

Солошенко А. Е., Витовтова О. В.,
Жилинкова Л. А.

**ОБЗОР СТАТИЧЕСКИХ МЕТОДОВ
БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ**

В XXI веке, времени всеобъемлющей информатизации общества, сложно удивить людей чем-либо новым. Все давно уже привыкли, что компьютеры, планшеты, сотовые телефоны, разнообразные гаджеты находятся с нами постоянно, практически каждую минуту нашей жизни. Собираемся ли мы на работу, отдыхаем, оплачиваем услуги, работаем, всегда нашими помощниками выступают разнообразные компьютерные технологии. Они стали такими привычными, что мало кто задумывается о том, а как же это все устроено? Что обеспечивает работу всех этих, так необходимых, нам вещей?

Возьмем, к примеру, операции с электронными деньгами, которые в настоящее время, практически на равных с материальными используются для оплаты услуг и покупки товаров.

При использовании электронных денег, одним из самых важных вопросов, является надежность и безопасность переводов. В данном случае эта проблема решается использованием криптографии.

Данный термин знаком не всем, а ведь в недалеком будущем с корректным использованием криптографической защиты будут сталкиваться абсолютно все, начиная с опытных пользователей ПК, специалистов различных областей и заканчивая, обычными домохозяйками и школьниками. И если первые две категории граждан, которые постоянно сталкиваются с компьютерными тех-

нологиями, уже выработали культуру обращения с совокупностью различных криптографических ключей, но и они зачастую сталкиваются с проблемами их сохранности, то оставшиеся постоянно будут ощущать дискомфорт от такого обилия криптографической информации, которую необходимо помнить и хранить в надежном месте. Именно эти проблемы можно решить с помощью использования биометрических технологий обеспечения безопасного получения, распространения и хранения ключей.

Как же это работает? Для каждого человека создается личный криптографический процессор, который представляет собой программу, по типу текстового процессора, и способен корректно выполнять различные криптографические операции. Его задача — надежно хранить криптографические ключи человека, самостоятельно узнавать своего пользователя и подчиняться только ему. Взлом биометрических фрагментов личного криптографического процессора пользователя по своей сложности должен быть сопоставим со взломом его криптографической части. В таком случае, криптографические процессоры можно открыто хранить и пересылать.

А ведь электронные деньги, это не единственная возможность применения биометрической идентификации. В связи с бурным развитием Internet-технологий виртуальными стали не только деньги, но и личность человека. Примером могут служить конференции при помощи Skype, когда люди, находящиеся за тысячами километров друг от друга, могут обсуждать различные проблемы. Более того, современные системы автоматизированного управления предприятиями, позволяют руководить всеми процессами множества филиалов, расположенных по всему миру, находясь у себя дома. И здесь вопрос конфиденциальности и идентификации личности играет главную роль.

Первым появился метод идентификации личности по рисунку кровеносных сосудов глазного дна. Этот метод является одним из наиболее надежных, поскольку еще в 1935 году Саймон и Голдштейн доказали уникальность дерева кровеносных сосудов глазного дна каждого человека. Даже у близнецов рисунок будет отличаться (рис. 1).

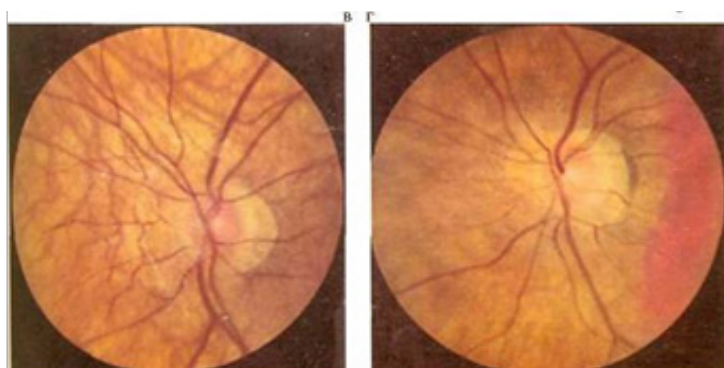


Рисунок 1. Дерево кровеносных сосудов глазного дна близнецов

Идентификация личности по этому признаку осуществляется следующим образом. Человек смотрит через специальный окуляр на удаленную световую точку, при этом его глазное дно подсвечивается инфракрасным светом. Вследствие этого, на нем выделяется дерево кровеносных сосудов. Затем оно сравнивается с эталоном. Конечно, этот метод не лишен недостатков. Они связаны с человеческим фактором, к примеру, отклонением головы от эталонного или неверная фокусировка на удаленном источнике света. Еще одним недостатком является стоимость устройств, они являются самыми дорогими, около 4000 долларов США.

