Аналитическая записка команды

«Экономическая безопасность СФУ»

(Сибирский федеральный округ)

«Удаленная идентификация на основе биометрических данных»

Авторы:

Серова Кристина Сергеевна – Капитан (Сибирский федеральный университет, Институт экономики управления и природопользования; KristinaSerova7@gmail.com)

Колмакова Юлия Эдуардовна – участник (Сибирский федеральный университет, Институт экономики управления и природопользования; JulKolmakova@yandex.ru)

Курьянов Константин Евгеньевич – участник (Сибирский федеральный университет, Институт экономики управления и природопользования; wildcare62@gmail.com)

Козлова Светлана Александровна – тренер (Сибирский федеральный университет, Институт экономики управления и природопользования; svekozlova@sfu-kras.ru)

ВВЕДЕНИЕ

Высокий темп жизни ведет к ужесточению тайм-менеджмента члена современного общества. У людей с каждым годом становится всё меньше и меньше свободного времени. Следствием этого является развитие и интеграция систем удаленного взаимодействия между потребителями и создателями материальных благ. Финансовые организации также следуют этой тенденции. Удаленный доступ к банковским продуктам или «цифровой банкинг», в том или ином виде, представлен всеми финансовыми организациями Российской Федерации и большинством финансовых организаций мира. [1]

В кейсе «Удаленная идентификация на основе биометрических данных» рассмотрена ситуация хищения денежных средств с банковского депозита при помощи обмана системы идентификации пользователя цифрового банкинга. Особенностью данной ситуации является то, что для идентификации и аутентификации пользователя, банк при помощи своего приложения или сайта использовал анализ биометрических данных (БД) клиента. То есть брал образец БД на анализ и сравнивал с образцами, полученными от клиента в ходе очной сдачи БД.

Цель нашего исследования – определение вероятности наступления событий, описанных в кейсе, в будущем, а также действий, которые должны предпринять стейкхолдеры для снижения данной вероятности.

Считается, что обмануть системы идентификации с помощью БД сложнее, нежели привычные нам системы идентификации с помощью пароля или чип-ключа, однако, полностью обеспечить защиту от несанкционированного доступа, по крайней мере, на данный момент даже метод идентификации по БД не позволяет. В предложенном кейсе, как возможный канал кражи БД, рассматривается видеозапись, на которой герой снимает свое лицо и произносит поздравительную речь. Гипотетически, если видеозапись достаточно высокого качества, существует вероятность обмануть используемые сейчас системы идентификации и аутентификации, просканировав запись лица или голоса. [9] Что, вероятно, и произошло в рамках рассматриваемой ситуации.

Актуальность данного кейса, обуславливается высокой вероятностью наступления событий, описанных в нем. Аналогичные ситуации имеют место быть уже сегодня. Рассматривая статистику, приведенную в обзоре несанкционированных переводов денежных средств за 2018 год, проведенным Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), обратим внимание на то, что из всех несанкционированных операций, совершенных с использованием платежных карт, эмитированных на территории Российской Федерации, в 2018 году, объем которых

составил 1384,7 млн рублей, 1077,5 млн рублей приходится на несанкционированные транзакции типа «Card Not Present» (CNP) – один из видов операций по платежной карте с помощью передачи её реквизитов (без предъявления ее материального носителя), то есть именно на операции, проводимые с помощью системы цифрового банкинга. Осуществляется смещение интересов злоумышленников в сторону осуществления незаконной деятельности с помощью CNP-транзакций – «С учетом развития финансовых услуг, совершаемых через сеть Интернет без предоставления карты, мы прогнозируем сохранение восходящего тренда миграции несанкционированных операций в CNP-среду», говорится в обзоре ФинЦЕРТ. [8]

ОСНОВНАЯ ЧАСТЬ

На данный момент, использование биометрических данных для идентификации личности (БИ) реализуется банками, в большинстве случаев, для удаленной идентификации клиента, то есть банковскими интернет-сервисами. Следовательно, для анализа ближайшей перспективы развития рынка БИ целесообразно рассматривать дальнейшее повышение спроса на использование данного метода идентификации на рынке интернет-банкинга.

Сфера отечественного цифрового банкинга развивается медленнее, чем за рубежом. В исследовании Internet Banking Rank, проводимым агентством Markswebb каждый год, рынок российского цифрового банкинга рассматривается с точки зрения бизнес-моделей Daily Banking и Digital Office, так как данные модели получили большее распространение в России. [22]

Модель Digital Office предлагает более широкий спектр услуг, нежели просто возможность следить за состоянием счета, как это реализуется в Daily Banking. Из понятия «Цифровой офис» становится ясно, что при использовании данной модели клиент не будет нуждаться в посещении отделений банка, ему будет необходимо лишь идентифицировать себя в системе, и он сможет использовать весь спектр банковских услуг через интернет.

Исходя из этого, можно говорить о перспективах развития системы БИ, в большей мере, в части рынка цифрового банкинга, представленной именно моделью Digital Office. Агентство Markswebb в ходе исследования составило топ кредитных организаций по уровню развития цифрового банкинга. Из представленных по всей территории РФ — это Тинькофф Банк, Райнффайзенбанк, Сбербанк и Альфа-Банк.

Развитие цифрового банкинга ведет к необходимости повышения уровня защиты от несанкционированного доступа. Системы идентификации и аутентификации на основе БИ

являются перспективным направлением для разработок и инвестирования средств банками как в России, так и за рубежом.

