Министерство образования республики Беларусь

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Институт информационных технологий

**Контрольная работа**

По курсу «Основы защиты информации»

Вариант 10

«Идентификация и аутентификация пользователя компьютерной системы»

Студента 2 курса 681072 группы

заочного отделения

Иванова Кирилла Евгеньевича

Зачетная книжка № 68107042

Домашний адрес: 213800 г. Бобруйск, ул. Энергетиков, л. 42, кв. 5,

тел. +375293194300

Проверил:

Минск, 2018

**Оглавление**

[Введение 3](#_Toc503128244)

[1. Процесс представления пользователя компьютерной системе 4](#_Toc503128245)

[2. Типовые схемы и биометрическая идентификация и аутентификация пользователя. 6](#_Toc503128246)

[3. Взаимная проверка подлинности пользователей. 12](#_Toc503128247)

[4. Упрощенный протокол идентификации с нулевой передачей знаний. 16](#_Toc503128248)

[Заключение 19](#_Toc503128249)

[Список литературы 21](#_Toc503128250)

### Введение

Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс представления компьютерной системе, который включает две стадии:

* идентификацию - пользователь сообщает системе по ее запросу свое имя (идентификатор);
* аутентификацию - пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль).

Для проведения процедур идентификации и аутентификации пользователя необходимы наличие соответствующего субъекта (модуля) аутентификации и наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя.

Различают две формы представления объектов, аутентифицирующих пользователя:

* внешний аутентифицирующий объект, не принадлежащий системе;
* внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Внешние объекты могут быть технически реализованы на различных носителях информации - магнитных дисках, пластиковых картах и т. п.

### 1. Процесс представления пользователя компьютерной системе

Совокупность выполнения процедур идентификации и аутентификации принято называть процедурой авторизации. Иногда не требуется идентифицировать пользователя, а достаточно только выполнения процедуры аутентификации. Например, это происходит, когда требуется подтвердить текущего (уже зарегистрированного) пользователя при выполнении каких-либо действий, требующих дополнительной защиты. В свою очередь, не всегда требуется осуществлять контроль идентификации, то есть в некоторых случаях аутентификация может не производиться.

Процедура авторизации имеет ключевое значение при защите компьютерной информации, т.к. вся разграничительная политика доступа к ресурсам реализуется относительно идентификаторов пользователей. То есть, войдя в систему с чужим идентификатором, злоумышленник получает права доступа к ресурсу того пользователя, идентификатор которого был им предъявлен при входе в систему.

Чтобы исключить работу с системой незаконных пользователей, необходима процедура распознавания системой каждого законного пользователя (или групп пользователей). Для этого в защищенном месте система обязана хранить информацию, по которой можно опознать пользователя, а пользователь при входе в систему, при выполнении определенных действий, при доступе к ресурсам обязан себя идентифицировать, т. е. указать идентификатор, присвоенный ему в данной системе. Получив идентификатор, система проводит его аутентификацию, т. е. проверяет его содержательность (подлинность) - принадлежность к множеству идентификаторов. Если бы идентификация не дополнялась аутентификацией, то сама идентификация теряла бы всякий смысл. Обычно устанавливается ограничение на число попыток предъявления некорректного идентификатора.

Аутентификация пользователя может быть основана на следующих принципах:

* на предъявлении пользователем пароля;
* на предъявлении пользователем доказательств, что он обладает секретной ключевой информацией;
* на ответах на некоторые тестовые вопросы;
* на предъявлении пользователем некоторых неизменных признаков, неразрывно связанных с ним;
* на предоставлении доказательств того, что он находится в определенном месте в определенное время;
* на установлении подлинности пользователя некоторой третьей, доверенной стороной.

Процедуры аутентификации должны быть устойчивы к подлогу, подбору и подделке. После распознавания пользователя система должна выяснить, какие права предоставлены этому пользователю, какую информацию он может использовать и каким образом (читать, записывать, модифицировать или удалять), какие программы может выполнять, какие ресурсы ему доступны, а также другие вопросы подобного рода. Этот процесс называется авторизацией. Таким образом, вход пользователя в систему состоит из идентификации, аутентификации и авторизации. В процессе дальнейшей работы иногда может появиться необходимость дополнительной авторизации в отношении каких-либо действий.

### 2. Типовые схемы и биометрическая идентификация и аутентификация пользователя.

Практически любому ключевому носителю информации, используемому для опознания, соответствует следующая структура данных о пользователе:

* IDi - неизменный идентификатор i-го пользователя, который является аналогом имени и используется для идентификации пользователя;
* Ki - аутентифицирующая информация пользователя, которая может изменяться и служит для аутентификации (например, пароль Pi=Ki).

