

## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ЦИФРОВАЯ ЭКОНОМИКА

УДК 658

### ПРОБЛЕМЫ РАЗВИТИЯ БИОМЕТРИИ КАК ОСНОВЫ ЦИФРОВИЗАЦИИ ОТЕЧЕСТВЕННОЙ ЭКОНОМИКИ И ПУТИ ИХ РЕШЕНИЯ

*Бутов Александр Владимирович (a.v.butov@yandex.ru)  
Российский экономический университет им. Г.В. Плеханова  
Карякин Александр Михайлович*

*Ивановский государственный энергетический университет им. В.И. Ленина*

**Состояние вопроса:** Ускорение процесса распространения цифровизации в РФ во многом зависит от успехов в формировании Единой биометрической системы (ЕБС), создании инфраструктуры для сбора, хранения и передачи биометрических данных, разработки продуктов и услуг, основанных на биометрической идентификации пользователей. Система формирования ЕБС, основанная на сборе и использовании данных только в банковском секторе замедляет развитие биометрии и требует ее распространения на другие сферы деятельности, в т.ч. на предприятия транспорта, госуслуг, торговли и ресторанного бизнеса и т.д.. Изучению этой проблемы в целях разработки рекомендаций по ее решению и посвящена представленная статья.

**Материалы и методы:** Исследование проведено на основе использования методов широкомасштабного сбора данных, бенчмаркинга, анализа и синтеза полученной информации, разработки рекомендаций по решению представленной проблемы,

**Результаты:** В результате проведенного исследования были определены факторы, сдерживающие сбор биометрических данных, включая: - капиталоемкий процесс сбора данных, требующий значительных затрат на организацию сбора данных, оснащение оборудованием и программным обеспечением, обучение персонала; - отсутствие доверия граждан к этому способу идентификации личности, неверие в надежность хранения личных данных ни в государственных учреждениях, ни в частных компаниях; - незаинтересованность банков в передаче биометрических данных своих клиентов в ЕБС, доступную для всех кредитных организаций. Также в статье разработаны конкретные предложения по ускорению распространения биометрии в различных отраслях и сферах деятельности.

**Выводы.** Для ускорения наполнения базы данных ЕБС необходимо: -убедить граждан в безопасности и надежности системы ЕБС путем публикации данных об используемых решениях и их эффективности с указанием показателей FAR и FRR и условий их получения; -наличие команды профессионалов-консультантов для обслуживания, анализа и принятия оперативных решений при сбоях и ошибках в работе системы ЕБС; -расширение мест сбора и применения биометрии не только в банковском секторе, но и за его пределами в других отраслях и сферах деятельности: -разработка новых продуктов и услуг, доступных с помощью базы ЕБС.

**Ключевые слова:** Единая биометрическая система, цифровизация, идентификация, конфиденциальность, безопасность, защита данных, имидж, резервирование.

**Введение.** Создание Единой биометрической системы (ЕБС) - основа государственной программы цифровизации отечественной экономики. Это важнейшая база данных для широкого использования в любой сфере – в медицине, банковской деятельности, на транспорте, в системе предоставления госуслуг и т.д. [1, с.18]. После сдачи биометрических данных любой гражданин может пользоваться услугами коммерческих организаций и государственных учреждений без личного присутствия. Но ее формирование продвигается крайне медленно. Выявлению проблем, связанных со сбором использованием биометрии и посвящена представленная статья.

Единая биометрическая система — цифровая платформа для дистанционной биометрической идентификации граждан. Инициатором ее создания выступили ЦБ и Минкомсвязь, разработчиком и оператором является «Ростелеком». На первом этапе реализации программы

предполагалось, что банки соберут биометрические данные клиентов для базы ЕБС и с помощью биометрии будут предоставлять ограниченный перечень финансовых услуг, включая открытие счетов и вкладов, денежные переводы, выдачу кредитов, а затем значительно расширят спектр этих услуг.

