ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ В РОССИИ И РИСКИ НА ПУТИ ЕГО РАЗВИТИЯ

Н.В. Самочетова,
студент Института заочного и открытого образования, Финансовый университет при Правительстве РФ

Н.Н. Мартыненко,
к.э.н., доцент, кафедра «Банки и банковский менеджмент», Финансовый университет при Правительстве

ONLINE BANKING IN RUSSIA AND RISKS ON THE WAY OF ITS DEVELOPMENT

Samochetova N.V., Martynenko N.N.

Annotation
Within this article the content of online banking is considered. Key risks specific to the online banking are analyzed and ways of the mitigation of these risks are proposed.

Key words:
Online banking, Internet banking, risks of online banking, risk minimization.

Аннотация
В рамках данной работы рассматривается содержание дистанционного банковского обслуживания. Анализируются основные риски, характерные для дистанционного банковского обслуживания, и предлагаются пути их минимизации.

Ключевые слова:
Дистанционное банковское обслуживание, интернет-банкинг, риски дистанционного банковского обслуживания, минимизация рисков.

Для банковского сектора характерна постоянная борьба за клиентов между банками. В связи с этим банки вынуждены непрерывно совершенствовать свою деятельность, меняя формы и методы обслуживания. Особое место в деятельности современного банка приобретают IT-технологии, которые позволяют обслуживать клиентов дистанционно. Однако, открывая новые возможности для клиентов, банки сталкиваются и с новыми рисками, которые не присущи традиционному банковскому обслуживанию.

В законодательстве РФ имеется определение понятия системы дистанционного банковского обслуживания, однако единого представления о понятии самого дистанционного банковского обслуживания (далее – ДБО) пока не сложилось. Согласно пункту 1.2 Письма ЦБР от 26 октября 2010 г. № 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания», система ДБО – это совокупность установленных в кредитной организации (её филиалах, представительствах и внутренних структурных подразделениях) аппаратно-программных средств, с помощью которых осуществляется дистанционное банковское обслуживание.

Понятие дистанционного банковского обслуживания не только не прописано в законодательстве РФ, но и не имеет общепринятой трактовки в научной и деловой литературе. Предлагается рассматривать ДБО как способ обслуживания клиентов банка с использованием информационно-телекоммуникационных технологий, предполагающий взаимодействие банка с клиентами без посещения последними банковского отделения, т.е. через удаленные каналы обслуживания.

Основные и наиболее развитые формы ДБО представлены через следующие каналы доступа к банковским услугам:

- ПС-банкинг (PC-banking) (системы «клиент-банк»);
- телефонный банкинг (phone-banking) или телебанкинг;
- интернет-банкинг (Internet-banking);
- мобильный банкинг (mobile-banking);
- обслуживание через банкоматы (ATM-banking), устройства банковского самообслуживания.

В связи с развитием ДБО к рискам традиционных банковских операций добавились риски, связанные с дистанционными банковскими сервисами. Несмотря на преимущества использования систем ДБО для банка и клиента, существуют неотъемлемые риски, которые необходимо минимизировать.

Очевидным является тот факт, что при использовании систем ДБО меняется профиль рисков банков. Появляются новые специфические риски, связанные с оказанием услуг при участии информационно-коммуникационных технологий. Однако не все банки разрабатывают систему управления подобными рисками, что впоследствии может повлечь финансовые потери, как самого банка, так и его клиентов. При использовании систем ДБО контролю должны подлежать внутрибанковские процессы и процессы, обеспечивающие взаимодействие с провайдерами, а также процессы обмена информацией при проведении клиентами расчетов.[1]

Риски ДБО в большей степени носят технологический характер. Кроме этого ДБО связано с операционными, правовыми, стратегическими рисками (в случае ошибочных решений органов управления банка о внедрении, сопровождении и развитии систем ДБО), риском потери деловой репутации (при потере данных клиентов, утечке финансовой информации клиентов, негативной оценке клиентами качества ДБО, сбоях функционирования систем ДБО и др.), риском ликвидности.[2]

Операционный риск – это риск, связанный с возникновением прямых и косвенных потерь в результате несоответствия характеру и масштабам деятельности банка или требованиям установленных банком внутренних порядков и процедур проведения операций и заключения сделок, их нарушение сотрудниками банка и иными лицами (например, вследствие непреднамеренных или умышленных действий и бездействий) или в результате воздействия внешних факторов.[3] Для минимизации операционного риска при дистанционном обслуживании необходимо иметь квалифицированный персонал в данной области, надлежащую систему безопасности для предотвращения несанкционированного доступа, правильную организацию информационных потоков, процессов и процедур.

