Банковская деятельность

УДК 336.71

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ РЕГУЛИРОВАНИЯ ЭЛЕКТРОННОГО БАНКИНГА

Павел Владимирович Ревенков,
доктор экономических наук,
профессор кафедры экономического анализа
и бухгалтерского учета,
Одинцовский гуманитарный университет,
Одинцово, Московская область,
Российская Федерация
pavel.renenkov@mail.ru

Алексей Леонидович Поспелов,
преподаватель кафедры экономического анализа
и бухгалтерского учета,
Одинцовский гуманитарный университет,
Одинцово, Московская область,
Российская Федерация
pal@cbr.ru

Предмет/тема. *В статье отмечается актуальность проблемы регулирования электронного банкинга.*

Цели/задачи. *Изучены наиболее важные направления регулирования банковской деятельности в условиях электронного банкинга.*

Методология. *Объектом исследования выступила банковская система Российской Федерации.*

Результаты. *Отмечено, что основу электронного банкинга составляют: интернет-банкинг (управление банковскими счетами и картами через Интернет и web-браузер в режиме on-line) и мобильный банкинг (управление банковскими счетами и картами с лэптопов, коммуникаторов, смартфонов и других аналогичных устройств). Системы электронного банкинга позволяют клиентам кредитных организаций иметь круглосуточный доступ к своим счетам и совершать банковские операции (разрешенные в соответствии с заключенным договором). Наряду с очевидными преимуществами эти системы привнесли в банковский бизнес дополнительные риски. Точнее, количество банковских рисков осталось прежним, но значительно возросла их техническая составляющая. На уровень рисков повлияли: расширение профиля операционного риска в условиях электронного банкинга; значительный рост числа киберпреступлений в финансовой сфере (включая хищения денежных средств в системах электронного банкинга); использование систем электронного банкинга в схемах, направленных на легализацию преступных доходов (отмывание денег); недостаточная подготовка сотрудников коммерческих банков по вопросам обеспечения информационной безопасности и управления сопутствующими рисками в условиях электронного банкинга.*

Проанализирована каждая из четырех указанных причин возникновения дополнительных источников рисков. Представлены наиболее актуальные задачи для регулирующих органов и кредитных организаций по минимизации рисков в условиях электронного банкинга.

Выводы/значимость*. Сделан вывод, что новейшие достижения в области информационных и коммуникационных технологий на основе использо-*

вания глобальной сети Интернет и возможностей сотовой связи создали идеальные условия для внедрения технологии электронного банкинга.

***Ключевые слова**: электронный банкинг, регулирование, операционный риск, информационная безопасность, отмывание денег*

Технический прогресс, достижения в сфере информационных и коммуникационных технологий, создание глобальной сети Интернет, возможности сотовой связи стали основной базой для внедрения и распространения технологии электронного банкинга.

Компонентами данной технологии являются:

– интернет-банкинг (управление банковскими счетами и картами через Интернет и web-браузер в режиме on-line);

– мобильный банкинг (управление банковскими счетами и картами с КПК, коммуникаторов, смартфонов и других аналогичных устройств) [11].

Системы электронного банкинга позволяют клиентам кредитных организаций иметь круглосуточный доступ к своим счетам и совершать разрешенные в соответствии с заключенным договором банковские операции.

Каждый крупный банк предлагает сейчас услуги электронного банкинга. Эти системы дают возможность клиентам, не посещая отделений банков, осуществлять большую часть банковских операций:

– управлять средствами на своих счетах;

– обменивать валюту;

– совершать платежи и переводы;

– оплачивать мобильную связь, Интернет, коммунальные услуги, налоги, штрафы, услуги государственных учреждений.

Электронный банкинг позволяет размещать и пополнять вклады и погашать кредиты, а также совершать многие другие операции [12].

С помощью таких систем не только расширяется перечень потенциальных возможностей клиента, но и значительно экономятся средства банка, расходуемые на поддержание дополнительных офисов и представительств на удаленных территориях.