Так для носителей типа пластиковых карт выделяется неизменяемая информация IDi и объект в файловой структуре карты, содержащий Ki.

Совокупную информацию в ключевом носителе можно назвать первичной аутентифицирующей информацией i-го пользователя. Очевидно, что внутренний аутентифицирующий объект не должен существовать в системе длительное время (больше времени работы конкретного пользователя). Например, Вы ввели пароль, который программа аутентификации занесла в переменную для сравнения с хранящимися в базе данных. Эта переменная должна быть обнулена не позже, чем Вы закончите свой сеанс. Для длительного хранения следует использовать данные в защищенной форме.

Существует две типовые схемы идентификации и аутентификации.

Первая из типовых схем – «С объектом-эталоном». В компьютерной системе выделяется объект-эталон для идентификации и аутентификации пользователей. Структура объекта-эталона показана в рис. 2.1. Здесь Ei=F(IDi, Кi), где F-функция, которая обладает свойством "невосстановимости" значения Кi по Еi и IDi. “Невоостановимость" Ki оценивается некоторой пороговой трудоемкостью Т0 решения задачи восстановления аутентифицирующей информации Кi по Еi и IDi. Кроме того, для пары Ki и Kj возможно совпадение соответствующих значений Е. В связи с этим вероятность ложной аутентификации пользователя не должна быть больше некоторого порогового значения Р0. На практике задают https://studfiles.net/html/1546/187/html_3hF24H6Ewf.w7M2/img-PnCfa7.jpg



Рисунок 2.1. «Структура объекта-эталона

Протокол идентификации и аутентификации следующий:

1. пользователь предъявляет свой идентификатор ID;
2. если ID не совпадает ни с одним IDi, зарегистрированным в компьютерной системе, то идентификация отвергается – пользователь не допускается к работе, иначе (существует IDi = ID) устанавливается, что пользователь, назвавшийся пользователем i, прошел идентификацию.;
3. субъект аутентификации запрашивает у пользователя его аутентификатор К;
4. субъект аутентификации вычисляет значение E=F(IDi , К);
5. субъект аутентификации производит сравнение значений E и Еi. При совпадении этих значений устанавливается, что данный пользователь успешно аутентифицирован в системе. Информация об этом пользователе передается в программные модули, использующие ключи пользователей (т.е. в систему шифрования, разграничения доступа и т.д.). В противном случае аутентификация отвергается - пользователь не допускается к работе.

Данная схема идентификации и аутентификации пользователя может быть модифицирована. Модифицированная схема обладает лучшими характеристиками по сравнению с первой схемой. Модифицированная типовая схема – «С модифицированным объектом-эталоном», рисунок 2.2.



Рисунок 2.1. «Структура объекта-эталона

В отличие от схемы 1, в схеме 2 значение Еi равно F(Si, Кi), где Si – случайный вектор, задаваемый при создании идентификатора пользователя, т.е. при создании строки, необходимой для идентификации и аутентификации пользователя; F–функция, которая обладает свойством "невосстановимости" значения Кi по Ei и Si.

Протокол идентификации и аутентификации (для схемы 2).

1. Пользователь предъявляет свой идентификатор ID.
2. Если существует i=1...n, для которого ID=IDi, то пользователь идентификацию прошел успешно. Иначе пользователь не допускается к работе.
3. По идентификатору ID выделяется вектор S.
4. Модуль аутентификации запрашивает у пользователя его аутентификатор K.
5. Вычисляется значение E=F(S, K).
6. Если E=Ei, то аутентификация прошла успешно. Иначе пользователь не допускается к работе.

Вторая схема аутентификации применяется в OC UNIX. В качестве идентификатора используется имя пользователя (запрошенное по Login), в качестве аутентификатора - пароль пользователя (запрошенный по Password). Функция F представляет собой алгоритм шифрования DES. Эталоны для идентификации и аутентификации содержатся в файле Etc/passwd.

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.). В последнее время все большее распространение получает биометрическая идентификация и аутентификация, позволяющая уверенно идентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

Основные достоинства биометрических методов идентификации и аутентификации:

* высокая степень достоверности идентификации по биометрических признакам из-за их уникальности;
* неотделимость биометрических признаков от дееспособной личности;
* трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые могут быть использованы для идентификации потенциального пользователя, используются:

* узор радужной оболочки и сетчатки глаз;
* отпечатки пальцев;
* геометрическая форма руки;
* форма и размеры лица;
* термограмма лица;
* форма ушей;
* особенности голоса;
* ДНК;
* биомеханические характеристики рукописной подписи;
* биомеханические характеристики "клавиатурного почерка".

