АНАЛИЗ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ КАК ОСНОВНОГО МЕТОДА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ КЛИЕНТА БАНКА

Колмакова Ю.Э., Курьянов К.Е., Серова К.С.
Научный руководитель – старший преподаватель Козлова С.А.
ФГАОУ ВО СФУ ИЭУиП

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]

Цель нашего исследования - изучить мировой опыт, провести анализ рынка использования биометрии и, на основании полученных данных, сделать вывод о вероятности краж денежных средств со счетов клиентов финансовых организаций, использующих биометрическую идентификацию, как метод идентификации и аутентификации в цифровом банкинге.

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.

Актуальность данного исследования, обуславливается высокой вероятностью наступления событий связанных с обходом систем Идентификации с помощью БД. 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. [3]

На данный момент, использование биометрических данных для идентификации личности (далее БИ) реализуется банками, в большинстве случав, 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. [8]

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, на 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.

К примеру, 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; [9]

KB Kookmin Bank - в его основном мобильном приложении доступны разнообразные формы биометрической аутентификации, включая сканирование радужной оболочки, а также распознавание пульса и голоса; [6]

Australia and New Zealand Banking Group (ANZ) - разработала 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. [7]

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. [5] 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. [4]

Как часто бывает с инновациями, обыватели, то есть среднестатистическим клиентам 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 о их намерении использовать услугу удаленной идентификации на основе БД. 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. 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.

Изучив мировой опыт, проведя анализ рынка использования биометрии, а также, изучив мнение потенциальных и реальных потребителей данной услуги, нами сделан вывод о том, что существует вероятность краж со счетов клиентов банков денежных средств, используя недостатки системы биометрической идентификации.

Исходя из 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.

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. 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

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

5. 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

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

7. 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

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

9. 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/