Лекция №3

Средства и методы аутентификации в операционных системах

(часть 2)

Технология однократного входа (SSO – Single Sign-on)

- В организациях часто сотрудникам необходимо работать с несколькими программами, требующими аутентификации.
- Технология однократного входа подразумевает использование одного пароля для получения доступа ко всем ресурсам.

Технология SSO

- Для хранения паролей пользователя ко всем ресурсам используется дополнительная база.
- Для доступа к хранимым паролям используется мастер-пароль.
- При правильном вводе мастер-пароля аутентификация пользователя при обращении к ресурсам происходит автоматически.

Преимущества и недостатки технологии SSO

Преимущества:

- пользователю не нужно запоминать несколько паролей, поэтому может быть выбран более стойкий мастер-пароль;
- на аутентификацию пользователь затрачивает меньше времени.

Недостатки:

- необходимо защищать базу для хранения паролей;
- в случае взлома мастер-пароля злоумышленник получает доступ ко всем ресурсам, к которым имеет доступ пользователь.

Разновидности парольной защиты

- Добавление к паролю случайных символов.
- Использование мастер-пароля.
- Пароли, основанные на фразах.
- Одноразовые пароли.
- PIN-код.

Добавление к паролю случайных символов

- С каждым паролем связывается псевдослучайный набор символов определённой длины.
- При хэшировании вместо пароля используется пароль, сцеплённый с набором символов.
- При смене пароля набор символов изменяется.

Преимущество: возрастает стойкость пароля, но пользователь запоминает более простой пароль.

Недостатки: необходимо поддерживать модуль для генерации дополнительного набора символов, усложнять процедуру регистрации и защищать от атак как сам модуль, так и базу для хранения набора символов.

Использование мастер-пароля

- При наличии у одного пользователя нескольких паролей (для доступа к различным ресурсам) возможно их хранение в системе.
- Для доступа к хранимым паролям используется мастер-пароль.

  Преимущество: пользователю не нужно запоминать несколько паролей, поэтому может быть выбран более стойкий мастер-пароль.

  Недостатки: необходимо защищать базу для хранения паролей, в случае взлома мастер-пароля злоумышленник получает доступ ко всем ресурсам.

Пароли, основанные на фразах

- В качестве пароля используются первые символы из не имеющей смысла фразы (например, «КОВёр ПИШет ОГУрцу»; пароль - ковпишогу).
- Фраза составляется путём случайного выбора каждого слова из базы.

  Преимущества: пароль установленной длины не имеет смыслового значения и прост для запоминания.

  Недостатки: низкое качество пароля (используются только буквы); необходимо защищать базу слов.

Одноразовые пароли

- Алгоритм основан на необратимой функции $y=f(x)$, обладающей тем свойством, что по заданному x легко найти y, но по заданному y подобрать x невозможно в приемлемое время из-за сложности вычислений.
- Пользователь выбирает секретный пароль s, который он запоминает, а также количество одноразовых паролей n. Тогда пароли могут вычисляться преобразованием: $P_{i-1}=f(P_i)$. (Пример: $P_{i-1}=2*P_i$; $s=2$).
- При $n=3$ пароли будут равны: $P_1= f(f(f(s)))$; $P_2= f(f(s))$; $P_3=f(s)$. (Пример: $P_1=2*(2*(2*s))=16$; $P_2= 2*(2*s)=8$; $P_3=2*s=4$).

Схема аутентификации на основе одноразовых паролей

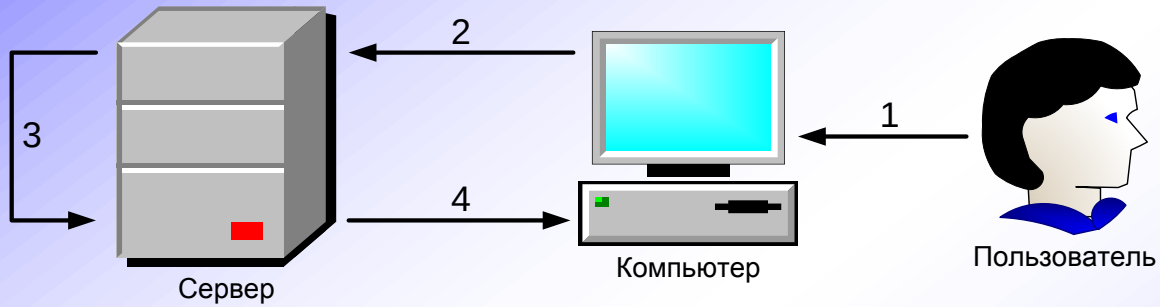
Данные, хранящиеся на сервере:

- реализация алгоритма *f*, осуществляющего необратимое преобразование пароля;
- P_{i-1} – последний использовавшийся пароль.

