация пользователей, ресурсов информационной компьютерной системы;

- распознавание и установление достоверности пользователя по вводимым учетным данным (на данном принципе работает большинство моделей информационной безопасности);

- допуск к определенным режимам работы согласно регламенту, соответствующему каждому отдельному пользователю (определяется средствами защиты информации и является основой информационной безопасности большинства моделей информационных систем);

- протоколирование обращений пользователей к ресурсам, информационная безопасность которых защищается от несанкционированного доступа, и отслеживание некорректного поведения пользователей системы.

Как видим, идентификация пользователей является неотъемлемым и важным элементом и основой эффективности системы управления доступом к информационным ресурсам компьютерных систем.

Каждый современный пользователь должен хорошо ориентироваться в современных подходах к реализации задачи идентификации. Основной целью исследования является попытка проанализировать существующие современные подходы к задаче идентификации пользователей компьютерных систем, выявление позитивных черт и недостатков каждого из них и формулирование выводов относительно целесообразности использования каждого из способов идентификации.

Основная часть. Задачей систем идентификации и аутентификации является определение и верификация набора полномочий субъекта при доступе к информационной системе.

Идентификация – это предъявление пользователем какого-либо уникального, свойственного только ему идентификатора (признака). Аутентификация – это процедура, которая проверяет, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу.

Эти процедуры (идентификация и аутентификация) неразрывно связаны между собой, поскольку способ проверки определяет, каким образом и что пользователь должен предъявить системе, чтобы получить доступ.

Сегодня существует несколько способов идентификации пользователей [144]. У каждого из них есть свои преимущества и недостатки, благодаря чему некоторые технологии подходят для использования в одних компьютерных системах, а некоторые – в других. Однако во многих случаях нет строгого определенного решения. Поэтому и разработчикам программного обеспечения,

я пользователям приходится самостоятельно делать вывод о том, какой способ идентификации реализовывать в собственных информационных компьютерных системах.

Современные подходы к задаче идентификации пользователей информационных компьютерных систем

Существует три самых распространенных способа идентификации:

1). Парольная идентификация. Еще не так давно парольная идентификация была едва не единственным способом определения личности пользователя. Дело в том, что парольная идентификация наиболее проста как в реализации, так и в использовании. Суть ее сводится к следующему. Каждый зарегистрированный пользователь какой-либо компьютерной системы получает набор персональных реквизитов (чаще всего используются пары логин-пароль). В дальнейшем, при каждой попытке входа в систему, он должен указать свою информацию. Ну а поскольку она уникальна для каждого пользователя, то на основании ее система делает заключение о личности и идентифицирует ее.

Главное преимущество парольной идентификации – это простота реализации и использования. Кроме того, введение парольной идентификации не требует совсем никаких расходов: данный процесс реализован в большинстве программных продуктов. Таким образом, система защиты информации оказывается простой и доступной.

Теперь перейдем к недостаткам. К сожалению, их много. И основной из них - огромная зависимость надежности идентификации от самих пользователей, точнее, от выбранных ими паролей. Дело в том, что большинство людей использует ненадежные ключевые слова, которые легко подбираются. К ним относятся слишком короткие пароли, общеизвестные сочетания символов и т.д. Поэтому некоторые специалисты в области информационной безопасности советуют использовать длинные пароли, которые состоят из случайного соединения букв, цифр и различных символов.

2). Аппаратная (или электронная) идентификация. Этот принцип идентификации основывается на определении личности пользователя по какому-либо предмету, ключу, который находится в его эксклюзивном пользовании [87]. На данный момент наибольшее распространение получили два типа устройств: разнообразные карты (проксимити-карты, смарт-карты, магнитные карты и т.д.) и так называемые токены (token), которые подключаются непосредственно к одному из портов компьютера.

