ГБПОУ
«ПЕРМСКИЙ РАДИОТЕХНИЧЕСКИЙ
КОЛЛЕДЖ ИМ.А.С. ПОПОВА»

РЕФЕРАТ

по дисциплине «Основы исследовательской деятельности»

Аутентификация. Методы аутентификации

Выполнила:
Паутова А. М.,
студентка гр. ОИБТС- 20-23

Руководитель работы:
Власова И. А.,
преподаватель
гуманитарных дисциплин

Пермь - 2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

У каждого субъекта: человека, сущности или процесса есть приватная информация, к которой не должно быть доступа для других субъектов. Для решения этой задачи человечество создало защищенные информационные системы, в которых пользователь может хранить свою информацию. Процедура доступа к информации происходит по принципу идентификация и аутентификации.

Тема актуальна в связи с повсеместным использованием информационных систем, как источников и хранителей информации, доступ к которым нужно регулировать.

Теоретическая значимость реферата заключается в уточнении понятия аутентификации и изучения принципа её работы, рассмотрение классификации и видов аутентификации.

Объект - средства защиты информации, предмет - аутентификация.

Цель: изучить процесс аутентификации.

Задачи:

1) изучить понятие аутентификация в связи с идентификацией;
2) рассмотреть принципы работы аутентификации;
3) ознакомиться с методами аутентификации и выделить их особенности.

В рамках анализа данной темы были изучены работы таких авторов как Барабанова М.И., Цирлов В.Л. и др.

Методы:

- анализ научной литературы;
- методы дедукции и изученности.

Работа состоит из введения, 3 глав, заключения, списка использованных источников, приложения.

1 АУТЕНТИФКАЦИЯ И ИДЕНТИФИКАЦИЯ

Основой любых систем защиты информационных систем являются идентификация и аутентификация, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами АС. Напомним, что в качестве субъектов АС могут выступать как пользователи, так и процессы, а в качестве объектов АС – информация и другие информационные ресурсы системы.

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. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

Идентификация обеспечивает выполнение следующих функций:

1) установление подлинности и определение полномочий субъекта при его допуске в систему,

2) контролирование установленных полномочий в процессе сеанса работы;

3) регистрация действий и др.

Аутентификацией (установлением подлинности) называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

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

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

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

1) что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);

2) как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив, по крайней мере, одну из следующих сущностей:

1) нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

2) нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);

3) нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики). [2]

В данной главе говорится о ключевых различиях понятий идентификация и аутентификация.

2 ПРОЦЕССАУТЕНТИФИКАЦИ. ВХОД В СИСТЕМУ

Процесс аутентификации пользователя компьютером можно разделить на два этапа:

1) подготовительный - выполняется при регистрации пользователясистеме. Именно тогда у пользователя запрашивается образец аутентификационной информации, например, пароль или контрольный отпечаток пальца, который будет рассматриваться системой как эталон при аутентификации;

2) штатный - образец аутентификационной информации запрашивается у пользователя снова и сравнивается с хранящимся в системе эталоном. Если образец схож с эталоном с заданной точностью - пользователь считается узнанным, в противном случае пользователь будет считаться чужим, результатом чего будет, скажем, отказ в доступе на компьютер.

Для аутентификации пользователя компьютер должен хранить некую таблицу имен пользователей и соответствующих им эталонов.

В наиболее простом варианте эталоном может быть просто пароль, хранящийся в открытом виде. Однако такое хранение защищает только от непривилегированных пользователей системы - администратор системы вполне сможет получить все пароли пользователей, хранящиеся в таблице, и впоследствии входить в систему от имени любого пользователя (скажем, для выполнения каких-либо злоумышленных действий, которые будут записаны на другого). Кроме того, известен факт, что подавляющее большинство пользователей используют 1-3 пароля на все случаи жизни. Поэтому узнанный злоумышленником пароль может быть применен и к другим системам или программам, в которых зарегистрирован его владелец. Наиболее часто эталон представляет собой результат какой-либо обработки аутентификационной информации, то есть:

$$Ei = f(Ai), \quad (2.1)$$

где:

Ai - аутентификационная информация, а f(...) - например, функция хэширования (расчет контрольной суммы данных с использованием криптографических методов - хэша).Хэширование достаточно часто применяется в протоколах межсетевого обмена данными, а также необходимо для использования электронной цифровой подписи.

