ISSN 2311-8768 (Online)
ISSN 2073-4484 (Print)

Риски, анализ и оценка

ИННОВАЦИОННЫЕ ФИНАНСОВЫЕ ТЕХНОЛОГИИ И ОПЕРАЦИОННЫЕ РИСКИ В СФЕРЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ*

Юлия Викторовна КУДРЯВЦЕВА

ассистент кафедры экономики, Тамбовский государственный технический университет,
Тамбов, Российская Федерация
Deutschenbebi@icloud.com

История статьи:
Получена 09.02.2017
Получена в доработанном виде 17.03.2017
Одобрена 05.04.2017
Доступна онлайн 15.06.2017

УДК 336.71
JEL: G15, G21, G29

https://doi.org/10.24891/fa.10.6.647

Ключевые слова:
IT-технология, кибермошенничество, фишинг, вредоносная программа, интернет-банк, мобильный банк

Аннотация

Тема. Преимущество развития дистанционного банковского обслуживания с использованием IT-технологий. Анализ выявленного кибермошенничества, пути предотвращения краж и тенденции дальнейшего развития инновационных финансовых технологий. Представление программного обеспечения ALTELL NEO.

Цели. Провести анализ убытков кредитных организаций от киберпреступлений в России и мире. Выявить причины развития жульничества, финансовые прогнозы на ближайшие годы, а также новые возможности в борьбе с кибермошенниками.

Методология. Применялись методы анализа и синтеза научной и информационной базы. Методологическую и теоретическую основу исследования составили труды отечественных и зарубежных ученых по теории и практике экономического и финансового обеспечения.

Результаты. Выявлена тенденция на рынке банковских услуг: противостояние банков и кредитных организаций возрастающей угрозе киберпреступности.

Выводы. Раскрытие и предотвращение киберпреступлений требуют возрастающих усилий. Банк России в сотрудничестве с правоохранительными органами и кредитными организациями реализует ряд программ для сохранения финансовой и информационной безопасности национальной платежной системы, коммерческих банков и граждан.

Последние пять лет под влиянием быстро развивающихся IT-технологий банки всего мира стремительно развивают дистанционное банковское обслуживание (ДБО). Только за два года программного обеспечения для рынка финансовых услуг появилось больше, чем за десять предыдущих лет.

У ДБО есть много преимуществ перед традиционными формами обслуживания, когда клиент вынужден приходить в отделение, филиал или офис банка.

Кратко перечислим эти плюсы.

1. Интернет-технологии позволяют крупным банкам сохранить разветвленную филиальную сеть, значительно снижая затраты на ее содержание.
2. Новые технологии обеспечивают монетизацию баз данных. Банки имеют сегодня большое количество информации о клиентах: их потребности, статьи доходов и расходов, привычки и интересы, основная профессиональная деятельность, социальное положение и т.д.
3. Индивидуализация клиента. IT-технологии позволяют практически любой цифровой сервис подключить к платежной банковской системе, что позволяет создавать новые возможности сотрудничества банка с клиентом.
4. Работа банка с клиентом 24 часа в сутки и 7 дней в неделю (в стиле 24/7). Банки активно внедряют для постоянного общения с клиентами такие интернет-сервисы, как

* Автор выражает огромную признательность доктору экономических наук, профессору, заведующему кафедрой экономики Тамбовского государственного технического университета Николаю Ивановичу КУЛИКОВУ за советы и ценные замечания во время работы над статьей.

Facebook, Google Hangouts, Whatsapp, WeChat и другие, что обеспечивает потребителям постоянный доступ к финансовым услугам. Одним из примеров подобного подхода в России является Тинькофф Банк.

5. Активное социальное взаимодействие с клиентом помогает обеспечить лояльность банку, когда тот позволяет потребителю самому предлагать, описывать, проектировать интересующие его (клиента) банковские продукты. Такое сотрудничество активно использует, например, итальянский банк Widiba.

6. Роботизация в оказании финансовых услуг. Машина в режиме реального времени консультирует состоятельных клиентов банка в сфере инвестиций и предлагает услуги по оценке капитала клиентов при помощи суперкомпьютера Watson от IBM.

7. Носимые платежные устройства позволяют клиенту в любой точке планеты произвести расчеты, отследить движение денег.

8. Консалтинговые услуги нового поколения. IT-технологии позволяют банкам не только напомнить клиенту, скажем, о дне рождения сестры, но и предложить подарок с учетом доходов клиента и предпочтений именинницы. Причем аналитическая платформа банка подскажет, где можно наиболее выгодно купить подарок[1].

Уже сегодня количество клиентов, использующих дистанционное банковское обслуживание, составляет в мире не менее 20%. В 2015 г. доля платежей, осуществленных юридическими лицами электронным путем, составила 94%, а число безналичных транзакций выросло до 270 млрд. По экспертным оценкам, к 2021 г. число безналичных транзакций вырастет почти в вдвое и достигнет 420 млрд. Только за 9 мес. 2016 г. объем названных операций в платежной системе Apple Pay вырос в 5 раз. Согласно финансовым результатам, за один лишь сентябрь этого года было проведено больше платежей, чем за весь 2015 г. Система с 2014 г. расширилась и охватывает уже более 15 национальных рынков, куда входят Австралия, Великобритания, Гонконг, Испания, Канада, Китай, Новая Зеландия, Россия, Сингапур, Франция, Швейцария и Япония [1].

При использовании дистанционного банковского обслуживания для клиентов все упрощается. Потребитель, используя Интернет, телефон, смартфон или колл-центр банка, может в любой момент в режиме реального времени получить нужную информацию, провести любую операцию со своими денежными средствами, получить консультацию от банка.

Однако преимущества, как правило, несут дополнительные риски и потери, как для банков, так и для клиентов. Развитие ДБО в мире сопряжено с новыми угрозами, и большей опасности подвергаются именно те клиенты, которые получают финансовые услуги дистанционно.

Особенностью банковских операций с использованием Интернета является то, что сами транзакции переходят в форму, при которой первичных документов на бумажном носителе физически не существует. Так как при ДБО финансовая услуга не имеет физической формы, возникает проблема уследить за всей информацией. Устранить угрозу перехвата данных, которыми должен владеть только клиент, почти невозможно. Если постоянно совершенствовать уровень защиты операционных систем, программ, коммуникаций, браузеров и снижать роль человеческого фактора, это будет создавать сложности для мошенников. Но пока хакеры могут взломать практически любую интернет-систему.

[1] *Тавасиев А.М.* Банковское дело. Управление и технологии. М: ЮНИТИ ДАНА, 2015. № 1. С. 56–64.

