Методы и средства идентификации и аутентификации пользователей автоматизированной системы (тема 33)

Идентификация (в информационных системах) — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе. Для выполнения процедуры идентификации в информационной системе субъекту предварительно должен быть назначен соответствующий идентификатор (то есть проведена регистрация субъекта в информационной системе).

Аутентификация — процедура проверки подлинности, например:

- проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов;
- подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
- проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Выделяют три основных метода аутентификации объектов, описанных Миллером . Они развивались по мере совершенствования технологий печати, фотографии и автоматизации; эти методы использовались задолго до того, как потребовалась автоматическая электронная аутентификация (рисунок 1).

К – по знаниям. Аутентификация здесь основана на секретных знаниях, таких, как пароль, шифр замка и ответы на вопросы. К данным методам можно отнести парольную аутентификацию и аутентификацию на основе модели «рукопожатия».

Р – по собственности. Любой человек, имеющий определенный предмет, например ключ или с магнитной полосой карту, может получить доступ к приложению (то есть быть авторизован).

В — по биометрическому параметру. Это характерная особенность человека, которая может быть как-то измерена (или с нее может быть получен образец) в форме биометрического идентификатора и которая отличает человека от всех других людей.

Рисунок 1 — методы аутентификации

Кроме того, иногда выделяют комбинированные методы, например, при взаимодействии с банкоматом, идентификация происходит на основе банковской карты (тип Р), а аутентификация уже за счет ПИН-кода (тип К).

Таблица 1 позволяет сравнить четыре наиболее популярных метода идентификации и аутентификации.

Метод	**Примеры**	**Свойства**
На основе собственности (Р)	Электронные карты, бейджи, ключи	Можно сделать дубликат (иногда) или украсть, может быть утерян
На основе знания (К)	Пароль, ПИН, секретная фраза	Может быть скомпромитирован, забыт
На основе собственности и знания (Р, К)	Кредитная карта + ПИН	Для использования уязвимости нужно завладеть и собственностью и

		знанием
Биометрия (В)	Отпечатки пальцев, геометрия лица, походка	Невозможно украсть, сложно подделать, почти невозможно потерять

К достоинствам метода аутентификации на основе физических носителей с ключевой информацией – их высокая надежность, недостаток – дороговизна и необходимость дополнительных устройств считывания, а также возможность их потери.

Биометрические признаки обладают некоторыми свойствами, которые определяют их выбор в тех или иных условиях. К этим свойствам относятся следующие:

1) Универсальность;

2) Уникальность (индивидуальность);

3) Постоянство (стабильность);

4) Собираемость.

Свойство универсальности означает, что используемым биометрическим параметром обладает любой человек. Свойство уникальности означает, что данный биометрический параметр не повторяется для двух людей. Свойство постоянства означает, что биометрический параметр не изменяется со временем. Собираемость – это такое свойство биометрического параметра, которое позволяет относительно легко и быстро его измерить.

Как видно из диаграммы на рисунке 2, не существует такого биометрического признака, который имеет высшие оценки по всем параметрам.

Выбор конкретного биометрического признака для приложения определяется не столько этими оценками, сколько условиями применения систем идентификации – их назначением, степенью ответственности при

принятии решений, степенью защиты от несанкционированного доступа к системе, степенью защиты от взлома системы.

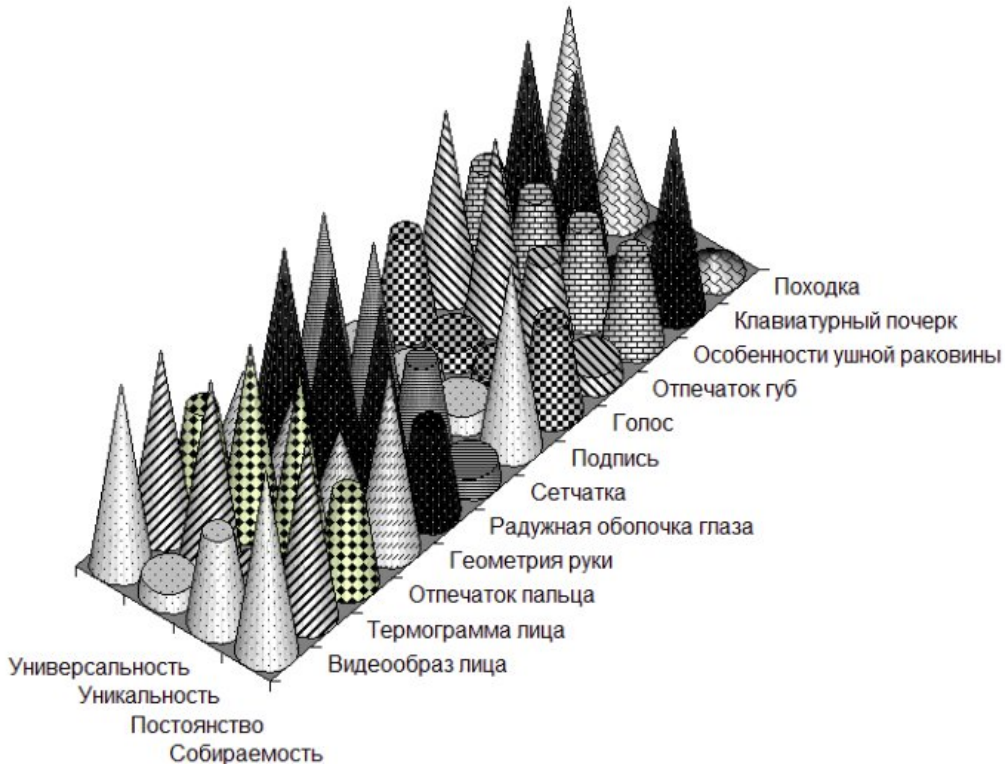

Рисунок 2 — оценка качественных свойств биометрических параметров

При использовании аутентификационных методов Р и К происходит сравнение информации, при этом пользователь (реальный человек) не связывается с более или менее установленной «личностью». Но личность, определяемая по владению собственностью Р, связывается с анонимным паролем К, а не с реально зарегистрированным человеком.

Аутентификационный биометрический метод В обеспечивает дополнительную защиту благодаря невозможности замены биометрических параметров, поэтому этот метод, а именно установление подлинности пользователей, является более надежным и заслуживает доверия.

Однако на практике биометрические методы аутентификации не получили широкого распространения вследствие определенных причин. Для защиты в настоящее время применяются программные и программно-аппаратные средства, использующие в своей работе процедуры аутентификации пользователей. К программно-аппаратным СЗИ от НСД можно отнести системы: - Аккорд-В, Соболь, АПМДЗ «КРИПТОН-ЗАМОК»,

Diamond ACS. К программным средствам защиты можно отнести Страж NT, Secret Net, Dallas Lock. Продукты имеют лицензии ФСТЭК, ФСБ, СВР и Министерства Обороны РФ. Сертифицирован ФСТЭК и ФСБ РФ, соответствует требованиям РД ФСТЭК РФ по уровню защиты гостайны.