УДК 336.71

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ КЛИЕНТОВ НА РЫНКЕ ФИНАНСОВЫХ УСЛУГ И ПЕРСПЕКТИВЫ ИХ ПРИМЕНЕНИЯ

Зинина О.С.

канд. экон. наук, доцент

Кубанский государственный аграрный университет имени И.Т. Трубилина

Краснодар, Россия

Корч Е.А.

студентка

Кубанский государственный аграрный университет имени И.Т. Трубилина

Краснодар, Россия

Тащилина Ю.В.

студентка

Кубанский государственный аграрный университет имени И.Т. Трубилина

Краснодар, Россия

Аннотация

В статье рассмотрено понятие биометрии, ее достоинства и недостатки как системы. Указаны методы обеспечения информационной безопасности при использовании биометрической системы. Приведено различие между биометрической идентификацией и аутентификацией. Перечислены виды биометрической идентификации, а также их достоинства и недостатки. Рассмотрены причины, по которым клиенты банка неохотно размещают свои биометрические данные в Единой биометрической системе (ЕБС). Также проанализирована статистика по сбору биометрии на текущее время и

сформулированы выводы о перспективах технологий аутентификации и идентификации в разрезе биометрических технологий.

Ключевые слова: аутентификация, идентификация, биометрические технологии, цифровая экономика, финансовый сектор, безопасность.

BIOMETRIC TECHNOLOGIES FOR IDENTIFICATION AND AUTHENTICATION OF CLIENTS IN THE FINANCIAL SERVICES MARKET AND PROSPECTS FOR THEIR APPLICATION

Zinisha O.S.
Cand. econ. sciences, associate professor of the department of monetary circulation and credit
Kuban state agrarian University named by I.T. Trubilin
Krasnodar, Russia

Korch E.A.
student
Kuban state agrarian University named by I.T. Trubilin
Krasnodar, Russia

Taschilina U.V.
student
Kuban state agrarian University named by I.T. Trubilin
Krasnodar, Russia

Annotation

The article considers the concept of biometry, its advantages and disadvantages as a system. Methods for ensuring information security using a biometric system are indicated. A distinction is made between biometric identification and authentication.

The types of biometric identification are listed, as well as their pros and cons. The reasons why bank customers are reluctant to submit their biometric data are considered. There are also statistics on the collection of biometrics for the current time.

Key words: authentication, identification, biometric technologies, digital economy, financial sector, security.

С первых чисел июля 2018 года в России заработала Единая биометрическая система (ЕБС) – масштабная цифровая платформа, которая позволяет удаленно идентифицировать человека по биометрическим характеристикам (лицу или голосу). Проект имеет масштабные задачи, которые сделают банковские услуги одинаково доступными без географического отношения, а также решат проблемы безопасности, с которыми сталкиваются банки. Например, уменьшат риск мошенничества и защитят клиентов от подбора или компрометации их пароля.

Цель внедрения ЕБС – повышение доступности финансовых услуг, а затем и иных, в первую очередь для людей из отдаленных регионов и маломобильных граждан. Для получения услуги не потребуется личное посещение, ее смогут предоставить удаленно, через Интернет.

Биометрия предполагает систему распознавания личности людей по одному или сразу нескольким физическим параметрам (голос, отпечаток пальца, черты и термограмма лица, ДНК, ладонь, сетчатка и радужная оболочка глаза и т.п.) или поведенческим чертам (походка, почерк и т.п.). Различные биометрические технологии используются в мире довольно давно – например, в криминалистике, при выдаче виз и паспортов.

Развитие биометрических технологий продолжается уже более полувека. По информации Русского биометрического общества, системы защиты от несанкционированного доступа к информации в персональном компьютере и банковским счетам на основе использования биометрических характеристик

человека начали создаваться еще в конце XX века. Они предназначались для обеспечения более надежной, по сравнению с паролями и микропроцессорными карточками, идентификации личности по голосу, отпечаткам пальцев, изображениям лица и радужной оболочки глаза [1].