При регистрации пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный "образ" законного пользователя. Этот образ пользователя хранится в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя.

Системы идентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса:

* использующие рисунок радужной оболочки глаза;
* использующие рисунок кровеносных сосудов сетчатки глаза.

Поскольку вероятность повторения данных параметров равна 10-78, эти системы являются наиболее надежными среди всех биометрических систем. Такие средства применяются, например, в США в зонах военных и оборонных объектов.

Системы идентификации по отпечаткам пальцев являются самыми распространенными. Одна из основных причин широкого распространения таких систем заключается в наличии больших банков данных по отпечаткам пальцев. Основными пользователями таких систем во всем мире являются полиция, различные государственные организации и некоторые банки.

Системы идентификации по геометрической форме руки используют сканеры формы руки, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы именно этого типа.

Системы идентификации по лицу и голосу являются наиболее доступными из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса широко применяются при удаленной идентификации в телекоммуникационных сетях.

Системы идентификации по динамике рукописной подписи учитывают интенсивность каждого усилия подписывающегося, частотные характеристики написания каждого элемента подписи и начертания подписи в целом.

Системы идентификации по биомеханическим характеристикам "клавиатурного почерка" основываются на том, что моменты нажатия и отпускания клавиш при наборе текста на клавиатуре существенно различаются у разных пользователей. Этот динамический ритм набора ("клавиатурный почерк") позволяет построить достаточно надежные средства идентификации.

Следует отметить, что применение биометрических параметров при идентификации субъектов доступа автоматизированных систем пока не получило надлежащего нормативно-правового обеспечения, в частности в виде стандартов. Поэтому применение систем биометрической идентификации допускается только в системах, обрабатывающих и хранящих персональные данные, составляющие коммерческую и служебную тайну.

### 3. Взаимная проверка подлинности пользователей.

Обычно стороны, вступающие в информационный обмен, нуждаются во взаимной аутентификации. Этот процесс выполняется в начале сеанса связи.

Для проверки подлинности применяют следующие способы:

* механизм запроса-ответа;
* механизм отметки времени ("временной штемпель").

Механизм запроса-ответа. Если пользователь A хочет быть уверен, что сообщения, получаемые им от пользователя B, не являются ложными, он включает в посылаемое для B сообщение непредсказуемый элемент - запрос X (например, некоторое случайное число). При ответе пользователь B должен выполнить над этим числом некоторую заранее оговоренную операцию (например, вычислить некоторую функцию f(X)). Это невозможно осуществить заранее, так как пользователю B неизвестно, какое случайное число X придет в запросе. Получив ответ с результатом действий B, пользователь A может быть уверен, что B - подлинный. Недостаток этого метода - возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить насколько "устарело" пришедшее сообщение и не принимать его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает проблема допустимого временного интервала задержки для подтверждения подлинности сеанса. Ведь сообщение с "временным штемпелем" в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

Для взаимной проверки подлинности обычно используют процедуру "рукопожатия", которая базируется на указанных выше механизмах и заключается во взаимной проверке ключей, используемых сторонами. Иначе говоря, стороны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами. Процедуру "рукопожатия" применяют в компьютерных сетях при организации связи между пользователями, пользователем и хост-компьютером, между хост-компьютерами и т.д.

В качестве примера рассмотрим процедуру "рукопожатия" для двух пользователей A и B, рисунок 3.1. Пусть применяется симметричная криптосистема. Пользователи A и B разделяют один и тот же секретный ключ KAB.



Рисунок 3.1. «Процедура рукопожатий» (А проверяет подлинности В)

* Пользователь A инициирует "рукопожатие", отправляя пользователю B свой идентификатор IDA в открытой форме.
* Пользователь B, получив идентификатор IDA, находит в базе данных секретный ключ KAB и вводит его в свою криптосистему.
* Тем временем пользователь A генерирует случайную последовательность S с помощью псевдослучайного генератора PG и отправляет ее пользователю B в виде криптограммы EKAB(S).
* Пользователь B расшифровывает эту криптограмму и раскрывает исходный вид последовательности S.
* Затем оба пользователя преобразуют последовательность S, используя одностороннюю функцию f.
* Пользователь B шифрует сообщение f(S) и отправляет криптограмму EKAB(f(S)) пользователю A.
* Наконец, пользователь A расшифровывает эту криптограмму и сравнивает полученное сообщение f'(S) с исходным f(S). Если эти сообщения равны, то пользователь A признает подлинность пользователя B.