Данные, хранящиеся на рабочей станции:

- реализация алгоритма *f*;
- *i* – номер используемого пароля.

Схема аутентификации на основе одноразовых паролей



1. Пользователь вводит пароль *s*.
2. Вычисление и передача значения P_i.
3. Вычисление значения $P_{i-1} = f(P_i)$и сравнение с хранящимся значением (при совпадении – перезапись хранящегося значения).
4. При совпадении значений – предоставление доступа.

Аутентификация на основе PIN-кода

- В локальном устройстве, в котором осуществляется аутентификация с помощью PIN-кода, имеется интерфейс для пользователя, а не для программ. Никто не может ввести PIN-код без использования клавиатуры данного устройства.
- PIN-код не передаётся по сети и не может быть перехвачен.

Аутентификация с использованием физического объекта

Аутентификация при помощи физического объекта

- Пластиковые карты.
- Смарт-карты – пластиковые карты со встроенной микросхемой (содержат микропроцессор и ОС).
- Touch Memory.
- USB-ключи.

Физические объекты чаще всего используются при двухфакторной аутентификации (кроме наличия объекта необходимо знать PIN-код и т.п.).

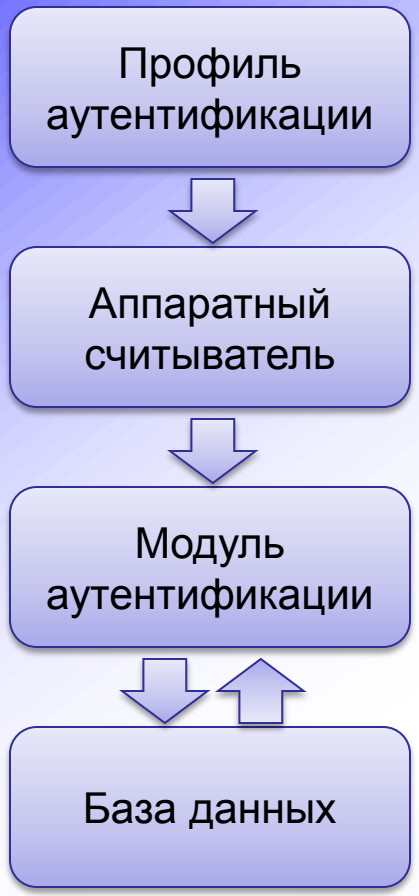
Аутентификация при помощи физического объекта

USB-ключ и смарт-карта

Touch Memory

Пластиковые карты

Схема аутентификации с использованием устройств



- Профиль аутентификации – запись на физическом объекте, в которой хранится информация для входа в систему (может содержать логин, пароль, имя домена и др.).
- Аппаратный считыватель – интерфейс между физическим объектом и системой (возможно подсоединение непосредственно к одному из портов или через дополнительное считывающее устройство).
- При двухфакторной аутентификации модуль аутентификации дополнительно делает запрос пароля на доступ к содержимому устройства.

Одноразовые пароли

Одноразовые пароли (OTP, One-Time Passwords) — динамическая аутентификационная информация, генерируемая для единичного использования с помощью аутентификационных OTP-токенов (программных или аппаратных).

Технологии аутентификации с использованием одноразовых паролей

- Программная – на стороне пользователя генерация одноразового пароля производится программными средствами (пользователь вводит только пароль).
- Аппаратная – генерация одноразового пароля производится аппаратно (пользователь вводит в устройство PIN-код, а в систему вводит пароль, сгенерированный устройством).

OTP-токен

OTP-токен — мобильное персональное устройство, принадлежащее определённому пользователю, генерирующее одноразовые пароли, используемые для аутентификации данного пользователя.

Методы аутентификации с использованием OTP

- Метод «Запрос-ответ».
- Метод «Только ответ».
- Метод «Синхронизация по времени».
- Метод «Синхронизация по событию».
- Смешанные методы.

Механизм аутентификации при использовании метода «Только ответ»

Данные, хранящиеся на сервере:

- реализация алгоритма *f*, осуществляющего необратимое преобразование пароля;
- *i* – номер используемого пароля;
- P_{i-1} – последний использовавшийся пароль.