Например, Lloyds Banking Group plc, крупный британский банк, заключил партнерское соглашение с Microsoft, чтобы предложить своим клиентам новый способ доступа к своим учетным записям с устройств Windows 10 – через распознавание отпечатков пальцев или лиц. [24]

KB Kookmin Bank предлагают в своем основном мобильном приложении разнообразные формы биометрической аутентификации, включая сканирование радужной оболочки, а также распознавание пульса и голоса; [23]

Australia and New Zealand Banking Group (ANZ) разработали Voice ID с ведущей в мире голосовой биометрической компанией Nuance. С помощью Voice ID клиенты ANZ теперь могут совершать платежи на сумму более 1000 долларов США на своем мобильном телефоне. [19]

Положительные примеры реализации систем БИ в зарубежных кредитных организациях стимулируют отечественные банки инвестировать в инновации. Ярким примером может служить Тинькофф Банк, лидер цифрового банкинга в России, в связи со спецификой организации своей деятельности (все банковские операции проводятся онлайн, без посещения отделений) в отчете о деятельности и перспективах развития говорит о БИ, как о приоритетном направлении развития систем идентификации клиентов. [14] В свою очередь Сбербанк России инвестировал более 450 миллионов рублей в акции компании VisionLabs (входит в топ-3 по точности FaceID в мире) с целью развития и поддержки систем БИ в своих приложениях. Так же другие, менее крупные банки подвержены тенденции внедрения БИ в свою деятельность. [10]

Как часто бывает с инновациями, обыватели, то есть среднестатистические клиенты финансовых организаций, скептически относятся к нововведениям, тем более в сфере безопасности личных денежных средств. В связи с введением систем удаленной идентификации с помощью БД, информационно-правовой портал «Гарант.ру» [2] провел опрос читателей об их намерении использовать услугу удаленной идентификации на основе БД (См. Приложение А). По результатам опроса можно сделать вывод, что большая часть респондентов (44% опрошенных) отрицательно относятся как к сбору БД, так и их использованию в сфере цифрового банкинга, 27% респондентов не знали о данном новшестве, 18% хотели бы воспользоваться, но рядом с их местом жизненных интересов нет организаций, предлагающих данную услугу, и лишь 11% опрошенных уже активно используют систему идентификации на основе БД. Из результатов данного опроса можно

сделать вывод о недостаточном информационном освещении введения инновационной системы удаленной идентификации на основе БД, так как почти треть респондентов не слышали о ней, а также почти половина относится к ней отрицательно в виду того, что, по нашему мнению, недостаточно осведомлены о повышении степени защиты данных по сравнению с традиционно используемыми системами идентификации по PIN или чип-ключу.

Так как пользователи системы «Гарант.ру», в большинстве своем, это специалисты в областях экономики или права, мы решили провести собственный, менее репрезентативный опрос, показывающий отношение к идентификации на основе БД студентов как экономических, так и других специальностей.

В опросе приняло участие 208 студентов разных специальностей СФУ (См. Приложение Б). Так, 52% опрошенных обучаются на специальности не связанной с экономикой; 67% – используют идентификацию по БД в повседневной жизни; 63% используют БД для доступа к банковским продуктам; 61% респондентов относятся к сбору БД банками положительно, а 10% – нейтрально; 57% опрошенных студентов считают безопасным БИ и 9% – затрудняются ответить на этот вопрос. Так как студенты – это экономически активное население, которое идет в ногу со временем и с интересом принимает инновации, мы считаем, что в скором будущем предрассудки по поводу небезопасности идентификации на основе БД и нежелание людей сдавать свои БД сойдет на нет. Особенно быстро развиваться начнет тенденция на использование БИ после окончательного закрепления всех аспектов использования БД в нормативной базе.

АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ

В ходе анализа нормативно-правовой базы по проблеме (См. Приложение В) было дано понятие персональным биометрическим данным (ПБД) и перечислены сведения, относящиеся к ним. Так же было рассмотрено законодательство, регулирующее сбор, обработку и хранение ПБД граждан РФ в банковских организациях (См. Приложение Г). ПБД в ФЗ №152-ФЗ рассматриваются как часть ПД поэтому, ответственность за их нарушение наступает в соответствии с этим законом.

С 30 июня 2018 года в РФ в соответствии с Федеральным законом от 31.12.2017 №482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» заработала система удаленной идентификации с использованием биометрических данных. Согласно данным с официального сайта Центрального банка «удаленная идентификация – это механизм, позволяющий физическим лицам получать

финансовые услуги дистанционно, подтвердив свою личность с помощью БПД (изображение лица и голос) в любом банке». [16]

Для осуществления гражданином своего права на получение банковских услуг удалённо с использованием БИ, ему необходимо пройти первичную идентификацию в одном из банков, который соответствует критериям, установленным пунктом 5.7 статьи 7 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». [3] Полученная информация хранится в Единой системе идентификации и аутентификации (ЕСИА) и Единой биометрической системе (ЕБС). Персональные данные хранится в ЕСИА, биометрические — в ЕБС. Связка между системами осуществляется по технологическому идентификатору ЕСИА.

В связи с эти Минкомсвязь РФ как орган, осуществляющий регулирование в сфере идентификации граждан РФ на основе БПД, разработала приказ, определяющий порядок обработки (включая сбор и хранение) параметров БПД, порядок их размещения и обновления в ЕБС.

