УДК 336.71:343.72

Н.А. Пономарёва,
канд. экон. наук,
доцент кафедры банковского дела
Хабаровского государственного университета экономики и права
Е.А. Михеева

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ ТЕХНОЛОГИЙ РОССИЙСКИМИ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

В данной статье раскрываются основные проблемы использования современных банковских технологий российскими кредитными организациями, рассматриваются возможные пути их преодоления.

Ключевые слова: *банковские технологии, киберпреступления, социальная инженерия, идентификация клиента, недоверие к банковскому сектору, геймификация, технология блокчейн.*

This article presents the main problems of the using the modern banking technologies by Russian credit institutions and considers possible ways to overcome.

Keywords: *banking technology, cybercrime, social engineering, customer identification, distrust of the banking sector, gamification, blockchain technology.*

В настоящее время в условиях высокой конкуренции в банковском секторе каждая кредитная организация заинтересована в поиске новых возможностей повышения эффективности деятельности и снижения расходов.

Решением такой проблемы может стать разработка и внедрение новейших технологий как в процесс создания и реализации банковских продуктов и услуг, так и во внутрибанковские процессы. Безусловно, использование новых технологий сопровождается различными рисками и сложностями.

Проблемы использования банковских технологий подразделяются на несколько групп [5], показанных авторами в приведённой ниже схеме (рисунок 1).

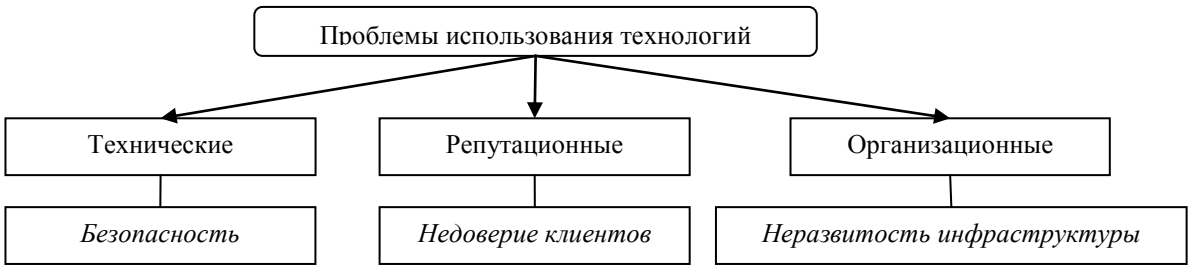

Рисунок 1 – Классификация проблем использования банками технологий (сост. авт.)

Наибольшую сложность представляют собой технические проблемы. В частности, к ним относится проблема безопасности использования клиентами банковских нововведений в рамках высокого распространения и постоянного роста киберпреступлений. С 2013 г. по 2017 г. число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, возросло в России практически в 10 раз – с 11 тыс. преступлений за год до 106 тысяч. За 2017 г. рост числа преступлений составил 26 % по сравнению с предыдущим периодом [11].

Следует отметить, что в 2017 г. более половины российских банков увеличили бюджет на информационную безопасность в связи с ростом киберугроз и активности вредоносных программ. Наиболее критическими последствиями такого рода преступлений для кредитных организаций являются репутационные и финансовые потери [6].

В России в 2017 г. 35 млн интернет-пользователей стали жертвами киберпреступлений. Во всём мире за 2017 г. от кибермошенников пострадали 978 млн пользователей. Соотношение в разрезе стран представлено на рисунке 2.

