Пронин М.О., Бобрышева Г.В. Безопасность биометрических систем. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XIX Междунар. научно-техн. конф. – Пенза: ПДЗ, 2019. – С. 108-113.

УДК 004.056.5

БЕЗОПАСНОСТЬ БИОМЕТРИЧЕСКИХ СИСТЕМ

М.О. Пронин, Г.В. Бобрышева

SECURITY OF BIOMETRIC SYSTEMS

M.O. Pronin, G.V. Bobrysheva

Аннотация. Биометрические системы контроля и управления доступом считаются наиболее надежными, т.к. биоматериал конкретного человека не может быть утерян, забыт или передан третьим лица. Наиболее популярными являются биометрические системы на основе отпечатков пальцев, безопасность которых во многом определяется надежностью оборудования.

Ключевые слова: биометрические признаки, идентификация человека, биометрические системы контроля доступа.

Abstract. Biometric access control systems are considered to be the most reliable, because the biomaterial of a particular person can not be lost, forgotten or transferred to a third party. The most popular are biometric systems based on fingerprints, the security of which is largely determined by the reliability of the equipment.

Keywords: biometric features, human identification, biometric access control systems.

В настоящее время наблюдается непрерывное развитие систем контроля и управления доступом (СКУД) на основе биометрических параметров. Биометрическая идентификация позволяет путем измерения, распознавания и сравнения с имеющейся базой эталонных характеристик с высокой точностью определить личность конкретного человека (пользователя) [1].

Наиболее часто на практике используют биометрические системы, осуществляющие идентификацию пользователя по отпечатку пальца, ладони, лица или радужной оболочки глаз. В частности, такие системы нашли применение в следующих областях:

криминология;

таможенное оформление и паспортный контроль;

борьба с терроризмом и мониторинг толпы;

организация защиты данных в портативных устройствах;

электронный банкинг;

онлайн-платежи и др.

Общая структура системы биометрической идентификации показана на рис. 1.

Рис. 1. Структура системы биометрической идентификации

Основным компонентом системы биометрической идентификации является модуль, отвечающий за сканирование и распознавание биометрических данных, который сопрягается с блоком принятия решений, сравнивающим полученный биоматериал с эталонными характеристиками. Предоставляет или запрещает доступ к определенной области данных исполнительный блок, основываясь на сигнале, поступающем из блока идентификации.

Наиболее известным и популярным является метод биометрической идентификации по отпечаткам пальцев, основанный на сканировании папиллярных узоров на коже, которые являются уникальными для каждого человека [2].

Существует три основных типа папиллярных линий:

- дуговой: папиллярные линии имеют форму простых дуг (имеют всего 5-10% населения);

- петлевой: папиллярные линии имеют форму петли (имеют 65% населения);

- завитковый: папиллярные линии в форме круга, овала, спирали с сердечником (завитковые папилляры имеют 25% населения).

Для осуществления точной идентификации личности разделения на основные типы папиллярных узоров недостаточно. При проведении сравнительного анализа узоры, одинаковые по типу и виду, исследуются на наличие особенностей и частных признаков папиллярного узора.

Безопасность таких биометрических систем, прежде всего, определяется надежностью датчиков, используемых для снятия отпечатков пальцев.

В настоящее время для снятия отпечатков пальцев в биометрических системах используются дактилоскопические сканеры, построенные с использованием оптического датчика, емкостного датчика, теплового считывателя или ультразвукового датчика.

Принцип работы оптических датчиков папиллярного узора основан на отражении и пропускании света. При попадании света фотодиоды создают электрический заряд, образуя снимок отпечатка пальца, и в зависимости от интенсивности света получают пиксели разной интенсивности. На полученном отпечатке определяется вид папиллярного узора и выделяются конкретные его особенности.

Емкостные датчики в настоящее время являются наиболее распространенными полупроводниковыми устройствами для получения изображения отпечатка пальца. Принцип работы данного датчика основан на измерении емкости p-n-перехода полупроводника при соприкосновении его с папиллярным узором пальца.

Тепловые считыватели (термосканеры) построены на пироэлектрических элементах, которые позволяют измерять разницы температур и преобразовывать полученные показатели в напряжение.

Ультразвуковые датчики (ультразвуковые сканеры) позволяют сканировать папиллярный узор ультразвуковыми волнами. Расстояния между источником волн и узором (выступами и впадинами) измеряются по отраженному от них эху.

Для проверки надежности датчиков отпечатков пальцев используются два основных параметра: коэффициент ложного принятия (FAR) и коэффициент ложного отклонения (FRR) [3].

