**УДК 340**

# ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ В БАНКАХ РЕСПУБЛИКИ БЕЛАРУСЬ

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

*В публикации рассматриваются правовые средства, методы и современные технологии биометрических данных используемых в банковской деятельности Республики Беларусь.*

До XXI века биометрические технологии использовались только для защиты военных, государственных секретов. Со временем биометрия начала применяться в правоохранительной деятельности и надежно укрепилась в такой юридической науке как криминалистика [4]. Чуть позже обстановка начала резко изменяться, так как появилась необходимость в обеспечении безопасности общественных мест (аэропорты, большие торговые центры, и иные крупные места скопления людей), которые снабдили биометрическими системами доступа.

Необходимость в оборудовании спровоцировало яркий всплеск спроса на рассматриваемые технологии, что в дальнейшем привело к множеству новых исследований и разработок в этой сфере.

На территории Республики Беларусь находятся 24 банка. Из них в 2015 году ОАО «Белгазпромбанк», ОАО «Белинвестбанк», а в 2017 году - ОАО «АСБ Беларусбанк», ЗАО «Альфа-Банк» и ЗАО «Банк ВТБ» внедрили подтверждение операций при помощи биометрических технологий Touch ID на базе операционной системы IOS [5]. Touch ID – это характерная функция для смартфонов Apple, которая позволяет с помощью отпечатка пальца разблокировать телефон.

Также с сентября 2019 года в ОАО «АСБ Беларусбанк» была добавлена возможность авторизации по биометрическим данным – с помощью распознавания лица или радужки. Возможность использования данной функции полностью зависит от системы устройства. Для использования такого вида авторизации система должна поддерживать распознавание лица или радужки для авторизации в сторонних приложениях, и версия устройства должна быть на базе Android 9 или выше [1].

Одним из наиболее эффективных для банков и для клиентов финансовых организация является голосовая биометрия, которая была запущена ОАО «Приорбанк» с ноября 2015 года. Подтверждение личности по голосу происходит в два этапа:

– первый этап заключается в регистрации в системе эталона голоса клиента. Создание эталона происходит во время разговора с оператором контакт-центра в фоновом режиме, пока заинтересованное лицо получает консультацию. Если все прошло без ошибок, то эталон голоса сохраняется в базе данных банка, а оператор уведомляет об этом клиента;

– второй этап заключается в том, что при последующих звонках система снова создаёт модель голоса и сравнивает её с эталоном. Результат сравнения появляется на мониторе оператора. Если голосовая аутентификация прошла успешно, оператор может предоставить клиенту необходимую информацию или проводить операции по требованию клиента без запрашивания дополнительной информации о нём.

В период использования голосовой биометрии «Приорбанк» смог выделить для себя много плюсов. Во-первых, клиенту не надо помнить номер паспорта, счетов, договоров и карточек, что существенно облегчило взаимодействие банков с лицами, достигшими пенсионного возраста. Так как раньше оператор мог подтвердить личность только запросив номер паспорта, кода и т.д. И если такие данные не предоставлялись то, оператор сообщал ограниченную информацию, которая бы не касалась данных о счете и операций по нему. Во-вторых, значительно сократилось время разговора, поскольку отпала необходимость подтверждения личности «по знаниям». В-третьих, сократилось время ожидания ответа оператора. Так как 68% обращений клиентов в контакт-центр требуют аутентификации, то сократив продолжительность этого процесса, специалисты «Приорбанка» смогут обслуживать заинтересованных лиц быстрее, тем самым сократив вероятность возникновения очередей на линии.

Еще одним немаловажным плюсом голосовой биометрической технологии является то, что если даже злоумышленник завладеет паспортом другого лица он не сможет получить доступ к данным. При звонке постороннего лица, представившегося другим лицом, система подаст сигнал на монитор оператора контакт-центра о полном несоответствии голосовому эталону. Такому абоненту будет отказано в обслуживании без проверки по знаниям. Паспортные данные потерпевшего ничем не помогут мошеннику. Однако, это работает только при условии наличия голосового эталона в базе данных банка.

Не стоит забывать, что особенности технологии позволяют подтвердить личность клиента по голосу при небольших физиологических отклонениях (небольшая хрипота, заложенность носа, алкогольное опьянение), а также при наличии посторонних шумов. В случае если система все же не подтвердила личность клиента по голосу, оператор контакт-центра предоставит информацию после проверки клиента по знаниям.