В Указаниях Банка России от №2 4859-У/01/01/782 содержится перечень угроз информационной безопасности, который банки учитывают при сборе, использовании и передаче БПД своих клиентов (См. Приложение Д). Основные угрозы, присутствующие почти на всех этапах сбора использования и передачи БПД, это:

- угроза нарушения целостности (подмены, удаления);
- нарушения достоверности БПД;
- угроза нарушения конфиденциальности (компрометации).

В случае с Е. Амбразоровым, банком не была устранена угроза нарушения достоверности БПД при обработке и проверке БПД, а также обработке и передаче информации о степени соответствия в ЕБС, что привело к известным печальным событиям.

Для устранения этих угроз Минкомсвязь РФ разработала Приказ от 21.06.2018 №307, содержащий методику о степени соответствия предоставленных БПД физического лица его БПД, содержащимся в единой информационной системе ПД. В приказе утверждены формулы определения степени взаимного соответствия указанных данных и установлено значение степени взаимного соответствия (не менее 0,9999). [12]

Так же ЦБ РФ 14.02.2019 были утверждены методические рекомендации №4-МР. В ст. 1.3 данных рекомендаций [7] говорится об обеспечении банками защиты информации при использовании ЕБС с применением средств криптографической защиты информации, имеющих подтверждение соответствия требованиям, установленным ФСБ России (СКЗИ),

разработанных и эксплуатируемых в соответствии с Положением, утвержденным Приказом ФСБ России от 09.02.2005 №66.

На данный момент, в мире нет отдельных законов о БД, и они обрабатываются в соответствии с законами, написанными для ПД. От страны и традиций, заложенных в ней, зависит отношение граждан к ПД. Так для стран Евросоюза с 25 мая 2018 года вступил в силу единый закон о защите ПД (General Data Protection Regulation, GDPR), принятый в 2016. Данный закон объединяет и ужесточает существовавшие до него нормы, защищающие ПД. Например, GDPR закрепляет право субъекта ПД в любой момент отозвать своё согласие на сбор и обработку своих ПД. Этот принцип называется «право быть забытым». В то же время, санкции за нарушение требований GDPR могут составлять до 20 миллионов евро или 4% от мирового годового оборота за серьёзные правонарушения (например, за несоблюдение принципов защиты данных). [21]

В США не существует единого всеобъемлющего федерального закона, регулирующего сбор и использование ПД в целом или БД в частности. Вместо этого в стране существует система лоскутных федеральных законов и законов штатов, которые иногда могут накладываться или противоречить друг другу. Жесткое законодательство относительно биометрии существует только в трех штатах: Иллинойсе, Техасе и Вашингтоне. [20]

Пока США и страны Евросоюза пытаются защищать ПД своих граждан, в Китае продолжается разработка системы социального кредита. Планируется, что к 2020 году у каждого гражданина Китая будет свой социальный рейтинг, от которого будут зависеть доступные ему услуги. Например, если вы не платите по счетам или слишком громко включаете музыку в поезде — вы можете потерять определенные права, такие как бронирование билета на самолет или поезд. [25]

«В России, где правовая система только складывается, выбран путь схожий с европейским. Законодательство построено по европейской модели. Поэтому нам нужно идти по пути улучшения защищенности персональных данных пользователей. Privacy должно однозначно соблюдаться по умолчанию». [6]

ОПИСАНИЕ ИНТЕРЕСОВ СТЕЙКХОЛДЕРОВ

Качество регулирования любой сферы общественных отношений зависит от грамотного урегулирования интересов всех заинтересованных сторон. В предложенной ситуации необходимо учитывать интересы следующих групп:

«Граждане» – в кейсе к данной группе относятся: Евгений Амбразоров, его коллеги. Взаимодействует со следующими группами: «Государство» (Взаимодействие носит исторический и юридический характер), «Кредитная организация» (Взаимодействие носит добровольный и договорной характер). Граждане заинтересованы в принятии мер, повышающих безопасность хранения и использования биометрических данных для удаленной идентификации, так как от этого зависит сохранность денежных средств, находящихся на банковских счетах.

«Кредитные организации» – к данной группе относится банк, в котором открыт счет у Евгения Амбразорова. Взаимодействуют со следующими группами: «Граждане», «Государство» (Играет роль регулятора деятельности). Банки заинтересованы в надежной защите биометрических данных клиента, т.к. от этого зависит уровень доверия клиентов, а соответственно и прибыль банка.

«Государство» – в условиях данного кейса под государством понимается Центральный банк. Взаимодействуют со следующими группами: «Граждане», «Кредитная организация». Государство, выполняя функции регулятора, заинтересовано в минимизации мошеннических операций, т.к. это подрывает доверие к финансовой и банковской сфере страны.

Более подробно взаимодействие и мотивация сторон поясняется в приложении (См. Приложение Е)

При анализе ситуации были выявлены следующие проблемы, а именно: На уровне государства – проблема нарушения прав и свобод граждан. На уровне финансовых институтов – проблема защиты персональных данных и средств на счетах клиента. Нарушение прав гражданина (на примере Е. Амбразорова) – проблема нарушения конфиденциальности персональных данных и потеря денежных средств.