Пользователь A проверяет подлинность пользователя B таким же способом. Обе эти процедуры образуют процедуру "рукопожатия", которая обычно выполняется в самом начале любого сеанса связи между любыми двумя сторонами в компьютерных сетях.

Достоинством модели "рукопожатия" является то, что ни один из участников связи не получает никакой секретной информации во время процедуры подтверждения подлинности.

Иногда пользователи хотят иметь непрерывную проверку подлинности отправителей в течение всего сеанса связи. Рассмотрим один из простейших способов непрерывной проверки подлинности, рисунок 3.2.

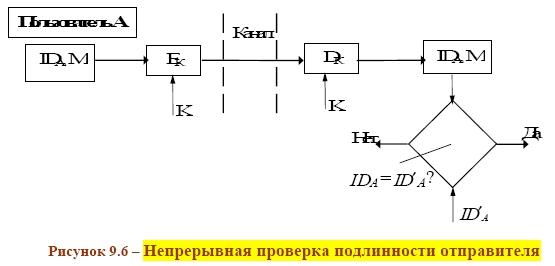


Рисунок 3.2. «Непрерывная проверка подлинности отправителя»

Чтобы отправить сообщение M, пользователь A передает криптограмму EK(IDA, M). Получатель расшифровывает ее и раскрывает пару (IDA, M). Если принятый идентификатор IDA совпадает с хранимым, получатель принимает во внимание это сообщение.

Вместо идентификаторов можно использовать секретные пароли, которые подготовлены заранее и известны обеим сторонам.

Такая процедура рукопожатия предполагает общий секретный сеансовый ключ для А и В.

Другие процедуры могут включать в себя как этап распределения ключей между партнёрами, так и этап подтверждения подлинности.

### 4. Упрощенный протокол идентификации с нулевой передачей знаний.

Широкое распространение смарт-карт (интеллектуальных карт) для разнообразных коммерческих, гражданских и военных применений (кредитные карты, карты социального страхования, карты доступа в охраняемые помещения, компьютерные пароли и ключи и т.д.) потребовало обеспечение безопасности идентификации таких карт и их владельцев. Во многих приложениях главная проблема заключается в том, чтобы при предъявлении смарт-карты оперативно обнаружить обман и отказать обманщику в допуске, ответе и обслуживании.

Для безопасного использования смарт-карт разработаны протоколы идентификации с нулевой передачей знаний. Секретный ключ владельца карты становится неотъемлемым признаком его личности. Доказательство знания этого секретного ключа с нулевой передачей этого знания служит доказательством подлинности личности владельца карты.

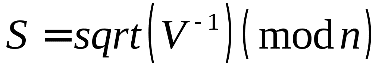
Схему идентификации с нулевой передачей знаний предложили в 1986 г. У.Фейге, А.Фиат и А.Шамир. Она является наиболее известным доказательством идентичности с нулевой передачей конфиденциальной информации.

В упрощенном варианте схемы иденти­фикации с нулевой передачей знаний выбирают случайное значение модуля https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-Q0HY_M.png, который является произведением двух боль­ших простых чисел. Модульhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-1LrFZs.pngдолжен иметь длину 512…1024 бит. Это значениеhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-BKdwGM.pngможет быть представлено группе пользова­телей, которым придется доказывать свою подлинность. В про­цессе идентификации участвуют две стороны:

– сторона *А*, доказывающая свою подлинность,

– сторона *В*, проверяющая представляемое стороной *А* доказательство.

Для того чтобы сгенерировать открытый и секретный ключи для стороны *А*, доверенный арбитр (Центр) выбирает некоторое число https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-mUBSxF.png, которое является квадратичным вычетом по модулюhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-Dv5R_Y.png. Иначе говоря, выбирается такое числоhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-PclE9k.png, при котором сравнениеhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-HX5sow.pngимеет решение и существует целое числоhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-O0LoY_.png.

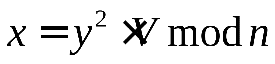
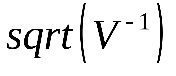
Выбранное значение https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-DJDlL2.pngявляется **открытым ключом**для *А*. Затем вычисляют наименьшее значение *S*, для которого . Это значение *S* является секретным ключом для *А*.

Теперь можно приступить к выполнению протокола иден­тификации.

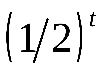
1. Сторона *А* выбирает некоторое случайное число https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-oKql4v.png, гдеhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-e1RDFO.png. Затем она вычисляетhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-vfxgT9.pngи отправляетhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-DPyOet.pngстороне *В*.

