УДК 340

ПЕРСПЕКТИВЫ РАЗВИТИЯ И РИСКИ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ В БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

К.А. ГАЙКОВА
(Представлено: А.С. ВАЛЕВКО)

В публикации рассматриваются перспективы развития и риски использования биометрические технологий, а также их практическое применение за рубежом.

Быстрое развитие информационного пространства повлияло на развитие использования биометрических технологий в соседних государствах. Плюсы биометрии не обошли стороной и стран-хранителей банковской тайны: Королевство Швеция, Великое герцогство Люксембург, Республика Сингапур, Французская Республика и т.д. Западные страны, состоящие в Европейском Союзе (далее – ЕС) имеют определенный стандарт, который регулирует основные вопросы, связанные со сбором, хранением и обработкой персональных данных – далее GDPR). Этот документ закрепляет в себе самые важные общие требования, которые предъявляются к организациям, использующим персональные данные для своей деятельности. GDPR помечает биометрическую информацию как специальную категорию персональных данных и помещает под общую защиту. Такая категория означает, что биометрические данные не могут быть обработаны в соответствии со ст. 9 пункта 1 без разрешения лица или его уведомления. Тем не менее, статья впоследствии также называет определенные исключения, которые позволяют общественным органам собирать и обрабатывать биометрические данные, прежде всего, однако банков и других небанковских финансово кредитных организаций это не касается. В государственных и негосударственных учреждениях биометрический контроль доступа через радужную оболочку, голос или отпечаток пальца может использоваться для обеспечения безопасности информации.

Принципиального запрета на обработку биометрических данных в связи с этим GDPR не называет. Но без юридического основания для этой обработки всегда должно быть получено согласие заинтересованных лиц. Кроме того, цель и соразмерность могут играть важную роль: поэтому государственные и негосударственные органы должны всегда взвешивать, чьи интересы, достойные защиты, перевешивают интересы заинтересованного лица или учреждения. Вдобавок, биометрическое распознавание геометрии лица, как правило, требует правовых оснований и может применяться, прежде всего, в рамках территориальных задач, таких как полиция и государственная охрана. Однако, для обработки биометрических данных, подозрительных для этой цели организаций, до сих пор требуется согласие заинтересованных лиц, о чем свидетельствует испытание федеральной полиции на Берлинском вокзале Зюд-Кройц [1].

Помимо GDPR в ЕС также действуют и другие, не менее важные, регламенты и директивы:

– Regulation 2016\679 (The General Date Protection Regulation) – относится к защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных [2];

– Regulation 2018\1725 – так же относится к защите физических лиц при обработке персональных данных, но только в учреждениях, органами и агентствами ЕС и, вдобавок, касается свободного перемещения таких данных [3];

– Directive 2002\58\EC – об обработке персональных данных и защиты конфиденциальности в сегменте электронных коммуникаций [4];

– Directive 2016\680 – касается защиты физических лиц при обработке персональных данных компетентными органами с целью предотвращения расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний [5].

Вход в систему с помощью отпечатка пальца становится все более популярным по сравнению с идентификацией по лицу. Таким образом, около года назад VISA International Service Association (далее – VISA) и MasterCard Incorporated (далее – MasterCard) – международные платёжные системы, создали биометрическую пластиковую карточку. Платеж совершается, как и раньше, кредитной картой. Однако, вместо чипа с PIN-кодом будет встроен чип с отпечатками пальцев, который позволит удостоверить подлинность владельца карты, когда он захочет произвести платеж. Также, если пользователю захочется оставить 4-хзначный пароль, то он может выбрать его вместо биометрических данных.

Принцип работы биометрической карты достаточно прост. Чтобы выполнить биометрическую проверку, держателю карты нужно положить палец на датчик, а затем вставить карту (при контактном режиме) или приблизить ее (при бесконтактном режиме) к платежному терминалу, чтобы подтвердить транзакцию. В случае невозможности использования отпечатков пальцев, например, при снятии наличных в банкомате, ПИН-код все-таки можно использовать.