Масштабы кибермошенничества стремительно растут с каждым годом, несмотря на все новые и новые разработки специалистов по защите информации. Мировые убытки только от мошенничества по банковским картам в 2015 г. составили 21,84 млрд долл. США. Ущерб от действий злоумышленников с банковскими картами вырос с 7,6 млрд долл. в 2010 г. до 21,84 млрд долл. в 2015 г., или почти в 3 раза.

По данным международного агентства Nilson Report, в 2015 г. было украдено 6,97 долл. с каждых потраченных 100 долл., рост составил более 12% по сравнению с 2014 г. Убытки эмитентов карт от общей суммы потерь в 2015 г. составили 72%, или 15,72 млрд долл., торговцы и пользователи карт потеряли 28% от общей суммы, или 6,12 млрд долл.

Наибольшая сумма потерь от мошенничества с картами в 2015 г. пришлась на США – около 39%, или 8,5 млрд долл., 22,9% от общемирового объема безналичных расчетов. В Америке украдены 11,76 долл. из каждых потраченных 100 долл., что в 1,7 раза превышает среднемировой показатель. Эксперты прогнозируют, что к 2019 г. объем мошенничества по банковским картам может достичь почти 33 млрд долл. [2].

По данным исследования Университета Ньюкасла, киберпреступникам требуется всего шесть секунд, чтобы получить данные о кредитной карте. Сегодня хакеры имеют в своем распоряжении программное обеспечение, которое позволяет, собирая данные с различных веб-сайтов о пользователе, быстро скомпилировать информацию о карте, в том числе адрес пользователя, почтовый индекс, дату окончания срока действия карты и код проверки ее подлинности.

В частности, по данным того же университета, если программное обеспечение хакеров угадывает на множестве различных сайтов одновременно код проверки подлинности карты, система безопасности банка практически не реагирует и не срабатывает, а владелец карты даже не получит уведомления о хакерской атаке [3].

Согласно названным исследованиям, такая брешь в программах безопасности была обнаружена в основном у банковских карт Visa. В Российской Федерации 61% пользователей имеют такие карты. Исследователи считают, что названная методика (использование множества различных сайтов одновременно), была применена хакерами в первой декаде ноября 2016 г. в кибератаке на британский Tesco Bank.

У российских пользователей системы Android с апреля 2015 г. по март 2016 г. кибермошенники украли с банковских счетов 348,6 млн руб., причем объем похищенных средств вырос в 4,7 раза по отношению к аналогичному периоду 2014–2015 гг., о чем сообщалось в годовом отчете компании Group-IB за 2015/2016 финансовый год [4].

Для хищений мошенники используют расширяющийся с каждым годом арсенал различных программ и средств. Ежемесячно растет число фальшивых промышленных приложений (например, мимикрирующих под популярные игры Pokémon Go). Кроме того, при помощи эксплойтов[2] хакеры распространяют свое программное обеспечение, позволяющее без ведома пользователя установить на устройство вредоносные программы при посещении зараженных сайтов.

Еще один способ позволяет мошенникам с помощью так называемых веб-инжектов[3] изменить отображение в браузере под мобильные устройства. Например, с помощью такого зловредного устройства можно в интернет-банке изменить поля на странице

[2] Эксплойт, эксплоит, сплоит (англ. exploit – эксплуатировать) – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

[3] Веб-инжект – изменение содержимого веб-страницы на стороне клиента, добавление туда своего контента.

авторизации или удалить хакерские операции в истории платежей. Специалисты компании Group-IB прогнозируют, что число хищений, подобных описанным, будет расти ближайшие три года темпами, обозначаемыми трехзначными числами, и в мире, и в России.

Голландский разработчик программного обеспечения Виллем Де Гроот проанализировал более 255 тыс. интернет-магазинов и пришел к выводу, что хакеры внедрили вредоносные программы в почти 6 тыс. из них, что позволило получить платежные данные покупателей. Впервые в ноябре 2015 г. программист просканировал онлайн-магазины и обнаружил, что 3,5 тыс. сайтов были взломаны, а к сентябрю 2016 г. это число уже выросло в 1,7 раза.

Хакеры смогли получить доступ к интернет-коду магазинов и с помощью внедренного вредоносного кода считывали данные банковских карт покупателей. Потом в Даркнете[4] продавались данные банковских карт покупателей по 30 долл. за одну штуку.

Виллем Де Гроот опубликовал полный список онлайн-магазинов, где есть или был замечен интернет-скимминг[5], среди которых оказались сайты Audi, Converse, Heels.com и многие другие [5].

Эксперты отмечают, что хакерские атаки на клиентов кредитных организаций в 2016 г. стали все больше отходить на второй план. Кибермошенники начали сосредоточивать свое главное внимание на незаконном выводе средств из самих банков и других финансовых учреждений. По прогнозам российской компании Positive Technologies, количество виртуальных мошенников в 2017 г. в отношении банков и других финансовых организаций вырастет на треть, а сумма украденных денег кибермошенниками может увеличиться вдвое.

Такой рост мошенничества обусловлен прежде всего тем, что преступники разрабатывают все новые и новые более совершенные способы краж денежных средств, их вредоносные программы становятся все изобретательнее. Другая причина состоит в том, что создатели зловредных программ стали объединяться, что позволяет проводить атаки на банки и финансовые компании все более организованно и протяженно по времени.

Среднее время с момента проникновения зловреда (трояна) в программное обеспечение банка до момента кражи в 2016 г. стало достигать шести месяцев, тогда как два года назад не превышало и трех. Но это не смущает хакеров. Появляющиеся вредоносные программы имеют более разнообразные модели и более широкий набор функций.

Например, вредоносный код из семейства Neurevt позволяет не только собирать данные в платежных системах онлайн-банкинга, но и рассылать вредоносный мусор. Если у кибермошенников не получается взломать конфиденциальные данные пользователя, все тот же троян может зашифровать эти данные и потребовать их выкуп у пользователя или банка.

Хакеры все чаще стали использовать вполне легальные каналы для атак на банки и другие финансовые организации. Так, в III квартале 2016 г. кибермошенники распространяли троян Svpeng, используя рекламную сеть Google Ad Sense. После установки и запуска Svpeng самостоятельно удаляется из списка установленных приложений программного обеспечения банка и начинает запрашивать права администратора. Троян имеет широкий

[4] Даркнет отличается от других распределенных одноранговых сетей, так как файлообмен проходит анонимно (поскольку IP-адреса недоступны публично) и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства.