По мнению основателя первого в мире мобильного банка Movebank Б. Кинга, к 2016 г. среднестатистический клиент розничного банка в развитых странах будет взаимодействовать с ним следующим образом:

– с отделением – 1–2 раза в год;

– с колл-центром, системой интерактивного речевого ответа IVR – 5–10 раз в месяц;

– через банкомат – 3–5 раз в месяц;

– через Интернет/планшетные экраны – 7–10 раз в месяц;

– через мобильный телефон – 20–30 раз в месяц [5].

По данным исследования, проведенного специалистами компании Juniper Research, к концу 2019 г. более 1,75 млрд владельцев мобильных устройств (каждый третий взрослый житель Земли) будут использовать их для банковских операций. Для сравнения, в настоящее время сервисами мобильного банкинга пользуются около 800 млн чел. во всем мире[1].

В РФ в 2013 г. выросло количество интернет-пользователей. Теперь интернет-ресурсы используют 68,7 млн россиян. Об этом свидетельствуют результаты исследования ЦСУ Enter и Google, которое было посвящено анализу онлайн-ритейла в России[2].

Но наряду с очевидными преимуществами, системы электронного банкинга привнесли в банковский бизнес дополнительные риски. А если быть точнее, то количество типичных банковских рисков[3] осталось прежним, а вот их техническая составляющая значительно возросла.

Непрерывность выполнения банковских операций стала во многом зависеть от различных факторов:

– различных сбоев в аппаратно-программном обеспечении систем электронного банкинга;

– качества и надежности каналов связи;

– наличия резервных источников электропитания;

– качества архивации данных об операциях с использованием систем электронного банкинга;

– надежности в обеспечении информационной безопасности конфиденциальных сведений.

Следует понимать, что, применяя современные технологии и средства, можно осуществить те или иные процедуры быстрее и в гораздо больших объемах, однако при этом не надо рас-

[1] Через 5 лет каждый третий взрослый житель планеты будет пользоваться мобильным банкингом // MoneyNews. 2014. 09 июля.

[2] 68,7 млн россиян пользуются Интернетом // НИА-Федерация (nia-rf.ru). 2014. 08 июля.

[3] Перечень типичных банковских рисков приведен в письме Банка России от 23.06.2004 № 70-Т «О типичных банковских рисках».

считывать на чудеса – за все приходится платить. И если регулирование в области дистанционного банковского обслуживания (ДБО), включая услуги электронного банкинга, будет отставать от распространения новых источников типичных банковских рисков, то все эти новшества в целом обойдутся дороже. В первую очередь возрастают затраты на обеспечение безопасности данного способа оказания банковских услуг, так как кредитные организации будут вынуждены учитывать не только внутрибанковские риски, но и риски, возникающие на стороне клиента и различных провайдеров (например, интернет-провайдеры в случае интернет-банкинга, сотовые операторы в случае мобильного банкинга)[4].

По мнению авторов, есть четыре причины, по которым применение систем электронного банкинга нуждается в дополнительном регулировании:

1) расширение профиля операционного риска в условиях электронного банкинга;

2) значительный рост числа киберпреступлений в финансовой сфере (включая хищения денежных средств);

3) использование систем электронного банкинга в схемах, направленных на легализацию преступных доходов (отмывание денег) [4];

4) недостаточная подготовка сотрудников коммерческих банков по вопросам обеспечения информационной безопасности и управления сопутствующими рисками в условиях электронного банкинга.

Причиной повышенного внимания к операционному риску стал выход соглашения Базельского комитета по банковскому надзору «Международная конвергенция изменения капитала и стандартов капитала: новые подходы» – Basel II.

Соглашение Basel II является одним из наиболее актуальных нормативных актов, регулирующих банковский сектор. Оно предъявляет требования к минимальному размеру банковского капитала, на основании которых кредитные организации обязаны оценивать операционные, рыночные и кредитные риски, а также резервировать капитал на их покрытие. Basel II трактует операционный риск как риск убытков, возникающий в результате неадекватных или ошибочных внутренних процессов, действий сотрудников и систем или в результате внешних событий.

В качестве возможных проявлений операционного риска можно выделить следующие типы событий:

– внешние воздействия (наводнения, пожары, аварии и т.п.);

– внутренние и внешние мошенничества;

– ошибки персонала;

– сбои в реализации бизнес-процессов и обслуживании клиентов;

– физический ущерб активам;

– сбои информационных систем;

– нарушение процессов обработки и хранения данных.

