Лебезов А.М., Шведов А.А. Риски и угрозы биометрической идентификации. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XIX Междунар. научно-техн. конф. – Пенза: ПДЗ, 2019. – С. 101-105.

УДК 004.056.53

РИСКИ И УГРОЗЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

А.М. Лебезов, А.А. Шведов

RISKS AND THREATS OF BIOMETRIC IDENTIFICATION

A.M. Lebezov, A.A. Shvedov

Аннотация. Рассматривается тенденция сбора и использования биометрических данных граждан коммерческими юридическими лицами и правительственными организациями. Были рассмотрены проблемы, связанные с идентификацией удостоверяющих данных, а также предложены решения, способные минимизировать риски.

Ключевые слова: биометрические данные, информационная безопасность, алгоритмы.

Abstract. The article deals with the trend of collection and use of biometric data of citizens by commercial legal entities and government organizations. The problems related to identification of certifying data were considered, as well as solutions that can minimize risks were proposed.

Keywords: biometric data, information security, algorithms.

В 2018 году в России вступил в действие закон о биометрической идентификации. В банках идёт внедрение биометрических комплексов и сбор данных для размещения в Единой биометрической системе (ЕБС) [1]. Так, человек, который хотя бы раз посетил офис какого-либо банка и согласился зарегистрировать свои биометрические образцы (лицо, голос), позднее может стать клиентом любого другого банка, уже не посещая его, также биометрическая идентификация даёт гражданам возможность получать банковские услуги дистанционно. Удобства дистанционной идентификации по фотографии или голосу по достоинству оценили не только клиенты банков, но и киберпреступники.

Внедрение Единой системы идентификации и аутентификации (ЕСИА) и Единой биометрической системы (ЕБС) решает часть задач, но, несмотря на стремление разработчиков сделать технологию безопасной, исследователи постоянно сообщают о появлении новых способов обмана таких систем. Часто финансово-кредитные организации манкируют своими обязанностями, а пользователи, в свою очередь, безоговорочно доверяют репутации банков. Однако риски, связанные с хищением биометрических данных, охватывают куда больший спектр возможностей, выходящих за рамки банковской сферы.

У биометрической идентификации есть особенности, которые отличают её от привычной пары логин/пароль или «безопасной» двухфакторной аутентификации:

1. Биометрические данные публичны. Любой может найти фотографии, видеоаудиозаписи практически любого человека и использовать их для идентификации.

2. Невозможно заменить лицо, голос, отпечатки пальцев или сетчатку с той же лёгкостью, как пароль, номер телефона или токен для двухфакторной аутентификации.

Биометрическая идентификация подтверждает личность с вероятностью, близкой, но не равной 100%. Другими словами, система допускает, что человек может в какой-то степени отличаться от своей биометрической модели, сохранённой в базе.

Киберпреступники и исследователи, связанные с информационной безопасностью, усиленно работают над способами обмана систем биометрической идентификации. Каждый год в программе конференции по информационной безопасности *BlackHat* неизменно присутствуют доклады, связанные с уязвимостями биометрии [2], но практически не встречается выступлений, посвящённых разработке методов защиты. В качестве основных проблем, связанных с биометрической идентификацией, можно выделить фальсификацию, утечки и кражи, низкое качество собранных данных, а также многократный сбор данных одного человека разными организациями.

Чтобы биометрические системы не принимали фотографии и маски за людей, в них используется технология выявления «живости» – *livenessdetection* – набор различных проверок, которые позволяют определить, что перед камерой находится живой человек, а не его маска или фотография. Но и эту технологию можно обмануть. В представленном на *Black Hat 2019* докладе *«Biometric Authentication Under Threat: Liveness Detection Hacking»* сообщается об успешном обходе *liveness detection* [3]. Точность идентификации сильно зависит от качества биометрических данных, сохранённых в системе. Чтобы обеспечить достаточное для надёжного распознавания качество, необходимо оборудование, которое работает в условиях шумных и не слишком ярко освещённых отделений банков.