Главным достоинством применения аппаратной идентификации является достаточно высокая надежность. И действительно, в памяти токенов могут

храниться ключи, подобрать которые достаточно сложно. Кроме того, в данных устройствах реализовано немало различных защитных механизмов. Ну а встроенный микропроцессор позволяет электронному ключу не только принимать участие в процессе идентификации пользователя, но и выполнять некоторые другие полезные функции.

Ну а теперь поговорим о недостатках аппаратной идентификации. Наиболее серьезной опасностью в случае использования аппаратной идентификации является возможность кражи злоумышленниками токенов или карт у зарегистрированных пользователей. Также они могут быть потеряны, переданные другому лицу, дублированы. Второй минус рассматриваемой технологии - цена. В последнее время стоимость как самых электронных ключей, так и программного обеспечения, которое позволяет работать с ними, заметно снизилась. Однако для введения в эксплуатацию системы такой идентификации все равно будут нужны некоторые вложения. Каждого зарегистрированного пользователя необходимо обеспечить персональным токеном. Кроме того, впоследствии некоторые типы ключей могут изнашиваться, могут быть утеряны и т.д. То есть, аппаратная идентификация требует некоторых эксплуатационных расходов.

3). Биометрическая идентификация. Биометрия - это идентификация человека по уникальным, свойственным только ему биологическим признакам. Можно сказать, что биометрические технологии исконно разрабатывались для точного установления личности человека, поэтому решение использовать их в области информационной безопасности выглядит вполне логичным. Причем данное направление развивается очень активно. Сегодня эксплуатируется уже более десятка различных биометрических признаков [74]. Причем для самых распространенных из них (отпечатки пальцев и радужная оболочка глаза) существует множество различных по принципу действия сканеров. Так что пользователям, которые решили использовать биометрическую идентификацию, есть из чего выбирать.

Главным достоинством биометрических технологий является наивысшая надежность. И действительно, все знают, что двух людей с одинаковыми отпечатками пальцев в природе просто не существует. Правда, сегодня уже известно несколько способов обмана дактилоскопических сканеров. Например, нужные отпечатки пальцев могут быть перенесены на пленку или может быть использована фотография пальца зарегистрированного пользователя. Впрочем, нужно признать, что современные устройства значительно более стойкие по отношению к подобной фальсификации.

Основным недостатком биометрической идентификации является стоимость оборудования. Ведь для каждого компьютера, который входит в информационную систему, необходимо приобрести собственный сканер. Конечно, в последнее время цены на биометрические устройства постоянно снижаются. Кроме того, не очень давно появились мыши и клавиатуры со встроенными дактилоскопическими сканерами. Но уверенно сказать, что биометрическая идентификация стала доступной для любого пользователя нельзя.

На данный момент было рассмотрено три способа (или подхода) однофакторной идентификации пользователей информационных компьютерных систем, то есть в рассмотренных системах для определения личности пользователя использовался только один фактор. Однако подобные системы сегодня нельзя назвать надежными. В последнее время все большее распространение получает комплексная или многофакторная идентификация.

В системах комплексной идентификации для определения личности пользователя компьютерной информационной системы применяется одновременно несколько параметров [149], причем комбинироваться эти параметры могут в произвольном порядке. Впрочем, сегодня в подавляющем большинстве случаев используется только одна пара: парольная защита и токен. В этом случае пользователь может не бояться подбора его пароля злоумышленником (без электронного ключа пароль работать не будет), а также кражи токена (он не будет работать без пароля). Впрочем, в некоторых системах применяются максимально надежные процедуры идентификации, в которых одновременно используются пароли, токены и биометрические характеристики человека.

Рассмотрим каждый из перечисленных подходов более обстоятельно.

Парольные системы защиты.

Главное преимущество парольной идентификации – простота и привычность. Пароли давно встроены в операционные системы и другие сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих пользователей уровень безопасности. Однако по совокупности характеристик их следует признать самым слабым средством идентификации. Именно слабый уровень парольной защиты является одной из основных причин уязвимости компьютерных систем к попыткам несанкционированного доступа. Но на данный момент пароль – самый распространенный способ идентификации пользователей и еще долго будет им оставаться. Поэтому целесообразными будут некоторые советы по созданию парольной защиты, которые позволят сделать ее более надежной.