Есть и другие варианты хранения эталонов, например:

$$Ei = f(IDi, Ai). \quad (2.2)$$

Этот вариант лучше предыдущего тем, что при одинаковых паролях двух пользователей их эталоны будут выглядеть по-разному. Впрочем, в данном случае вместо имен пользователей подойдет и любая случайная последовательность, ее лишь придется хранить в той же таблице для последующего вычисления эталонов в процессе аутентификации.

В любом случае функция вычисления эталона из аутентификационной информации должна быть однонаправленной, т. е. легко рассчитываться, но представлять собой вычислительную проблему при попытке вычисления в обратном направлении. [3]

В открытой сетевой среде между сторонами идентификации / аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть — это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

В данной главе был рассмотрен процесс аутентификации. Он состоит из двух этапов подготовительного, при котором создается эталонная информация и штатного, где введённую информацию пользователем сравнивают с эталонной.

3 МЕТОДЫ УТЕНТИФИКАЦИИ

3.1 Аутентификация по паролям

Методы аутентификации классифицируют по используемым средствам. В этом случае указанные методы делят на четыре группы:

1. Основанные на знании лицом, имеющим право на доступ к ресурсам системы, некоторой секретной информации – пароля.
2. Основанные на использовании уникального предмета: жетона, электронной карточки и др.
3. Основанные на измерении биометрических параметров человека – физиологических или поведенческих атрибутах живого организма.
4. Основанные на информации, ассоциированной с пользователем, например, с его координатами. [1]

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на паролях – секретных идентификаторах субъектов. Здесь при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам АС.

Парольные методы следует классифицировать по степени изменяемости паролей:

- методы, использующие постоянные (многократно используемые) пароли;
- методы, использующие одноразовые (динамично изменяющиеся) пароли.

В большинстве АС используются многоразовые пароли. В этом случае пароль пользователя не изменяется от сеанса к сеансу в течение установленного администратором системы времени его действительности. Это упрощает процедуры администрирования, но повышает угрозу

рассекречивания пароля. Известно множество способов вскрытия пароля: от под смотра через плечо до перехвата сеанса связи. Вероятность вскрытия злоумышленником пароля повышается, если пароль несет смысловую нагрузку (год рождения, имя девушки), небольшой длины, набран на одном регистре, не имеет ограничений на период существования и т. д. Важно, разрешено ли вводить пароль только в диалоговом режиме или есть возможность обращаться из программы.

В последнем случае, возможно запустить программу по подбору паролей – «дробилку».Более надежный способ – использование одноразовых или динамически меняющихся паролей.

Известны следующие методы парольной защиты, основанные на одноразовых паролях:

- методы модификации схемы простых паролей;
- методы «запрос - ответ»;
- функциональные методы.

В первом случае пользователю выдается список паролей. При аутентификации система запрашивает у пользователя пароль, номер в списке, которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

При использовании метода «запрос-ответ» система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Функциональные методы основаны на использовании специальной функции парольного преобразования. Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени. Указанная функция должна удовлетворять следующим требованиям:

- для заданного пароля x легко вычислить новый пароль;
- зная x и y, сложно или невозможно определить функцию.

Наиболее известными примерами функциональных методов являются: метод функционального преобразования и метод «рукопожатия».

Идея метода функционального преобразования состоит в периодическом изменении самой функции. Последнее достигается наличием в функциональном выражении динамически меняющихся параметров, например, функции от некоторой даты и времени. Пользователю сообщается исходный пароль, собственно функция и периодичность смены пароля. Нетрудно видеть, что паролями пользователя на заданныхпериодах времени будут следующие: x, f(x), f(f(x)), ..., f(x)n-1.

Метод «рукопожатия» состоит в следующем. Функция парольного преобразования известна только пользователю и системе защиты. При входе в АС подсистема аутентификации генерирует случайную последовательность x, которая передается пользователю. Пользователь вычисляет результат функции y=f(x) и возвращает его в систему. Система сравнивает собственный вычисленный результат с полученным от пользователя. При совпадении указанных результатов подлинность пользователя считается доказанной.

Достоинством метода является то, что передача какой-либо информации, которой может воспользоваться злоумышленник, здесь сведена к минимуму.

В ряде случаев пользователю может оказаться необходимым проверить подлинность другого удаленного пользователя или некоторой АС, к которой он собирается осуществить доступ. Наиболее подходящим здесь является метод «рукопожатия», так как никто из участников информационного обмена не получит никакой конфиденциальной информации.