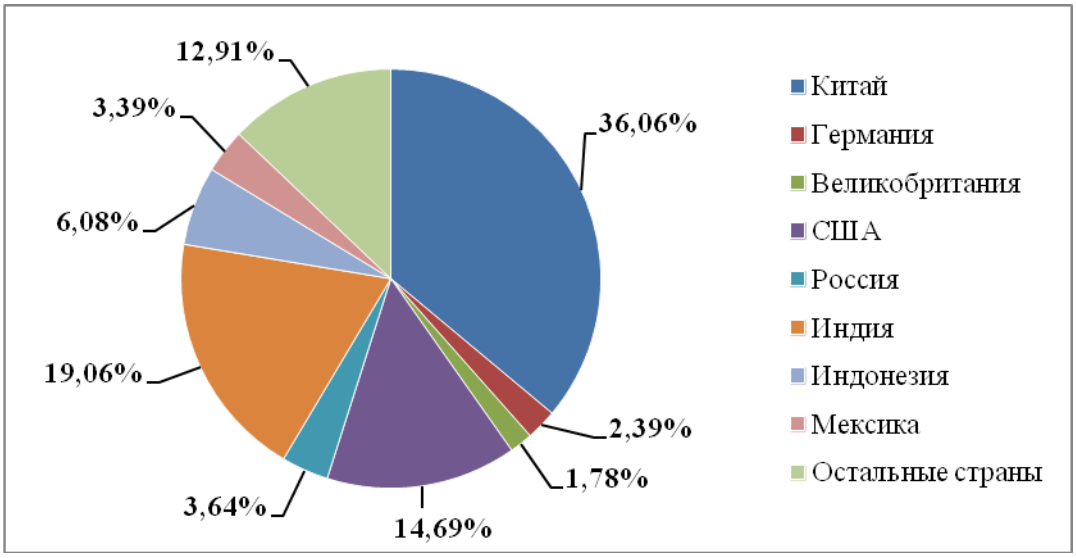

Рисунок 2 – Страновая структура интернет-пользователей, пострадавших от кибермошенников, в 2017 г. [11]

Наибольшее количество пострадавших от кибератак лиц в 2017 г. было в Китае – более 36 % от общего количества, Индии (19,06 %), США (14,69 %) и Индонезии (6,08 %). В России жертв мошенничества гораздо меньше – 3,64 % от общего числа. Более 53 % кибератак осуществлены посредством распространения компьютерных вирусов, 38 % атак приходится на так называемый «фишинг» (кража паролей, информации о банковских картах и т.д.). В последнее

время большое распространение (28 % от всех киберпреступлений) получили DdoS-атаки, суть которых состоит в блокировании систем интернета или мобильного банка. Зачастую такой вид атак используется мошенниками для получения вознаграждения взамен прекращения атаки. Недоступность банковских онлайн-сервисов в течение нескольких часов может значительно испортить репутацию кредитной организации или привести к финансовым потерям.

В конце 2017 г. отмечалось большое количество распространения вредоносных программ для смартфонов, распространяемых через рекламные объявления в поисковых системах под видом мобильных приложений ведущих российских банков. Качество таких программ было достаточно высоким и многие клиенты банков воспользовались такими приложениями, что в итоге привело к потере ими денежных средств со счетов.

Остальные виды атак связаны с социальной инженерией, когда мошеннические действия нацелены на психологическое воздействие, посредством которого пользователи сообщают конфиденциальную информацию о своих паролях, банковских счетах и прочих данных.

Следует отметить, что многие банки отправляют бесконтактные карты клиентам по почте в целях удобства для клиента, но, безусловно, такой метод не обеспечивает безопасность. Даже без вскрытия конверта карта может быть считана специальным сканером и полностью обналичена. То же самое касается и отправки почтой обычных карт. Зачастую клиент получает уже вскрытый конверт, а значит, всеми данными карты уже обладает злоумышленник, и дальнейшее пользование такой картой приведёт к потере денежных средств.

В денежном выражении наибольшие потери приходятся также на Китай (более 66 млрд дол.), США (свыше 19 млрд дол.) и Индию (более 18 млрд дол.). Денежные потери в России составляют в совокупности 40 млн дол., что занимает всего лишь 0,02 % от объёма похищенных средств через кибер-среду в 2017 г. (рисунок 3).