Требования, предъявляемые документами Basel II, были дополнены в документах Basel III, в том числе и в отношении операционного риска.

Отметим, что Базельский комитет по банковскому надзору рекомендует привлекать к процессу управления рисками, возникающими при внедрении в кредитных организациях систем электронного банкинга (ЭБ), не только риск-подразделения, но и совет директоров, высшее руководство банка, а также топ-менеджеров банка [17–21].

Операционный риск является одним из основных типичных банковских рисков, на который в большей степени оказывают влияние системы ЭБ. Он определяется как вероятность образования убытков и/или неполучение прибыли вследствие сбоев в выполнении каждодневных, рутинных банковских операций.

Применительно к электронному банкингу выделяются три главные зоны операционного риска:

– функционирование системы безопасности;

– привлечение сторонних организаций к предоставлению некоторых видов электронных банковских услуг (аутсорсинг);

– освоение новых технологий сотрудниками банка.

В первом случае речь идет о том, что возможны нарушения в процессах электронного хранения, передачи и обработки информации (искажение, уничтожение, перехват данных или злоупотребление ими в результате технических неполадок, действий хакеров, ошибок или мошенничества персонала и клиентов) и отказы в функционировании банковских информационных систем (возникновение перегрузок из-за недостаточной мощности аппарат-

[4] Следует отметить, что риски, возникающие на стороне различных провайдеров и сотовых операторов, контролировать сотрудникам кредитных организаций весьма затруднительно (а в ряде случаев – невозможно).

но-программного обеспечения и целенаправленных DoS-атак[5] на web-серверы банка) [1, 7, 13].

Вторая потенциально подверженная операционному риску сфера становится в последнее время весьма значимой. Предоставление банковских услуг в области информационных технологий посредством специализированных фирм (в первую очередь банки сотрудничают с компаниями по разработке прикладных программ) позволяет сократить инвестиционный бюджет и избежать найма дорогостоящих специалистов, что особенно важно для небольших финансовых учреждений. В то же время банки становятся в определенной степени зависимыми от подобных партнеров, а общий уровень банковского обслуживания начинает определяться результатами работы нескольких, нередко никак не связанных между собой компаний, сотрудники которых могут и не обладать достаточными знаниями о специфике банковского дела.

Наконец, ускорение процесса модернизации информационных систем повышает требования к адаптационным способностям персонала банков и увеличивает опасность возникновения трудностей при переходе ко все более сложным интегрированным электронным решениям. Довольно часто внедрение более «умной» и производительной технологии оборачивается для работников и клиентов банков значительными проблемами[6].

Смысл управления операционным риском заключается в прогнозе периодичности различных сбоев и нарушений непрерывности функционирования аппаратно-программного обеспечения систем электронного банкинга и в оценке величины вероятных убытков. Отметим, что у потерь есть и положительная сторона: они вскрывают слабые места и открывают новые возможности. Поэтому самая большая ошибка – сокрытие нежелательного инцидента. Даже после устранения рисковой ситуации или последствий неблагоприятного события нельзя оставлять происшедшее в тайне, гораздо лучше использовать инцидент в качестве наглядного урока для других сотрудников [15].

Формы проявления операционного риска в условиях электронного банкинга могут быть самыми разнообразными. Однако все они вызваны, как правило, несоответствием определенных процедур требованиям законодательства, несоразмерностью технических возможностей систем и объема бизнеса, техническими сбоями и отказами оборудования, непреднамеренными или умышленными действиями персонала и внешних субъектов, что соответствует классическому определению операционного риска.

Минимизировать операционный риск в условиях электронного банкинга можно с помощью общепринятых стратегий:

– принятие риска (отказ от превентивных мероприятий, воздействие на источники риска, самострахование – в том числе через кэптивные страховые компании, диверсификация активов и т.д.);

– полная или частичная передача риска (страхование, хеджирование, синдицирование и т.п.);

– избежание риска (отказ от применения данной системы, профилактика как устранение источников риска и проч.).

