Идентификация и аутентификация

Идентификация и аутентификации применяются

для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы)

Общий алгоритм работы таких систем:

- Нужно получить от субъекта (например, пользователя) информацию, удостоверяющую его личность,
- проверить подлинность,
- затем предоставить (или не предоставлять) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является *обязательным условием* любой защищенной системы, т.к. все механизмы защиты информации рассчитаны на работу с поименными субъектами и объектами информационных систем.

Идентификация – это присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) – это проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности (т.е. аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает).

В качестве идентификатора используют:

- **Набор символов** (пароль, секретный ключ, персональный идентификатор и т.п.), который пользователь запоминает или для их запоминания используют специальные средства хранения (электронные ключи);
- **Физиологические параметры человека** (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.). Обеспечивают почти 100% идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Используют такие методы пока только на особо важных объектах, т.к. требуют сложного и дорогостоящего оборудования.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

- Методы, использующие **постоянные** (многократно используемые) **пароли**;
- Методы, использующие **одноразовые** (динамично изменяющиеся) **пароли** (более надежный метод парольной защиты).

Комбинированные методы идентификации и аутентификации

требуют, помимо знания пароля, наличие *карточки (token)* – специального устройства, подтверждающего подлинность субъекта.

Два типа карточек:

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

Пассивные карточки с магнитной полосой (самые распространенные)

считываются специальным устройством, имеющим клавиатуру и процессор.

1. Пользователь вводит свой идентификационный номер;
2. Если совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему.

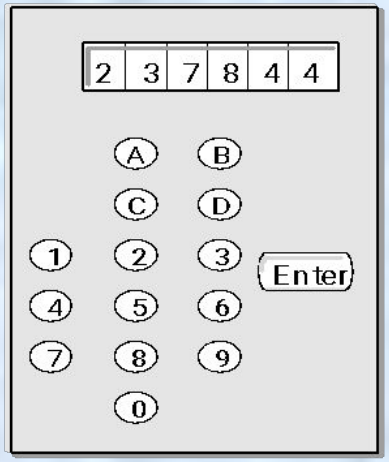
Это позволяет достоверно установить лицо, получившее доступ к системе, и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ называют ***двухкомпонентной аутентификацией.***

Интеллектуальные карточки имеют:

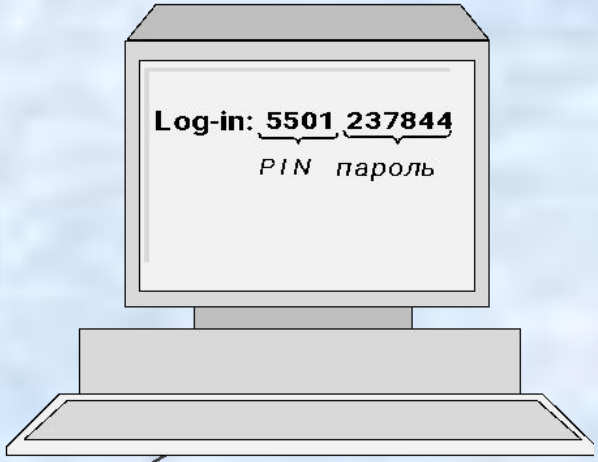
1. память;
2. собственный процессор.

Это позволяет реализовать различные варианты парольных методов защиты, например, многоразовые пароли, динамически меняющиеся пароли.

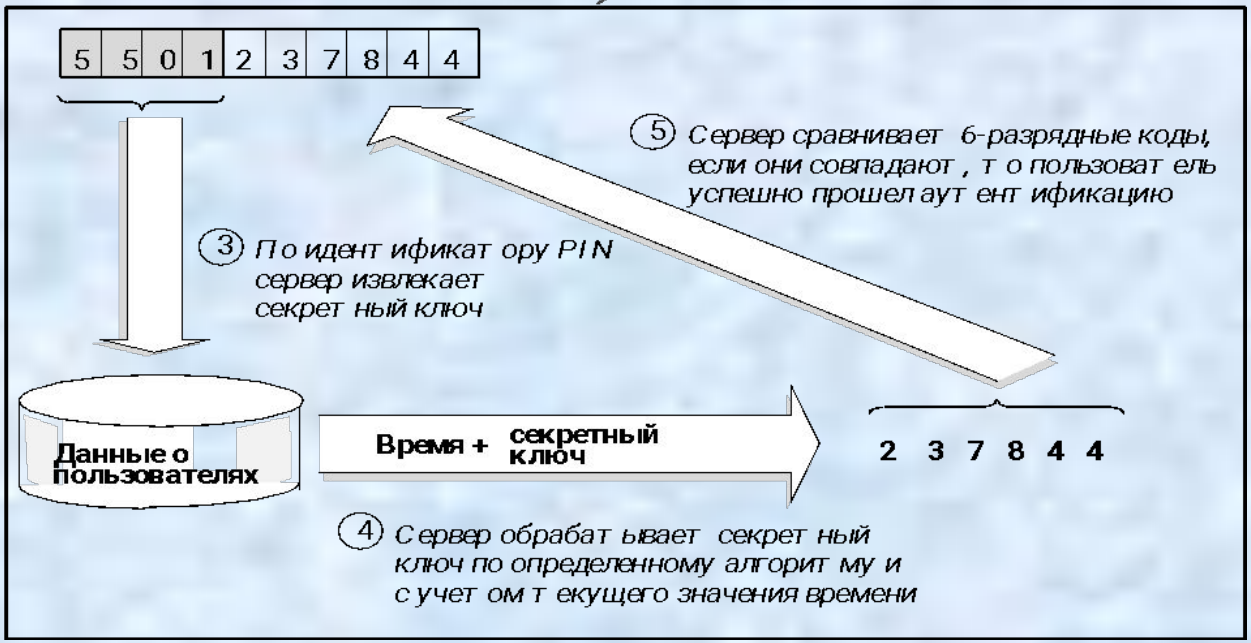
① Токен генерирует 6-разрядный пароль в соответствии с алгоритмом, временем и ключом



② При логическом входе пользователь вводит свой идентификатор PIN и 6-разрядный пароль



Сервер аутентификации



Новейшее направление аутентификации

– это 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:

1. орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно;
2. координаты постоянно меняются, что исключает их перехват.

Механизм идентификации и аутентификации пользователей

1. пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатков);
2. система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами;
3. если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий (совокупность прав);
4. в случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор;
5. Если пользователь превышает лимит возможных повторов ввода информации, система временно блокируется и выдается сообщение о несанкционированных действиях.

Три категории аутентификации по уровню ИБ:

1. Статическая аутентификация
2. Устойчивая аутентификация
3. Постоянная аутентификация

Статическая аутентификация

обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию.

Пример: традиционные постоянные пароли.
Их эффективность зависит от сложности угадывания паролей и от того, насколько хорошо они защищены.

Устойчивая аутентификация

использует динамические данные аутентификации, меняющиеся с каждым сеансом работы.

Пример: системы, использующие одноразовые пароли и электронные подписи.

УА *обеспечивает защиту от* ***атак***, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

УА *не обеспечивает защиту от* ***активных атак***, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация

обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки.

Пример: использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.