Следующие мероприятия позволят значительно повысить надежность парольной защиты:

- наложение технических ограничений: установление минимальной длины пароля, использования в пароле разных групп символов (пароль должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическое изменение;
- ограничение доступа к файлу паролей;
- ограничение количества неудачных попыток входа в систему;
- использование программных генераторов паролей (программ, которые, основываясь на несложных правилах, могут генерировать только благозвучные легко запоминающиеся пароли).

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя – некоторое уникальное количество информации, которое позволяет различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя – некоторое секретное количество информации, известное только пользователю и парольной системе, которое предъявляется пользователем для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многократный пароль может быть использован для проверки достоверности многократно.

Учетная запись пользователя – совокупность его идентификатора и его пароля.

База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будет понимать программно-аппаратный комплекс, который реализует системы идентификации и аутентификации пользователей автоматизированных систем на основе одноразовых или многократных паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль соединения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система является «передним краем обороны» всей системы безопасности. Некоторые ее элементы (в частности те, которые реализуют интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

Важным аспектом стойкости парольной системы, является способ хранения паролей в базе данных учетных записей. Возможные следующие варианты хранения паролей:

- в открытом виде;
- в виде сверток (хеширование);
- зашифрованными с использованием некоторого ключа.

Наибольший интерес представляют второй и третий способы, которые имеют ряд особенностей.

Хеширование (использование необратимой хеш-функции к какой-либо информации превращает ее в уникальный код - свертку) не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником. При выборе алгоритма хеширования, который будет использован для расчета сверток паролей, необходимо гарантировать несовпадение значений сверток, полученных на основе разных паролей пользователей. Кроме того, следует предусмотреть механизм, который обеспечивает уникальность сверток в том случае, если два пользователя выбирают одинаковые пароли. Для этого при расчете каждой свертки обычно используют некоторое количество «случайной» информации, например, выдаваемой генератором псевдослучайных чисел.

При шифровке паролей особенное значение имеет способ генерации и хранения ключа шифровки базы данных учетных записей. Перечислим некоторые возможные варианты:

- ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки;
- ключ генерируется программно и хранится на внешнем носителе, из которого прочитывается при каждом запуске;

- ключ генерируется на основе выбранного администратором пароля, который вводится в систему при каждом запуске.

Во втором случае необходимо обеспечить невозможность автоматического перезапуска системы, даже если она выявляет носитель с ключом. Для этого можно затребовать от администратора подтверждать продолжение процедуры загрузки, например, нажатием клавиши на клавиатуре.

Наиболее безопасное хранение паролей обеспечивается при их хешировании и последующей шифровке полученных сверток, то есть при комбинации второго и третьего способов.

Учитывая, что пользователи нередко выбирают недостаточно стойкие пароли, можно сделать вывод, что получения базы данных учетных записей или перехвата переданного по сети значения свертки пароля представляют серьезную угрозу безопасности парольной системы.

В большинстве случаев аутентификация происходит в распределенных системах и связана с передачей по сети информации о параметрах учетных записей пользователей. Если передаваемая по сети информация не защищена должным образом, возникает угроза ее перехвата злоумышленником и использование для нарушения защиты парольной системы.

Еще одним способом повышения стойкости парольных систем является применение одноразовых (one-time) паролей. Общий подход к применению одноразовых паролей основан на последовательном использовании хеш-функции для расчета дежурного одноразового пароля на основе предыдущего. Сначала пользователь получает упорядоченный список одноразовых паролей, последний из которых также хранится в системе аутентификации. При каждой регистрации пользователь вводит дежурный пароль, а система рассчитывает его свертку и сравнивает с эталоном, хранящимся в системе. В случае совпадения пользователь успешно проходит аутентификацию, а введенный им пароль хранится для использования как эталон при следующей регистрации. Защита от сетевого перехвата в такой схеме основана на свойстве необратимости хеш-функции.