Отметим, что методы аутентификации, основанные на одноразовых паролях, также не обеспечивают абсолютной защиты. Например, если злоумышленник имеет возможность подключения к сети и перехватывать передаваемые пакеты, то он может посылать последние как собственные.

3.2 Аутентификация с помощью уникального предмета

Уникальность предмета, по которому выполняется аутентификация пользователя. Чаще всего это карточки (token) - специальное устройство, подтверждающее подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

К достоинству использования карточек относят то, что обработка аутентификационной информации выполняется устройством чтения, без передачи в память компьютера. Это исключает возможность электронного перехвата по каналам связи.

Недостатки пассивных карточек, следующие: они существенно дороже паролей, требуют специальных устройств чтения, их использование подразумевает специальные процедуры безопасного учета и распределения. Их также необходимо оберегать от злоумышленников, и, естественно, не оставлять в устройствах чтения. Известны случаи подделки пассивных карточек.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты: многоразовые пароли, динамически меняющиеся пароли, обычные запрос - ответные методы. Все карточки обеспечивают двухкомпонентную аутентификацию.

К указанным достоинствам интеллектуальных карточек следует добавить их многофункциональность. Их можно применять не только для целей безопасности, но и, например, для финансовых операций. Сопутствующим недостатком карточек является их высокая стоимость.

Перспективным направлением развития карточек является наделение их стандартом расширения портативных систем PCMCIA (PC Card). Такие карточки являются портативными устройствами типа PC Card, которые вставляются в разъем PC Card и не требуют специальных устройств чтения. В настоящее время они достаточно дороги.

3.3 Биометрическая аутентификация

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100 % идентификацию, решая проблемы утраты паролей и личных идентификаторов. Однако такие методы нельзя использовать при идентификации процессов или данных (объектов данных), так как они только начинают развиваться (имеются проблемы со стандартизацией и распространением), требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах и системах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК. [4]

В таблице 1 представлены примеры методов биометрии.

Таблица 1 - Примеры методов биометрии

Физиологические методы	Поведенческие методы
Снятие отпечатков пальцев Сканирование радужной оболочки глаза Сканирование сетчатки глаза Геометрия кисти руки Распознавание черт лица	Анализ подписи Анализ тембра голоса Анализ клавиатурного почерка

Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его.Наиболее используемые биометрические атрибуты и соответствующиесистемы:

Отпечатки пальцев. Такие сканеры имеют небольшой размер, универсальны, относительно недороги. Биологическая повторяемость отпечатка пальца составляет 10-5 %. В настоящее время пропагандируются правоохранительными органами из-за крупных ассигнований в электронные архивы отпечатков пальцев.

Геометрия руки. Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2 %.

Радужная оболочка глаза. Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из 1078.

Термический образ лица. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных

сотрудников и отсеивания посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок.

Голос. Проверка голоса удобна для использования в телекоммуникационных приложениях. Необходимые для этого 16-разрядная звуковая плата и конденсаторный микрофон стоят менее 25 $. Вероятность ошибки составляет 2 – 5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления идентификации личности и его состояния по голосу – возбужден, болен, говорит правду, не в себе и т.д.

Ввод с клавиатуры. Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями.

Подпись. Для контроля рукописной подписи используются дигитайзеры.

3.4 Аутентификация по местоположению

Одним из методов аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что сводит на нет возможность их перехвата.

Аппаратура GPS проста и надежна в использовании и сравнительно недорога. Это позволяет ее использовать в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Суммируя возможности средств аутентификации, ее можно классифицировать по уровню информационной безопасности на три категории:

1. Статическая аутентификация.

2. Устойчивая аутентификация.

3. Постоянная аутентификация.

Первая категория обеспечивает защиту только от НСД в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Для компрометации статической аутентификации нарушитель может подсмотреть, подобрать, угадать или перехватить аутентификационные данные и т. д.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Усиленная аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и пытаться использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных. [1]

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной

модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

ЗАКЛЮЧЕНИЕ

Цель аутентификации — максимально затруднить использование чужих (украденных, подобранных) учетных данных. Сам же этот процесс должен быть простым для легального пользователя.

Для каждой автоматизированной системы выбирается наиболее подходящий метод.

Аутентификация является обязательной процедурой проверки подлинности данных, без которой защищаемая информации может оказаться под угрозой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс»

2. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях. – Санкт-Петербург: СПбГУЭФ, 2010. – 267 с.