Сбор биометрических данных граждан начался в июле 2018 года в 400 отделениях девяти российских банков. С тех пор число кредитных организаций, собирающих биометрию, выросло до 172, в состав которых входит уже более 10 тыс. отделений (рис.1). Но до сих пор рост числа точек сбора биометрических данных не привел к существенному наполнению базы ЕБС. По данным ЦБ, в ней собрано только 30 тыс. слепков, что свидетельствует о крайне низкой заинтересованности граждан и банков в процессе ее создания [2, с.10]. Причины кроются в отсутствии преимуществ и бонусов от участия в этой программе, отсутствии ее реклам-

ной кампании, а также в ограниченных возможностях использования базы ЕБС и высоких рис-

ках для населения.



**Рисунок 1. Характеристики системы сбора биометрических данных в РФ**

В августе 2018 года ЦБ представил перечень угроз конфиденциальности информации ЕБС, к которым отнес следующие их виды: доступность данных при их блокировке и передаче, сохранность данных в случае их подмены или удаления и конфиденциальность данных клиентов. Сегодня продажа «цифровых личностных данных» — это процветающий хакерский бизнес. Люди, пострадавшие от их похищения, сообщают, об открытых на их имя кредитах, обремененных долгами компаниях, проданных без их ведома квартирах и т.п. [3].

В настоящее время существуют две основные метрики обнаружения ошибок биометрической идентификации - FAR, определяющей ошибки ложного обнаружения и FRR, регистрирующая ошибки ложного не обнаружения. В первом случае, система подтверждает, что человек, проходящий идентификацию, именно тот, за кого он себя ложно выдает, а во-втором, система не распознает человека, хотя его биометрические данные есть в базе. Показатели FAR и FRR не всегда раскрываются производителями оборудования, в т.ч. для формирования ЕБС. А те, кто раскрывает эти показатели имеет широкие возможности выбора способов тестирования:

- во-первых, самостоятельно провести тесты и опубликовать их;
- во-вторых, провести тестирование публично, но и здесь есть возможность выбора под свой алгоритм «удобной» базы данных, показывающей высокие результаты, недостижимые в реальных условиях эксплуатации оборудования;
- в-третьих, участие в открытых конкурсах (MegaFace и т.п.), где результаты более надеж-

ны, но и здесь есть возможность подстроиться под методику тестирования;

- в-четвертых, самый надежный способ - проходить тестирование в независимых организациях (например, в американском институте стандартов и технологий NIST). Но даже NIST не раскрывает какие базы данных для тестирования он использует-паспортные фото, любительские фото и т.д., что может привести к ошибкам при идентификации.

Кроме того, в AppStore и Google Play можно скачать приложение Deepfake, чтобы создать цифрового двойника любого известного человека. Но как утверждает бизнес-консультант по безопасности Cisco Systems А. Лукацкий: «есть и более серьезные проекты, когда можно создать полноценную цифровую копию нужного вам человека, который говорит и движется так, как «жертва», у него та же мимика» [8, с.34]. И это серьезная угроза для всех биометрических систем до сих пор еще не решена.

Поэтому сейчас у граждан просто нет стимулов для сдачи биометрии, поскольку высоки риски ее использования, а также мало продуктов и услуг, предоставляемых с помощью ЕБС: лишь немногие банки дистанционно предоставляют услуги для клиентов, сдавших данные в ЕБС. В настоящее время используют данные ЕБС только 5 банков: Промсвязьбанк, Почта-банк, ХКФ-банк, Совкомбанк, Тинькофф-банк, из которых только первые два предлагают все опции - открытие счетов и вкладов, выдачу кредитов, переводы [2, с.10].

Банки тоже не спешат расширять линейки за счет продуктов, формируемых через ЕБС. Пока нет спроса на такие сервисы, банки не хотят нести значительные затраты по сбору

биометрии и предоставлению продуктов с ее использованием. Банки, которые все же предлагают продукты через ЕБС, делают это в рекламных или имиджевых целях. Реальных стимулов нет не только у граждан, но и у банков. Единственная льгота, которую на данный момент предложил банкирам ЦБ, — это снижение ставок по резервированию кредитов, выданных с использованием ЕБС [3]. Но банкиры явно не оценили предложенных регулятором выгод. Экономия на резервах для банков не окупит уже понесенные расходы на организацию процесса сбора биометрии и будущие расходы на встраивание биометрической идентификации в дистанционные каналы продаж [4, 9].