Аппаратная (или электронная) идентификация.

Каждый аппаратный (электронный) идентификатор является физическим устройством, обычно небольших размеров, для удобства его ношения с собой. Для подключения электронных идентификаторов чаще всего используют USB порт.

В состав электронных систем идентификации и аутентификации входят:

1). Переносные токени:

- асинхронные - пользователь вводит строку в устройство, получает ответ и вводит полученную информацию в компьютер;

- PIN/асинхронные - асинхронный метод дополняется введением PIN-кода в устройство;

- синхронные – токен синхронизирован по времени с сервером и генерирует для данного пользователя в данную минуту пароль, который и вводится в систему;

- PIN/синхронные.

2). Разнообразные карты – это устройства, похожие на переносные идентификаторы, но более сложные по своему составу.

Карты бывают:

- пассивные (карты с памятью);

- активные (интеллектуальные карты).

Последние включают CPU (процессор), миниатюрную операционную систему, часы, программы на ROM (read-only memory - память только для чтения), буферную память (RAM) для криптографических расчетов, независимую память или EEPROM (Electrically Erasable Programmable Read-Only Memory) для хранения цифровых ключей. С помощью смарт-карты проводится расчет одноразовых паролей и осуществляется взаимодействие с устройством через картридер. После введения PIN-кода картридер сам затребует смарт-карту, и последующий процесс протекает без участия человека, благодаря чему можно использовать достаточно длинные ключи.

Существует достаточно большое количество карт и работают они по разным принципам. Например, достаточно удобные в использовании бесконтактные карты (их еще называют проксимити-карты), которые позволяют пользователям проходить идентификацию как в компьютерных системах, так и в системах доступа в помещение. Наиболее надежными считаются смарт-карты – аналоги банковских карт, привычных для многих людей. Кроме того, есть и более дешевые, но менее стойкие к взлому карты: магнитные, со штрих-кодом и т.д.

В основе большинства устройств на базе бесконтактных смарт-карт лежит технология радиочастотной идентификации.

Основными компонентами бесконтактных устройств является чип и антенна. Идентификаторы могут быть как активными (с батареями), так и пассивными (без источника питания). Идентификаторы имеют уникальные 32/64 разрядные серийные номера.

Системы идентификации на базе Proximity криптографически не

защищены, за исключением специальных рекомендованных систем.

USB-ключи – это наследники смарт-карт, из-за этого структуры USB-ключей и смарт-карт идентичны.

Биометрическая идентификация.

Биометрическая идентификация - это способ идентификации личности по отдельным специфическим биометрическим признакам, свойственным конкретному человеку [74]. Современный уровень развития компьютерных технологий позволил использовать подобные признаки как основу для идентификации человека и принятия решения о возможности (невозможности) доступа к ресурсам компьютерных систем.

Среди биометрических механизмов идентификации можно выделить такие:

1) по статическим признакам – это те признаки, что практически не меняется со временем, начиная с рождения человека (физиологичные характеристики);

2) по динамическим признакам - поведенческие характеристики, то есть те, которые построены на особенностях, характерных для подсознательных движений в процессе воссоздания какого-либо действия. Динамические признаки могут изменяться со временем, но не резко, а постепенно.

Среди статических методов в задачах идентификации пользователя компьютерных систем используются следующие:

1. Идентификация по отпечатку пальца. В основу этого метода положена уникальность рисунка папиллярных узоров на пальцах. Идентификация построена таким образом: с помощью сканера получают изображение отпечатка, потом это изображение по сложному алгоритму превращается в специальный цифровой код. Дальше этот код сравнивается с эталонными кодами, которые хранятся в базе данных.