Сама процедура регистрации может быть выполнена дома или в самом банке. При регистрации дома данные отпечатков пальцев держателя карты надежно хранятся на карте с помощью так называемого «разъема

активации», входящего в комплект карты. Вставив новую карту в этот «разъем» и выполнив очень простую процедуру, держатель завершает регистрацию в течение нескольких секунд. Затем активация завершается во время первой транзакции. Владелец карты также может посетить свой банк и получить помощь консультанта, используя безопасный планшет регистрации или в течение 24 часов в сутки и 7 дней в банкомате [6].

На данный момент такие карты уже тестируются в Соединенных Штатах Америки (далее – США), Государстве Японии, Королевстве Норвегии. В процессе тестирования такой биометрической платежной карты были выявлены как плюсы, так и минусы. К плюсам можно отнести:

- более облегченные платежи;
- дополнительная безопасность от риска кражи или мошенничества;
- сохранение возможности настройки старого 4-хзначного пароля;
- воспринимаются пользователями как более удобная и безопасная технология.

Что касается минусов, то к ним относятся:

- нет предельного порога для суммы, которая будет сниматься с помощью биометрической оплаты;
- велик риск сбоев, связанных с компьютерными ошибками;
- способ оплаты не является надежным на 100%;
- небрежное отношение к защите данных и их конфиденциальности.

Защита биометрических данных всегда стояла одним из главных вопросов по использованию подобных технологий. Появление биометрической карты может повернуть ситуацию совершенно в другую сторону. Это связано с тем, что биометрический отпечаток будет считаться более безопасным и эффективным, чем пин-код или бесконтактная проверка. Данные, связанные с банковским отпечатком, будут храниться на банковской карте, а не передаваться банку и или небанковским финансовым организациям. Кроме того, биометрические платежи обеспечивают дополнительную безопасность благодаря распознаванию отпечатков пальцев, которые почти невозможно взломать через платежный терминал. С другой стороны, на стороне онлайн-платежей биометрическая карта не предвещает больших новинок в отношении защиты транзакций. Если только некоторые банки не дойдут до конца, добавив динамическую криптографическую систему. Это позволит значительно снизить риск мошенничества или кражи банковских данных через интернет [7].

Первым государством, которое ввело такие карты является Соединенное Королевство Великобритании и Северной Ирландии. Инновационная биометрическая платежная карта была впервые опробована в начале 2019 года в рамках трехмесячного пилотного проекта через бренды RBS Group и NatWest с участием 150 человек, использующих дебетовые карты Visa. Результаты эксперимента подтвердили, что потребители готовы к дальнейшему использованию и с энтузиазмом относятся к удобству, которое предлагают эти технологии. Испытуемые также подтвердили, что теперь являются поклонниками светодиодных огней на карте, поскольку могут быть уверены в том, что транзакция была проведена успешно. RBS Group проводит аналогичный пилотный проект с октября 2020 года, на этот раз с использованием кредитных карт Mastercard, и рассмотрит возможность более широкого коммерческого внедрения в 2021 году, если это подтвердит их ожидания [8].

Ранее упомянутый крупный банк NatWest в Великобритании использует технологию израильского стартапа BioCatch. Система создает «уникальный профиль пользователя», захватывая более 500 поведенческих характеристик таких, как координация рук и глаз, нажатие клавиш, моторика, жестикуляция, прокрутка и другие движения пальцев. Шаблоны постоянно проверяются не только при входе в систему, но и во время сеанса онлайн-банкинга. Эта непрерывная аутентификация позволяет мгновенно обнаруживать аномалии в поведении. Система также обнаруживает автоматизированные боты, вредоносные программы и другие вредоносные атаки на захват учетных записей. По данным банка, уже в первые месяцы работы система смогла предотвратить потери в следующих областях:

- предотвращение мошеннических попыток делать переводы;
- идентификация троянских вирусных программ удаленного доступа во время онлайн-сеанса;
- идентификация попыток мошенничества, происходящих по нескольким каналам (онлайн и мобильный).

Зарубежные банки также пользуются и голосовой биометрией. Голос человека так же уникален, как и его отпечаток пальца. Он состоит из более чем 100 индивидуальных признаков, основанных на физическом взаимодействии рта и гортани. Barclays Bank использует эти функции для распознавания голоса и идентификации клиентов в своих колл-центрах. Когда клиент звонит в сервисный центр, идентификация осуществляется на основе первых произнесенных слов. Клиенты должны зарегистрироваться для этого с помощью голосового сканирования. После теста, продолжающегося в Wealth Management с 2013 года, процедура была развернута для всех клиентов банка в 2016 году. Barclays обещает больше удобства для клиента, более быстрое время обработки и меньше случаев мошенничества [9].