Ошибкой регулятора стало принятое им решение по организации сбора биометрии только через банковскую систему. К факторам, сдерживающим сбор биометрических данных, следует отнести:

- ресурсоемкий процесс сбора данных, требующий значительных затрат на организацию сбора данных, оснащение оборудованием и программным обеспечением, обучение персонала;

- люди все еще не доверяют такому способу идентификации личности, т.к. не верят в надежность хранения их личных данных ни в государственных учреждениях, ни в частных компаниях;

- клиенты, сдавшие биометрические данные в ЕБС, становятся доступны для всех кредитных организаций, что неизбежно увеличит стоимость их удержания для банка.

Банкам гораздо интереснее развивать собственные базы биометрических данных, направленных на развитие внутренних сервисов и удержание клиентов, чем наполнять единую базу ЕБС. Позицию Сбербанка и всего банковского сообщества по данному вопросу однозначно выразил его глава Герман Греф на встрече со студентами Новосибирского государственного университета: «Мы и другие финансовые учреждения в первую очередь имеем значительно выше уровень биометрии, Биометрия — это одна из конкурентных вещей. Ее нельзя ни в коем случае монополизировать. Государство никогда не будет конкурентоспособным в этом» [2, с.10].

На фоне отсутствия заметного энтузиазма в сборе биометрических данных и их применении, регулятор обязал все банки с генеральной лицензией предоставлять основные виды банковских услуг физлицам, включая открытие счетов и вкладов, переводы, выдачу потребительских кредитов, дистанционно через Единую биометрическую систему с 2020 года. Для банков с базовой лицензией такая обязанность будет введена с 2021 года.

Следует отметить, что далеко не все банки медленно внедряют новые продукты и услуги с использованием ЕБС. Ведь очевидно, что сбор

биометрии приносит банкам не только дополнительные расходы, но и ощутимые преимущества - позволяет не только ускорить идентификацию и скорость обслуживания клиентов, но повысить безопасность. Так, сбор фотобиометрии улучшает узнаваемость клиентов, снижает риски обращения в банк с поддельным паспортом. Например, при открытии вклада помимо копии паспорта берется также фото клиента, чтобы при повторных обращениях операторист видел, как выглядит клиент. В данном случае фотобиометрия является дополнительным подтверждением личности клиента наряду с паспортом, т.к. она не позволяет точно идентифицировать личность клиента. Кардинальное решение — сбор комплекса биометрических данных для точной идентификации клиента, когда паспорт в банке уже не понадобится. Главный управляющий директор «Альфа-банка» В. Верхошинский заявляет, что банк переведет 20% отделений к 2021 году на обслуживание клиентов без паспортов. В этих отделениях для распознавания клиента потребуются только его биометрические данные и смартфон [6, с.33].

Понимая ограниченность предоставляемых в настоящее время финансовых продуктов с использованием биометрии банки предлагают все новые виды услуг. Так, банк «Русский стандарт» совместно с «Ростелекомом» предоставил клиентам возможность оплаты товаров «лицом». Для оплаты без кошелька, банковской карты или гаджета пользователям необходимо сдать биометрические данные в ЕБС, затем привязать свою платежную карту в мобильном приложении, которое поддерживает функцию «оплата по лицу» (например, в приложении «Биометрия» от «Ростелекома») к своему цифровому образу и затем осуществлять эти платежи через Систему быстрых платежей. Система платежей «лицом» очень привлекательна для всех участников, т.к. сокращает процесс оплаты с традиционных 15 сек. до 5 сек. В настоящее время система «оплаты лицом» уже работает в качестве пилотного проекта: в кофейнях CofeBean по ней можно оплатить покупки и как уверяет председатель правления банка «Русский стандарт» А. Самохвалов: «Мы планируем подключить к биометрическому платежу около десятка новых клиентов в конце 2019-начале 2020 года» [6, с.34].

Совершенствуя качество обслуживания клиентов банки, предлагают новую инновационную услугу-обслуживание через банкоматы с идентификацией по лицу. В Сбербанке для того, чтобы банкомат узнал клиента по лицу необходимо сдать биометрию во внутренней биометрической системе Сбербанка, нажать клавишу «Обслуживание по биометрии», а потом с помощью банковской карты получить специальный биометрический код. В дальнейшем

для пользования банкоматами потребуются только лицо и код клиента.