2. Идентификация по расположению вен на ладони. Прибор, который прочитывает информацию в этом случае - инфракрасная камера. В результате на входе программы при формировании цифрового кода появляется рисунок вен на руке человека. Данный метод не нуждается в контакте человека с устройством для сканирования. Имеет высокие показатели надежности и достоверности.

3. Идентификация по сетчатке глаза. В данном случае сканируется рисунок кровеносных сосудов глазного дна, который имеет неподвижную структуру, неизменную во времени. Понятно, что этот рисунок наблюдается только при определенных условиях: при сканировании человек смотрит на

аленный световой источник и специальная камера сканирует глазное дно, что свою очередь может вызывать неприятные ощущения у человека. Считается дним из самых надежных биометрических методов.

4. Идентификация по радужной оболочке глаза. Рисунок радужной оболочки глаза – уникален для каждого человека. В этом методе важна не только специальная камера, но и надежное программное обеспечение. Ведь именно с помощью программного обеспечения из изображения выделяется рисунок нужной радужной оболочки. Этот метод является одним из наиболее точных среди биометрических методов.

5. Идентификация по форме кисти руки. Этот метод основывается на распознавании геометрических особенностей кисти руки. Специальный сканер формирует трехмерный рисунок кисти. При анализе этого рисунка выполняются измерения, с помощью которых формируется соответствующий цифровой код.

6. Идентификация по форме лица. На практике используется как двухмерное, так и трехмерное изображение. Причем двумерное распознавание лица на сегодняшний день - один из самых неэффективных методов биометрии, поэтому имеет ограниченный круг применения или используется только в совокупности с другими методами. Распознавание по трехмерному изображению лица чем-то похоже на метод идентификации по форме кисти руки. Здесь так же строится трехмерный образ лица. Специальное программное обеспечение выделяет из этого образа контуры глаз, губ и других частей лица. Дальше проводятся точные измерения между заданными контурами. Именно по этим данным строится цифровой код.

Среди динамических методов, которые используются для идентификации личности пользователя, можно назвать следующие:

1. Идентификация по голосу. В настоящее время существует множество программ по распознаванию голоса. В методе идентификации по голосу важны частотные характеристики голоса человека. Именно по частотным характеристикам и строится цифровая модель.

2. Идентификация по почерку. При идентификации по данному методу обычно исследуется подпись человека. В данном случае используется специальный планшет. Проверяются такие динамические характеристики, как: графические параметры, сила натиска на поверхность, скорость нанесения подписи. На основе этих характеристиках строится цифровой код.

3. Идентификация по клавиатурному почерку. Данный метод аналогичный идентификации по почерку, но вместо того, чтобы ставить

автограф, человеку необходимо напечатать кодовое слово. Цифровой код строится по динамике набора определенного слова или фразы.

При всем теоретическом многообразии возможных биометрических методов применяемых на практике среди них немного. В основном используются следующие: распознавание по отпечатку пальца, по изображению лица (двухмерному или трехмерному), по радужной оболочке и по сетчатке глаза.

На сегодняшний день все биометрические технологии являются вероятностными, и нередко данное обстоятельство служит основой для критики биометрии.

Однако, невзирая на активную деятельность на протяжении последних лет в направлении разработки и совершенствования методов идентификации пользователей с целью управления доступом к ресурсам информационных систем, надежность и стойкость существующих систем недостаточная для потребностей сегодняшнего дня.

Комплексная (или многофакторная) идентификация.

Внедрение комбинированных систем увеличивает количество идентификационных признаков и тем самым повышает безопасность.

На сегодняшний день существуют комбинированные системы следующих типов:

- системы на базе бесконтактных смарт-карт и USB-ключей;
- системы на базе гибридных смарт-карт;
- биоэлектронные системы.