Данные, хранящиеся на OTP-токене:

- реализация алгоритма *f*;
- *i* – номер используемого пароля.

При использовании ассиметричной криптографии дополнительно необходимо хранить закрытый ключ пользователя (и на сервере и на OTP-токене).

Механизм аутентификации при использовании метода «Только ответ»

1. Пользователь вводит PIN-код к OTP-токену (*s*).
2. Вычисление и отображение пользователю значения P_i.
3. Ввод пользователем одноразового пароля (P_i).
4. Передача одноразового пароля (P_i) серверу.
5. Вычисление значения $P_{i-1} = f(P_i)$и сравнение с хранящимся значением (при совпадении – перезапись хранящегося P_i).
6. При совпадении значений предоставление доступа.

Сравнение методов аутентификации с использованием OTP

Кроме PIN-кода для генерации одноразового пароля могут использоваться (в качестве значения s):

- показания часов, встроенных в OTP-токен и синхронизированных с сервером (метод «Синхронизация по времени»);
- количество аутентификаций с использованием OTP-токена (метод «Синхронизация по событию»);
- значение сгенерированное сервером и переданное пользователю (метод «Запрос-ответ»).

Метод «Синхронизация по времени»

1. Активизация пользователем своего OTP-токена, который вычисляет и отображает ответ на запрос, являющийся показаниями часов (используются длинные интервалы времени, как правило, равные 30 секундам).
2. Ввод на рабочей станции имени пользователя и ответа, отображённого на токене; передача их по сети в открытом виде.
3. Шифрование сервером аутентификации для полученного имени пользователя показаний своих часов; в результате – получение сервером ответа.
4. Сравнение сервером полученного от пользователя ответа с ответом, полученным в результате собственных вычислений.

Метод «Синхронизация по событию»

- Активизация пользователем своего OTP-токена, который вычисляет и отображает ответ на запрос, основанный на количестве прохождения процедуры аутентификации данным пользователем (количество – хранится на токене).
- Ввод на рабочей станции имени пользователя и ответа, отображённого на токене; передача их по сети в открытом виде.
- Шифрование сервером аутентификации для полученного имени пользователя количества раз прохождения процедуры аутентификации; в результате – получение сервером ответа.
- Сравнение сервером полученного от пользователя ответа с ответом, полученным в результате собственных вычислений.

Метод «Запрос-ответ»

1. Ввод и передача имени пользователя по сети в открытом виде.
2. Генерация сервером аутентификации случайного запроса и его передача по сети в открытом виде.
3. Ввод запроса пользователем в свой OTP-токен.
4. Шифрование токеном запроса с помощью секретного ключа пользователя; в результате – отображение на экране токена ответа.
5. Ввод пользователем ответа на рабочей станции и передача этого ответа по сети в открытом виде.
6. Шифрование сервером аутентификации запроса с помощью секретного ключа пользователя; в результате – вычисление сервером ответа.
7. Сравнение сервером полученного от пользователя ответа с ответом, полученным в результате собственных вычислений; в случае совпадения – аутентификация считается успешной.

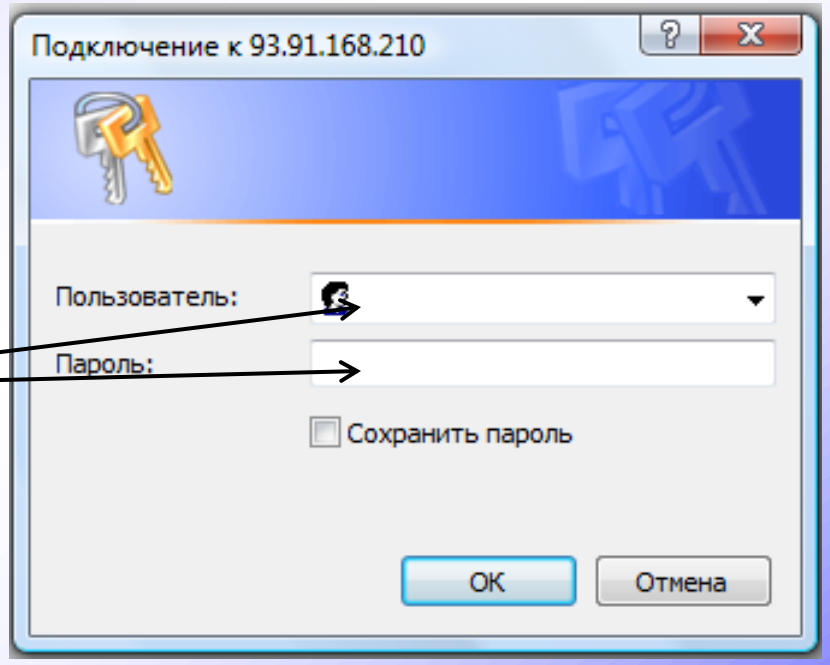
Аутентификация в программном обеспечении