[5] Скимминг – вид мошенничества с банковскими картами, который предусматривает использование различных устройств типа скиммера. С помощью таких устройств мошенники считывают информацию, содержащуюся на магнитной полосе карты.

набор функций и высокую мобильность, с помощью фишинговых[6] окон может получать информацию о банковских картах пользователей, отправлять текстовые сообщения, перехватывать и удалять информацию [6].

Сегодня все больше и больше банковских платежных приложений атакуется зловредными троянами. Так, известный троян Acecard способен атаковать одновременно более 30 финансовых приложений банка, включая системы мобильного банка и платежный сервис PayPal, а также ряд мобильных приложений социальных сетей (Instagram, Facebook, Twitter, Одноклассники, ВКонтакте) и популярных мессенджеров[7] (Skype, Viber, WhatsApp).

Как выяснили специалисты Лаборатории Касперского, ряд модификаций трояна Acecard, чтобы получить данные банковской карты пользователя, способны закрывать окно приложений Google Music и Google Play. Именно в этом эксперты видят причину роста объема потерь банков и финансовых организаций от кибератак [7].

Согласно результатам анализа компании Cybersecurity Ventures, в 2015 г. на планете создавали в день до 230 тыс. вредоносных программ, а в 2016 г. этот показатель составил 300 тыс. Если в 2015 г. жертвами кибермошенников ежесекундно становились 12 чел., то годом позже – 16. По оценкам экспертов, к 2021 г. убытки от IT-мошенников могут достичь 6 трлн долл. и вырасти в 2 раза по сравнению с 2015 г., когда ущерб от киберпреступлений составил 3 трлн долл.

Много это или незначительно для мировой экономики – 6 трлн долл.? Сравним: валовой внутренний продукт (ВВП) США в 2016 г. составил 18,1 трлн долл. А его доля в мировой экономике достигает 23%. Другими словами, убытки от кибермошенничества к 2021 г. могут составлять 8% мирового ВВП, или ВВП вместе взятых таких стран, как Бразилии (1,9 трлн долл.), Италии (1,8 трлн долл.), Канады (1,6 трлн долл.) и Австралии (1,2 трлн долл.). Такие потери могут оказать значительное влияние на развитие мировой экономики [8].

В течение следующих пяти лет целями кибермошенников станут не только компьютеры и мобильные телефоны, но и Internet of Things[8], предприятия промышленности, транспортного сектора, энергетики, добычи полезных ископаемых, экспорта.

По утверждению председателя Центрального банка РФ Эльвиры Набиуллиной, уже в 2017 г. кроме банков в зону хакерских атак попадут процессинговые и брокерские конторы, а также финтех-стартапы и компании, занимающиеся денежными переводами. Э. Набиуллина, в частности, сказала в интервью «Известиям»: «За последние несколько лет мы видим рост атак, связанных с получением инсайдерской информации, которая способна повлиять на стоимость акций публичных компаний. Например, возможность ознакомиться с отчетностью компании до ее публикации дает шанс обыграть рынок и неплохо заработать».

В итоге кибермошенники могут повлиять на общую стабильность банка, финансовой компании, а проблемы кредитной организации в итоге могут создать проблемы для его (банка) клиентов.

[6] Фишинг (*англ*. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

[7] Мессенджер (*англ*. messenger) – это программа, мобильное приложение или веб-сервис для мгновенного обмена сообщениями.

[8] Интернет вещей (*англ*. Internet of Things, IoT) – методология вычислительной сети физических предметов (вещей), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Распространение кибермошенничества по всему миру в экономике и финансах государств будет приводить:

1) к краже денег и интеллектуальной собственности;
2) мошенничеству;
3) удалению или восстановлению взломанных систем;
4) повреждению или уничтожению финансовых и персональных данных;
5) угрозе деловой репутации;
6) падению производительности труда в результате атаки хакеров.

Распространение киберпреступности по всему миру приведет к увеличению расходов на программы для обеспечения защиты в период 2017–2021 гг. более чем на 1 трлн долл. Полностью оценить урон от мошенничества невозможно, так как не все компании сообщают об ущербе от атак хакеров [9].

Если говорить о Российской Федерации, то она традиционно остается в центре внимания финансовых кибермошенников. Согласно данным Лаборатории Касперского, Россия занимает первое место в мире по проценту пользователей, подвергшихся атакам мобильными банковскими троянами, и второе место в списке стран, жители которых чаще всего атакуются банковским вредоносным программным обеспечением.

По данным Банка России, за 9 мес. 2016 г. объем хищений денежных средств из финансовых организаций достиг 5 млрд руб., хакерам удалось украсть около 2 млрд руб. Как отмечает президент ассоциации «Электронные деньги» Виктор Достов, в 2017 г. эти потери могут увеличиться в два раза, а количество виртуальных атак на банки России вырастет почти на треть.

По данным мировой статистики, среднее соотношение числа кибератак на банки и их клиентов равняется 40% на 60%. В России все по-другому: 30% всех кибератак приходится на банки, 26% – на органы государственной власти, 17% – на средства массовой информации и только 17% – на клиентов банков. Можно объяснить такую статистику несколькими основными причинами.

Первая – в России 72% населения получают в месяц менее 20 тыс. руб., а клиенты с низкими доходами малопривлекательны для хакеров. Да и банковские интернет-услуги в России не настолько распространены, как в странах Евросоюза, США, Японии. Только 20% россиян используют при проведении финансовых платежей интернет-банки, мобильные приложения, остальные 80% по-прежнему только снимают наличные деньги с банковских карт [10].

Вторая причина – в связи с экономическим и финансовым кризисом в России банки, особенно средние, вынуждены сокращать вложения в безопасность и защиту программного обеспечения.

Третья причина – наступил кризис традиционной банковской IT-архитектуры, существовавшей последние 15 лет, на основе которой и сегодня строится работа многих банков и финансовых организаций. Из-за технологического отставания атаки хакеров чуть ли не с каждым месяцем становятся все более эффективными.

Объем программного кода сильно разросся, доли его базовых элементов стали очень большими, и кибермошенники стали этим активно пользоваться. Сегодня ни про один программный код нельзя сказать, что хакеры не найдут в нем дырок.

Согласно данным компании Experian, число киберпреступлений, связанных с банковскими счетами, в 2016 г. выросло в три раза по сравнению с показателем двухлетней давности. Взлом одного корсчета банка может дать мошенникам возможность украсть одномоментно от 500 млн до 1 млрд руб. Хотя

в России в 2016 г. число хакерских транзакций с помощью карт-клонов уменьшилось почти на 38%, эксперты утверждают, что интерес преступников к деньгам физических лиц по-прежнему сохраняется[9].