2. Сторона *В* посылает *А* случайный бит https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-vjrSe_.png.

3. Если https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-0Kkzbb.png, тогда *А* отправляет https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-epAQDq.pngстороне *В*. Если https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-NITomY.png, то *А* отправляет стороне *В* https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-ljCgpH.png.

4. Если https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-8yTGWX.png, то сторона*B* проверяет, что https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-VxhT_m.png,чтобы убедиться, что *А* знает . Еслиhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-1AfFc8.png, сторона *В* проверяет, что , чтобы быть уверенной, что *А* знает .

Эти шаги образуют один цикл протокола, называемый ак­кредитацией. Стороны *А* и *В* повторяют этот цикл https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-WJ3ToG.pngраз при разных случайных значенияхhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-EL1u8X.pngиhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-3I0YBD.pngдо тех пор, пока *В* не убедится, что *А* знает значение *S*.

Если сторона *А* не знает значения *S*, она может выбрать такое значение https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-n_46Q6.png, которое позволит ей обмануть сторону *В*, если *В* отправит ей https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-9KXq9n.png, либо *А* может выбрать такое https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-_GO3mT.png, которое по­зволит обмануть *В*, если *В* отправит ейhttps://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-Wi_RfX.png. Но этого невозмож­но сделать в обоих случаях. Вероятность того, что *А* обманет *В* в одном цикле, составляет https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-AcbaLH.png. Вероятность обмануть*B* https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-CiCryP.pngциклах равна.

Для того чтобы этот протокол работал, сторона *А* никогда не должна повторно использовать значение https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-0dNZqk.png. Если *А* поступила бы таким образом, а сторона *В* отправила бы стороне *А* на шаге 2 другой случайный бит https://studfiles.net/html/2706/349/html_D3rXCzWP_r.3nmH/img-0drXgG.png, то *В* имела бы оба ответа *А*. После этого *В* может вычислить значение *S*, и для *А* все закончено.

### Заключение

С каждым объектом компьютерной системы (КС) связана некоторая информация, однозначно идентифицирующая его. Это может быть число, строка символов, алгоритм, определяющий данный объект. Эту информацию называют идентификатором объекта.

Идентификация объекта - одна из функций подсистемы защиты. Эта функция выполняется в первую очередь, когда объект делает попытку войти в сеть. Следующий шаг-аутентификация объекта (проверка подлинности объекта). Эта процедура устанавливает, является ли данный объект именно таким, каким он себя объявляет.

После того как объект идентифицирован и подтверждена его подлинность, можно установить сферу его действия и доступные ему ресурсы. Такую процедуру называют предоставлением полномочий (авторизацией).

Допустим, что в компьютерной системе зарегистрировано n пользователей. Пусть i-й аутентифицирующий объект i-гo пользователя содержит два информационных поля IDi-неизменный идентификатор i-гo пользователя и Ki-аутентифицирующая информация пользователя. Описанная структура соответствует практически любому ключевому носителю информации, используемому для опознания пользователя. Для длительного хранения следует использовать данные в защищенной форме.

Существует две типовые схемы идентификации и аутентификации: с объектом-эталоном и с модифицированным объектом-эталоном.

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.). В последнее время все большее распространение получает биометрическая идентификация и аутентификация пользователя, позволяющая уверенно идентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения

### Список литературы

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. - М.:Радио и связь, 2001. - 376 с.: ил.
2. Голиков, В. Ф., Лыньков, Л. М., Прудник, А. М., Борботько, Т. В. Правовые и организационно-технические методы защиты информации. – Мн.: БГУИР, 2004. – 81 с.
3. Современные технологии защиты информации – Интуит [Электронный ресурс]. – Режим доступа: www.intuit.ru/studies/courses/1162/285/lecture/7164. – Дата доступа 25.05.2015.
4. Основы информационной безопасности и защита ... – Sites [Электронный ресурс]. – Режим доступа: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1
5. Борботько, Т. В. Лекции по курсу «Основы защиты информации». – Мн.: БГУИР, 2006. – 81 с.
6. Сечко, Г. В. Конспект лекций по курсу «Основы защиты информации». – Мн.: БГУИР, 2015. – 81 с.
7. Методы и средства защиты информации [Электронный ресурс]. – Режим доступа: abc.vvsu.ru/Books/inform\_tehnolog/page0025.asp.
8. Криштопова, Е. А. Основы защиты информации: методическое пособие. – Мн.: 2012. – 176 с.
9. Романец, Ю.В., Тимофеев, П.А., Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.