Данные проблемы были рассмотрены с позиций интересов всех сторон и нами были разработаны следующие **решения**:

1. **Защита фото-, видео- и аудио-материалов в интернете цифровыми знаками.** Для реализации данных мер необходимо обязать все Интернет-ресурсы при публикации фото-, видео- и аудио-материалов, содержащих биометрические данные пользователя (распознается автоматически), наносить на них специальные цифровые знаки. Также при просмотре публикации каждый пользователь автоматически наносит свой уникальный цифровой знак, сгенерированный программой при регистрации на ресурсе. «След» такого рода невозможно увидеть невооружённым глазом, он не станет помехой для просмотра/прослушивания материалов. Так же реализация данных мер позволит

значительно сузить круг подозреваемых в мошенничестве, если оно все-таки имело место быть.

Данные меры затруднят использование биометрических данных, найденных мошенниками в сети Интернет, и получение несанкционированного доступа к персональным данным и банковским счетам граждан.

Плюсами данного решения являются: Относительно небольшие финансовые затраты на реализацию; Простота административного регулирования; Возможность оперативного введения; Отсутствие необходимости вовлечения пользователей в реализацию.

Слабыми местами является то, что интернет-сфера слабо поддается регулированию. Высокий риск нарушения требований защиты данных со стороны интернет-сайтов; Мошенники могут получать доступ к материалам с фейковых аккаунтов, тем самым делая свой след бесполезным; Появление системы, наносящей цифровые знаки на материалы, приведет к немедленному началу разработки приложений по «очистке» данных; Возможность общественного недовольства повышением государственного контроля в сети; Активизация хакеров и интернет-мошенников, отслеживающих действия пользователя в сети с целью вымогательства, шантажа и т.п.

2. Совершенствование технологии шифрования и дешифрования биометрических данных (двухфакторная аутентификация). В случае взлома базы данных с БД граждан (клиентов банка) без знания ключа дешифровки, данные не будут представлять никакой ценности.

Для осуществления данных мер необходимо разработать программный продукт. Прототипом может стать технология биометрической системы личностного шифрования, предложенная А. Шамиром в 1984 году. Она отличается от ближайших аналогов постоянным размером шифртекста, меньшей сложностью шифрования и расшифрования и сводится к более трудной задаче, чем аналоги.

Это позволит обеспечить надежную защиту биометрических данных пользователей при сохранении скорости обработки удаленных данных. Однако, препятствиями для реализации являются: высокая стоимость разработки и внедрения и возможность удорожание банковских услуг из-за увеличения трат на обслуживание.

3. Популяризация использования идентификации на основе биометрических данных клиентами банков. Чем больше база для распознавания биометрических данных, тем меньше вероятность погрешности и технической ошибки. Банки заинтересованы в улучшении качества обработки данных клиентов. Для поощрения граждан к активному

использованию систем БИ при удаленной идентификации возможно введение систем премирования по операциям (повышенный кэшбек по операциям или бонусы), осуществленным с использованием систем БИ.

При осуществлении данного сценария вероятно: улучшение качества обработки данных; уменьшение возможной погрешности при распознавании биометрической информации; повышение уровня безопасности, как частного клиента, так и всей системы в целом; получение экономической выгоды клиентом, использующим биометрические данные для удаленной идентификации;

Однако, банки несут как финансовые затраты на введение и обслуживание системы, так и недополучают выгоду, а также чем больше база данных, тем больший объем информации требуется защищать и обслуживать, что само по себе является угрозой нарушения конфиденциальности информации.

4. Внедрение технологий, связанных с подтверждением операции по альтернативному каналу связи. Предотвращение перехвата информации об аутентификации путем разделения и отправки пакета данных с помощью нескольких разнородных каналов связи. Например, Интернет и Push-уведомление или СМС.

Преимуществом является относительно низкая стоимость реализации проекта, отсутствие необходимости нормативного закрепления, невосприимчивость к кибер-атакам, направленным на определенный вид устройства или канал связи. Минусами метода будут восприимчивость к комплексным кибер-атакам, необходимость иметь рядом альтернативный источник идентификации (например, при работе на компьютере – иметь телефон под рукой), возможность взимания платы оператором связи за активное пользование телефонными каналами передачи данных.

5. Комбинирование биометрических и технологических методов идентификации. Для повышения уровня защищенности информации целесообразно комбинировать биометрические (сетчатка глаза, отпечатки пальца и т.д.) с технологическими методами защиты (например, имплантация подкожных чипов, надежно защищенных от повреждений и подмены). Чип, имплантированный под кожу человека, не портится со временем, не подвержен изменению, а значит, не имеет срока использования. У данной комбинации методов высокая степень надежности защиты биометрических данных пользователей.

Проблемами для реализации являются: болезненность имплантации, что повлечет непопулярность такой меры у граждан; психологические препятствия у пользователей;

вероятность отторжения и непереносимости чипа; техническая сложность и дороговизна реализации.

Проанализировав интересы стейкхолдеров, можно говорить о том, что в улучшении систем защиты персональных данных в первую очередь заинтересованы финансовые институты, так как для них это является конкурентным преимуществом. Это в определенной степени перекладывает на них ответственность за разработку и внедрение новых технологий защиты ПБД.

Нами не было выявлено ошибок в действиях Евгения Амбразорова. Он проявляет достаточную степень осторожности при использовании социальных сетей и гаджетов, однако, это не спасло его от действий мошенников. Необходимо проводить активную работу по распространению социальной рекламы по повышению финансовой грамотности населения. Быть финансово грамотным гражданином должно быть модно, только так можно не допустить бесконтрольное попадание биометрических данных в сеть.

ЗАКЛЮЧЕНИЕ

Изучив нормативно-правовую базу, мировой опыт, проведя анализ рынка биометрии, нами сделан вывод о том, что только общими усилиями всех стейкхолдеров возможно предотвращение событий описанных в кейсе, а именно краж со счетов денежных средств, используя недостатки системы биометрической идентификации.