Сбор, обработка, передача и хранение биометрических данных в Соединенном Королевстве Великобритании и Северной Ирландии осуществляется согласно общему публичному акту 2018 года «Закон о защите данных» (Data Protection Act 2018). Закон состоит из 7 частей и 215 статей [10]. Рассматриваемый

нормативный акт создавался на основе Общего Положение о Защите Данных (General Data Protection Regulation далее – GDPR) с целью вернуть гражданам контроль над своими данными при одновременном упрощении нормативной базы компаний. Нормативный акт не только устанавливает четкий набор прав потребителей, но и включает в себя меры, направленные на повышение безопасности организации. Например, если компания обнаруживает нарушение данных, то операторы должны сообщить об этом соответствующим государственным органам в течение 72 часов с момента обнаружения утечки [10]. Вдобавок компании, управляющие биометрической информацией, в том числе и банки, могут быть подвергнуты массовым штрафам, если они не защитят биометрические данные. Взыскания могут достичь около 17 миллионов фунтов стерлингов или 4% от годового мирового оборота.

Однако, после того как правительство Великобритании опубликовало стратегию развития в области биометрии (Biometrics strategy and forensic services), спровоцировало массу недовольств у граждан. Сам документ состоит из 27 страниц, что не отвечает на критические вопросы, связанным с ним [11]. Первое, что беспокоило граждан так это то, каким образом полиция будет собирать и хранить данные изображения лиц. Некоторые лица сравнивали стратегию с «рекомендацией», в которой предусмотрены лишь «советы» для осуществления тех или иных действий, а не прямые указания. В своем докладе о стратегии правительства в области биометрии и судебной экспертизы, опубликованном в мае 2019 года. Комитет по науке и технике заявил, что существуют серьезные этические последствия с использованием и хранением изображений лица, которые правительство должно принять во внимание для решения проблемы, путем использования более совершенных биометрических технологий [12]. Многие также отмечали, что слишком резкий скачок использования биометрии очень сильно повлиял на права человека. Так как после публикации стратегии о развитии биометрических технологий Министерство внутренних дел Великобритании показало себя с достаточно некомпетентной стороны, холодно относясь к сбору биометрической информации с помощью биометрических технологий. Например, не раз было зафиксировано, как компании и организации, у которых не было юридического разрешения на сбор, считывали изображения лиц граждан без их ведома [13]. Данный вопрос до сих пор остается нерешенным.

Зарубежная практика использования биометрических технологий отлично показала себя в Государстве Японии. Банк Ogaki Kyoritsu с начала 2012 года начал заменять обычные банкоматы на биометрические. Устройству достаточно сканировать ладонь пользователя без использования дебетовой карты. Ogaki Kyoritsu преследовал цель стать первым японским банком, который в своей деятельности бы использовал биометрические технологии. Новые банкоматы позволяют клиентам подтвердить свою личность, сканируя ладонь, вводя ПИН-код и дату рождения. После чего пользователи могут получить доступ к своим счетам чтобы снять или внести деньги, или проверить баланс счета. Целевой аудиторией рассматриваемой инновации стали выжившие после землетрясения и цунами в Тохоку в марте 2011 года. Граждане потеряли карты и сберкнижки из-за стихийных бедствий, а биометрические банкоматы помогли многим не потерять свои счета [14].

С 2019 года в Японии продолжается тестирование банкоматов, которые идентифицируют токийских клиентов японского банка – Seven Bank. Организация раскрыла свои планы по сканированию лиц в банкоматах в начале 2019 года с целью обеспечения биометрической аутентификации клиентов. А также предоставления пользователям возможности открывать новые счета через банкомат благодаря дополнительной возможности считывания документов. Теперь Seven Bank сообщил, что работает со специалистом по распознаванию лиц NEC над разработкой новых банкоматов. Устройства имеют множество других технологически сложных функций, выходящих за рамки распознавания лиц. Они также предназначены для считывания QR-кода и имеют функцию Bluetooth для сопряжения со смартфонами. В том числе имеют встроенные сейсмометры, чтобы помочь уполномоченным лицам собирать данные о стихийных бедствиях [15].