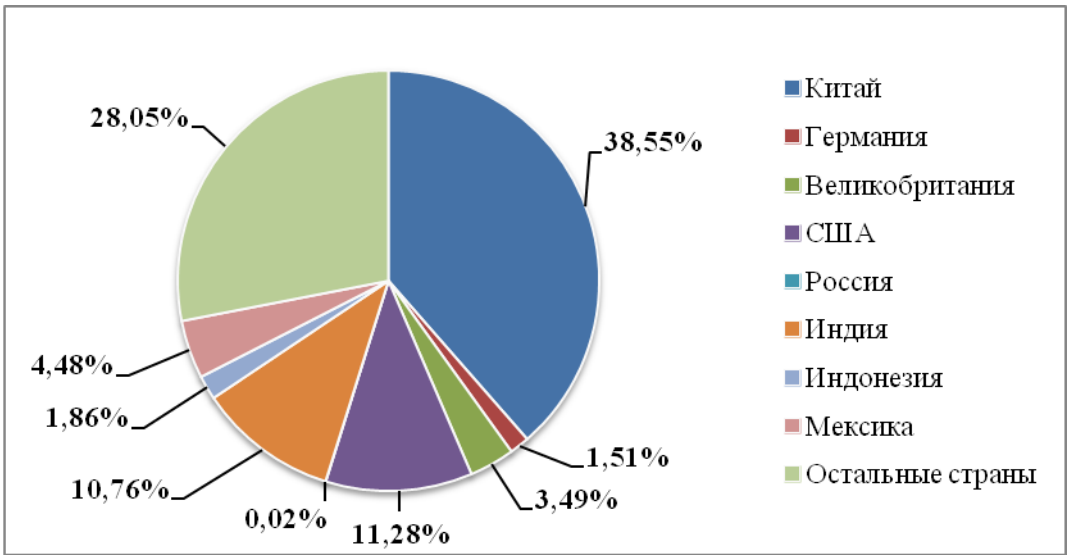

Рисунок 3 – Страновая структура финансовых потерь
от кибермошенничества в 2017 г. [11]

Всего посредством кибератак в 2017 г. похищено со счетов пользователей 172 млрд долларов. Во всём мире большая часть жертв кибермошенников – это люди в возрасте от 55 до 64 лет.

Пути сокращения количества киберпреступлений и ущерба от их совершения заключаются, прежде всего, в повышении финансовой грамотности населения. Кроме того, важность представляет собой совершенствование методов идентификации клиента. К таковым относят аутентификацию пользователя, подтверждение выполнения операции, которое в современных условиях следует осуществлять с использованием биометрических данных клиента. В настоящее время появились сканеры сетчатки глаза, сканеры капилляров, датчики сердцебиения, устройства для аудиоидентификации. Для доступа и совершения операций в мобильном банке следует задействовать фронтальную камеру смартфона, которая также может идентифицировать пользователя [5]. Зачастую хищение средств с банковских счетов и иные преступления совершаются сотрудниками кредитной организации, в связи с чем появляется необходимость распределения основных функций по осуществлению каких-либо операций между сотрудниками так, чтобы ни одна операция не могла быть выполнена полностью только одним сотрудником.

Репутационные проблемы непосредственно связаны с техническими. Так, в условиях постоянного роста киберпреступлений степень доверия населения к банкам сокращается. В частности, около 47 % населения в 2017 г. выражают недоверие к российской банковской системе. В 2016 г. недоверие к кредитным организациям выражали 41 % населения [11]. При этом важную роль играют репутационные факторы как отдельного банка, так и всего банковского сектора. Ухудшение репутации одного из банков влечёт за собой снижение доверия и ко всем остальным кредитным

организациям. Данная проблема решается преимущественно Банком России, посредством мониторинга, контроля и надзора которого наиболее неблагонадёжные кредитные организации прекращают свою деятельность. Следует отметить, что опасения применения новейших банковских технологий возникают у клиентов всех возрастных категорий. Для преодоления данной проблемы в случае с более старшим населением важность приобретает квалификация сотрудников банка и эффективность внутреннего порядка работы с фронт-персоналом. Клиент и желание удовлетворить прежде всего его потребности должны быть главной ценностью кредитной организации. На сегодняшний день наиболее успешными являются клиентоориентированные банки, уделяющие большое значение лояльности своих клиентов.