Хотелось бы отметить, что для создания голосового эталона требуется выполнение нескольких важных условий. Среди них отсутствие сильных посторонних шумов (гул, эхо, нарушения связи), отсутствие физиологических отклонений в голосе (хрипоты, сильного напряжения голосовых связок, алкогольного опьянения). Также для создания эталона требуется определенная продолжительность звучания голоса клиента, что возможно не при каждой консультации. Кроме того, важно понимать, что для записи и хранения голосового эталона необходимо согласие клиента. В большинстве случаев клиент дает такое согласие, открывая первый продукт в «Приорбанке» и подписывая «Общие условия обслуживания», предусматривающие согласие на создание, хранение и использование биометрических параметров, а именно эталонного отпечатка голоса. Если заинтересованное лицо такой документ не подписывало, то голосовой эталон не будет создан [2].

Публичное акционерное общество «Сбербанк России» также использует голосовую биометрию. Однако в отличии от ранее упомянутого банка он пошел дальше и персонализировал банкоматы. Механизм устройств подстраивается под каждого клиента. В тот момент, когда клиент осуществляет идентификацию, т.е. вставляет карту или прикладывает к бесконтактному банкомату, появляются пункты или разделы, которые формируется на основе недавних проведенных лицом финансовых операций. Банкомат также может поздравить пользователя с днем рождения.

Дети клиентов Сбербанка также могут оплачивать обед в школьной столовой с помощью ладони. Данная функция получила соответствующее название – «Ладошки». Сама процедура происходит следующим образом: карту одного из родителей привязывают к счету ребенка, для доступа к которому предварительно берутся биометрические данные, т.е. отпечаток вен ладони. Инфракрасное излучение проходит сквозь ткани руки и поглощается гемоглобином крови. Примечателен тот факт, что родители могут контролировать, что ест школьник, так как информация о купленных продуктах поступает в профиль одного из родителя и по СМС. Эта функция удобна еще и тем, что клиенты не рискуют потерять денежные средства на карте и саму карту, а также стать жертвой грабителей [3].

Однако, стоит учитывать, что на данный момент не существует 100% защищенных систем, так как всегда будут риски обхода защитных программ, отличается лишь их величина. С каждым днем схемы киберпреступлений совершенствуются, тем самым становясь сложнее, все чаще появляются новые риски и угрозы в информационном пространстве. Только за последний год число банковского мошенничества превысило несколько тысяч. Несмотря на динамичное развитие банковского и кредитно-денежного рынка по защите информации, злоумышленники работают с опережением. Главная причина такого большого количества преступлений – отсутствие механизма многоуровневой системы защиты. Еще одним минусом использования биометрических технологий является индивидуальность информации. То есть при ее утечке заменить такие данные будет невозможно.

Следует понимать, что неосторожное отношение к защите информации для банков, которые собирают биометрические данные может негативно сказаться на их репутации. Так как сбор и хранение персональных данных недостаточны для защиты подобной информации.

Также пострадает и само лицо, данные которого были украдены или сфальсифицированы.

Мы полагаем, что для защиты биометрических данных в Республике Беларусь требуются не только наличие самой информации, но также и подтверждение использования данных путем введения дополнительного пароля или кода, который известен только идентифицируемому. Вдобавок, наличие качественной, специально предназначенной для сбора биометрических данных, техники позволит снизить риск не санкционируемого доступа. Кроме того, необходимо добавить некоторые гарантии для возмещения причиненного вреда банком или не банковской кредитно-финансовой организацией, которая осуществляла сбор, хранение и передачу персональных данных, но не смогла обеспечить защиту доверенной информации, допустив утечку.

Однако нельзя не упомянуть о использовании биометрических технологий в эпоху COVID-19, так как множества систем утратили свой авторитет до распространения вируса. В конце 2020 года Национальный институт стандартов и технологий (NIST) Соединенных Штатов Америки провел исследования о распознавании лиц в условиях масочного режима. В ходе изучения исследователи протестировали 89 алгоритмов на 6 миллионов фотографий в процессе верификации. Результаты же показали, что в 50% случаев система ошибалась и давала сбой [6].