Для этого гражданам, использующим свои биометрические данные для удаленной идентификации, необходимо проявлять достаточную степень осторожности при публикации своих ПБД, исполнять рекомендации, составленные как их финансовой организацией, так и центральным Банком РФ по поводу использования своих ПБД, а так же интересоваться тенденциями в сфере личной финансовой безопасности.

Финансовым организациям, в свою очередь, необходимо совершенствовать систему защиты ПБД клиентов, системы идентификации и аутентификации на основе БД, а также доносить до своих клиентов, в доступной форме, информацию о повышенном уровне защищенности средств граждан, использующих БИ, по сравнению с традиционными методами защиты, не только статистического, но и практического характера. Для этого можно использовать видеоролики, брошюры и контекстную рекламу в социальных сетях.

Регулятор, в лице государства, обязан нормативно закрепить механизм взаимодействия между финансовой организацией и клиентом, по поводу использования БД, а так же права, обязанности и ответственность каждой стороны, ужесточить надзор за

использованием биометрических данных. Так же необходимо разработать и внедрить механизм защиты ПБД граждан.

При анализе проблемы и существующих методов ее решения, как в России, так и за рубежом, нами составлен перечень мер, позволяющих повысить уровень защищенности ПБД: Защита фото-, видео- и аудио-материалов в интернете цифровыми знаками; Совершенствование технологии шифрования и дешифрования биометрических данных (двухфакторная аутентификация); Популяризация использования идентификации на основе биометрических данных клиентами банков; Внедрение технологий, связанных с подтверждением операции по альтернативному каналу связи; Комбинирование биометрических и технологических метолов идентификации. Данные решения не противоречат друг другу и могут быть совмещены, грамотная их комбинация позволит добиться баланса интересов всех заинтересованных сторон.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Интернет-банкинг: медленно, но верно [Электронный ресурс] // URL: http://www.cnews.ru/reviews/free/finance/ibanking/
2. Информационно-правовой портал «Гарант.ру» Электронный ресурс] // URL: http://www.garant.ru/
3. Информация по кредитным организациям [Электронный ресурс] // URL: http://www.cbr.ru/credit/default.aspx#a_115
4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) [Электронный ресурс] // СПС КонсультантПлюс
5. Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993) [Электронный ресурс] // СПС КонсультантПлюс
6. Кража онлайн: когда российские банки научатся защищать клиентов [Электронный ресурс] // РБК. URL: https://www.rbc.ru/spb_sz/24/07/2018/5b56e5089a794783c84a4652
7. Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (утв. Банком России 14.02.2019 N 4-МР) [Электронный ресурс] // СПС КонсультантПлюс
8. Обзор несанкционированных переводов денежных средств за 2018 год. Материал подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Департамента информационной безопасности Банка России [Электронный ресурс] // URL: https://www.cbr.ru/Content/Document/File/62930/gubzi_18.pdf
9. Обмани меня: как хакеры обходят системы биометрической защиты [Электронный ресурс] // URL: https://www.forbes.ru/tehnologii/367261-obmani-menya-kak-hakery-obhodyat-sistemy-biometricheskoy-zashchity

10. ПАО Сбербанк России. Годовой отчет [Электронный ресурс] // URL: https://www.sberbank.com/common/img/uploaded/files/pdf/yrep/sberbank_annual_report_2017_rus.pdf

11. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс] // СПС КонсультантПлюс

12. Приказ Минкомсвязи России от 21.06.2018 N 307 "Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации" [Электронный ресурс] // СПС КонсультантПлюс

13. Разъяснения Роскомнадзора "О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки". [Электронный ресурс] // СПС КонсультантПлюс

14. Тинькофф Банк (TCS): годовой финансовый отчет МСФО [Электронный ресурс] // URL: https://static.tinkoff.ru/documents/eng/investor-relations/financial-results/2017/TCS_FSPWC_CY_FY2017.pdf

15. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ [Электронный ресурс] // СПС КонсультантПлюс

16. Удаленная идентификация [Электронный ресурс] // URL: http://www.cbr.ru/fintech/remote_authentication/

17. Указание Банка России N 4859-У, Публичного акционерного общества "Ростелеком" N 01/01/782-18 от 09.07.2018 "О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", в единой биометрической системе" [Электронный ресурс] // СПС КонсультантПлюс

18. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [Электронный ресурс] // СПС КонсультантПлюс

19. ANZ first Australian bank to roll out Voice ID for mobile banking [Электронный ресурс] // URL: https://media.anz.com/posts/2017/09/anz-first-australian-bank-to-roll-out-voice-id-for-mobile-bankin

20. Biometric data and the General Data Protection Regulation [Электронный ресурс] // URL: https://www.gemalto.com/govt/biometrics/biometric-data

21. GDPR – готова ли ваша компания? Презентация EY [Электронный ресурс] // URL: https://www.ey.com/Publication/vwLUAssets/EY-gdpr-presentation/$FILE/EY-gdpr-presentation.pdf

22. Internet Banking Rank [Электронный ресурс] // URL: http://markswebb.ru//upload/pdf/Markswebb_Internet_Banking_Rank_2018_Intro_Report.pdf

23. KB Kookmin Bank brings digital transformation to finance services [Global Finance Awards] [Электронный ресурс] // URL: http://www.koreaherald.com/view.php?ud=20181127000850