Если говорить о клиентах возрастной категории от 18 до 30 лет, то для преодоления сложностей и повышения доверия к банковским услугам может использоваться метод геймификации. Он представляет собой процесс применения игровых подходов для мотивации клиента выполнять какие-либо действия чаще или в больших объёмах путём предложения различных привилегий [3].

Рассмотрим, к примеру, сервис Alfa Activity от Альфа-Банка. Его суть состоит в увязке учётной записи фитнес-трекера с интернет-банком для накопления денежных средств на специальном счёте с повышенной процентной ставкой. Для пользователей данным сервисом и для привлечения новых участников Альфа-Банк использует игровые механики в виде обращения к клиентам в мобильном или интернет банке с предложением накопить денежные средства на покупку конкретных полезных атрибутов для занятий спортом (в соответствии с выявленными потребностями клиента на основании отслеживания направленности расходов). При этом подчёркивается, что деньги будут автоматически перечисляться на накопительный счёт пропорционально совершённым действиям. Использование такой методики позволяет мотивировать клиентов на достижение собственных целей, а также обучить их использованию новых банковских продуктов [2].

В Тинькофф банке геймификация использовалась в 2015 г. в виде программы стимулирования использования определённого банковского продукта. За 35 дней участники программы должны были выполнить 7 заданий разной степени сложности, связанные с использованием кобрендинговых карт: совершать платежи в определённых объёмах и с установленной частотой, проводить операции через мобильный банк и др.. Участники в итоге получили бонусные баллы, а также различные призы. Результатом акции стало привлечение большого количества новых клиентов. К тому же количество транзакций по кобрендинговым картам увеличилось на 20 % [9]. Таким образом, геймификация позволяет вовлечь клиентов в активное использование онлайн-сервисов (в частности, Интернет и мобильный банк), повысить спрос на различные продукты и

услуги банка, а также в определённой степени повысить финансовую грамотность пользователей за счёт упрощения восприятия «сложных» банковских продуктов.

Наиболее обширными проблемами использования современных банковских технологий являются организационные проблемы. Прежде всего, к ним можно отнести неразвитость соответствующей инфраструктуры в масштабах всей страны. С одной стороны, производятся непрерывные разработки всё более новых и технологичных решений для банковского сектора, но, с другой стороны, в ряде небольших населённых пунктов страны отсутствует даже мобильная связь и сеть Интернет. Безусловно, это задерживает развитие и кредитных организаций в том числе. Решение проблемы состоит в развитии экономики, развитии отдельных регионов. Однако это может быть реализовано только при участии государства.

К организационным проблемам следует отнести отсутствие определённых правил и стандартов использования различных новшеств. Например, в банковском секторе России всё больше возрастает интерес к технологии блокчейн, которая позволяет значительно увеличить безопасность и скорость проведения расчётов. Так, Альфа-Банк в 2016 г. совместно с авиакомпанией S7 Airlines первым провёл сделку-аккредитив с использованием блокчейн. В октябре 2016 г. была создана платформа Банка России «мастерчейн» при участии Сбербанка России, Альфа-Банка, ФК «Открытие» и Тинькофф Банка. Данная платформа представляет собой сервис для обмена данными о клиентах разных банков и выступает пилотной реализацией технологии blockchain для нужд финансового рынка с использованием технологии Ethereum [2].