Следующая проблема связана с возрастанием активности киберпреступников, чьи усилия направлены на хищение денежных средств клиентов банков, использующих для выполнения своих операций системы электронного банкинга.

В связи с этим Банк России рекомендовал кредитным организациям организовать сбор информации о выявленных атаках вредоносным кодом на системы ДБО и об обстоятельствах их обнаружения, провести систематизацию и анализ такой информации, довести ее до сведения органов управления кредитной организации, а также информировать компании – разработчиков средств защиты от вредоносного кода. Также регулятор предложил информировать клиентов (пользователей систем ДБО) банков о новых разновидностях вредоносного кода, угрожающих безопасности клиентских автоматизированных рабочих мест систем ДБО, способах защиты от их воздействия и устранения последствий такого воздействия[7].

По данным, полученным Центром стратеги-

[5] DoS-атака (от англ. Denial of Service – отказ в обслуживании) и DDoS-атака (от англ. Distributed Denial of Service – распределенный отказ в обслуживании) – разновидности атак на вычислительную систему. Цель этих атак – довести систему до отказа, т.е. создать такие условия, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет затруднен.

[6] В основном это связано с обучением персонала и совершенствованием методик проведения проверок специалистами риск-подразделений и служб внутреннего контроля.

[7] Письмо Банка России от 24.03.2014 № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности».

ческих и международных исследований (CSIS), киберпреступления ежегодно наносят ущерб мировой экономике в размере 445 млрд долл.

В 2013 г. из-за киберпреступлений пострадали как минимум 40 млн американцев, а также одна нефтяная компания, чьи сведения по разведке месторождений попали к хакерам. США, Китай, Япония и Германия ежегодно теряют около 200 млрд долл. Потери, связанные с личными данными граждан, оцениваются в 150 млрд долл[8].

По статистике известной российской компании Group-IB, специализирующейся на расследовании компьютерных преступлений, объем российского рынка киберпреступности в 2013 г. достиг 2,44 млрд долл.[9].

Компьютерные злоумышленники в настоящее время совсем не похожи на тинэйджеров, получивших первоначальные знания с хакерских web-сайтов. Это специалисты с достаточно высокой подготовкой в области информационных технологий и в финансовых вопросах. Причем большинство их них действуют в составе организованных преступных групп. Доходы от компьютерных преступлений значительно превышают доходы, получаемые от продажи оружия и наркотиков[10].

Очевидно, в будущем эти угрозы не станут меньше. Уже сейчас многие кибератаки – это комбинации различных методик. Использование только традиционных систем (таких, как сигнатурные антивирусы) не дает возможности адекватно защищаться от современных типов атак. Кредитные организации, которые поставили блоки лишь от известных угроз, всегда рискуют, поскольку атакующие продолжают выдумывать и создавать новые техники атак.

Одним из способов решения данной проблемы является формирование специализированного центра по обеспечению кибербезопасности в кредитно-финансовой сфере, который мог бы оперативно реагировать на инциденты и координировать действия различных служб и организаций по предотвращению и предупреждению противоправных действий. Подобные центры успешно функционируют во многих странах, а в РФ такой организации пока нет.

Банк России регулярно получает отчетность от кредитных организаций по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств»[11].

Учитывая, что проведение оперативно-розыскных мероприятий не входит в функции Банка России, такое взаимодействие с правоохранительными органами помогло бы лучше разобраться в уязвимостях различных систем электронного банкинга и повысить качество выпускаемых рекомендаций для кредитных организаций.

Следующая проблема, связанная с применением электронного банкинга, заключается в активном привлечении данных систем к процессу легализации преступных доходов. В последнее время отмывание денег стало одной из основных международных проблем, к решению которой привлечены ведущие страны мира.

Процедура отмывания денег имеет решающее значение для функционирования практически всех форм транснациональной и организованной преступности. Различные меры экономического характера, призванные исключить или ограничить возможность использования приобретенных незаконными путями доходов, представляют собой важнейший и действенный компонент программ по борьбе с преступностью.

