Продолжение табл. 1

Ситуация	Вариант ответа	Мероприятие по сокращению риска
Были ли случаи включения процентов по инвестиционному кредиту в момент приостановления приобретения, сооружения, изготовления внеоборотного актива более, чем на 3 месяца, в стоимость этого актива?	Да/Нет	Мероприятие 3
Были ли случаи нецелевого использования кредитных средств?	Да/Нет	Мероприятие 1
Фиксируются ли направления расходования полученных кредитных денег?	Да/Нет	Мероприятие 1
Были ли случаи оформления договора кредитования в целях последующей оплаты кредиторской задолженности по ранее полученным кредитам?	Да/Нет	Мероприятие 2, 4
Были ли случаи превышения показателей кредитной нагрузки предельного уровня?	Да/Нет	Мероприятие 4
Проводится ли инвентаризация кредиторской задолженности по привлеченным кредитам и займам перед составлением годовой финансовой отчетности?	Да/Нет	Мероприятие 5

Исходя из ответов на указанные вопросы, можно составить представление об уровни внутреннего контроля операций, связанных с банковским кредитованием. После оценки сложившейся ситуации, руководство организации совместно с контролирующими органами рассматривает вопрос о необходимости повышения уровня контроля. Для указанной цели могут быть рассмотрены мероприятия, предложенные автором.

Подводя итог данной работе, отметим, что значимость банковского кредитования в процессе реализации предпринимательской деятельности достаточно высока. Принимая во внимание серьезность оценки банковских учреждений потенциальных дебиторов, обмен информацией внутри банковской системы, необходимо обеспечить репутацию добросовестного должника.

Литература

1. Приказ Минфина России от 06.10.2008 г. № 107-н «Об утверждении Положения по бухгалтерскому учету «Учет расходов по займам и кредитам» (ПБУ 15/2008)».
2. Приказ Минфина РФ от 13.06.1995 г. № 49 «Об утверждении Методических указаний по инвентаризации имущества и финансовых обязательств».

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ДАННЫХ

Кадирова Алия Рифатовна

Казанский (Приволжский) федеральный университет, Казань, Россия

Аннотация. Статья посвящена актуальной на сегодняшний день проблеме защите биометрических данных. В статье анализируется применение в России биометрических систем, и способы защиты биометрической информации. В заключении были предложены многофакторная аутентификации.

Ключевые слова: биометрия, биометрическая информация, удаленная идентификация, ЕБС, пандемия, кража биометрических данных, защита информации, информационная безопасность.

Роботы, многофункциональные смартфоны, беспроводные наушники, безоткатный платеж на сегодняшний день этим не удивишь. Новые технологии вошли в жизнь человека с быстрой скоростью и «захватили» многие аспекты жизни. Они во много раз упрощают жизнь человека. Так в обыденность вошла и биометрия. Если раньше только шпионы в фильмах использовали для аутентификации сетчатку глаза, отпечаток пальца и даже голос, то сейчас она активно используется в обыденной жизни. Многочисленное количество паролей, заменяют безопасная и легкая аутентификация и идентификация по отпечатку пальцев и расписывание лица. Биометрическая информация используется не только на iPhone Apple и некоторых устройств Android, но также для получения некоторых услуг и поиски, ловля преступников.

На 2021 год это особенно актуально, ведь во время пандемии финансовые организации были вынуждены как можно быстро адоптироваться и обеспечить безопасное удаленное предоставление услуг. Поэтому все больше популярность набирали новые технологии, в частности – сервисы удаленной идентификации клиентов. Суммарное количество скачиваний приложения «Биометрия» от «Ростелекома», с помощью которого производится удаленная идентификация, превысило 250 тысяч. Защищенное мобильное приложение со встроенным алгоритмом шифрования доступно в официальных магазинах приложений AppStore и Play.

Официальная история биометрии в России началась в 2018 году, была запущена Единая биометрическая система (далее – ЕБС). Основой ее внедрения стало принятие Федерального закона от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». «Ростелеком» был назначен разработчиком, оператором ЕБС [1]. Были разработан специальное мобильное приложение «Ключ Ростелеком» для клиентов банка проходить удаленную биометрическую идентификацию с помощью смартфона, с помощью которого собираются биометрическая информация. Протоколам, биометрические образцы пользователя регистрируются в базе данных. При биометрической аутентификации, секретными данными пользователя могут служить, как глазная сетчатка, так и отпечаток пальца. Эти биометрические образы являются уникальными для каждого пользователя, что обеспечивает высокий уровень защиты доступа к информации.