Считается, что блокчейн со временем может существенно изменить банковские продукты и услуги, так как сделки между клиентами будут максимально прозрачными и защищёнными от неисполнения условий участниками процесса. Блокчейн подходит для сделок с большим количеством участников либо если участники сделки ранее не сотрудничали и не доверяют друг другу. Однако на данный момент возникла ситуация, при которой каждый участник рынка имеет своё видение применения технологии блокчейн. Какие-либо общие стандарты отсутствуют, поэтому нельзя говорить о развитии в этой сфере. Для появления практической ценности использования такой технологии несколько наиболее крупных банков должны выработать единое направление применения блокчейн. Вокруг такой «группы» будут концентрироваться и все остальные участники банковского рынка. Считается, что в краткосрочной перспективе блокчейн наиболее целесообразно применять при расчётах аккредитивами и при сделках своп. Однако вопросы безопасности проведения сделок по технологии блокчейн ещё не продуманы, и пока

необходимый уровень безопасности не может быть обеспечен. Тем не менее платформа «мастерчейн» может стать основой для распространения и выработки стандартов и основных параметров применения технологии блокчейн. Таким образом, важнейшими проблемами использования банковских технологий российскими кредитными организациями являются проблемы технического характера (проблемы безопасности использования банковских продуктов и услуг), которые приводят к возникновению репутационных проблем – недоверию клиентов к банковскому сектору в условиях роста кибермошенничества и распространения негативной информации о кредитных организациях в СМИ, потери их деловой репутации. Технология блокчейн может выступить в качестве решения ряда вопросов безопасности, однако для её эффективного использования должны быть разработаны определённые стандарты и правила, позволяющие всем участникам банковского рынка однозначно воспринимать и использовать такую технологию. Существуют и общегосударственные организационные проблемы, негативно воздействующие на банковский сектор. В частности, такой проблемой является неразвитость внутри страны инфраструктуры, необходимой для использования технологичных банковских продуктов.

Для решения существующих проблем банкам следует уделять большое внимание внедрению и развитию технологий, позволяющих обеспечить безопасность проведения операций. Проведение мероприятий, направленных на улучшение деловой репутации, также имеет высокую значимость.

Список использованных источников

1 О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга : письмо Банка России от 31.03.2008 г. № 36-Т // www.consultant.ru/document/ cons_doc_LAW_76122/5d77a7d21bcfec93fd587630954c26a95611f842 (дата обращения 01.02.2018).

2 Альфа-Банк [сайт] // alfabank.ru/make-money/savings-account/ activity/ (дата обращения 05.02.2018).

3 Бикмухаметова К. Геймификация в банковской сфере / К. Бикмухаметова, А. Политунов, Н. Репина // Новое поколение. 2016. № 9. С. 28–33.

4 Васильев К. П. Анализ способов защиты данных при использовании бесконтактной оплаты банковской картой / К. П Васильев, М. А. Филиппов, А. С. Шабуров // Инновационные технологии : теория, инструменты, практика. 2016. Т. 1. С. 266–271.

5 Гадиева Т. Х.-М. Проблемы и перспективы применения финансовых технологий в Российской Федерации / Т. Х.-М. Гадиева // Инновационное развитие

экономики. 2017. № 3. С. 98–104.

6 Загоскина Е. О. Интернет-банкинг в Российской Федерации : проблемы и перспективы развития / Е. О. Загоскина, В. С. Кудряшов // Juvenis Scientia. 2017. № 4. С. 27–31.

7 Зайцев В. Г. Кибербезопасность как неотъемлемая часть защиты информации в кредитных организациях / В. Г. Зайцев, Н. А. Пономарева // Вестник ХГАЭП. 2015. № 3. С. 74–78.

8 Маркеева А. В. Геймификация в бизнесе : проблемы использования и перспективы развития / А. В. Маркеева // Лидерство и менеджмент. 2015. Т. 2. № 3. С. 169–190.

9 Тинькофф Банк [сайт] // www.tinkoff.ru/about/news (дата обращения 05.02.2018).

10 Фалалеева С. Е. Особенности использования технологий при обслуживании клиентов в банковской сфере / С. Е. Фалалеева, И. В. Черпаков // Центральный научный вестник. 2017. Т 2. № 21. С. 57–58.

11 URL: https://us.norton.com/cyber-security-insights-2017 (дата обращения 07.02.2018).