24. Lloyds Banking Group says Hello to Windows 10 [Электронный ресурс] // URL: http://www.lloydsbankinggroup.com/Media/Press-Releases/press-releases-2017/lloyds-banking-group/lloyds-banking-group-says-hello-to-windows-10/

25. The complicated truth about China's social credit system [Электронный ресурс] // URL: https://www.wired.co.uk/article/china-social-credit-system-explained

ПРИЛОЖЕНИЯ

Приложение А

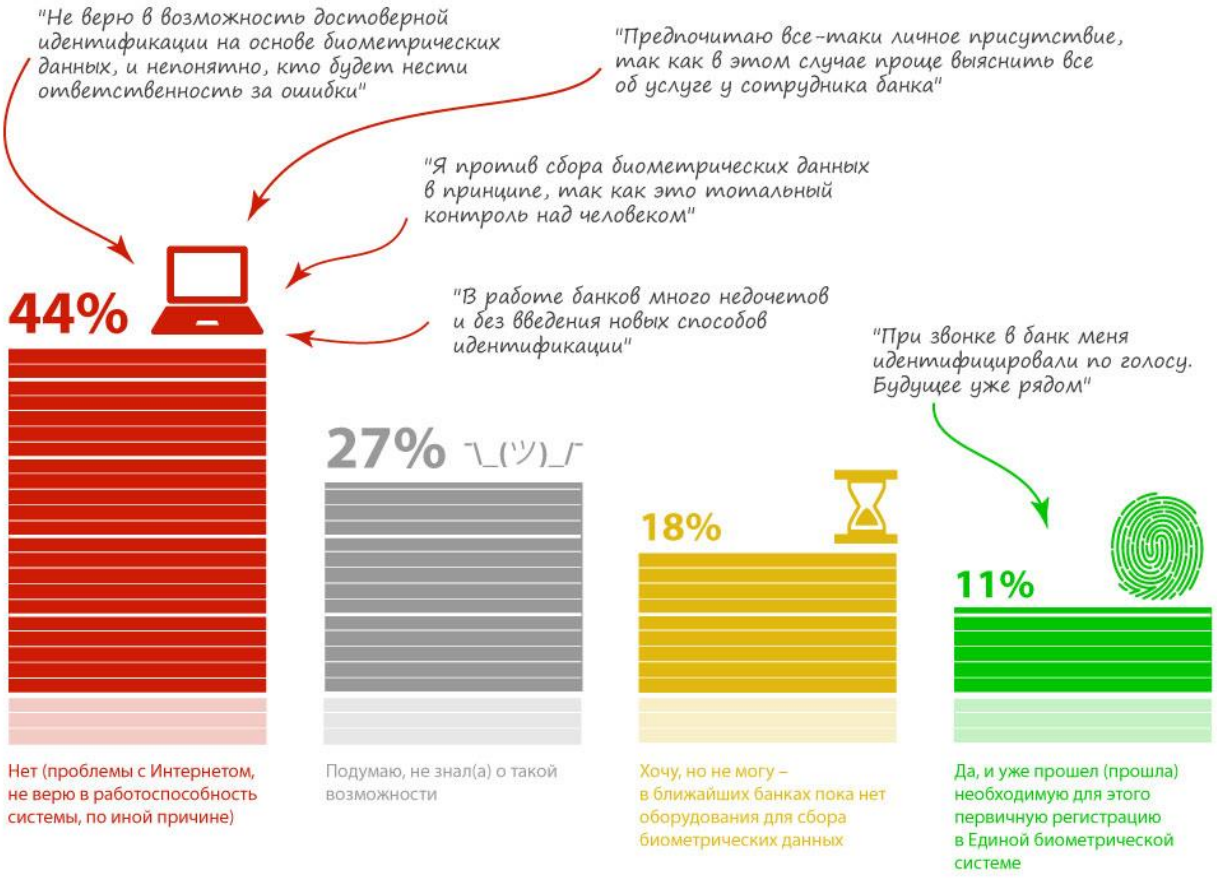

Рисунок 1 – Результаты опроса, проводимого информационно-правовым порталом «Гарант.ру».

Приложение Б

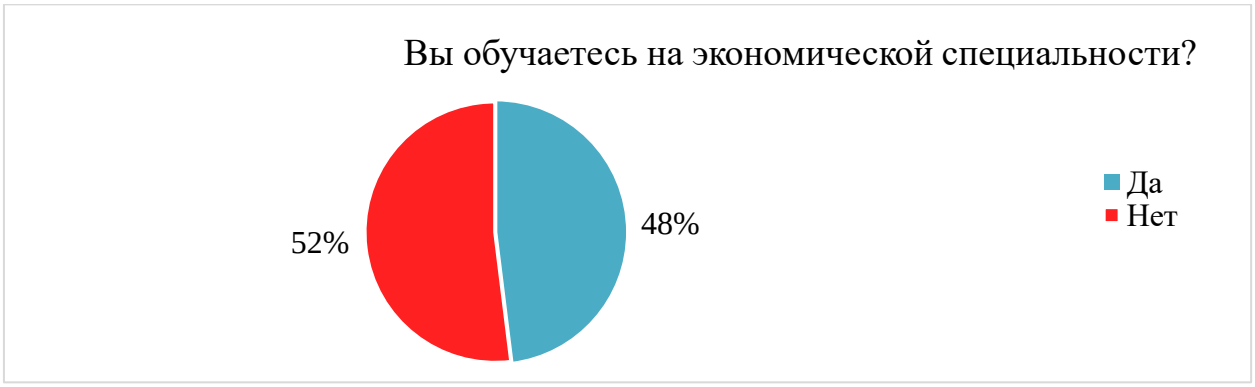

Диаграмма 1 – Опрос студентов СФУ.