На основе данной проблемы в Российской Федерации было разработано комплексное решение для идентификации по геометрии лица системы контроля и управления доступом (далее – СКУД) под названием – BioSmart Quasar. Рассматриваемое устройство представляет собой инновационный терминал для биометрической идентификации по геометрии лица в СКУД и системах учета рабочего времени. Терминал работает даже в полной темноте, подсветку обеспечивает адаптивная система инфракрасного и белого освещения. Датчик освещенности позволяет автоматически подбирать необходимый уровень освещенности лица. Камера глубины с высокой эффективностью определяет попытки фальсификации системы при помощи цветных фотографий, видео или фото с мобильного телефона. Она представляет собой комплексное решение, состоящее из 3D-ИК-проектора, который проецирует на лицо около 10 тысяч точек,

и высокочувствительной камеры, анализирующей отраженное изображение. На сегодняшний день в терминале Quasar применяется самая передовая технология антиспуфинга. Алгоритм BioSmart построен на основе сверхточных нейронных сетей и эффективно обучен для распознавания лиц разных национальностей. Алгоритм с высокой точностью распознает лица в масках. Отличает даже близнецов благодаря высокому качеству сканирующей оптики, динамическому распределению освещения лица и передовым решениям в области машинного зрения. Для управления доступом могут применяться различные режимы прохода с биометрической идентификацией по лицу и дополнительному идентификатору – карте, цифровому коду, QR-коду. BioSmart Quasar распознает человека в медицинской маске с дополнительной идентификацией по ПИН-коду, QR-коду либо карте, т.е. производит бесконтактную гигиеничную идентификацию (дистанционное распознавание). Дополнительно терминал может быть оборудован высокоточным бесконтактным датчиком для дистанционного измерения температуры. Если в помещение попытается войти человек с температурой тела выше 36,8 °С, датчик сработает и автоматически заблокирует доступ. Погрешность термодатчика – всего 0.2°С [7].

Рассматриваемое устройство может купить любой банк и установить в самом здании. Терминал легко встраивается в любой программный комплекс и интегрируется с устройствами доступа (замки, турникеты, шлюзовые кабины). Сетевой интерфейс терминала работает на скоростях до 1 Гб, имеет гальваническую развязку для защиты от перенапряжений и гроз. Также подключение возможно организовать по беспроводной сети Wi-Fi, имеется беспроводной интерфейс Bluetooth для конфигурирования и настроек терминала через мобильный телефон. Что касается практического применения то технология распознавания лиц Quasar успешно работает в российских и европейских компаниях. В рамках реализации пилотного проекта по использованию Единой биометрической системы терминалы BioSmart Quasar интегрированы в СКУД правительственного комплекса на Пресненской набережной в Москве. Сотрудники министерств, сдавшие биометрические образцы, заходят в здание по биометрии. Терминалы с успехом распознают человека даже в медицинской маске [8]. Такое стремительное развитие инновационных технологий позволяет обеспечивать наиболее эффективную борьбу с COVID-19, снижая риск заражения до минимума.

## ЛИТЕРАТУРА

1. Появилась возможность авторизации в приложении по биометрическим данным! [Электронный ресурс]. – Режим доступа: m-belarusbank.by/poyavilas-vozmozhnost-avtorizacii-v – Дата доступа: 17.09.2021.
2. Контакт-центр Приорбанка [Электронный ресурс]. – Режим доступа: www.priorbank.by/priorbank-main/priorbank-today/contacts/contact-center-voice-biometrics - Дата доступа: 17.09.2021.
3. Банки, которые продвинулись в биометрии [Электронный ресурс] – Режим доступа: finuslugi.ru/navigator/stat_banki_kotorye_prodvinulis_v_biometrii – Дата доступа: 17.09.2021.
4. Колотушкин С. М., Лосева С. Н. Биометрические технологии в правоохранительной деятельности: международный и отечественный опыт / Колотушкин С. М., Лосева С. Н. – Социально-политические науки, 2018. – 1 с.
5. Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: www.belstat.gov.by/upload/iblock/d17/d17cf9f5b0888846924ad77ac181275c.pdf. – Дата доступа: 23.09.2021.
6. Пандемия COVID-19 VS биометрия: вызовы и перспективы [Электронный ресурс]. – Режим доступа: bio-smart.ru/tpost/jpb55eb2nf-pandemiya-covid-19-vs-biometriya-vizovi – Дата доступа: 23.09.2021.
7. BioSmart Quasar [Электронный ресурс]. – Режим доступа: bio-smart.ru/quasar – Дата доступа: 23.09.2021.
8. QUASAR [Электронный ресурс] – Режим доступа: biosmartquasar.tech – Дата доступа: 23.09.2021.