

Использование биометрических технологий при организации защиты информации

Use of biometric technologies in organizing information protection

УДК 004.056

Получено: 19.10.2023

Одобрено: 12.11.2023

Опубликовано: 25.12.2023

Шабанова Н.Ю.

Канд. экон. наук, доцент кафедры «Вычислительная техника и информационные технологии»
ФГБОУ ВО РХТУ им. Д.И. Менделеева Новомосковский институт (филиал)
e-mail: shabanova.n.i@muctr.ru

Shabanova N.Y.

Candidate of Economic Sciences, Associate Professor, Department of Computer Engineering and
Information Technology, Federal State Budgetary Educational Establishment of Higher Technical
Education named after DI. Mendeleev Novomoskovsk Institute (branch)
e-mail: shabanova.n.i@muctr.ru

Ефремова О.А.

Старший преподаватель кафедры «Вычислительная техника и информационные технологии»
ФГБОУ ВО РХТУ им. Д.И. Менделеева Новомосковский институт (филиал)
e-mail: efremova.o.a@muctr.ru

Efremova O.A.

Senior Lecturer, Department of Computer Engineering and Information Technology, Federal State
Budgetary Educational Establishment of Higher Technical Education named after DI. Mendeleev
Novomoskovsk Institute (branch)
e-mail: efremova.o.a@muctr.ru

Аннотация

Биометрическая технология - наиболее заметное из последних достижений в области методов идентификации и контроля доступа к информации. Приведены некоторые результаты аналитического исследования современного состояния и перспектив развития российского рынка биометрических средств защиты информации.

Ключевые слова: защита информации, биометрия, биометрическая технология, идентификация, аутентификация.

Abstract

Biometric technology is the most noticeable of the latest achievements in the field of methods of identification and access control to information. Some results of an analytical study of the current state and development prospects of the Russian market of biometric information security tools are presented.

Keywords: information protection, biometrics, biometric technology, identification, authentication.

Проанализировав текущее состояние отечественного рынка технических средств обеспечения информационной безопасности, можно сделать вывод, что на сегодняшний день индустрия обеспечения безопасности информации выходит на новый этап развития. Отмечается, что самый быстрый рост показывает класс систем идентификации и аутентификации личности, применяемые при организации защиты информации.

Особое место среди подобных систем занимают биометрические средства защиты информации (БСЗИ) [1].

Сегодня биометрия представляет собой одно из перспективных направлений в идентификации человеческой личности (пользователя) и впоследствии предоставления ему доступа к защищенной информации. Использование биометрии в наше время все более распространено, она снижает свою стоимость при сохранении высокой точности распознавания.

На сегодняшний момент рынок предоставляет большой выбор систем для контроля доступа к информации, поэтому выбор одного из методов контроля или их сочетаний становится отдельной проблемой.

Доступ в систему с помощью биометрической информации является наиболее надежным по сравнению с системами, где используются ключи, карты и т.д. К сожалению, высокая надежность обуславливает и высокую стоимость данных систем при максимальной безопасности [2].

Ранее данные системы применялись в основном в учреждениях государственного характера и в случаях, когда требовалось обеспечить особые условия безопасности. В современных реалиях растет популярность использования систем контроля на основе биометрических данных (шаблонов) в банках, информационных фирмах и телекоммуникационных фирмах.

Существуют требования к защите биометрических данных (шаблонов), среди которых можно отметить основные:

- необратимость – означает невозможность восстановления преступниками биометрических характеристик пользователя, а также изготовления физической подделки;
- различимость – точность аутентификации личности пользователя не зависит от способа защиты шаблона;
- отменяемость – при использовании одних биометрических данных и используя всего один шаблон, возможно создание нескольких защищенных шаблонов.

Схема защиты шаблонов в биометрии основана на следующих принципах, а именно, применение биометрических криптосистем, а также трансформации биометрических параметров пользователя [3].

Биометрические криптосистемы представляют собой системы, обеспечивающие хранение криптографических ключей в конечном виде, т.е. в виде, пригодном для последующего извлечения. Также в системах используется тот факт, что пользователь обладает именно тем биометрическим параметром, который впоследствии будет применяться при его регистрации в системе. Особенность и отличие биометрических криптосистем в том, в них хранятся только те данные, которые получаются от биометрического шаблона.

При трансформации биометрических параметров пользователя используется так называемая необратимая функция трансформации, основанная на индивидуальных характеристиках пользователя. При аутентификации система использует эту же необратимую функцию к запросу, и сопоставление происходит по созданному шаблону для трансформированного образа.

Организация безопасности с применением БСЗИ обуславливается тем, что исходные биометрические данные, на основе которых построена система, не могут быть утеряны пользователем, украдены или скопированы. Из-за своего принципа работы системы с защитой на основе биометрии обладают низкой скоростью и малой пропускной способностью, но являются единственно верным решением, когда требуется обеспечить контроль на важных объектах с малым персоналом.

Классификация биометрических средств идентификации основана на различных принципах:

1) по признаку действия средства защиты бывают:

- статистические;
- динамические;
- комбинированные.