Для обеспечения информационной безопасности реализовано распределенное хранение данных: используются современные средства шифрования, сертифицированные Федеральной службой безопасности (ФСБ) и Федеральной службой по техническому и экспортному контролю (ФСТЭК). Передача информации происходит по защищенным каналам связи. Голос и изображение лица проверяются одновременно по множеству разных параметров. Как утверждают специалисты Ростелекома, вероятность ошибки – 1 на 10 000 000. Биометрический шаблон хранится в обезличенной форме отдельно от персональных данных человека (Ф.И.О., паспортных данных, СНИЛС и др.), включенных в базы Единой системы идентификации и аутентификации (Портал госуслуг) [3].

При возникновении какой-либо внештатной ситуации восстановить биометрические данные по персональным параметрам будет невозможно, как и наоборот. В банках не хранятся фотографии, записи голоса, а есть лишь математическая модель обработки тех данных, которые были записаны. Именно эта модель и станет доступна злоумышленнику, а восстановить по ней биометрию человека невозможно, как и понять, каким персональным данным она принадлежит.

Биометрическая идентификация (БИ) от аутентификации (БА) отличается тем, что при идентификации пользователь определяется путем сравнения его биометрических данных со всеми, имеющимися в системе, до момента нахождения совпадения. При биометрической аутентификации пользователь говорит системе, кто он (например, вводит уникальный логин), система по этому логину считывает его эталонные биометрические данные из базы данных и затем производит их сверку с теми, которые предоставляет пользователь [5].

В последние годы интерес к биометрической идентификации значительно возрос, так как с развитием современных технологий стало возможным быстро и точно определять уникальные физиологические данные человека. Когда дело доходит до биометрического банкинга, речь идет о поиске баланса между комфортом и безопасностью. Биометрическая технология обычно зависит от одного действия, а не от необходимости вводить, например, пароль длиной от 8 до 16 символов. Однако прежде чем остановить свой выбор в пользу биометрии, следует обратить внимание на ее достоинства и недостатки, приведенные в таблице 1.

Чтобы обеспечить высочайший уровень безопасности при минимальных затратах для конечных пользователей, новые биометрические технологии постоянно тестируются. Цель состоит в том, чтобы найти тот, который имеет лучший баланс FAR (уровень ложного принятия) и FRR (уровень ложного отклонения). FAR измеряет вероятность аутентификации неверного пользователя, а FRR - противоположность - измерение вероятности отказа авторизовать легального пользователя.

Таблица 1 – Плюсы и минусы существующих систем биометрии

Плюсы	Минусы
Идентификатор неотделим от человека	Доступность биометрических идентификаторов для копирования и проведения атаки в большинстве систем биометрической идентификации
Воссоздать (подделать) идентификатор достаточно сложно	Необходимость наличия определенных окружающих условий для проведения биометрической идентификации
Биометрическая идентификация удобна в использовании	Повреждения или недоступность для считывания биометрических идентификаторов
Идентификация может проводиться прозрачно (незаметно) для человека.	Вероятность ошибки доступа первого рода, когда система не идентифицирует зарегистрированного человека, и вероятность пропуска чужого (ошибка второго рода).
Экономия времени персонала за счет сокращения времени, затрачиваемого на различные операции	Для многих систем биометрической идентификации биометрические сканеры достаточно дорогие

Дополнительный технологический и современный имидж для банка	Необходимо обеспечивать требования регуляторов по защите биометрических персональных данных

На практике технологии, которые очень хороши с точки зрения FAR, имеют тенденцию быть слишком строгими, что приводит к большому количеству отказов законных пользователей. Так как используется много параметров, выбор наилучшей технологии является сложной задачей. Поиск такого, который не требовал бы каких-либо компромиссов, продолжается [6].

Несанкционированный доступ становится более сложным, когда системы требуют несколько средств идентификации. Некоторые системы безопасности также включают дополнительные параметры, такие как возраст, пол и рост, чтобы помешать хакерам.

Исходя из этого, можно сделать вывод о том, что система сбора и хранения биометрических данных вполне безопасна, что является существенным преимуществом.

