УДК 004.932.2 **Технические науки**

Митрошина Е.В. *студентка 4 курса электротехнического факультета,*
Пермский национальный исследовательский политехнический университет

ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В статье рассматриваются основные методы аутентификации с использованием биометрических данных человека.

Ключевые слова: идентификация, аутентификация, биометрические данные.

Abstract. This article describes the main methods of authentication with using of biometric human data.

Keywords: identification, authentication, biometric data.

Кражи идентификационных данных вызывают обеспокоенность в современном обществе. В настоящее время такие методы аутентификации, как пароли и различные электронные ключи, которые можно украсть, потерять или забыть, уже не достаточны для обеспечения безопасности. Соответственно использование биометрических данных человека, становится одним из самых перспективных направлений в системах контроля доступа. Биометрические данные – это биологические и физиологические особенности человека, на основании которых можно установить его личность.

Все методы биометрической аутентификации делятся на два класса. Первый – это статистические методы, которые основываются только на физиологические характеристики человека. Физиологические характеристики имеются абсолютно в каждом, они присутствуют всю жизнь и их нельзя украсть или потерять. Второй класс – динамические методы, основанные на поведенческих особенностях людей, таких как повторение или воспроизведение какого-нибудь конкретного обыденного действия.

Статистические методы:

1. Аутентификация по отпечатку пальца.

Данный способ аутентификации является самым распространенной биометрической технологией для обеспечения безопасного доступа к компьютеру или сети. Аутентификация предполагает сканирование отпечатков пальцев. Отпечатки пальцев каждого человека уникальны по своему рисунку и не совпадают даже у одного человека на разных пальцах, а так же они не меняются на протяжении всей жизни, что немаловажно. После сканирования полученные данные преобразуются в цифровой код по средствам программных драйверов, затем цифровой код сравнивается с наборами эталонов, введенных ранее, с помощью соответствующих программ. Сканеры отпечатков пальцев сегодня можно установить практически везде, в клавиатуры, мышки, ноутбуки, смартфоны, USB флеш-накопители, замки, что обеспечивает удобство в использовании и простоту данного способа аутентификации.

2. Аутентификация по сетчатке глаза.

В 50-е годы прошлого века установили уникальность рисунка кровеносных сосудов глазного дна, в связи с этим и получил развитие данный метод аутентификации. Для сканирования сетчатки глаза применяют инфракрасное излучение. Они получили широкое распространение в системах контроля доступа, так как у них мала вероятность отказа в доступе зарегистрированных пользователей и практически не бывает ошибок при разрешении доступа. Однако сканеры сетчатки не получили массового распространения из-за дороговизны и сложности оптической системы сканирования, а также из-за дискомфорта у человека, чьи данные идентифицируют. К тому же исследователи обнаружили, что сетчатка глаза имеет свойство меняться в разные периоды жизни, что не обеспечивает надежности на протяжении долгого времени.

3. Аутентификация по радужной оболочке глаза.

В этой технологии биометрической аутентификации используется уникальность признаков и особенностей радужной оболочки человеческого глаза. Технология заключается в процессе получения радужной оболочки специальной камерой (сканирующим оборудованием). Считается, что эта технология произошла еще он не менее известной технологии, такой как аутентификации по сетчатке глаза. Однако аутентификация по радужной оболочке глаза имеет ряд преимуществ,

одно из которых то, что радужная оболочка глаза остается неизменной, в то время как сетчатка глаза человека может меняться со временем. Также доказано, что невозможно найти два абсолютно одинаковых рисунка радужной оболочки глаза, даже у близнецов, что позволяет использовать эту технологию в качестве защиты данных. Рисунок радужной оболочки очень сложен, поэтому удается отобрать порядка 200 точек, которые в свою очередь обеспечивают высокую степень надежности аутентификации, в то время как при распознавании по отпечатку пальца используют около 60-70 точек [1]. Несмотря на все достоинства данной аутентификация, она имеет один значительный недостаток – это стоимость внедрения данной технологии.

Динамические методы:

1. Аутентификация по голосу.

Этот метод биометрической технологии очень простой в применении, поскольку для его реализации не требуется дорогостоящая аппаратура, а необходим только микрофон и звуковая плата. Существуют различные способы построения шаблонов по голосу. Например, комбинации частотных и статистических характеристик голоса, интонация, высота тона и множество других способов. Несмотря на низкую стоимость, данная технология значительно проигрывает технологиям, рассмотренным ранее. Основным недостатком аутентификации по голосу является низкая точность в достоверном определении личности. Так как система может не опознать человека, с осипшим из-за простуды голосом или наоборот принять злоумышленника за достоверное лицо, ведь голос имеет свойство изменяться под воздействие различных факторов (возраста, состояния здоровья).

2. Аутентификация по рукописному почерку.

Для аутентификации этим способом необходима подпись человека. Для того чтобы сохранить подпись используются специальные ручки или поверхности, восприимчивые к давлению. Шаблон создается в зависимости от того, какой уровень защиты необходим. Существует несколько способов обработки подписи: либо анализируется сам фрагмент, при установлении степени совпадения двух картинок, либо – динамические характеристики написания, для этого сверяют его временные и статистические параметры [2].

В заключение хочется сказать, что биометрические данные являются очень удобным для людей способом аутентификации, так как их невозможно забыть или потерять. Также обеспечивается достаточно высокая степень защиты данных, так как подделать их очень трудно.

Библиографический список

1. Болл Р., Коннел Дж. Руководство по биометрии. - М.: Техносфера, 2007. – 368 с.

2. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. - Пенза: Изд-во Пенз. гос. ун-та, 2000. - 188 с.

3. Журнал "Information Security/ Информационная безопасность" #6, 2009 [Электронный ресурс]. URL: http://www.itsec.ru/articles2/allpubliks (дата обращения 16.08.2016).