Атака хакеров на корсчет банка требует значительных затрат, больше времени и человеческих ресурсов – в такой схеме участвует большое количество людей от 50 до 100 чел., а иногда и больше, и полученный доход хакерам нужно делить на всех участников.

Надо отметить, банки постоянно работают над совершенствованием программного обеспечения и усиливают меры защиты информации. Аналитическое агентство Markswebb Rank & Report впервые провело углубленное исследование безопасности интернет-банков и мобильных российских банков на базе 21 российской кредитной организации с наибольшим количеством онлайн-пользователей.

В целом агентство пришло к выводу, что у банков РФ не самые жесткие требования к защите и безопасности. Пять банков вообще не используют одноразовые пароли для входа в интернет-банк или мобильный банк пользователя, в двух программное обеспечение позволяет СМС-пароль одной операции использовать для другой и только четыре банка требуют подтвердить новый номер телефона после выпуска новой сим-карты, а остальные по-прежнему продолжают присылать пароли на новый номер телефона.

Наибольшее количество баллов, по оценке аналитического агентства, получили Ситибанк, Альфа-банк и небольшой Интерактивный Банк[10], занимавший 496-е место по величине активов из почти 600 кредитных организаций РФ. Крупный Сбербанк в рейтинге оказался только на 8-м месте (*табл. 1*) [11].

У маяков рейтинга оказалась и самая сложная система идентификации пользователя при оплате через интернет-банк или мобильный банк. Например, в Ситибанке, который стал первым среди 20 крупнейших банков России, все операции в интернет- и мобильном банке пользователем подтверждаются с помощью мобильного телефона с применением одноразового пароля.

Система идентификации пользователя в Интерактивном банке состоит из четырех ступеней. Две обязательные ступени: клиент вводит самостоятельно свой многоразовый пароль и код, который получает от банка в СМС-сообщении. Затем еще две ступени клиент проводит онлайн аналог-картой со стирающимся защитным слоем, как на лотерейном билете (скритч-картой), которую клиент получает один раз и использует ее для проведения операций в онлайн-банке. Наконец, клиент получает обратный СМС-пароль от банка, на экране телефона видит код, который отправляет с помощью СМС-сообщения банку.

В статье «Состояние интернет-банкинга в России сегодня: оценка, перспективы и возможности» автор рассматривал рейтинг эффективности интернет-банков с точки зрения многообразия функций, доступности и удобства интерфейсов для клиентов. Можно провести сравнение на примере Промсвязьбанка, который в рейтинге эффективности интернет-банкинга расположился на второй строчке, а в рейтинге безопасности – только на 10-м месте среди 20 крупнейших банков, Сбербанк, соответственно, – на 4-м и 8-м местах [12, 13].

Банки сегодня стоят перед дилеммой: с одной стороны, чтобы выжить, надо привлекать клиентов, а с другой стороны, надо повышать безопасность интернет- и мобильных банков.

[9] Платежные и расчетные системы: международный опыт. Вып. 3. Общее руководство по развитию национальной платежной системы. URL: http://www.cbr.ru/publ/?Prtid=prs

[10] У организации 26.04.2016 Банком России была отозвана лицензия.

Повышение безопасности интернет-банка зачастую приводит к снижению доступности и удобства интерфейсов, и потребители в итоге могут уйти в другой банк. Но клиенту тоже, чтобы сохранить деньги и не допустить их кражи, необходимо прежде всего знать, насколько защищены и безопасны интернет- и мобильный банк его (клиента) кредитной организации.

Вернуть украденные деньги пока практически невозможно. Банки отказывают потребилеям в этом, ссылаясь на то, что сами клиенты допустили кражу денег. Да и суды российские в 85% случаях принимают сторону банка.

Борьба правоохранительных органов с незаконной деятельностью кибермошенников оказалась неэффективной. Эксперты заявляют, что расследования преступлений, связанных с кражей денег, длительны и сложны, нередко продолжаются несколько лет и даже на международном уровне не всегда приносят положительный результат.

Нередко кибермошенники, находясь в какой-нибудь африканской стране, а взламывают серверы в странах Евросоюза, России, США. Но можно привести пример, когда преступник получил пять лет тюрьмы за мошенничество с онлайн-счетами.

В июне 2016 г. Томаш Сковрон был приговорен к пяти годам и трем месяцам тюрьмы британским судом Кройдона, следствие продолжалось около двух лет. Правоохранительным органам Великобритании удалось доказать ключевую роль Т. Сковрона в преступной сети, которая осуществляла незаконные операции с банковскими онлайн-счетами по всему миру, похитив таким образом около 840 тыс. ф.ст.

Следователи доказали, что в декабре 2014 г. Т. Сковрон запустил вредоносный вирус, который заразил персональные компьютеры большого количества людей по всему миру, включая программное обеспечение нескольких австралийских компаний. Правоохранителям удалось определить общий IP-адрес, с помощью которого были осуществлены выплаты, совершенные в Великобритании. Следствие показало, что данный IP-адрес принадлежит именно Т. Сковрону.

Эксперты отмечают, что количество мошенничеств с финансовыми инструментами в сотни тысяч, если не в миллионы, раз больше числа дошедших до суда.

Еще надо сказать, что банки и люди сообщают не обо всех случаях краж денег кибермошенниками. За 10 мес. 2016 г. в такой маленькой стране, как Латвия, полиция завела 130 уголовных дел об изготовлении и распространении зловредных программ, получении и использовании данных для незаконной транзакции с финансовыми инструментами и платежными средствами.

Заместитель начальника полиции по борьбе с экономическими преступлениями Илзе Соколовска рассказала, что такие уголовные дела заводятся почти каждый день, а количество зарегистрированных преступлений на порядок больше, и 84% всех краж связаны с платежами в Интернете.

Специалисты SEB bank сказали, что от клиентов регулярно поступают жалобы об исчезнувших с их счетов деньгах.

Эксперты заявляют о необходимости дополнительных действий со стороны государств и банковского сообщества против растущей угрозы кибермошенничества. Банки всего мира, в том числе и России, пытаются ответить на возрастающие угрозы, увеличивают ежегодно на 4–10% затраты на создание систем защиты и безопасности интернет- и мобильных банков. Так, английский банк Barclays в ноябре 2016 г. запустил в работу новую систему безопасности, которая позволяет отслеживать мобильные банковские транзакции пользователей во избежание мошеннических действий. Программа

безопасности дает возможность банку получить информацию о нахождении клиента, а также его дебетовой или кредитной карты.