Однако в таком технологически развитом государстве также имеются свои минусы в биометрических технологиях. Во-первых, устройства не справляются с изменениями во внешности лица, так как биометрические или физические особенности человека при определении внешности изменяются, а точность аутентификации соответственно снижается. Во-вторых, похищенные данные быстро восстановить в современных реалиях невозможно.

Китайская Народная Республика (далее – КНР) выработала целый алгоритм по внедрению биометрических технологий в банковскую систему. Прежде чем приступить к их использованию, специалисты конкретного банка должны оценить различные типы биометрических технологий, доступных для внедрения и наиболее вероятную реакцию клиентов этого банка на нововведение. В зависимости от организации может проводится прямой опрос самих клиентов, а затем на основе ответов банк делает выводы. Если большинство клиентов не хотят регистрироваться или сопротивляются использованию биометрический аутентификации – инвестирование в биометрические технологии бесполезны. Организациям важно подобрать такую систему, которую бы клиенты могли быстро и легко использовать [16].

Наиболее распространенной биометрической технологией в КНР является – 3D аутентификация по геометрии лица. Если сравнивать с другими видами биометрии, рассматриваемый способ имеет достаточно много преимуществ. Во-первых, идентификация проходит без касание самого устройства для считывания, что в эпоху COVID-19 снижает риск заболеваемости. Во-вторых, решает проблемы с плохим

освещением, так как считыватель оборудован телевизором. В-третьих, сама стоимость таких технологий достаточно низкая по сравнению с другими, а качество намного превышает цену. Устройства с распознаванием лиц широко используются в аэропортах, на таможне и в других местах с большим потоком людей в качестве «ворот» для сравнения входящих и выходящих людей в режиме реального времени. Все быстро может подключиться к Интернету для устранения неполадок с людьми, которые занесены в так называемые «черные списки» компаний.

В последние годы почти все банки используют технологию распознавания лиц в качестве основного метода аутентификации пользователя на счетчике в сочетании с паролем для оплаты банковской картой, а также для дальнейшего повышения безопасности аутентификации личности. Есть банки, которые запустили новую операционную модель обслуживания под названием «умная кассовая машина», которая полностью сочетает в себе биометрические технологии такие, как платежный пароль и распознавание лиц, что значительно повышает эффективность обслуживания. Взяв в качестве примера «супер счетчик» Сельскохозяйственного банка Китайской Народной Республики, он интегрирует аппаратные устройства, такие как камеры распознавания лиц, считыватели отпечатков пальцев и считыватели удостоверений личности. Среди них находится модуль сравнения лиц, объединенный в сеть с информационной системой Министерства Общественной Безопасности для проверки личности пользователя, что является более авторитетным и юридически эффективным [17].

Что касается регулирования использования биометрических технологий на законодательном уровне то, Китай еще не ввел законы, которые были бы специально направленны на биометрические технологии. Однако та информация о геометрии лица, отпечаток пальцев, радужки глаз и т.д., собранная, с помощью рассматриваемых способов аутентификации, как биометрическая информация, относится к категории личной информации и должна регулироваться законами, касающимися защиты персональных данных. На данный момент существуют следующие законодательные нормативно-правовые акты:

Закон о сетевой безопасности. Например, статья 41 Операторы сети, собирающие и использующие персональные данные, должны следовать принципам законности, законности и необходимости, раскрывать правила сбора и использования, а также выражать цель, метод и объем сбора и использования информации с согласия собственника этой информации [18];

Закон о защите прав и интересов потребителей. Например, статья 29 Коммерческие операторы, собирающие и использующие личную информацию потребителей, должны следовать принципам законности, законности и необходимости, указывать цель, метод и объем сбора и использования информации, получать согласие потребителей. Операторы предпринимательских компаний, собирающие и использующие личную информацию потребителей, должны раскрывать свои правила сбора и использования и не должны собирать и использовать информацию в нарушение положений законов и нормативных актов и соглашений между двумя сторонами [18];

Закон об электронной торговле. Например, статья 23 Операторы электронной торговли, собирающие и использующие персональные данные своих пользователей, должны соблюдать положения законов и административных регламентов о защите персональных данных [18].