Стратегический риск связан с отсутствием и недостаточной проработанностью стратегии развития ДБО в банке. Банк может выбрать неоптимальный набор услуг, который будет предоставляться через дистанционные сервисы. Все это ведет к нерациональным затратам на развитие ДБО. Для решения данной проблемы банки при разработке стратегии должны определиться, для какого клиентского сегмента будет использоваться ДБО. Необходимо просчитать финансовые показатели различных направлений развития ДБО и определить, какие из них будут приносить выгоду. Коммерческие банки в России не всегда уделяют этой проблеме должное внимание. Проблема оценки эффективности внедрения и развития систем ДБО заключается в том, что ДБО зачастую предлагает бесплатное оказание услуг, то есть судить об эффективности по прибыли не является верным. Эффект от применения ДБО заключается в экономии затрат на содержание банковской сети офисов, расширении и удержании клиентской базы банка и повышении качества обслуживания. Данные эффекты, в свою очередь, повышают конкурентоспособность банка.

Для рациональной оценки эффективности ДБО банкам стоит использовать комплексные подходы, включающие в себя аспекты различных методов оценки. Определить чистую прибыль или доход от ДБО сложно, поскольку ДБО влияет на сокращение издержек банка и расширение клиентской базы, прирост дохода от платы клиентов за дистанционное обслуживание незначителен. Поэтому необходимо использовать качественные критерии оценки и проводить сравнительную характеристику затрат по обслуживанию клиентов при дистанционном и традиционном подходах.

Актуальным в период кризиса может стать риск потери деловой репутации. Он связан с недоверием клиентов к банку вследствие нарушений в функционировании систем ДБО. Для предотвращения ухода клиентов из банка необходимо постоянно

---

[1] Курныкина О.В., Курныкин Н.Е. Организация системы внутреннего контроля в условиях развития электронных банковских технологий и ДБО // Банковское дело. 2013. № 5. С. 78.

[2] Ковалева Н.А. Поле дистанционного обслуживания: грамотный клиент, безопасный сервис // Управление в кредитной организации. – 2014. – №4. – С.4.

[3] Смагина М.Н., Сорина Е.И., Золотарева Г.М. Внутренний аудит и менеджмент операционных рисков системы дистанционного банковского обслуживания // Вестник ТГУ. – 2015. – №8 (148). – С. 38.