- Шаблон окна приложения – набор правил и параметров для приложения; идентифицирует приложение, экранное окно и поля, в которые необходимо подставить данные.
- Профиль пользователя – сохранённая на физическом объекте информация, содержащая данные (логин, пароль и т.д.) пользователя для конкретного окна приложения; создаётся на основе шаблона окна приложения.

Шаблон окна приложения

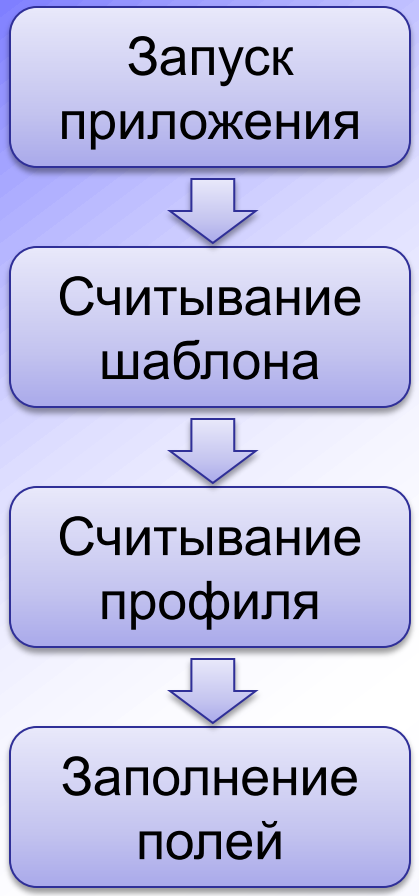
Шаблон окна приложения включает:

- название окна приложения;
- поля для ввода данных (сами данные в шаблоне не хранятся).



Администратор создаёт шаблон окна приложения и делает его доступным для пользователя.

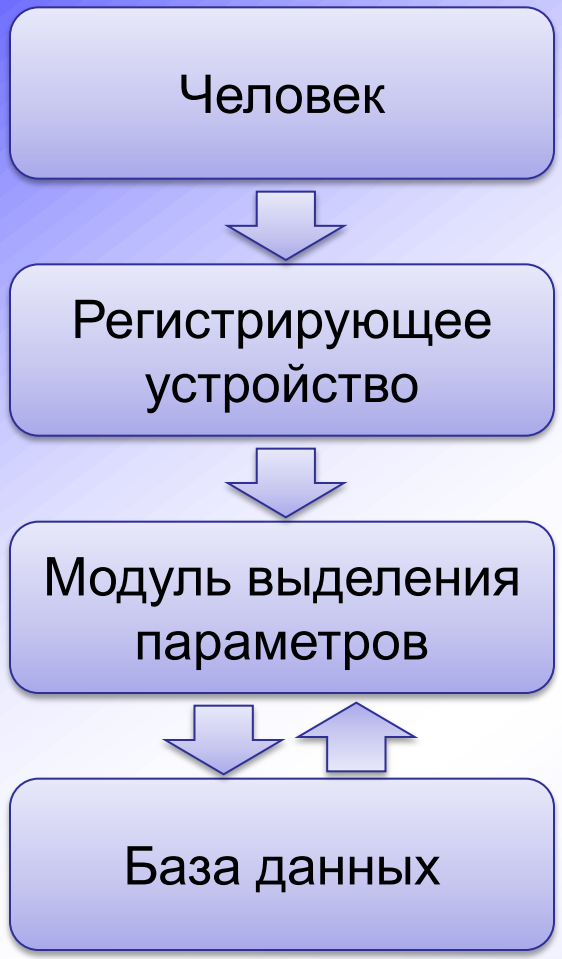
Схема аутентификации в программном обеспечении



- При запуске окна приложения проходит проверка наличия его шаблона; в случае наличия – из шаблона считываются необходимые поля.
- С физического объекта считывается профиль (данные пользователя для необходимых полей окна приложения) и заносится в соответствующие поля.