Например, если сделка была совершена во Франции, а программа показала, что телефон клиента в это время находится в Великобритании, банк сразу блокирует карту. Если телефон клиента также находился бы во Франции, блокировка не наступила бы [4].

В октябре 2016 г. Сбербанк и компания Microsoft договорились о создании центра кибербезопасности как для собственных нужд банка, так и для оказания услуг другим финансовым организациям в области интернет-безопасности.

Центр создается на базовых мощностях Сбербанка с использованием технологий, компетенций и экспертизы компании Microsoft. Планируется создать виртуальную лабораторию и киберполигон, где в условиях, максимально приближенных к реальности, будут проводиться тренинги по совершенствованию навыков противодействия кибератакам.

Центр разработает набор типовых параметров, позволяющих оценивать зрелость (возможность) финансовой компании в области киберзащиты и способствовать повышению уровня безопасности. Планируется также оказывать финансовым компаниям помощь в безопасном переходе Интернета в облачную или гибридную среду.

В век интернет-технологий защита информации стала головной болью и политиков, и экономистов, и финансистов, и рядовых граждан. Тратятся огромные деньги, работают большие коллективы IT-специалистов, чтобы обеспечить защищенный доступ к локальным сетям интернет- и мобильных пользователей.

В качестве примера автор представляет программное обеспечение ALTELL NEO (межсетевой экран), которое позволило бы управлять доступом в Интернет для всех сотрудников банка, протоколировало бы историю посещения интернет-ресурсов, вело учет и блокировало нежелательные трафик и программы, обеспечивало защищенное соединение с офисами и филиалами банка и отражало кибератаки на банки. Все это можно показать в виде схемы (рис. 2) [14].

В России борьба с финансовыми кибермошенниками была инициирована еще в декабре 2014 г., когда Совет Безопасности РФ своим решением создал Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере (ФинЦЕРТ), который начал свою деятельность с 1 июня 2015 г. на базе главного управления безопасности и защиты информации Банка России.

Следует признать, что обязанность информировать ФинЦЕРТ о возможных и выявленных кибератаках вменена только для банков, да и деятельность центра в основном сконцентрирована на кибератаках. Это учреждение сформировало достаточно большой черный список мошенников и подозреваемых в мошенничестве, куда включены несколько тысяч лиц [15].

Российские банки являются активными участниками информационного обмена о кибератаках, организованного ФинЦЕРТ. Когда в начале ноября 2016 г. пять из топ-10 крупнейших отечественных банков подверглись кибератакам, представленная ими информация и сведения других банков в ФинЦЕРТ были положены в основу разосланных участникам информационного обмена рекомендаций Банка России по коллективному реагированию на действия хакеров.

Скоординированные и своевременные меры позволили успешно противостоять преступникам. Руководитель Сбербанка Герман Греф сказал: «Эта атака была в тысячу раз мощнее, чем те, что наблюдались раньше».

Центральный банк РФ, Минкомсвязи России, банки и мобильные операторы разрабатывают

новые меры борьбы с кибермошенниками. Так, 26 декабря 2016 г. на закрытом совещании была одобрена схема, предусматривающая предоставление мобильными операторами банкам данных о том, менял ли тот или иной клиент SIM-карту. Такая информация позволит предотвратить случаи кибермошенничества, когда хакеры с помощью вредоносных клонов узнают логин и пароль пользователя в интернет-банке, а потом у оператора мобильной связи приобретают новую SIM-карту для доступа к счетам клиентов, используя фальшивые номера и доверенности.

Эксперты отмечают, что данная схема взаимодействия в перспективе может стать альтернативой единой базе сотовых номеров российских граждан. 30 декабря 2016 г. Центральный банк РФ получил принципиально новые возможности в борьбе с вредоносными клонами. Имея особый статус компетентной организации, Банк России получил право выявлять распространяемые вредоносные программы, сайты с противоправным контентом и фишинговые окна.

Источниками информации о хакерских сайтах для Банка России будут собственный центр AIN SERT, информация правоохранительных органов, сведения от банковских и финансовых организаций и обращения российских граждан. Центральный банк РФ будет самостоятельно закрывать вредоносные сайты и предоставлять данные о кибермошенниках Координационному центру национального домена сети, что позволит в течение одного дня оперативно блокировать вредоносные и подозрительные сайты.

В прошлом году при содействии подразделения ФинЦЕРТ было заблокировано 1 588 распространяющихся вредоносных программ и фишинговых сайтов, угрожающих национальной платежной системе и финансовой и информационной безопасности кредитных организаций и граждан. При этом наибольшее число закрытых вредоносных сайтов пришлось на IV квартал 2016 г., только за ноябрь и декабрь их было закрыто более 1 000 [3].

Но эти показатели, надо признать, являются очень скромными по сравнению с общим количеством потенциально вредоносных сайтов, с помощью которых кибермошенники крадут деньги и у кредитных организаций, и у граждан. По данным Центрального банка РФ, ежемесячно выявляется в среднем от 3 до 4 тыс. новых вредоносных сайтов.

В любой момент в мире активно могут действовать сотни тысяч фишинг-страниц и сайтов, распространяющих вредоносное программное обеспечение. Получение Банком России новых возможностей в борьбе с кибермошенниками позволит реагировать более оперативно и значительно увеличить объемы блокирования опасных сайтов.

Банки, особенно крупные, научились противостоять атакам мошенников. По данным Центрального банка РФ, за последние полгода не было зафиксировано ни одной хакерской атаки на корсчета российских банков, которая завершилась бы кражей денег. При этом ФинЦЕРТ отмечает, что данный период ознаменовался ростом числа массовых рассылок электронных писем, содержащих зловредные программные клоны или ссылки на них, что говорит об усилении внимания кибермошенников к банкам.

Сегодня основной целью злоумышленников все-таки остаются интернет- и мобильные банки. Количество атак на них, по данным правоохранительных органов, ежегодно растет от 80 до 200%.

Взлом корсчета банка с помощью вредоносного программного обеспечения для преступников очень удобен – можно украсть и 50 млн, и 100 млн, и 500 млн руб., не вставая с дивана. И границы не имеют значения – мошенник, сидя дома в удобном кресле, в состоянии совершать преступные действия одновременно в ста странах.