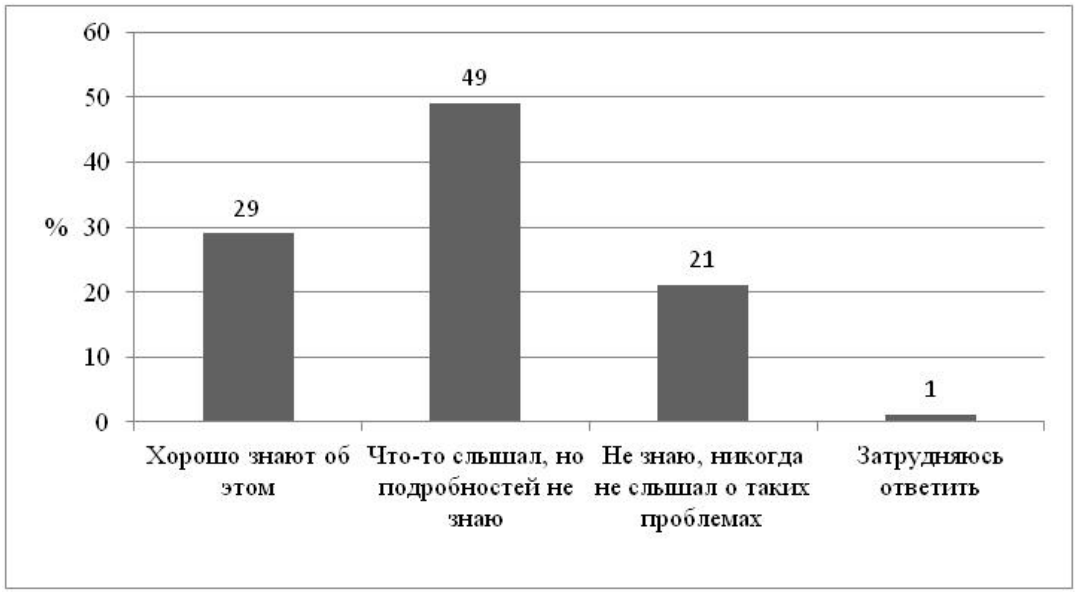

График 1. Ответы на вопрос: «Знаете ли вы о том, что бывают случаи мошенничества в сфере использования банковских карт?», % от всех опрошенных.

Составлено автором, источник: Исследование НАФИ «Проблемы мошенничества в сфере использования банковских карт», 2014.

проводить мониторинг качества обслуживания клиентов. В период экономической нестабильности малейший сбой в обслуживании клиентов может повлиять на отношение к банку и спровоцировать сокращение клиентской базы.

Одной из самых острых проблем ДБО является безопасность дистанционных сервисов. Технологические риски будут всегда сопровождать ДБО, поэтому управление данными рисками должно стать одной из приоритетных задач развития системы ДБО любого банка. С каждым годом увеличиваются случаи кибератак, мошенничество активно развивается в сети Интернет. Особенно привлекательными для мошенников являются дистанционные сервисы банков. По данным МВД России, средний ущерб по каждой кибератаке составляет более 3 млн. руб. Анализ возможных косвенных потерь банка: от 1,3 до 1,5 млн. руб. за день проведения атаки.[4]

Безусловно, ни один банк не сможет обеспечить абсолютную защиту от кибермошенничества. Но непрерывная работа по поддержанию должного уровня информационной безопасности может существенно осложнить и/или свести к минимуму возможности кибермошенников.

Согласно исследованиям PwC, несмотря на рост расходов ИТ-бюджетов компаний по всему миру на обеспечение информационной безопасности, убытки от кибератак растут более высокими темпами, чем расходы на их предотвращение. На круглом столе Ассоциации российских банков в марте 2015 года руководитель проектов ООО “С-Терра СиЭсПи” Роман Харитонов отметил, что российские банки часто не только не увеличивают бюджет на ИТ-безопасность, но и сокращают его. По его прогнозам, банки будут приобретать меньше инструментов информационной безопасности, чем раньше.[5] При этом в мире в 2015 году наблюдался рост инвестиций компаний в сферу кибербезопасности, развивалось страхование киберрисков, возрастала значимость роли руководителя по информационной безопасности.[6]

Кибермошенники постоянно совершенствуют методы своей незаконной деятельности. Перед банком стоит непростая задача – найти решение для обеспечения информационной безопасности,

[4] «Денис Калемберг: «подводные камни» безопасности ДБО. – [URL]: http://www.itsec.ru/articles2/Oborandteh/podvodnie-kamni-bezopasnosti-dbo-opit-realizovannih-proektov

[5] Информационная безопасность банков: допустимо ли в сложившейся ситуации экономить на ней? // Национальный банковский журал. – 2015. – №3 (131). – [URL]: http://www.aladdin-rd.ru/company/pressroom/articles/42782/

[6] Кибербезопасность в России: только факты. Ответ бизнеса на актуальные вызовы и угрозы. – [URL]: http://www.pwc.ru/ru/press-releases/2015/global-state-information-security.html

при котором клиент еще соглашается потратить некоторую сумму на защиту своих операций, а мошеннику уже невыгодно совершать незаконное действие. Такое решение может включать:

1) выполнение организационных мероприятий;
2) выбор аппаратно-программного средства защиты;
3) тщательный подход к составлению договора и т.д.[7]

Важнейшей проблемой не только ДБО, но и всей финансовой системы России является низкий уровень финансовой грамотности населения. Данная проблема повышает риски информационной безопасности ДБО. В конце 2014 г. НАФИ представило результаты исследования информированности россиян о схемах мошенничества с банковскими картами.