Некоторые банки начали внедрение собственной биометрической системы раньше, чем заработала ЕБС. Сдав свою биометрию, человек считает, что может воспользоваться новой технологией обслуживания в других банках, а когда выясняется, что это не так, сдаст данные повторно.

Ситуация с наличием нескольких параллельных биометрических систем создаёт риск, что:

1. У человека, дважды сдавшего биометрию, скорее всего, уже не вызовет удивления предложение повторить эту процедуру, и в будущем он может стать жертвой мошенников, которые будут собирать биометрию в своих преступных целях.

2. Чаще будут происходить утечки и злоупотребления, поскольку увеличится количество возможных каналов доступа к данным.

Может показаться, что утечка или кража биометрических данных – настоящая катастрофа для их владельцев, но в действительности всё не так плохо. В общем случае биометрическая система хранит не фотографии и записи голоса, а наборы цифр, характеризующие личность – биометрическую модель. Каждая организация или структура в большинстве случаев создаёт алгоритм вычисления этих точек, отличается от системы к системе и является секретом разработчиков. Информация о пользователе хранится в виде массива чисел, который и представляет собой биометрическую модель. Из принципа построения модели имеются важные следствия:

1. Использовать данные, похищенные из одной биометрической системы для обмана другой, вряд ли получится из-за разных алгоритмов.
2. Обмануть систему с помощью похищенных из неё данных тоже не получится – для идентификации требуется предъявление фотографии или аудиозаписи, по которой уже будет проведено построение модели и сравнение с эталоном.

Даже если база хранит не только биометрические модели, но и фото и аудио, по которым они построены, обмануть систему с их помощью «в лоб» нельзя: алгоритмы проверки на «живость» считают ложными результаты с полным совпадением дескрипторов.

Ввиду неиспытанности правового поля в данной отрасли и только пополняющейся базы прецедентов, первой, кто дополнил основные уложения оказания платежных услуг, стала Европейская комиссия. Вступившая в действие 14 сентября 2019 года директива *PSD2* требует от банков внедрения многофакторной аутентификации для обеспечения безопасности удалённых транзакций, выполняемых по любому каналу. Это означает обязательное использование двух или трёх компонентов:

1) знания – определенной информации, известной только пользователю, например, пароля или контрольного вопроса;

2) владения – определенного устройства, которое имеется только у пользователя, например, телефона или токена;

3) уникальности – чего-то неотъемлемого, присущего пользователю и однозначно идентифицирующего личность (биометрические данные).

Эти три элемента должны быть независимыми так, чтобы компрометация одного элемента не влияла на надёжность других (такие случаи участились в банковской сфере).

Данные требования также можно расценивать базовым стандартом при обмене информацией в настоящее время для обеспечения ее безопасности. С распространением и удешевлением технологий биометрической идентификации другие методы отходят на второй план, что и ухудшает безопасность данных. Желательно использовать биометрическую идентификацию в редких случаях и не в качестве основного средства защиты. Если же без биометрической идентификации никак не обойтись, необходимо использовать её совместно с многофакторной аутентификацией, чтобы хотя бы частично снизить риски.

Библиографический список

1. Федеральный закон от 31 декабря 2017 г. № 482-фз «О внесении изменений в отдельные законодательные акты Российской Федерации».
2. Dr. Thomas P. Keenan. Hidden Risks of Biometric Identifiers and How to Avoid Them. InBlackHat USA, 2015.
3. Yu Chen, Bin Ma, Zhuo Ma. Biometric Authentication Under Threat: Liveness Detection Hacking. In Black Hat USA, 2019.

Лебезов Антон Михайлович
Тверской государственный
технический университет,
г. Тверь, Россия
E-mail: Lebezov.anton@gmail.com

Lebezov A.M.
Tver State Technical University,
Tver, Russia

Шведов Александр Александрович
Тверской государственный
технический университет,
г. Тверь, Россия

Shvedov A.A.
Tver State Technical University,
Tver, Russia