Кроме того, Китай также издал национальные стандарты, касающиеся биометрической информации или информации о распознавании лиц такие, как «спецификации безопасности персональных данных в области информационной безопасности», серия стандартов: «интерфейс программирования приложений для биометрической идентификации информационных технологий», «технические требования к изображениям приложений для распознавания лиц общественной безопасности» и так далее [18].

Подводя итог обоснованных фактов и доводов, можно сделать вывод, что наибольших успехов в использовании биометрических технологий в банковской деятельности добилась Китайская Народная Республика. Так как это государство имеет большую законодательную базу по регулированию отношений в области биометрических персональных данных и эффективно ее применяет на практике.

ЛИТЕРАТУРА

1. Biometrische Daten: Besondere Schutzwürdigkeit bei sensibelsten Daten! [Electronic resource]: - Access mode: www.datenschutz.org/biometrische-daten – Date of access: 18.09.2021.
2. Регламент (ЕС) 2016/679 ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС» [Электронный ресурс]: - Режим доступа: ogdpr.eu/ru/gdpr-2016-679 – Дата доступа: 18.09.2021.
3. Regulation (EU) 2018/1725 [Electronic resource]: - Access mode: edps.europa.eu/data-protection/our-work/publications/legislation/regulation-eu-20181725_en – Date of access: 18.09.2021.
4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Electronic resource]: - Access mode: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 – Date of access: 18.09.2021.

5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [Electronic resource]: - Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680&qid=1631965176655 – Date of access: 18.09.2021.
6. Carte EMV avec biométrie par empreintes digitales [Electronic resource]: - Access mode: www.thales-group.com/fr/europe/france/dis/banque/cartes/biometrique-emv – Date of access: 18.09.2021.
7. Qu'est-ce que le paiement biométrique ? [Electronic resource]: - Access mode: reassurez-moi.fr/guide/banque/carte-bancaire-biometrique#:~:text=Le%20 principe% – Date of access: 18.09.2021.
8. Innovative payments with fingerprint biometric cards: RBS Group heralds UK first [Electronic resource]: - Access mode: www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cust omer-cases/rbs-biometric-card – Date of access: 18.09.2021.
9. Fünf Beispiele für den Einsatz von Biometrie in Banking und Payment [Electronic resource]: - Access mode: www.der-bank-blog.de/fuenf-beispiele-biometrie/technologie/30357/ – Date of access: 18.09.2021.
10. Data Protection Act 2018 [Electronic resource]: - Access mode: www.legislation.gov. uk/ukpga/2018/12/contents/enacted – Date of access: 18.09.2021.
11. Biometrics Strategy. Better public services. Maintaining public trust [Electronic resource]: - Access mode: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometr ics_Stra-tegy_-_2018-06-28.pdf – Date of access: 18.09.2021.
12. Biometrics strategy and forensic services. Fifth Report of Session 2017–19 [Electronic resource]: - Access mode: publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf – Date of access: 18.09.2021.
13. UK biometrics strategy criticised for lack of content [Electronic resource]: - Access mode: www.compute-rweekly.com/news/252443933/UK-biometrics-strategy-criticised-for-lack-of-content – Date of access: 18.09.2021.
14. Ogaki Kyoritsu Bank to install palm-scanning ATMs [Electronic resource]: - Access mode: www.retail-bankerinternational.com/news/ogaki-kyoritsu-bank-to-install-palm-scanning-atms/ – Date of access: 18.09.2021.
15. Japanese Bank Begins Deployment of Biometric ATMs Featuring NEC Tech [Electronic resource]: - Access mode: findbiometrics.com/japanese-bank-begins-deployment-of-biometric-atms-featuring-nec-tech-609121/ – Date of access: 18.09.2021.
16. 银行业生物识别技术能否引领一个让欺诈无所遁形的未来 [Electronic resource]: - Access mode: www.ctifo-rum.com/news/guandian/578015.html – Date of access: 18.09.2021.
17. 金融业生物特征识别技术应用与风险分析 [Electronic resource]: - Access mode: www.secrss.com /articles/32948 – Date of access: 18.09.2021.
18. Юридические и практические исследования в области технологии распознавания лиц [Электронный ресурс]: - Режим доступа: www.junhe.com/legal-updates/1054 – Дата доступа: 18.09.2021.