Половина опрошенных «что-то слышали, но не знают подробностей» о случаях мошенничества банковских карт, лишь 29 % хорошо знают об этом. 17 % респондентов считают, что оплачивать товары и услуги через интернет-банки очень опасно. Процент опрошенных, сталкивающихся с мошенничеством в течение последних пяти лет, в 2014 г. увеличился по сравнению с 2013 г. до 15 % (с 12 %). При этом осведомленность опрошенных о способах защиты от мошенничества увеличилась в 2014 г. по сравнению с 2013 г.

Риск информационной безопасности также связан с законодательством, которое, по мнению автора, недостаточно его ограничивает в России. Нормативная база отстает от изменений в сфере ДБО. Целесообразно считать, что в России полностью еще не сформировалась нормативно-правовая база в области ДБО.

В законодательстве Российской Федерации (далее – РФ) существует Письмо Банка России от 26.10.2010 N 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания». Рекомендации, указанные в данном письме, ориентированы на снижение уровня банковских рисков, связанных с использованием кредитными организациями аутсорсинга.

Одним из важнейших нормативно-правовых актов РФ в области ДБО является Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 29.12.2014) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 01.03.2015). С 1 января 2014 года в закон была внесена поправка, согласно которой банки обязаны возместить клиенту денежные средства в случае, если они были украдены мошенниками.

На многих сайтах в сети Интернет клиенты банков рассказывают истории о столкновении с мошенниками при работе в сервисах ДБО. Одна из частых историй описывает ситуацию, когда клиент заходит в интернет-банк через сайт, вводит свои данные, но войти в личный кабинет ему не удается. Как правило, это означает, что клиент банка зашел на поддельную страницу официального сайта (фишинговую страницу) и предоставил свои данные мошенникам.

Должен ли банк в подобной ситуации вернуть денежные средства клиенту? Фишинг – это вид мошенничества, целью которого является получения конфиденциальной информации о банковских картах, логинах и паролях интернет-банков и т.д., создание мошеннических копий официальных сайтов банков и приложений банков для телефонов.[8] Попасть на подобный сайт клиент может, если не проверил правильность адреса сайта банка. Согласно п. 15 ст. 9 161-ФЗ в случае исчезновения средств клиента с его счета, оператор по переводу денежных средств обязан вернуть деньги клиенту, если не докажет, что незаконное списание произошло по вине клиента. В данном случае клиент стал жертвой мошенника по своей вине в связи с недостаточной осведомленностью о мерах безопасности работы в интернет-банке.

Из 161-ФЗ для банков вытекает правовой риск. Он связан с тем, что в случае спорной ситуации, связанной с хищением средств клиентов, банк могут обязать возместить средства, даже если хищение произошло не по его вине. Однако на практике банки не всегда возмещают средства, а правоохранительные органы неохотно берутся за расследование киберпреступлений.

Основные проблемы при расследовании подобных уголовных дел связаны со сложностью в

[7] Ревенков П.В., Бердюгин А.А. Безопасность электронного банкинга: услуга и обязанность банка // Банковское дело. – 2015. – №8 (632). – С. 5-6.

[8] Волков Д. Кибермошенничество в России: эволюция угроз // Банковские технологии. 2015. № 01 (228). С. 26.

установлении самого события преступления, отсутствием у следователей опыта расследования подобных преступлений и знания компьютерной техники.[9]

В России на сегодняшний момент не существует единых требований к обеспечению безопасности систем ДБО. Однако такие требования планируется ввести в 2017 году. Это следует из плана развития электронного взаимодействия на финансовом рынке, утвержденного Зампредом Правительства РФ Аркадием Дворковичем. В разработке стандартов информационной безопасности активно будет участвовать Центр по борьбе с киберугрозами, созданный при ЦБ РФ (документы о его создании подписаны в мае 2015 года).[10] На первый взгляд, данный шаг должен был быть принят давно. Однако не все представители банковского бизнеса согласны с таким подходом. Так, директор департамента корпоративных финансов Deloitte & Touche CIS Алексей Ивлев, уверен, что об обязательности выполнения банками стандартов ЦБ РФ в сфере ДБО речи быть не должно – это должно быть заложено в политике риск-менеджмента банка и допустимого риска в каналах ДБО.