1). Бесконтактные смарт-карты и USB-ключи

В корпус брелока USB-ключа встраивается антенна и микросхема для создания бесконтактного интерфейса. Это позволит организовать управление доступом в помещение и к компьютеру, используя один идентификатор. Данная схема использования идентификатора может исключить ситуацию, когда сотрудник, бросив рабочее место, оставляет USB-ключ в разъеме компьютера, что позволит работать под его идентификатором. В случае же, когда нельзя выйти из помещения, не используя бесконтактный идентификатор, данной ситуации удастся избежать.

RFID-технология (Radio Frequency Identification, радиочастотная идентификация) является самой популярной на сегодня технологией бесконтактной идентификации. Радиочастотное распознавание осуществляется с помощью закрепленных за объектом так называемых RFID-меток, несущих идентификационную и другую информацию.

2). Гибридные смарт-карты

Гибридные смарт-карты содержат разнородные чипы. Один чип поддерживает контактный интерфейс, другой - бесконтактный. Как и в случае гибридных USB-ключей, гибридные смарт-карты решают две задачи: доступ в помещение и доступ к компьютеру. Дополнительно на карту можно нанести логотип компании, фотографию сотрудника или магнитную полосу, что делает возможным полностью заменить обычные пропуски и перейти к единственному «электронному пропуску».

3). Биоэлектронные системы

Как правило, для защиты компьютерных систем от несанкционированного доступа применяется комбинация из двух систем - биометрической и контактной на базе смарт-карт или USB-ключей.

В качестве биометрической системы, как правило, применяется система распознавания отпечатков пальцев. При совпадении отпечатка с шаблоном разрешается доступ к ресурсам компьютерных систем. К недостаткам такого способа идентификации можно отнести возможность использования муляжа отпечатка.

Достичь повышения надежности и точности автоматизированных систем идентификации пользователей можно за счет объединения использования биометрических характеристик вместе с классическими способами идентификации пользователей (например, парольная защита, PIN-код, использование разнообразных карт и т.д.) [149].

Актуальной видится проблема разработки и исследования комплексных систем, которые используют для принятия решения доступа к информационным системам несколько биометрических характеристик пользователя (например, использовать совместно особенности клавиатурного почерка, голоса, динамики работы пользователя с манипулятором «мышь» или использование отпечатков нескольких пальцев и т.д.) [84]. Некоторые производители уже начали интеграцию двух методов распознавания лиц, включая двух- и трехмерные изображения.

Заключение. На основе анализа угроз информационной безопасности и существующих средств идентификации пользователей информационных систем, можно уверенно сказать, что парольная защита на сегодня является одним из самых распространенных способов защиты информации от несанкционированного доступа как в отдельных компьютерах и системах, так и в сетях мирового масштаба. Однако без использования других механизмов защиты, парольная защита не является надежной, поскольку не может

обеспечить защиты необходимого для сегодняшнего дня уровня. Достаточно распространенными в качестве идентификаторов являются также разнообразные электронные ключи (токени, карты и т.д.). Но следует заметить, что в последнее время все большее распространение получают системы идентификации, которые используют биометрические характеристики человека при решении задачи доступа к информационным системам.

Таким образом, рассмотрев технологии аппаратной (или электронной), парольной, биометрической идентификации можно сделать вывод, что в дальнейшем по мере роста вычислительных мощностей все более востребованным будет именно использование систем комплексной (или многофакторной) идентификации, что позволит избежать человеческих ошибок, связанных с применением слабых паролей и усилить требования к парольной идентификации.

Относительно выбора системы идентификации непосредственно в каждой отдельной ситуации, пользователь должен: объективно оценить соотношение ценности защищаемой информации и стоимости выбираемого программно-аппаратного обеспечения идентификации/аутентификации (включая сопровождение); оценить удобство в использовании (контактные, бесконтактные) и восприятие избранного подхода пользователями; определить нужный уровень защищенности. Но бесспорным советом является использование комплексной системы идентификации, которая объединяет несколько подходов к решению задач доступа к информационным ресурсам компьютерных систем.