Биометрическая аутентификация

Структура биометрических систем



- Уникальная физиологическая характеристика человека.
- Стандартное (микрофон, веб-камера) или специфичное (сканер отпечатка пальца) регистрирующее устройство.
- Программный модуль выделения набора параметров, описывающих уникальную физиологическую характеристику человека, и сравнения их с пороговыми.
- База данных для хранения значений эталонных параметров.

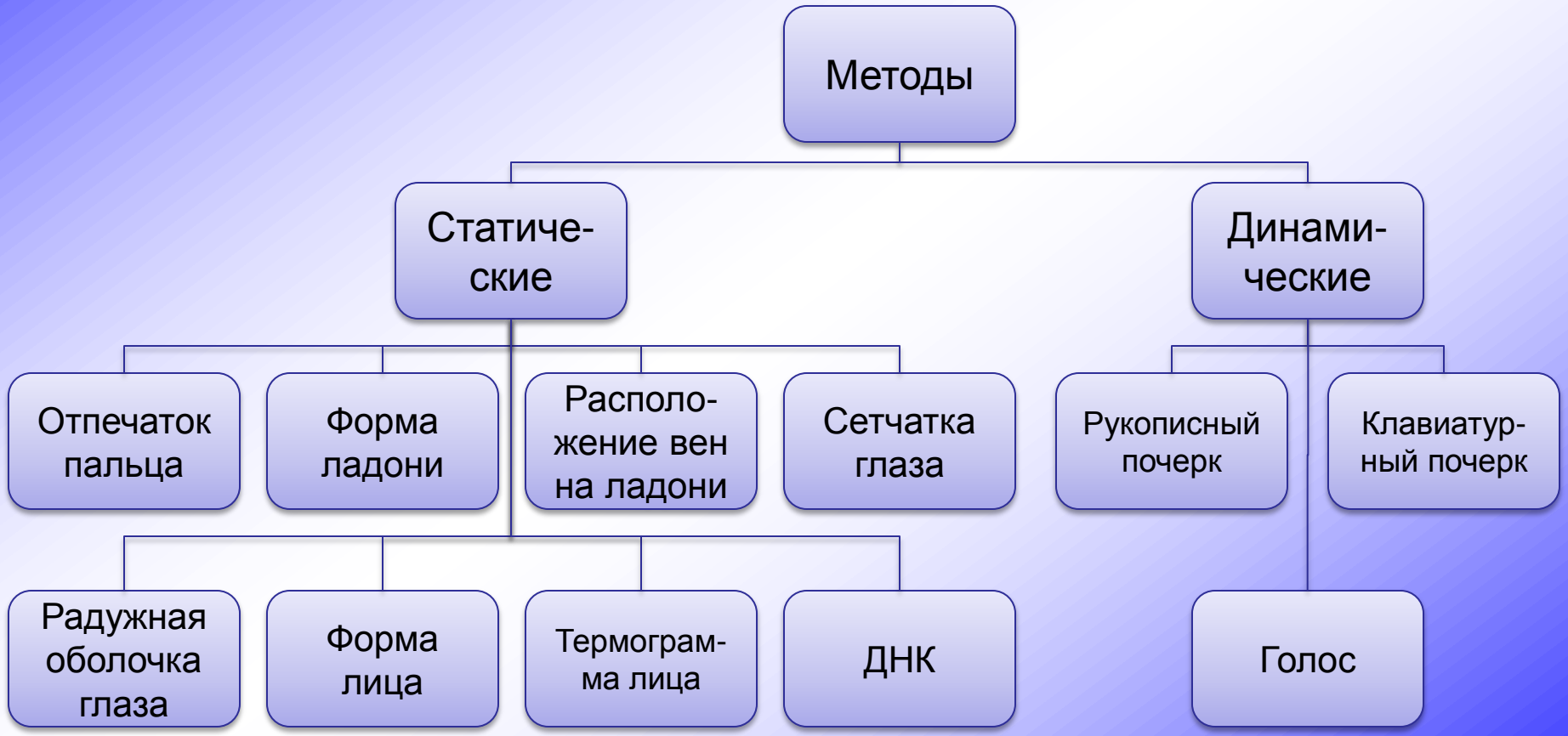
Схема создания эталонного шаблона

- Однократное или многократное снятие биометрической характеристики (в зависимости от метода).
- Вычисление значений (либо усреднённых значений) эталонных и пороговых значений параметров и запись их в базу в закрытом формате.
- Для характеристик, изменяющихся во времени, возможно автоматическое изменение эталонных и пороговых значений.