В качестве примера для дальнейшего развития биометрии в кредитных организациях можно привести опыт Китая, где банкоматы уже превратились в мини-офисы: они не только умеют узнавать клиентов по лицу, но и через них можно открыть вклад, выпустить карту, купить акции и облигации, оформить кредит и даже получить онлайн-консультацию специалиста во время совершения операций. Это самое перспективное направление развития банковской сферы, но оно имеет ряд ограничений: во-первых, такой банкомат в десять раз дороже обычного банкомата и во-вторых, использование таких устройств потребует от банков создания специальной группы высококвалифицированных консультантов, а также кардинальной перестройки операционной деятельности [6, с.35].

К сбору данных и их применению следует также подключить нефинансовые организации и госструктуры. Прежде всего, для быстрого масштабирования технологии использования биометрии необходимо поручить МФЦ собирать биометрические данные через собственную инфраструктуру. И ЦБ уже работает над этим: такая опция скоро появится в МФЦ Москвы и Московской области, а в дальнейшем может быть масштабирована на всю страну [4].

Также в процесс сбора данных в ЕБС уже вовлечена «Почта России» через расположенные в ее отделениях офисы Почта-банка. Пока необходимым оборудованием оснащено только одно отделение в Москве, но до конца 2019 года банк начнет масштабирование проекта в более чем 240 почтовых отделениях [5].

Применение биометрии не должно ограничиваться лишь банковским сектором. Важно, чтобы другие отрасли и сектор госуслуг тоже подключились к процессу и люди могли с помощью биометрического шаблона получить многочисленные, продукты, услуги и сервисы. Сейчас обсуждается возможность применения биометрических технологий для идентификации граждан при покупке билетов на общественном транспорте, в электричках и поездах, в аэропортах. Также рассматривается возможность сбора и использования биометрических данных для идентификации граждан в МФЦ, использования биометрии лица для подтверждения возраста при онлайн-торговле алкоголем. С использованием биометрии появилась возможность автоматизировать выдачу пропусков и билетов на любые мероприятия и в различные учреждения. Достаточно посмотреть в камеру видеонаблюдения и приложить к сканеру ладонь-система сама идентифицирует личность посетителя и его место в списке приглашенных. Данную систему идентификации посетителей уже протестировали участники Форума

финансовых технологий, прошедшего в октябре 2019г. [7, с.35].

Все это вселяет уверенность в том, что соотечественники скоро оценят преимущества биометрических платежей без смартфонов, карт и паспортов несмотря на то, что запуск новых биометрических сервисов потребует времени и технической доработки существующей инфраструктуры. Совершенно очевидно, что решить технологические вопросы гораздо проще, чем создать для людей условия, при которых они будут уверены в защищенности своих интересов и начнут доверять государству и бизнесу использование собственных биометрических данных.

**Выводы.** Для ускорения наполнения базы данных ЕБС необходимо:

- убедить граждан в безопасности и надежности системы ЕБС путем публикации данных об используемых решениях и их эффективности с указанием показателей FAR и FRR и условий их получения;
- наличие команды профессионалов-консультантов для обслуживания, анализа и принятия оперативных решений при сбоях и ошибках в работе системы ЕБС;
- расширение мест сбора и применения биометрии не только в банковском секторе, но и за его пределами в других отраслях и сферах деятельности,
- разработка новых продуктов и услуг, доступных с помощью базы ЕБС.

Без принятия перечисленных мер ЕБС так и останется экспериментом ЦБ и Минкомсвязи, невостребованным гражданами.

### Литература

1. Бутов А.В. Достижение и последствия четвертой промышленной революции Вестник Российского экономического университета им. Г.В. Плеханова. 2019. № 4 (106), с. 17-22.
2. Мануйлова А. Биометрия застряла в банках. Коммерсант, №171 от 20.09.19, с.10.
3. Биометрический тоталитаризм [Электронный ресурс] // Режим доступа: <https://versia.ru/iniciirovav-sbor-bankami-biometricheskix-dannyx-rossiyan-german-gref-otkryl-yashhik-pandory> (дата обращения 18.01.2020).
4. Как работает Единая биометрическая система [Электронный ресурс] // Режим доступа: <https://habr.com/post/424751/> (дата обращения 18.01.2020).
5. В отделениях почты начали собирать биометрические фото и записи голоса [Электронный ресурс] // Режим доступа: <https://banki.ru/news/bankpress/?id=10906040> (дата обращения 18.01.2020).