Правовые законодательные акты, как правило, не поспевают за действиями преступников, в итоге те зачастую уходят от наказания. С развитием интернет-сервиса финансовых технологий число кибератак и на банки, и на клиентов будет возрастать. Кибермошенники не стоят на месте, активно привлекая IT-специалистов к разработке зловредных программных клонов. Однако президент компании Group-IB Илья Сачков, занимающийся расследованием интернет- и мобильных преступлений, считает: если сотрудники и клиенты банка знают правила технической защиты от преступников, то и сервер учреждения, и счета потребителей будут в безопасности [4].

Глава Банка России Эльвира Набиуллина, выступая на форуме Finopolis 2016 в Казани, предупредила банки о возрастающей угрозе киберпреступности. И это основной вызов, на который банкам нужно обращать особое внимание [5].

В настоящее время в РФ насчитывается 130 всевозможных нормативно-правовых актов, в которых подробно прописана правовая ответственность подразделений информационной безопасности банков и финансовых компаний. Автор считает, что назрела необходимость упорядочить все эти документы и на этой основе разработать единый отраслевой документ (закон) по информационной безопасности, который позволял бы банкам и финансовым организациям успешно и оперативно реагировать на постоянно растущие киберугрозы.

Предлагается разработать стратегии развития информационной безопасности финансово-кредитных организаций. К этому целесообразно привлечь все заинтересованные организации (банки, финансовые и IT-компании, операторов мобильной связи, МВД, ФСБ, Минкомсвязи России и др.), а Центральному банку РФ предложить роль межведомственного координатора.

Стратегия развития информационной безопасности позволит эффективно проводить целенаправленное прогнозирование, планирование и программирование в сфере информационной безопасности и позволит упорядочить совместную работу в этом сегменте заинтересованных лиц.

В настоящее время все хакерские сайты, имеющие российские домены, моментально блокируются или их обнаруживают сотрудники подразделения ФинЦЕРТ, но это не оказывает влияния на значительную часть вредоносных файлов, так как названные сайты обычно располагаются за пределами зон, контролируемых администраторами национальных, российских доменов верхнего уровня. А российские регистраторы не несут никакой ответственности за регистрируемые ими сайты.

Настало время разработать механизм срочной блокировки вредоносных сайтов с иностранными доменами. Для этого можно было бы заключить соответствующее соглашение и разработать механизм блокирования мошеннических сайтов с государствами СНГ, ОДКБ, Евразийского Союза.

Кроме того, сегодня не регламентируются требования к российским провайдерам и хостингам по качеству и срокам хранения данных о ресурсе и его владельце. Этот вопрос неоднократно поднимали не только банки, но и силовые структуры, так как у провайдеров невозможно получить сведения для проведения расследования. Предложения автора могли бы помочь в решении острой проблемы, связанной с отсутствием механизмов срочной блокировки вредоносных сайтов.

Таблица 1

Рейтинг безопасности интернет-банков по версии Markswebb Rank & Report

Table 1

Online Banking Security Rank: the Markswebb Rank & Report version

Банк	Итоговая оценка безопасности интернет-банка по шкале от 0 до 100 баллов
1. Интерактивный Банк	69,8
2. Ситибанк	61,5
3. Альфа-Банк	52
4. Тинькофф Банк	48,5
5. ВТБ24	47,5
6. Русский стандарт	47
7. Банк Москвы	45
8. Сбербанк	42,5
9. УРАЛСИБ	41,5
10. Промсвязьбанк	37,5
11. Росбанк	37,5
12. Хоум Кредит	37,5
13. Газпромбанк	37
14. Траст	33,5
15. Ренессанс Кредит	33,5
16. Открытие	29,5
17. ОТП Банк	29
18. Авангард	28,5
19. Райффайзенбанк	27,5
20. МТС Банк	25,5
21. БИНБАНК	25

Источник: Internet Banking Rank 2016

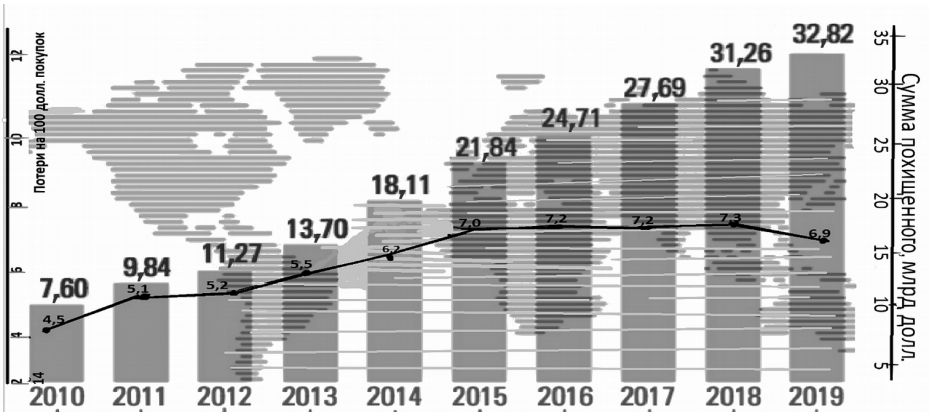
Source: Internet Banking Rank 2016

Рисунок 1

Объем мошенничества по банковским картам в 2010–2019 гг.