Приведем лишь некоторые факторы, способствующие отмыванию денег:

– высокая доля неофициальных доходов населения и бизнеса (существование параллельной экономики и/или «черного рынка»);

– несовершенство механизмов контроля и мониторинга за деятельностью кредитных организаций;

– несоблюдение международных стандартов регулирования финансовой деятельности, разработанных специализированными международными организациями;

[8] Мировая экономика недополучает $445 млрд ежегодно из-за киберпреступлений» // Ведомости. 2014. 09 июня.

[9] Доходы хакеров снижаются // Ведомости. 2014. 15 октября.

[10] Такой взгляд на данную проблему высказывали многие докладчики на VI Уральском форуме «Информационная безопасность банков», который проходил в феврале 2014 г. в Республике Башкортостан. По мнению ведущих экспертов в области информационной безопасности, данный форум является одним из самых авторитетных мероприятий по вопросам обеспечения информационной безопасности в банках России.

[11] Данная отчетность введена в действие указанием Банка России от 09.06.2012 № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств».

– распространение коррупции в различных органах власти;

– законодательное закрепление тайны финансовых операций;

– широкое использование предприятиями и банками операций с вовлечением офшорных компаний и др. [8, 12].

Как правило, в процесс отмывания денег включается целый ряд операций, направленных на сокрытие источника финансовых активов, но все они входят в одну из трех составляющих (стадий) обобщенной модели отмывания денег.

Обобщенная модель отмывания денег включает три стадии:

1) размещение (placement);
2) расслоение (layering);
3) интеграцию (integration).

Указанные стадии могут осуществляться одновременно или частично накладываться друг на друга в зависимости от выбранного механизма легализации и от требований, предъявляемых преступной организацией.

На стадии размещения необходимо изменить форму денежных средств в целях сокрытия их нелегального происхождения. Например, поступления от незаконной торговли наркотиками чаще всего представляют собой мелкие купюры. Конвертирование их в более крупные купюры, чеки или иные финансовые документы часто производится с помощью предприятий, имеющих дело с большими суммами наличных денег (рестораны, гостиницы, казино, мойки машин), используемых в качестве прикрытия.

На стадии расслоения лица, отмывающие деньги, стараются еще больше скрыть следы, по которым их могут обнаружить. Для этого одни сложные финансовые сделки наслаиваются на другие. Например, для отмывания больших денежных сумм создаются фиктивные компании в странах, отличающихся строгими законами о банковской тайне или слабыми механизмами обеспечения соблюдения законодательных положений, касающихся отмывания денег. Затем «грязные» деньги переводятся из одной фиктивной компании в другую до тех пор, пока не приобретут видимость законно полученных средств.

На этой стадии активно используются системы электронного банкинга (см. рисунок).

На стадии интеграции преступник пытается трансформировать денежные доходы, полученные от противозаконной деятельности, в средства, имеющие внешне легальное происхождение (деньги обычно вкладываются в бизнес, недвижимость, покупку драгоценностей и др.).

Обобщенная схема отмывания денег с использованием систем электронного банкинга (ЭБ)

Поскольку процесс отмывания денег в определенной степени полагается на существующие финансовые системы и операции, имеющиеся у преступника, выбор конкретных механизмов ограничивается лишь его изобретательностью. Деньги отмываются через валютные и фондовые биржи, торговцев золотом, казино, компании по продаже автомобилей, страховые и торговые компании. Частные и офшорные банки, подставные корпорации, зоны свободной торговли, электронные системы и торгово-финансовые учреждения – все эти структуры могут скрывать незаконную деятельность.

Приведем наиболее распространенные негативные последствия отмывания денег.

1. Бесконтрольное отмывание денег способно нанести серьезный *удар по репутации банков* страны, негативно повлиять на курсы валют и процентные ставки вследствие высокой интеграции фондовых рынков. Эти деньги могут поступать в глобальные финансовые системы и подрывать экономику и валюту отдельных стран. Возможность проведения банковских операций через Интернет позволила значительно сократить время на осуществление различных платежей.

2. *Подрыв целостности финансовых рынков*. Кредитные организации, полагающиеся на доходы от преступных деяний, сталкиваются с дополнительными трудностями. Например, крупные суммы отмытых денег могут поступить в банк и затем внезапно бесследно исчезнуть через электронные переводы в ответ на такие нерыночные факторы, как операции правоохранительных органов.