Говоря о принципах риск-менеджмента в банке, необходимо отметить рекомендации Базельского комитета по банковскому надзору. Еще в 2003 году Базельский комитет по банковскому надзору выпустил документ под названием Принципы риск-менеджмента электронного банкинга (Risk Management Principles for Electronic Banking). Данный документ содержит 14 принципов управления рисками электронного банкинга. Первые три принципа относятся к установлению контроля со стороны Совета директоров и менеджмента банка. Следующие семь принципов объединяются в группу по контролю безопасности. Наконец, последние четыре принципа относятся к управлению правовым и репутационным рисками. Данные принципы носят рекомендательный характер и являются актуальными и в настоящее время.

Подводя итог проведенному анализу рисков ДБО, можно предложить следующие пути минимизации рисков.

Необходимо повысить финансовую грамотность населения. Это позволит снизить недоверие клиентов к банкам, следовательно, уменьшить репутационные риски и повысить осведомленность граждан о возможных мошеннических схемах, то есть снизить риски информационной безопасности. Банки должны информировать клиентов о рисках ДБО. Возможно введение в договоре пункта обязательного ознакомления с основными принципами безопасного пользования дистанционными сервисами.

В России остается непроработанной законодательная база в сфере ДБО. Следует ввести общие требования к минимальному уровню безопасности систем ДБО банков, разместить на сайте ЦБ РФ Принципы риск-менеджмента электронного банкинга, представленные Базельским комитетом по банковскому надзору.

В крупных банках, активно оказывающих услуги дистанционного обслуживания, целесообразно создать специальные отделы (форензик), занимающиеся расследованием кибермошенничества. К основным задачам, решаемым с помощью такого отдела, относятся:

1) разработка тактики оперативно-розыскных мероприятий и следственных действий, связанных с компьютерной информацией;
2) создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений;
3) установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.[11]

ДБО будет активно развиваться в будущем, а риски, его сопровождающие, модифицироваться. Поэтому банки должны тщательно подходить к вопросам риск-менеджмента в сфере ДБО, учитывать все имеющиеся риски и использовать в совокупности различные меры для их минимизации. В свою очередь ЦБ РФ должен способствовать разработке более полного законодательства в сфере ДБО и учитывать зарубежный опыт.

[9] Ревенков П.В., Тер-Аветисян Х.А. Возрастание правового риска в условиях дистанционного банковского обслуживания // Финансы и кредит. – 2014. – №18 (594). – С. 30.

[10] В России появятся правила безопасного интернет-банкинга. – [URL]: http://izvestia.ru/news/587549

[11] Ревенков П.В., Бердюгин А.А. Безопасность электронного банкинга: услуга и обязанность банка // Финансы и кредит. – 2015. – №8 (632). – С. 4.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 29.12.2014) «О национальной платежной системе»
2. Письмо ЦБР от 26 октября 2010 г. № 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания»
3. Волков Д. Кибермошенничество в России: эволюция угроз // Банковские технологии. 2015. № 01 (228). С. 26-28.
4. Ковалева Н.А. Поле дистанционного обслуживания: грамотный клиент, безопасный сервис // Управление в кредитной организации. – 2014. – №4. – С.1-7.
5. Курныкина О.В., Курныкин Н.Е. Организация системы внутреннего контроля в условиях развития электронных банковских технологий и ДБО // Банковское дело. 2013. № 5. С. 78-81.
6. Ревенков П.В., Тер-Аветисян Х.А. Возрастание правового риска в условиях дистанционного банковского обслуживания // Финансы и кредит. – 2014. – №18 (594). – С. 29 – 35.
7. Ревенков П.В., Бердюгин А.А. Безопасность электронного банкинга: услуга и обязанность банка // Финансы и кредит. – 2015. – №8 (632). – С. 2-10.
8. Смагина М.Н., Сорина Е.И., Золотарева Г.М. Внутренний аудит и менеджмент операционных рисков системы дистанционного банковского обслуживания // Вестник ТГУ. – 2015. – №8 (148). – С. 38-44.
9. Информационная безопасность банков: допустимо ли в сложившейся ситуации экономить на ней? // Национальный банковский журнал. – 2015. – №3 (131). – [URL]: http://www.aladdin-rd.ru/company/pressroom/articles/42782/
10. Кибербезопасность в России: только факты. Ответ бизнеса на актуальные вызовы и угрозы. – [URL]: http://www.pwc.ru/ru/press-releases/2015/global-state-information-security.html
11. В России появятся правила безопасного интернет-банкинга. – [URL]: http://izvestia.ru/news/587549