2) по биопризнаку:

- форма кисти руки;
- папиллярные линии пальца;
- термограмма лица;
- сетчатка глаза;
- радужная оболочка глаза;
- голос;
- почерк;
- клавиатурный почерк;
- биопризнаки.

3) в зависимости от применяемой технологии:

- оптоэлектронные;
- полупроводниковые;
- ультразвуковые;
- пироэлектрические;
- электрооптические;
- комбинированные (ПЗС + оптика);
- телевизионные;
- тепловизионные [4].

На данный момент наиболее распространенными системами биометрического контроля являются системы, основанные на данных отпечатка пальца конкретного человека. Они основаны на считывании трехмерного отпечатка, записывающегося в виде изображения. Оцифрованное изображение система сохраняет в памяти, а впоследствии использует его для определения личности человека, пытающегося авторизоваться как пользователь.

Ключевой особенностью данных систем является то, что реальных отпечатков в памяти нет, их хранение длится не более 30 секунд, а время идентификации составляет от 0,5 до 2 с. Иногда существует возможность аутентификации по нескольким отпечаткам пальцев.

К достоинствам систем, основанных на данных отпечатка пальца, относят низкий процент ошибок, невысокую стоимость оборудования и простоту проведения процедуры. А к недостаткам уязвимость подделки отпечатка пальца и возможные проблемы при распознавании сухой и поврежденной кожи.

Системы биометрического контроля основываются на узоре сетчатки глаза как характеристики идентификации. Рисунок кровеносных сосудов глазного дна не повторяется даже у близнецов, поэтому данный вид аутентификации максимально защищен. Глазное яблоко человека сканируется с помощью оптической системы и определяется распределение кровеносных сосудов. Для сканирования используется низкоинтенсивное инфракрасное излучение, а современные приборы используют лазеры мягкого действия. Информация в данном случае хранится и используется для контроля. Вероятность сбоя данного метода крайне мала, около одного раза на миллион считываний. Время определения пользователя не более 1 мин. [5].

Также существует способ идентификации пользователя с небольшого расстояния по отражающим и поглощающим характеристикам сетчатки. Высокая надежность этого метода и невозможность его фальсификации компенсируется рядом недостатков: длительное время определения, стоимость, габариты устройства и неприятная процедура идентификации.

Использование данного метода может быть затруднено при наличии у человека некоторых серьезных заболеваний глаза.

Данные недостатки отсутствуют у устройств, использующих ладонь человека как идентификационную функцию. Личность в этом случае определяется по ладонной фотографии, сравниваемой с эталоном.

Для аутентификации удаленных пользователей одним из наиболее перспективных методов является метод распознавания клавиатурного почерка. Он основан на таких характеристиках каждого пользователя как: скорость ввода, количество ошибок, время удержания клавиш и интервал между нажатием, а также использование функциональных кнопок.

Распознавание голоса один из самых доступных методов определения личности. Для аутентификации достаточно использовать микрофон и записывающее устройство, а пользователю достаточно произнести одно слово, что упрощает процедуру. Огромное его преимущество – возможность скрытой аутентификации. Человек может и не догадываться о проведении проверки [2].

Специалисты сделали анализ русского рынка БСЗИ и выяснили, что на нем можно найти большой выбор идентифицирующих устройств, основанных на считывании различных биометрических характеристик. Данные устройства различаются друг от друга скоростью передачи информации, надежностью, а также стоимостью.

Во многих странах ведется активная работа по созданию новых биометрических систем защиты информации, а также поиску новых биометрических технологий. Планируется разработать технические средства идентификации, основываясь на индивидуальных особенностях человека:

- ДНК-код;
- запах;
- походка;
- характеристики кардиограммы.

Эти методы еще в разработке, так как требуют много времени и труда, а также имеют ряд некоторых недостатков, такие как нестабильность результатов и низкая надежность [5].

Технологии не стоят на месте, а биометрическая технология развивается все больше и больше и, следовательно, проблема оптимального выбора становится очень актуальной и сложной для пользователей. Из-за многообразия биометрических методов аутентификации на рынке становится проблематично выбрать метод, который будет наиболее эффективен. Поэтому проблема выбора системы для той или иной организации весьма актуальна.

В данное время на рынок представляется все больше и больше различных систем защиты информации с применением биометрии, что положительно сказывается на усовершенствовании их технических, эксплуатационных характеристиках, а также стоимости.

Литература

1. Анализ механизмов защиты информации с использованием биометрических данных [электронный ресурс] URL: <https://www.elibrary.ru/item.asp?id=42838168&>.
2. Биометрическая идентификация по рисунку лица в вопросах и ответах [Электронный ресурс] // Security News : URL: <http://www.secnews.ru/articles/2323.htm>
3. Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации [электронный ресурс] URL: <https://securityrussia.com/blog/biometriya.html>
4. Обзор международного рынка биометрических технологий и их применение в финансовом секторе [электронный ресурс] URL: https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf
5. Ворона В.А. Биометрическая идентификация личности – М.: Горячая линия – Телеком, 2022. – 228 с.
6. Антти Суомалайнен: Биометрическая защита. Обзор технологии – М.: ДМК-Пресс, 2019. – 104 с.