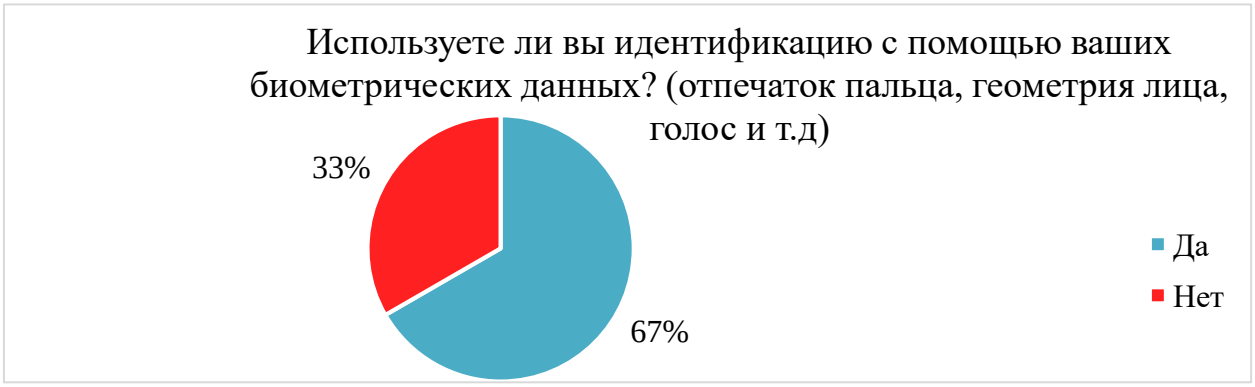

Диаграмма 2 – Опрос студентов СФУ.

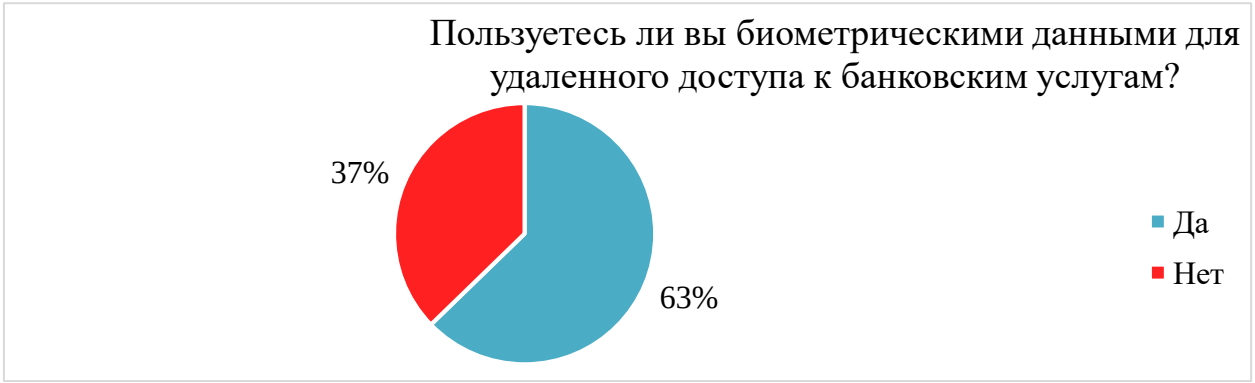

Диаграмма 3 – Опрос студентов СФУ.

Диаграмма 4 – Опрос студентов СФУ.

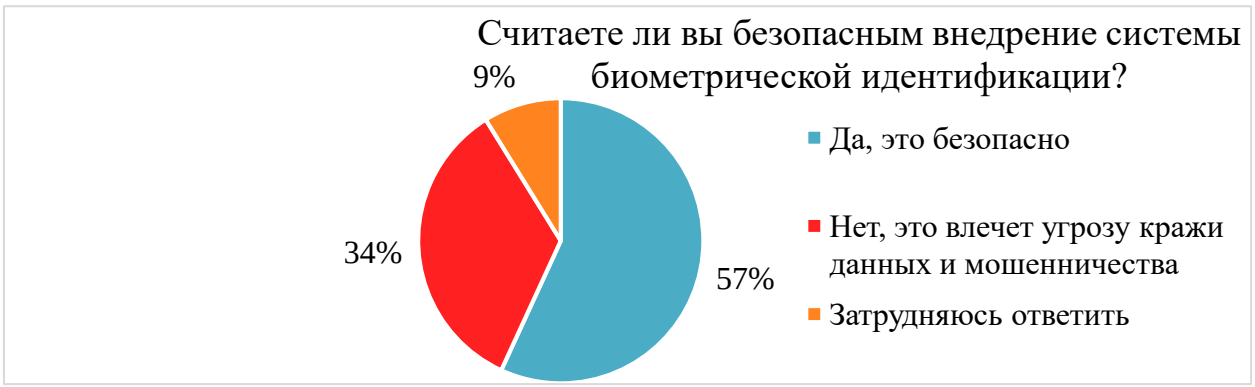

Диаграмма 5 – Опрос студентов СФУ.

