Аутентификация пользователей.

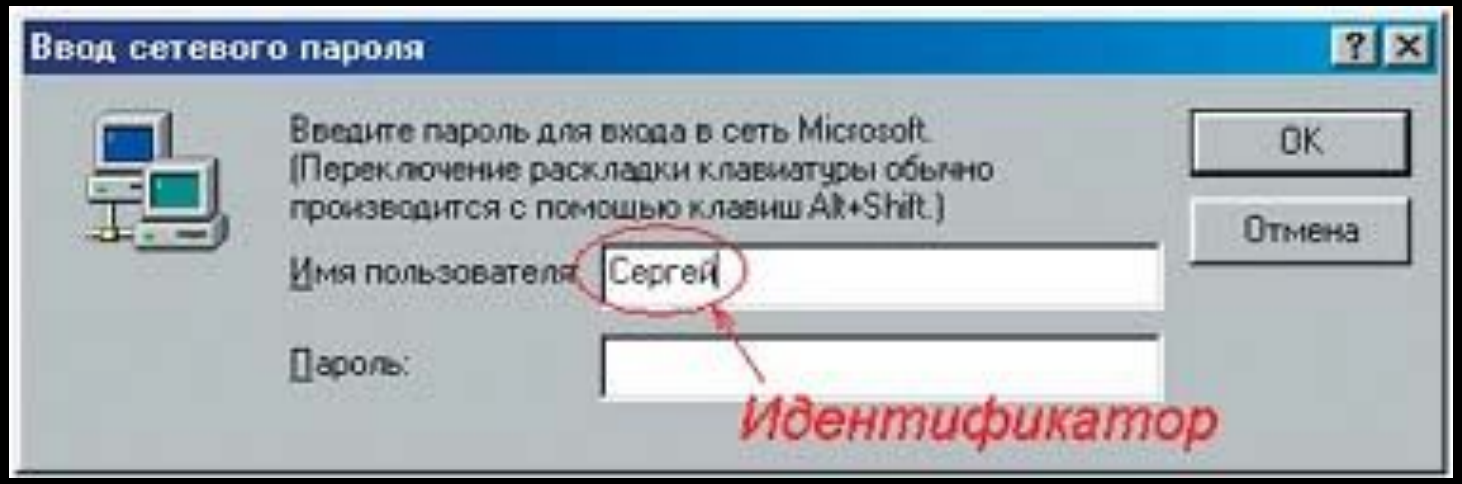
Выполнила:
Боровкова Ксения
гр. И-411

Аутентифика́ция (англ. *Authentication*) или *подтверждение подлинности* — процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, в простейшем случае — с помощью имени и пароля.

Данную процедуру следует отличать от идентификации (опознавания субъекта информационного взаимодействия) и авторизации (проверки прав доступа к ресурсам системы).

Идентификация и аутентификация

Прежде чем проверять истинность пользователя, его нужно идентифицировать, т.е. из многих пользователей, зарегистрированных в системе, выбрать по некоему уникальному идентификатору одного. Его-то система и будет проверять. Идентификатор — это имя, под которым зарегистрирован пользователь в проверяющей его компьютерной системе. Например, в окне «Ввод сетевого пароля», которое знакомо многим, идентификатором пользователя является содержимое поля «Имя».



Аутентификация пользователей обычно выполняется неким программным модулем, находящимся непосредственно на компьютере, на который пользователь пытается получить прямой или удаленный доступ. Всю работу данного модуля можно условно разделить на два этапа.

Предварительный, на котором модуль формирует «эталонный образец», например, запрашивает пароль пользователя (это именно тогда пароль запрашивается дважды, чтобы исключить ошибку его ввода) — по нему пользователь будет опознаваться впоследствии. Пароль (или другой эталон) может и назначаться пользователю — так бывает, например, в различных системах доступа в Интернет. Обычно модуль аутентификации хранит эталонные образцы в таблице соответствий «пользователь — эталон».

И завершающий этап, когда пользователь проходит аутентификацию и у него запрашивается аутентификационная информация, которая сравнивается с эталоном. На основании этого сравнения он считается опознанным или нет.

На самом деле в реальных системах эталонный пароль может храниться в таблице в зашифрованном виде или вместо пароля сохраняется его хэш. Это не позволит злоумышленнику, получившему доступ к хранилищу эталонов, ознакомиться с паролями всех пользователей системы.