FAR – это частота, с которой неавторизованное лицо принимается в качестве авторизованного. Данная величина является статическим значением, точность которого зависит от количества измерений. Вероятность успеха в отношении определенного зарегистрированного человека измеряется как

$$FAR = \frac{\text{кол} - \text{во успешных попыток несанкционированного доступа}}{\text{кол} - \text{во всех попыток}}.$$

Попытка мошенничества будет успешной, если пользовательский интерфейс приложения выдает “успешное” сообщение или если же желаемый доступ предоставлен.

FRR – это частота, с которой авторизованному лицу отказано в доступе. Значение FAR для N участников определяется как:

$$FAR = \frac{1}{N}\sum_{n=1}^{N} FAR(n). \quad (1)$$

Параметр FRR часто считается критерием комфорта пользования той или иной СКУД, т.к. ложное отклонение доступа, как правило, раздражает. Значения параметра FRR зависят как от самой системы, так и от пользователя, а его точность – от количества измерений. Существует также понятие “личная FAR” – это параметр, зависящий от качества изображения, на которое могут повлиять, например, грязные пальцы.

Значение параметра FRR для конкретного человека может быть определено по формуле

$$FRR = \frac{\text{отклон. попытки идентификации для авторизованного лица}}{\text{кол} - \text{во всех попыток}}.$$

Общий FRR для N участников определяется как

$$FRR = \frac{1}{N}\sum_{n=1}^{N} FRR(n). \quad (2)$$

Также существуют вторичные параметры, помогающие определить надежность датчиков:

1) FER – отказ в регистрации: доля людей, которые по тем или иным причинам не могут быть успешно авторизованы в системе;

2) FIR – коэффициент ложной идентификации: вероятность того, что биометрические характеристики смогут быть ложно присвоены эталону;

3) FMR – коэффициент ложных совпадений: частота, с которой система неверно сравнивает входной образец с несоответствующей в базе данных эталонной характеристикой.

Соотношение параметров FAR и FRR показано на рис. 2.

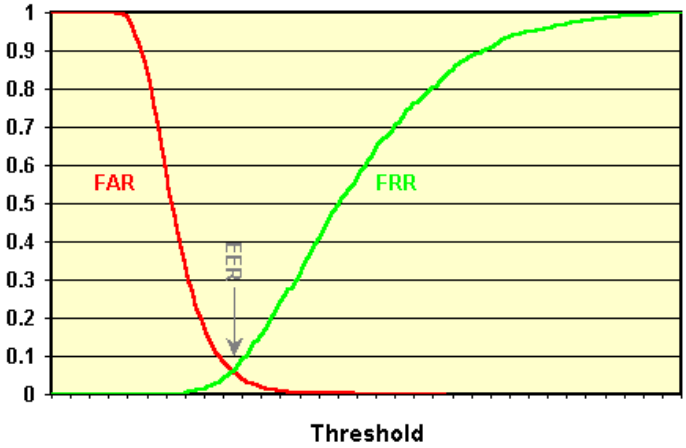

Рис. 2. Диаграмма соотношения параметров FAR и FRR

Точка ERR – показатель эффективности работы биометрических устройств.

Биометрические системы на основе отпечатков пальцев чаще всего подвержены следующим видам атак:

1) использование поддельных биометрических данных;
2) атака на канал передачи данных между датчиком и системой оценки;
3) подмена в базе данных эталонной характеристики;
4) искажение информации, полученной исполнительным блоком.

Повышение безопасности таких биометрических систем возможно за счет использования многофакторной идентификации.

Библиографический список

1. Джейн А., Нандакумар К. Биометрическая аутентификация: защита систем и конфиденциальность пользователей. URL: http://www.osp.ru/os/2012/10/13033122/ (дата обращения: 18.09.19).

2. Комиссаров М. Вопросы терминологии при создании платежно-пропускных систем для стадионов и массовых мероприятий. URL: http://algoritm.org/arch/arch.php?id=74&a=1754 (дата обращения: 10.09.19).

3. Рыканов А.С. Анализ методов распознания отпечатков пальца. URL: http://nbuv.gov.ua/j-pdf/soi_2010_6_37.pdf (дата обращения: 16.09.19).

Пронин Максим Олегович
Пензенский государственный университет, г. Пенза, Россия

Pronin M.O.
Penza State University, Penza, Russia

Бобрышева Галина Владимировна
Пензенский государственный университет, г. Пенза, Россия

Bobrysheva G.V.
Penza State University, Penza, Russia