Приложение В

Таблица 1 – Что понимается под биометрическими данными в РФ (составлено авторами)

Документ	Трактовка
Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [18] ч. 1 ст. 11	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.
Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [11] п. 5	Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.
Разъяснения Роскомнадзора "О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки" [13]	К биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись),

Приложение Г

Таблица 2 – Примерный перечень норм, регулирующих сбор, обработку и хранение ПБД граждан РФ в банковских организациях (составлено авторами)

Документ	Статья	Трактовка
"Конвенция о защите физических лиц при автоматизированной обработке персональных данных" [4]	Ст. 7 Ст. 8	Предусматривает охрану ПД при их автоматизированной обработке, и дополнительных гарантий для субъекта ПД
Конституции РФ [5]	Ст. 23 Ст. 24	Гарантирует каждому право на неприкосновенность частной жизни, личную и семейную тайну. Эта норма определяет границы, которые оператор ПД не вправе переступать при получении и при обработке информации о человеке.
ФЗ «О персональных данных» [18]	п. 1 ст. 10	Обработка ПД, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев предусмотренных законодательством.
	п.1 ст. 9 п.4 ст. 9	Обработка ПБД возможна только при наличии письменного согласия субъекта ПД. Согласие на обработку ПД должно быть конкретным, информированным и сознательным.
	Ст. 7	Операторы и иные лица, получившие доступ к ПД не могут передавать ПД третьим лицам без согласия субъекта ПД, за исключением случаев предусмотренных законодательством.
Трудовой Кодекс РФ [15]	Ст. 86	В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке ПД работника обязаны соблюдать определённые требования.
Политика в отношении обработки персональных данных банка (в соответствии с ФЗ «О персональных данных»)	-	Политика разработана в целях реализации требований законодательства в области обработки и обеспечения безопасности ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД в банке.

Приложение Д

Таблица 3 – Перечень угроз информационной безопасности, которые банки учитывают при сборе, использовании и передаче биометрических персональных данных своих клиентов (составлено авторами в соответствии с Указаниями Банка России от N2 4859-У/01/01/782 [17])

Этапы сбора, использования и передачи БПД	Возможные угрозы
при обработке, включая сбор, биометрических персональных данных на устройстве клиента	– угроза нарушения целостности (подмены, удаления); – нарушения конфиденциальности (компрометации); – нарушения целостности (подмены, удаления) информации о степени соответствия биометрических персональных данных гражданина Российской Федерации, предоставленным им биометрическим персональным данным в единой биометрической системе (далее – информация о степени соответствия) в целях передачи биометрических персональных данных в банки или единую биометрическую систему.
при сборе биометрических персональных данных в государственных органах, банках и иных организациях, включая сбор биометрических персональных данных и передачу собранных биометрических персональных данных между структурными подразделениями государственного органа, банка и иной организации	– угроза нарушения целостности (подмены, удаления); – нарушения конфиденциальности (компрометации); – нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных).
при передаче собранных биометрических персональных данных между государственным органом, банком, иной организацией и единой биометрической системой	– угроза нарушения целостности (подмены, удаления); – нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных); – угроза нарушения конфиденциальности (компрометации).

Продолжение Таблицы 3

Этапы сбора, использования и передачи БПД	Возможные угрозы
при обработке информации о степени соответствия в банках	– угроза нарушения целостности (подмены, удаления) информации о степени соответствия в банках.
при передаче информации о степени соответствия между банком и единой биометрической системой	– угроза нарушения целостности (подмены, удаления) информации о степени соответствия; – угроза нарушения конфиденциальности (компрометации) информации о степени соответствия.
при обработке, хранении, проверке биометрических персональных данных, обработке и передаче информации о степени соответствия в единой биометрической системе	– угроза нарушения целостности (подмены, удаления) биометрических персональных данных; – нарушения конфиденциальности (компрометации) биометрических персональных данных; – нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных); – нарушения целостности (подмены, удаления) информации о степени соответствия; – нарушения доступности (блокирования передачи) информации о степени соответствия.

Приложение Е

Таблица 4.1 – Стейкхолдеры (по цели взаимодействия). (Составлено авторами)

Кто? / С кем?	Граждане	Кредитная организация	Государство
Граждане	-	Внедрение технологии БИ с целью повышения доступности банковского продукта и противодействия мошенничеству.	Охрана законных интересов граждан.
Кредитная организация	Упрощение процедуры получения банковских услуг для экономии временных ресурсов.	-	Обеспечение безопасности в банковской сфере, путем внедрения системы БИ
Государство	Соблюдение требований законодательства.	Соблюдение требований по контролю над оборотом денежных средств, противодействием отмыванию доходов и финансированию терроризма.	-

Таблица 4.2– Стейкхолдеры (проблемы во взаимодействии). (Составлено авторами)

Кто? / С кем?	Граждане	Кредитная организация	Государство
Граждане	-	Внедрение системы БИ приводит к появлению новых мошеннических схем. Это требует от банка кадровых и финансовых вложений для обеспечения безопасности вкладов и персональных данных клиентов.	Использование систем БИ требует совершенствования законодательства о персональных данных и разработки, новых мер противодействия и защиты интересов государства и общества.
Кредитная организация	Использование систем БИ в банках требует от клиентов принятия разумных рисков передачи своих персональных данных.	-	Использование систем БИ требует совершенствования законодательства о персональных данных и разработки, новых мер противодействия и защиты интересов государства и общества.
Государство	Добровольно-принудительный характер сбора биометрических данных.	Добровольно-принудительный характер сбора биометрических данных.	-