В более сложных случаях предъявляемая пользователем аутентификационная информация и ее эталонный образец могут дополнять друг друга, участвуя в каких-либо криптографических преобразованиях. Для этого используются различные протоколы сетевой аутентификации.

Информация, по которой опознается пользователь, бывает трех видов:

- Пользователь знает нечто уникальное и демонстрирует компьютеру это знание.
- Пользователь имеет предмет с уникальным содержимым или с уникальными характеристиками.
- Аутентификационная информация является неотъемлемой частью пользователя.

Пароль

По парольному принципу строятся простейшие системы аутентификации, в которых пользователю достаточно ввести правильный пароль для получения доступа к нужному ему ресурсу. Парольная аутентификация является наиболее распространенной:

- во-первых, это самый простой из рассматриваемых методов аутентификации;
- во-вторых, он появился намного раньше остальных, поэтому к настоящему времени реализован в огромном количестве различных компьютерных программ.

Недостатков же у парольной аутентификации не счесть.

- Во-первых, очень часто неискушенные пользователи выбирают простые или легко угадываемые пароли:
  - какую-либо производную от идентификатора пользователя ;
  - слово какого-либо языка или общеупотребительную фразу.
  - нередко пользователи применяют короткие пароли, которые легко подбираются перебором всех возможных вариантов.

- Во-вторых, пароль могут подсмотреть или перехватить при вводе.
- В-третьих, пароль может быть получен путем применения насилия к его владельцу.
- Наконец, существуют и применяются злоумышленниками действенные методы *социальной инженерии*, с помощью которых можно получить пароль пользователя обманным путем — неопытный пользователь сам назовет его лиходею, если тот сможет ловко притвориться администратором системы.

Нельзя сказать, что технический прогресс в отношении парольной аутентификации стоит на месте. Не прекращаются попытки построить сильную аутентификацию в сочетании с удобством и простотой применения паролей.

Разработано множество программных и аппаратных *генераторов паролей*, которые вырабатывают длинные и сильные случайные пароли, неуязвимые для словарных атак и других вариантов подбора. Обратная сторона медали: пользователи вынуждены запоминать длинные и сложные пароли, результат — искушение записать пароль на бумажку и повесить ее на монитор.

Уникальный предмет

Для аутентификации пользователей наиболее часто применяются следующие предметы: смарт-карты, карты с магнитной полосой, электронные таблетки iButton, USB-токены.

Уникальность каждого из перечисленных предметов определяется информацией, которую он содержит. В простейшем случае эта информация представляет собой идентификатор и пароль пользователя, которые просто считываются с носителя и передаются модулю аутентификации. Более сложный случай — носитель содержит криптографический ключ, который используется в каком-либо из протоколов удаленной аутентификации.

Недостатков у «предметной» аутентификации несколько меньше, чем у парольной, а именно следующие:

- предмет может быть похищен или отнят у его владельца;
- в большинстве случаев требуется специальное оборудование для работы с предметами;
- иногда возможно изготовление копии или эмулятора предмета.

Биометрическая аутентификация

В качестве аутентификационной информации в данном случае берутся во внимание оригинальные и неотъемлемые характеристики человека. Наиболее часто используются следующие из них:

- Отпечатки пальцев. Известно, что они уникальны для каждого человека, причем не меняются на протяжении жизни. Для сканирования отпечатков пальцев применяется самое дешевое оборудование, данный метод привычен для пользователей и не вызывает каких-либо опасений.

- Рисунок радужной оболочки глаза. Это на сегодня наиболее точный метод биометрической аутентификации. Но многие пользователи боятся процесса сканирования радужной оболочки, да и оборудование для сканирования является дорогостоящим.
- Черты лица. Данная технология распознавания считается очень перспективной, поскольку именно по чертам лица узнают друг друга люди. К сожалению, системы, реализующие данный метод, пока не блещут точностью.

В качестве уникальных признаков человека используются также характеристики его голоса, образец рукописной подписи, «клавиатурный почерк» (интервалы времени между нажатиями клавиш, составляющих кодовое слово, и интенсивность нажатий), геометрия руки и др. Однако эти технологии значительно меньше распространены, чем описанные выше.

С детства каждому из нас известно, что «все работы хороши — выбирай на вкус». Аналогичным образом можно охарактеризовать и методы аутентификации — применение найдется для любого из них. Все зависит от степени важности информации, к которой получает доступ аутентифицируемый пользователь.