6. Горячева В., Джафаров Э., Жданов А. Плати лицом. - Коммерсант Деньги №52 от 20.11.19, с.33-35
7. Беров И. Биометрия в иных областях. - Коммерсант Деньги №52 от 20.11.19, с.35.
8. А.Лукацкий. Мне нужны твоё лицо, голос и ключи от квартиры. - Коммерсант Деньги №52 от 20.11.19, с.34.
9. Khachatryan M.V., Klicheva E.V., Velikorossov V.V. Digital Mechanisms of Development of Possessory Risk Management Systems under New Economic Conditions // 2019 International Conference on Politics, Economics and Management (ICPEM 2019). - p. 6-10.

УДК 681.5

## АНАЛИЗ ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В РАБОТЕ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

*Грачёв Виталий Эдуардович (gra4yow.vital@yandex.ru)*

*Сизова Ольга Владимировна*

*Ивановский государственный химико-технологический университет*

В работе проведен анализ применения одной из современных информационных технологий хранения данных – блокчейн в работе медицинских учреждений. В ходе анализа были выделены основные системы управления базами данных, применяемые в медицинской отрасли. Была выделена наиболее распространенная СУБД, доля которой составляет более 50%. При проведении сравнительного анализа традиционных способов хранения данных с технологией блокчейн, были проанализированы новейшие разработки компании зарубежных стран, внедривших блокчейн в сферу здравоохранения. Сравнение проводилось по таким параметрам, как: полномочия, архитектура, обработка данных, неизменность, прозрачность, стоимость и производительность. Проведенный анализ позволил выявить основные сферы применения, в которых преимущества технологии блокчейн являются наиболее важными. Также в работе рассмотрены основные различия традиционных баз данных, гибридного блокчейна и обычного блокчейна. По результатам анализа были сделаны выводы о возможностях и преимуществах внедрения технологии блокчейн в работу российских медицинских учреждений.

*Ключевые слова:* технология блокчейн, медицинские учреждения, системы управления базами данных, традиционные способы хранения данных, гибридный блокчейн, защита данных.

### *Введение*

Одной из главных составляющих долгой жизни человека является его здоровье. Поддерживать его помогают медицинские учреждения, в деятельность которых необходимо внедрять надежные и современные технологии для ускорения процессов излечения пациентов. Однако, медицинская отрасль не спешит внедрять передовые технологии в свои организации. Парадокс отторжения современных технологий при наличии в своих «рядах» самых умных и образованных людей во всем мире обусловлен наличием большой опасности при неверном выборе новой медицинской технологии. От правильного выбора зависят множество жизней пациентов.

На наших глазах эпоха индустриального общества сменяется эпохой информационных технологий, когда человечество переходит на новый этап развития - информационный. Информация стала стратегическим ресурсом общества, а совокупность знаний стала решающим фактором развития любой страны.

Медицинские организации хранят большое количество сложной информации. Для того, чтобы работа сотрудников медицинских учреждений была слаженной, важно систематизировать все данные, которые обрабатывают работники. Такую работу более десятка лет вы-

полняют системы управления базами данных [1].

С прогрессом технологий растет необходимость улучшения защиты всех данных пользователя. Традиционные системы защиты могут обеспечивать сохранность важных данных еще какое-то время, однако в области здравоохранения к вопросу защиты следует подходить наиболее осторожно. В такой отрасли, как медицина, подмена данных является опасным явлением, от которого могут пострадать пациенты. В настоящее время технология блокчейн зарекомендовала себя, как одна из самых надежных систем сохранности данных пользователей.

Blockchain - это криптографически защищенная, публичная и распределенная база данных [2]. Технология блокчейн изначально разрабатывалась для биткоина, однако она может быть использована для любого другого вида записи данных. В технологию блокчейн изначально заложена безопасность на уровне базы данных. Концепцию цепочек блоков предложил в 2008 году Сатоши Накамото (Satoshi Nakamoto).

*Анализ существующих баз данных в медицинской отрасли*

Изучая историю развития медицинских информационных систем, можно сказать, что за 20 лет своего существования они развивались