Figure 1

The volume of fraud with bank cards in 2010–2019



Источник: авторская разработка

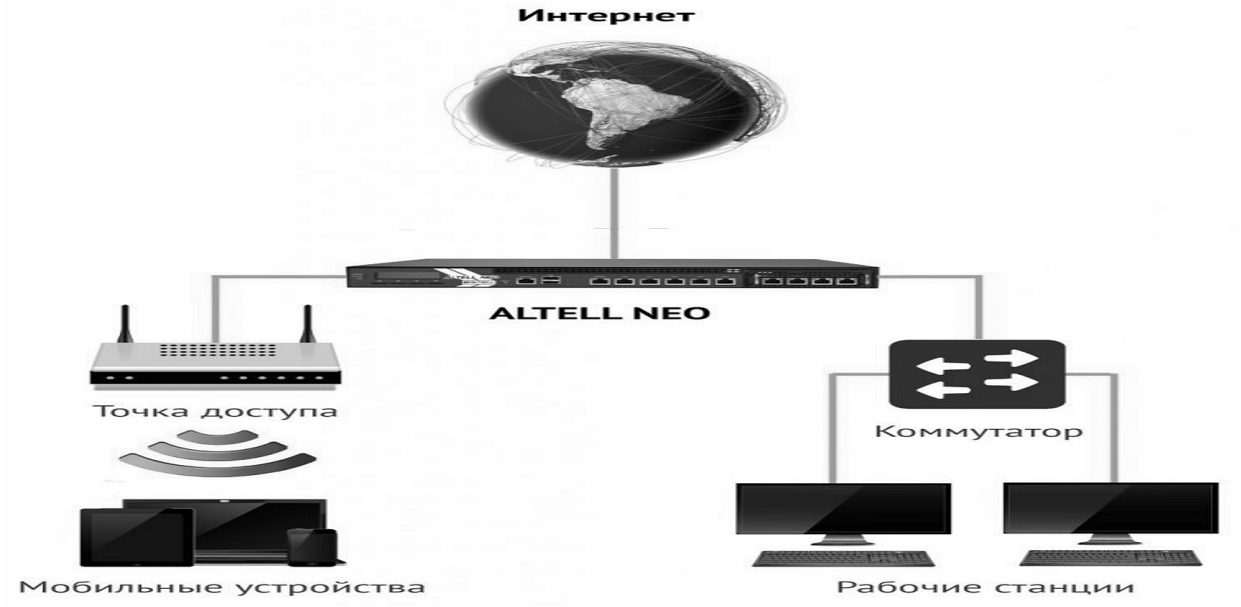
Source: Authoring

Рисунок 2

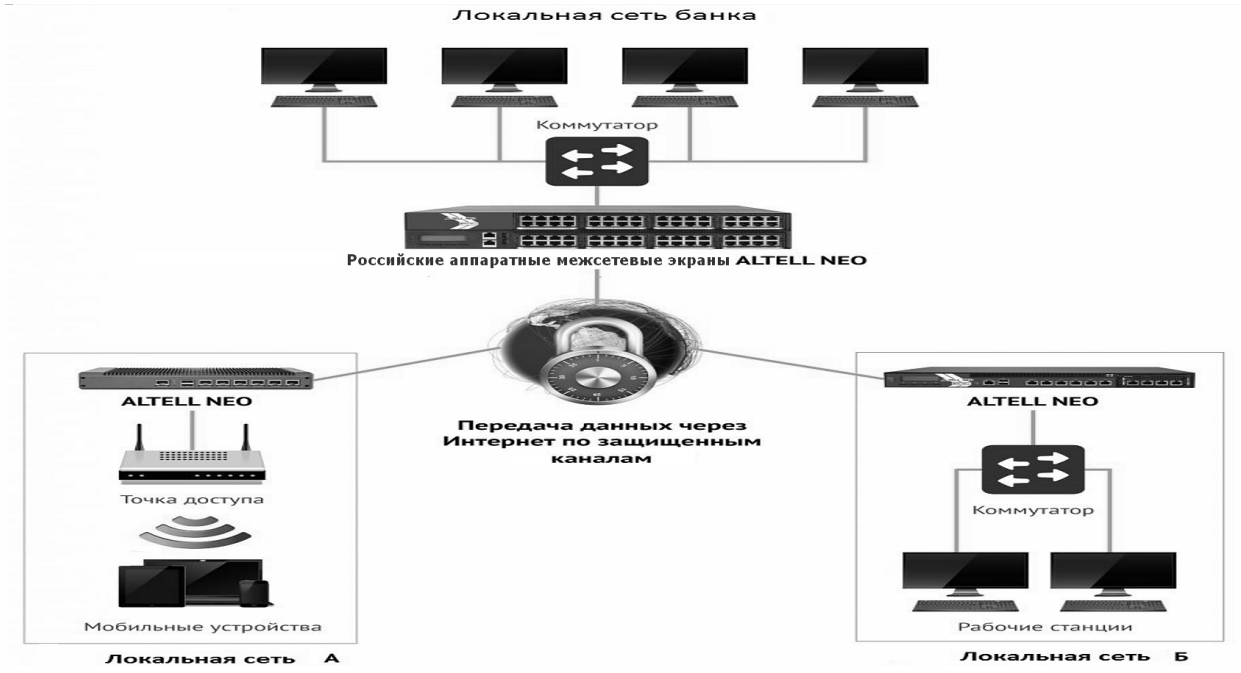
Организация защищенных информационных каналов:
а **– головных офисов;** *б* **– филиалов банка**

Figure 2

Organization of secure channels of head offices and branches of the bank:
а **– head offices;** *б* **– branches**



а



б

Источник: авторская разработка

Source: Authoring

Список литературы

1. *Данилин В.А., Барманова О.Р.* Рынок банковских карт в Самарской области – проблемы и перспективы // Деньги и кредит. 2004. № 12. С. 18–21.
2. *Киреева О.Л.* Банковская карта – прошлое, настоящее и будущее (гражданско-правовой аспект). URL: http://protivkart.org/main/515-kireeva-ol-bankovskaya-karta-proshloe-astoyaschee-i-buduschee-grazhdansko-pravovoy-aspekt.html
3. *Кондрашов В.А.* Тенденции развития банковских инноваций в современной России // Российское предпринимательство. 2012. № 8. С. 101–105.
4. *Косой А.М.* Современные деньги // Деньги и кредит. 2002. № 6. С. 42–52.
5. *Крахмалев С.В.* Современная банковская практика проведения международных платежей. М.: ГроссМедиа, РОСБУХ, 2007. 208 с.
6. *Куришев О.Ю.* Банковские карты как важный элемент банковского розничного бизнеса // Банковский ритейл. 2007. № 1. С. 18–22.
7. *Лукашок Ю.В.* Российский рынок пластика: тенденции развития и перспективные продукты // Банковский ритейл. 2008. № 3. С. 12–16.
8. *Лямин Л.В.* Анализ факторов риска, связанных с интернет-банкингом // Расчеты и операционная работа в коммерческом банке. 2006. № 5. С. 52–63.
9. *Мацепуро Н.А.* Принимаем к оплате пластик // Главная книга. 2009. № 9. С. 10–11.
10. *Панова Г.С.* Инновации в банковском бизнесе – искусство банковских технологий / Современные банковские технологии: теоретические основы и практика: под ред. Н.Ф. Карпычевой. М.: Финансы и статистика, 2005. С. 73–84.
11. *Пухов А.В.* Организация операционной работы по приему платежей физических лиц без открытия счета // Расчеты и операционная работа в коммерческом банке. 2007. № 5. С. 15–19.
12. *Спиранов И.А.* Правовое регулирование операций с банковскими картами. М.: ИнтерКрим-Пресс, 2000. 160 с.
13. *Куликов Н.И., Сизов А.А.* Банковское обслуживание с использованием пластиковых карт / Актуальные проблемы развития экономики, финансов, бухгалтерского учета и аудита в регионе. Вып. 2. Тамбов: ТГТУ, 2014. С. 135–140.
14. *Куликов Н.И., Сизов А.А.* Рынок пластиковых карт в России / Актуальные проблемы развития экономики, финансов, бухгалтерского учета и аудита в регионе. Вып. 2. Тамбов: ТГТУ, 2014. С. 140–144.
15. *Куликов Н.И., Сизов А.А.* Анализ схем правонарушений в области использования пластиковых карт // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2015. Вып. № 2. С. 61–69.