В настоящее время наиболее распространенными являются следующие виды биометрической идентификации:

- по отпечатку пальца;
- по лицу, как по двухмерному, так и по трехмерному изображению;
- по голосу;
- по сетчатке глаза.

На данный момент возможность использования биометрии в банках находится на стадии реализации. Поэтому недостатки некоторых видов идентификации порой превышают достоинства, что можно проанализировать на основе данных, представленных в таблице 2.

Таблица 2 – Преимущества и негативные характеристики основных видов биометрической идентификации

Биометрическая идентификация	Плюсы	Минусы
Дактилоскопия	Высокая надежность; низкая стоимость сканеров; простая процедура	Папиллярный узор отпечатка легко повреждается царапинами, порезами; возможна фальсификация; высокая чувствительность к влиянию внешних факторов.
Распознавание лиц	Бесконтактность; низкая чувствительность ко внешним факторам	Высокая стоимость техники; изменения мимики ухудшают надежность метода; недостаточно хорошо разработан; возможна фальсификация.
Голос	Бесконтактность; подходит для удаленного использования; низкая стоимость техники	Высокий уровень ошибки; возможна фальсификация.
Сетчатка	Бесконтактность; высокая надежность; быстрая идентификация	Высокая стоимость системы; высокая чувствительность к влиянию внешних факторов.

Теоретически Единая биометрическая система дает клиентам банков довольно много преимуществ. Однако, если программное обеспечение банка не настроено должным образом, процесс сбора является длительным и не всегда безопасным для потребителя. В частности, банки жалуются на качество полученных образцов лица и голоса. Например, неправильно настроенный микрофон может привести к перегрузке. В результате биометрические данные низкого качества отправляются в ЕБС, которые затем не могут использоваться банками [5].

Около 35% клиентов банков, которые используют ЕБС, предпочитают дактилоскопию. На втором месте – распознавание лиц – 30%. Сканирование сетчатки глаза выбрали 18% клиентов, голоса – 5%. Почти 12% предпочитают другие виды биометрии [2].

Несмотря на многие преимущества биометрии, некоторые клиенты банков неохотно сдают свои биометрические данные. Тому есть несколько причин:

1. Если пароль был скомпрометирован, он может быть изменен. Биометрия неотлучна от человека и не может быть подвержена кардинальным изменениям.

2. Любой сканер биометрических свойств несовершенен и может быть обманут. В некоторых случаях усилия, чтобы обмануть, невелики - например, сканер радужной оболочки, «одураченный» фотографией. В других, усилия огромны, но это не остановит мошенника. После того, как биометрическое свойство было нарушено, единственный способ восстановить его - это полностью изменить систему распознавания биометрических данных.

3. Опасения людей касаются безопасности их биометрических данных. Случаи мошенничества с банковскими картами, банкоматами, а также кредитами, которые берут злоумышленники на подделанные паспорта, хорошо известны и регулярно освещаются в СМИ. Теперь же прямой опасности могут подвергнуться биометрические данные человека, которые хранятся к тому же в облачном пространстве.

4. Опасения перед новыми и труднопонимаемыми технологиями.

И все же, трое из пяти человек (61%) считают, что биометрическая идентификация является такой же безопасной или более безопасной, чем нынешние системы паролей.

Данные в ЕБС могут храниться не более трех лет, после чего должны быть обновлены. Сейчас специалисты работают над увеличением срока хранения данных. Также пересдать биометрические персональные данные потребуется в случае серьезных лицевых травм или при повреждении голосовых связок, которые привели к изменению голоса [1].

Цена подключения банка к ЕБС начинается с 3 млн. руб. за обеспечение киберзащиты и покупку оборудования. Последующее подключение каждого отделения обойдется еще в 130 тыс. руб., годовое обслуживание — в 1,2 млн. руб. Далеко не все банки могут себе это позволить, ведь даже при успешной реализации проекта затраты окупятся лишь частично, и через много лет. Поэтому

одними из первых к биометрической системе подключились крупнейшие банки страны, для которых такие расходы проходят в рабочем режиме.