2. Галатенко В. А. Основы информационной безопасности. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с.

3. Тихонов И.А. Информативные параметры биометрической аутентификации пользователей информационных систем по инфракрасному изображению сосудистого русла Биомедицинская техника и радиоэлектроника. 2010.- №9. - С. 26 - 32

4. Корабельников Н. Зачем нужен сервер аутентификации // PC Week/RE. – 2015.- №5.- С.20.

5. Алпатов А. В. основы информационной безопасности. — Саратов: Профобразование, Ай Пи Эр Медиа, 2019. — 162 с. [Электронный ресурс] — URL: https://profspo.ru/books/80328

6. Михайлов С.А. Введение в законодательство Европейского сообщества. - [Электронный ресурс]. – URL: http:// www.elibrary.ru

ПРИЛОЖЕНИЕ А

Общая процедура идентификации и аутентификации пользователя в автоматизированной системе

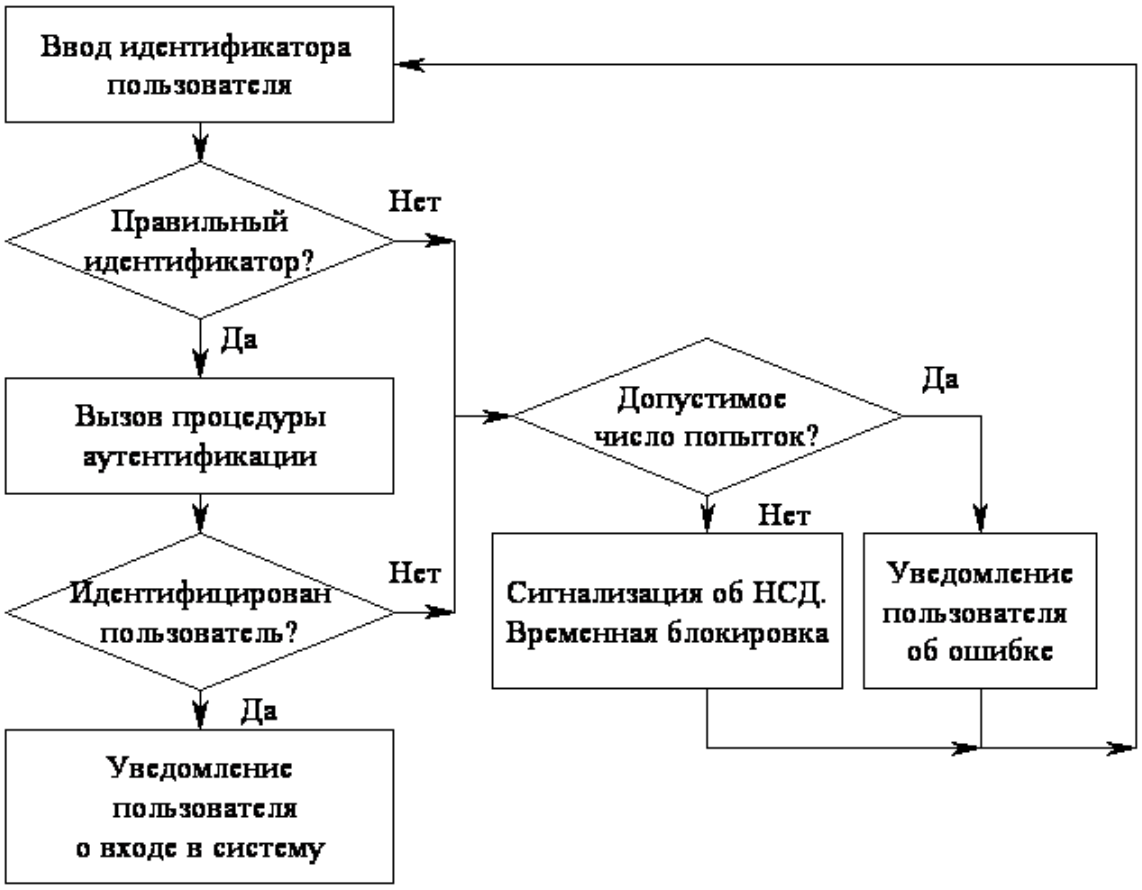

Рисунок А1 - Общая процедура идентификации и аутентификации пользователя в автоматизированной системе