В 2018 году Банк России начал сбор биометрических информаций, предоставил возможность гражданам открывать счета, вклады и получать кредиты с помощью идентификации через Единую биометрическую систему и Единой системы идентификации и аутентификации (далее – ЕСИА). На конец прошлого года в ЕБС зарегистрированы около 160 000 пользователей [3].

В 2021 году такие услуги предоставляют 232 банка и МФЦ, среди которых ВТБ, «Тинькофф», «Почта Банк», «Совкомбанк», «Хоум Кредит», «Россельхозбанк», «Ак Барс Банк», СКБ-Банк, «Промсвязьбанк» и другие банки. Таким образом, Российские банки параллельно развивают собственные биометрические базы. Из-за возможности кражи биометрической информации, пользователи отдают большее предпочтение предоставить биометрическую информацию «своим» банкам, чем сдавать информацию в ЕБС. К примеру, «Сбер» уже собрал данные нескольких миллионов клиентов, ВТБ – более 130 000, писал ранее РБК.

Применение биометрических систем связано трудностями защиты данных. И вот, на прошедшем 27–28 ноября 2018 г. SOC-форуме, ЦБ указал ФСБ на невозможность в полном объеме выполнить ее требования по защите собираемых банками биометрических персональных данных граждан.

Законодательство достаточно четко регулирует вопросы безопасности базы биометрических данных. Так, Постановление Правительства РФ от 06.07.2008 г. № 512 закрепляет требования к материальным носителям биометрических персональных данных. В частности,

они должны обеспечивать защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из системы персональных данных; невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. № 321 предусматривает, что банк должны информировать Банк России о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при обработке (включая сбор и хранение) параметров биометрических персональных данных в целях идентификации, которые привели или могут привести к нарушению или попыткам нарушения целостности, конфиденциальности и (или) доступности защищаемой информации.

Первый замглавы Департамента информационной безопасности ЦБ Артем Сычев отметил, что отечественного крипто оборудования, которое может обеспечить защиту собранных у граждан, биометрических данных по классу КВ, – нет. А ведь именно этот класс защиты (на уровне гостайны) определен в приказе ФСБ №378.

На практике буквально каждую неделю становится известно об утечках информации о клиентах крупных банков. Более того, в некоторых странах биометрические данные являются инструментом для контроля действий граждан:

– 2016. В Гане похищены биометрические данные избирателей.

– 2017. Украдены биометрические данные филиппинских избирателей. У американской компании Avanti Markets, похищены отпечатки пальцев покупателей. Утечка данных из индийской биометрической системы Aadhaar.

– 2018. В Зимбабве похитили отпечатки пальцев и фотографии избирателей. Компрометация биометрических данных миллиарда граждан Индии.

– 2019. В открытый доступ попала многомиллионная база отпечатков пальцев из южнокорейской компании Suprema. Похищены записи голоса клиентов Сбербанка [2].

Для защиты биометрических данных, вступившая в действие 14 сентября 2019 года директива Евросоюза PSD2, также известная как Open Banking, требует от банков внедрения многофакторной аутентификации для обеспечения безопасности удалённых транзакций, выполняемых по любому каналу. Это означает обязательное использование двух их трёх компонентов:

– знания – какой-то информации, известной только пользователю, например, пароля или контрольного вопроса.

– владения – какого-то устройства, которое имеется только у пользователя, например, телефона или токена.

– уникальности – чего-то неотъемлемого, присущего пользователю и однозначно идентифицирующего личность, например, биометрических данных.

Эти три элемента должны быть независимыми так, чтобы компрометация одного элемента не влияла на надёжность других [4].

Таким образом, банки для защиты биометрической информации не должны опираться лишь на один из способов идентификации или аутентификации, они должны обеспечить дополнительные проверкам с помощью пароля, токена или PUSH/SMS-кодов.

Литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. *Горшков А.* Как защитить биометрические данные пользователей от криминального использования. – URL: https://rb.ru/opinion/ (Дата обращения: 08.05.2021).
3. *Панасенко А*. Обзор российского рынка биометрической идентификации и аутентификации. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-biometric-technology-market-overview#part3 (Дата обращения: 05.05.2021).
4. Интернет-ресурс «habr.com». – URL: https://habr.com/ru/ (Дата обращения: 05.05.2021).