Первыми удаленную биометрическую идентификацию запустили в Почта банке и Совкомбанке. Еще через неделю - в банке «Тинькофф», Альфа-банке и Газпромбанке. В последние годы российские банки стали активно использовать биометрические технологии.

По данным ЦБ РФ, лишь 40% отделений банков России собирают биометрическую информацию пользователей. В РФ действует 30 214 подразделений различных банков, из них биометрию собирает лишь 11 270 отделений [7].

На данный момент сбор биометрии в России нельзя назвать массовым. Среди россиян-клиентов банков данная услуга не очень востребована, что подтверждает и статистика сбора таких данных: на начало января 2020 г. в ЕБС было зарегистрировано около 110 тыс. человек. Лидерами по количеству сданных шаблонов являются Сибирский регион, Северо-Запад, Москва и Поволжье. Важно, что это не только города-миллионники, наблюдается активность граждан и в средних, и малых городах, где также расположены клиентские центры, сдают биометрию и в сельских населенных пунктах.

В основном пользуются этой услугой люди из так называемой «экономически активной категории» — от 20 до 50 лет, но также есть пенсионеры и молодые люди [4].

Пока невозможно открыть счет только на основании идентификации по биометрическим данным. С этими данными еще в целом мало что можно задействовать. Банки пытаются с их помощью выявлять мошенничество, но очевидной выгоды для бизнеса эта технология не несет, при этом требует значительных инвестиций в установку записывающего оборудования. А когда нет явной выгоды, внедрение технологии тормозится.

Сейчас действующий сервис позволяет проводить удаленную идентификацию по слепку голоса, подтверждать-акцептовать переводы,

оформлять заявку на кредит. В ближайшем будущем планируется расширение спектра банковских услуг, осуществляемых с использованием биометрической идентификации.

Таким образом, данная система видится полезной и перспективной, но, тем не менее, она требует еще ряд доработок. Особенно по части конфиденциальности информации. Кроме того, необходимо максимально ограничить человеческий фактор в работе данной системы.

Библиографический список:

1. Антипов, Н. Биометрия в банках: сдавать или не сдавать / Н. Антипов [Электронный ресурс]. – Режим доступа: URL: https://www.banki.ru/news/columnists/?id=10903594 (дата обращения: 18.03.2020).

2. Афонина, А. Биометрия против банковского PIN-кода – кто победит и когда? / А. Афонина [Электронный ресурс]. – Режим доступа: URL: https://www.banki.ru/news/bankpress/?id=8223899 (дата обращения: 18.03.2020).

3. Дементьева, К. Биометрия застряла в банках / К. Дементьева // Газета «Коммерсантъ». - 2019. - №171 [Электронный ресурс]. – Режим доступа: URL: https://www.kommersant.ru/doc/4097181 (дата обращения: 18.03.2020).

4. Медведева, Е. Биометрия: как банки узнают клиентов? / Е. Медведева [Электронный ресурс]. – Режим доступа: URL: https://info.sibnet.ru/article/552480/ (дата обращения: 18.03.2020).

5. Рындина, И.В. Роль инновационных рисков в деятельности коммерческих банков / И.В. Рындина, А.В. Борисов, О.М. Ермоленко. - В сборнике: Финансовая грамотность населения: проблемы, перспективы, решения. Материалы Всероссийской научно-практической конференции. Под ред. П.А. Канапухина, Е.Ф. Сысоевой, Е.А. Фендюшиной. - Воронеж: издательско-полиграфический центр «Научная книга», 2019. - С. 34-38.

6. Терновская, Т. В российских банках возникли проблемы со сбором биометрии / Т. Терновская [Электронный ресурс]. – Режим доступа: URL:

https://iz.ru/850489/2019-02-26/v-rossiiskikh-bankakh-voznikli-problemy-so-sborom-biometrii (дата обращения: 18.03.2020).

7. Токарев, А. Биометрический паспорт в банке — как работает ЕБС? / А. Токарев [Электронный ресурс]. – Режим доступа: URL: http://tatcenter.ru/rubrics/razbor/biometricheskij-pasport-v-banke-kak-rabotaet-ebs/ (дата обращения: 18.03.2020).

Оригинальность 80%