Информация о конфликте интересов

Я, автор данной статьи, со всей ответственностью заявляю о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке информации, написанию и подготовке статьи, принятию решения о публикации рукописи.

ISSN 2311-8768 (Online)
ISSN 2073-4484 (Print)

Risk, Analysis and Evaluation

INNOVATIVE FINANCIAL TECHNOLOGIES AND OPERATIONAL RISK IN REMOTE BANKING

Yuliya V. KUDRYAVTSEVA

Tambov State Technical University, Tambov, Russian Federation
Deutschenbebi@icloud.com

Article history:
Received 9 February 2017
Received in revised form
17 March 2017
Accepted 5 April 2017
Available online 15 June 2017

JEL classification: G15, G21, G29

https://doi.org/10.24891/fa.10.6.647

Keywords: IT-technology, cyber crime, fishing, malware, online bank, mobile banking

Abstract

Importance The article analyzes the advantage of development of remote banking with the use of IT-technologies, the revealed cyber crime, the way of theft prevention and trend in further development of innovative financial technologies and presents ALTELL NEO software.

Objectives The research aims at analyzing the losses of credit organizations on cyber crimes in Russia and all over the world. I show the reasons of swindler development, financial forecast for the next few years as well as new ways of struggle against cyber crime.

Methods I applied methods of analysis and synthesis of scientific and information base. Works of Russian and foreign scientists and experts in the field of theory and practice of economic and financial support form the methodological and theoretical basis of the study.

Results The paper reveals a trend in the bank services market: banks and credit organizations' counteraction to an increasing threat of cyber crime.

Conclusions and Relevance Disclosure and prevention of cyber crimes require growing up efforts. The Bank of Russia in collaboration with law enforcement and credit organizations carries out a range of programs of financial and informational security of the national payment service, commercial banks and citizens.

Acknowledgments

I express my great appreciation to Nikolai I. KULIKOV, Doctor of Economics, Professor, Head of Economics Department of the Tambov State Technical University, for advice and valuable comments on this article.

References

1. Danilin V.A., Barmapova O.R. [The development of banking card market in the Samara oblast – Problems and Perspectives]. *Den'gi i kredit = Money and Credit*, 2004, no. 12, pp. 18–21. (In Russ.)
2. Kireeva O.L. *Bankovskaya karta – proshloe, nastoyashchee i budushchee: grazhdansko-pravovoi aspekt* [The bank card and its past, present and future: civil and legal prospects]. Available at: http://protivkart.org/main/515-kireeva-ol-bankovskaya-kartaproshloe-nastoyaschee-i-buduschee-grazhdansko-pravovoy-aspekt.html (In Russ.)
3. Kondrashov V.A. [Trends in the development of banking innovations in modern Russia]. *Rossiiskoe predprinimatel'stvo = Russian Journal of Entrepreneurship*, 2012, no. 8, pp. 101–105. (In Russ.)
4. Kosoi A.M. [Modern money]. *Den'gi i kredit = Money and Credit*, 2002, no. 6, pp. 42–52. (In Russ.)
5. Krakhmalev S.V. *Sovremennaya bankovskaya praktika provedeniya mezhdunarodnykh platezhei* [Modern banking practice of international payments]. Moscow, GrossMedia, ROSBUKH Publ., 2007, 208 p.

6. Kurishev O.Yu. [Bank cards as an important element of retail banking business]. *Bankovskii riteil = Retail Banking*, 2007, no. 1, pp. 18–22. (In Russ.)

7. Lukashok Yu.V. [Russian plastics market: trends and promising products]. *Bankovskii riteil = Retail Banking*, 2008, no. 3, pp. 12–16. (In Russ.)

8. Lyamin L.V. [Analysis of risk factors associated with online banking]. *Raschety i operatsionnaya rabota v kommercheskom banke = Settlements and Transaction Activity in Commercial Bank*, 2006, no. 5, pp. 52–63. (In Russ.)

9. Matsepuro N.A. [We accept plastic cards]. *Glavnaya kniga = General Ledger*, 2009, no. 9, pp. 10–11. (In Russ.)

10. Panova G.S. *Innovatsii v bankovskom biznese iskusstvo bankovskikh tekhnologii. V kn.: Sovremennye bankovskie tekhnologii: teoreticheskie osnovy i praktika* [Innovation in the banking business: The art of banking technologies. In: Modern banking technology: Theoretical basis and practice]. Moscow, Finansy i Statistika Publ., 2005, pp. 73–84.

11. Pukhov A.V. [Organization of operations on acceptance of physical persons' payments without opening an account]. *Raschety i operatsionnaya rabota v kommercheskom banke = Settlements and Transaction Activity in Commercial Bank*, 2007, no. 5, pp. 15–19. (In Russ.)

12. Spiranov I.A. *Pravovoe regulirovanie operatsii s bankovskimi kartami* [Legal regulation of operations with bank cards]. Moscow, InterKrim-Press Publ., 2000, 160 p.

13. Kulikov N.I., Sizov A.A. *Bankovskoe obsluzhivanie s ispol'zovaniem plastikovykh kart. V kn.: Aktual'nye problemy razvitiya ekonomiki, finansov, bukhgalterskogo ucheta i audita v regione* [Banking services using plastic cards. In: Actual problems of economics, finance, accounting and auditing in the region]. Tambov, Universitetskaya kniga Publ., 2014, vol. 2, pp. 135–140.

14. Kulikov N.I., Sizov A.A. *Rynok plastikovykh kart v Rossii. V kn.: Aktual'nye problemy razvitiya ekonomiki, finansov, bukhgalterskogo ucheta i audita v regione* [Plastic cards market in Russia. In: Actual problems of economics, finance, accounting and auditing in the region]. Tambov, Universitetskaya kniga Publ., 2014, vol. 2, pp. 140–144.

15. Kulikov N.I., Sizov A.A. [The analysis schemes of offenses in the use of plastic cards]. *Nauchnyi zhurnal NIU ITMO. Seriya: Ekonomika i ekologicheskii menedzhment = Scientific Journal NRU ITMO. Series: Economics and Environmental Management*, 2015, no. 2, pp. 61–69. (In Russ.)

Conflict-of-interest notification

I, the author of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.