Следующим уникальным свойством личности является радужная оболочка глаза. Она обусловлена генотипом человека и у каждого индивидуальна (рис. 2).



Рисунок 2. Радужная оболочка глаза различных людей

Системы этого класса захватывают изображение на расстоянии 20–30 см от видеокамеры и осуществляют автоматическое выделение зрачка и радужной оболочки. Стоимость таких систем составляет от 500 до 6500 долларов США. Недостатком, опять же, является стоимость, которая обусловлена использованием видеокамер высокого разрешения.

Еще одним классом систем идентификации являются системы, распознающие силуэт кисти рук. Для реализации распознавания личности, используют видеокамеру и инфракрасную подсветку руки под разными углами. Трехмерную модель обеспечивают несколькими подсвечивающими светодиодами. Недостатком таких систем являются их размеры. Стоимость сопоставима с предыдущим классом систем.

Отпечатки пальцев, которые широко используются в полицейской практике, также образуют класс систем идентификации личности. Он является одним из старейших методов. Такие системы называются дактилоскопическими. Они, используя телевизионную камеру, снимают папиллярный узор с пальца и сравнивают с эталоном. Недостатком такого метода является достаточно большой процент ошибок. Стоимость систем этого класса относительно низкая — от 150 до 500 долларов США.

Другим методом биометрической идентификации является отслеживание индивидуальных особенностей геометрии лица. Видеокамера снимает пользователя, находящегося перед ней, далее программа сравнивает полученное изображение с эталоном. Наибольшие трудности, возникающие при разработке этих систем, возникают вследствие внешних помех и человеческого фактора (например, недостаточная освещенность, отличный поворот головы от эталонного и т.д.). Стоимость всей системы, включающую в себя видеокамеру и программное обеспечение, составляет от 70 до 500 долларов США.

Усовершенствованным методом предыдущего варианта является идентификация с помощью термографического наблюдения лицевых артерий и вен. Для такой системы используется инфракрасный диапазон. Это помогает устранить проблему освещенности, которая присутствовала в методе, описанном выше, поскольку устройство фиксирует температуру лица, и не зависит от уровня освещенности. Недостатком таких систем является их высокая стоимость 55000 долларов. Она обусловлена применением видеокамеры дальнего инфракрасного диапазона.

Достаточно, малочисленной группой систем биометрической идентификации являются устройства, распознающие расположение вен на руках. Видеокамерой снимается тыльная сторона руки,

сжатая в кулак в инфракрасном диапазоне, а затем производится его оцифровывание.

Все эти методы являются статическими, то есть основанными на неизменяющихся образах личности. Вышеперечисленные методы используются давно и заняли устойчивое положение на рынке устройств статической биометрии. Сложно представить, что же еще можно изобрести в этой области, однако уже активно развивается методы распознавания генетического кода личности. И хотя сейчас они применяются только в единичных случаях, с развитием технологий стоимость и время обработки генетического материала снижается, что позволяет рассматривать этот метод, как достаточно перспективный для широкого использования.

Список литературы:

1. Волчихин В.И., Иванов А.И. Механизм биометрической адресации виртуального денежного обращения в открытом информационном пространстве // Специальная техника средств связи. Серия: Системы, сети и технические средства конфиденциальной связи. — Пенза, ПНИИИ, 1999. — Вып. № 2.
2. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Кн. 15: Монография. — М.: Радиотехника, 2004. — 144 с.
3. Филипп К. Ваше лицо — гарант безопасности // PCWEEK RUSSIAN EDITION. — 1997. — 3 ИЮНЯ. — С. 35–38.