Схема аутентификации

- Пользователь предоставляет образец с помощью регистрирующего устройства (сканера, камеры и т.д.).
- Полученный биометрический образец обрабатывается для получения информации об отличительных признаках, в результате чего получается контрольный шаблон. Образец невозможно восстановить из шаблона.
- Контрольный шаблон сравнивается с эталонным, созданным на основе нескольких образцов, взятых при регистрации пользователя в системе.
- Контрольный и эталонный шаблон полностью не всегда совпадают, поэтому система учитывает степень совпадения, основываясь на настраиваемой пороговой величине.

Методы биометрической аутентификации



Типы методов биометрической аутентификации

- Статические методы основываются на физиологической (статической) характеристике человека, то есть уникальной характеристике, данной ему от рождения и неотъемлемой от него.
- Динамические методы основываются на поведенческой (динамической) характеристике человека, то есть построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия.

Статические методы биометрической аутентификации

- По отпечатку пальца (регистрирующее устройство – специальный сканер).
- По форме ладони. Трёхмерный образ формируется при помощи камеры и нескольких подсвечивающих диодов, которые, включаясь по очереди, дают разные проекции ладони.
- По расположению вен на лицевой стороне ладони. Регистрирующее устройство – инфракрасная камера для считывания рисунка расположения вен.
- По сетчатке глаза (по рисунку кровеносных сосудов глазного дна). Подсвеченное глазное дно сканируется специальной камерой.

Статические методы биометрической аутентификации

- По радужной оболочке глаза. Регистрирующее устройство – портативная камера.
- По форме лица. Строится несколько вариантов трехмерного образа лица (на случаи поворота лица, наклона, изменения выражения): выделяются контуры бровей, глаз, носа, губ и т.д., вычисляется расстояние между ними.
- По термограмме лица (распределение на лице артерий, снабжающих кровью кожу). Регистрирующее устройство – специальная инфракрасная камера.
- По ДНК. Недостаток – длительная обработка.

Динамические методы биометрической аутентификации

По рукописному почерку. Используется роспись человека (иногда написание кодового слова). Регистрирующее оборудование – графический планшет, экран карманного компьютера и т.д.

Формирование шаблона:

- по самой росписи, то есть для идентификации используется степень совпадения двух картинок;
- по росписи и динамическим характеристикам написания (информация по непосредственно подписи, временным характеристикам нанесения росписи и статистическим характеристикам динамики нажима на поверхность).

Динамические методы биометрической аутентификации

- По клавиатурному почерку. Регистрирующее устройство – клавиатура. Вместо росписи используется некое кодовое слово. Основная характеристика – динамика набора кодового слова.
- По голосу. Регистрирующее устройство – микрофон.

Градация методов по количеству ошибок второго рода

В порядке увеличения количества ошибок:

- ДНК;
- радужная оболочка глаза, сетчатка глаза;
- отпечаток пальца, термография лица, форма ладони;
- форма лица, расположение вен на кисти руки и ладони;
- подпись;
- клавиатурный почерк;
- голос.

Преимущества биометрической аутентификации

- Биометрический параметр уникален для данного человека.
- Биометрическая аутентификация обычно является одним из наиболее лёгких подходов для пользователей, которые должны проходить аутентификацию. Пользователю не нужно запоминать длинные пароли, поэтому исключается возможность их записи.
- Многие биометрические характеристики обычно неизменны в течение жизни человека и не могут быть изменены без существенного воздействия на человека.

Недостатки биометрической аутентификации

- Возможность изменения физиологической характеристики со временем (роспись, голос, клавиатурный почерк).
- Возможность изменения динамических характеристик при различном эмоциональном или физическом состоянии.
- Не все биометрические методы применимы (например, анализ крови) или правильно воспринимаются пользователем (отпечаток пальца).
- Не все методы теоретически гарантируют уникальность.

Компании – разработчики биометрических систем

- Biolink, Digital Persona, Смартлок – сканирование отпечатков пальцев.
- Sonda Technologies – сканирование отпечатков пальцев и ладоней.
- Asia software – по изображению лица (WIN-FACELOGON и др.).
- Центр речевых технологий – по голосу (Трал-М).
- Recognition Systems – по геометрии ладони.

Рассмотренные вопросы

- Физические объекты, используемые для аутентификации в ОС.
- Методы аутентификации с применением одноразовых паролей при использовании физических объектов.
- Метод аутентификации в программном обеспечении.
- Аутентификация с использованием биометрических данных.

Всем спасибо – все свободны,

если нет вопросов