3. *Утрата контроля за экономической политикой*. В некоторых странах с формирующейся рыночной экономикой незаконные доходы могут намного превосходить государственные бюджеты, что приводит к утрате правительственного контроля за экономической политикой. В ряде случаев огромная база активов, накопленная за счет отмытых доходов, может использоваться для спекулятивной скупки рынков или даже целой экономики небольшой страны.

4. *Экономические деформации и нестабильность*. Лица, отмывающие деньги, заинтересованы не столько в извлечении прибыли, сколько в защите доходов. Они направляют свои средства в области, не обязательно приносящие экономическую выгоду той стране, в которой они размещены.

5. *Потеря доходов*. Отмывание денег снижает налоговые доходы правительства и тем самым наносит косвенный ущерб честным налогоплательщикам (затрудняется государственный сбор налогов). Данная потеря доходов означает более высокие ставки налогообложения по сравнению с нормальной ситуацией, при которой преступные доходы были бы законными и облагались налогами.

6. *Риск для программ приватизации*. Отмывание денег угрожает стремлению многих стран реформировать свою экономику путем приватизации. Преступные организации располагают финансовыми средствами, позволяющими давать за предприятия, прежде находившиеся в государственной собственности, более высокие цены, чем легальные покупатели.

7. *Социальные издержки*. Отмывание денег ведет к росту государственных расходов на правоохранительные органы (создание специализированных подразделений) и здравоохранение (например, лечение наркотической зависимости) для преодоления возникающих серьезных последствий.

В целом отмывание денег ставит перед мировым сообществом сложную задачу, постоянно приобретающую новые формы. Характер процессов требует разработки глобальных стандартов и международного сотрудничества для уменьшения возможности преступников осуществлять свою деятельность.

Регулирующие органы рекомендуют банкам эффективнее использовать все ресурсы для выявления сомнительных операций, направленных на отмывание денег.

Меры по предотвращению отмывания денег предпринимаются банками не только в соответствии с требованиями законодательства, но и в собственных интересах.

В рамках проведения процедур по идентификации клиентов кредитным организациям следует:

– разработать и внедрить комплексные процедуры, связанные с открытием счетов, установлением кредитных и других деловых взаимоотношений, а также совершением операций с лицами, не имеющими счетов;

– иметь данные о действительной личности пользующегося услугами клиента, в том числе о подлинном владельце счета, открытого на другое имя;

– подвергать проверке данные, удостоверяющие личность, во избежание открытия счетов для фиктивных пользователей;

– располагать данными о роде занятий или профессиональной деятельности клиента, источниках

его доходов, состояния или активов, а также о конкретном источнике денежных средств, вовлеченных в совершаемые через банк операции;

– знать цель, с которой открывается счет, и представлять типы операций, в которые обычно вовлечен данный клиент. При открытии счета сотрудники банка должны понимать, нужно ли отнести клиента к категории высокого риска, требующей повышенного внимания.

В рамках выполнения процедуры мониторинга кредитные организации должны:

– иметь внутренние системы для идентификации и мониторинга вызывающих подозрения операций;

– оценивать риск, исходя из конкретных видов счетов, регионов и операций;

– обращать внимание на любую операцию, превышающую установленный денежный порог депозитов при открытии счета, для ежемесячных телеграфных переводов, операций с наличностью, дорожными чеками, при получении кредитов и заключении сделок, включая покупку и продажу валют, опционов и драгоценных металлов и т.п.;

– обращать внимание на усиление активности по банковским счетам, особенно тем, которые могут стать объектами сомнительных операций (офшорные и корреспондентские счета, счета небанковских финансовых институтов, политических деятелей и личных инвестиций сотрудников компаний, счета, информация о которых может быть затребована судебными органами и др.);

– установить пороговые размеры сделок и время от времени проверять их адекватность.

Отдельно следует отметить роль топ-менеджеров кредитных организаций. Они должны стремиться к постановке и практической реализации задач в области предотвращения незаконных операций и демонстрировать, что банк как субъект корпоративной культуры заботится о своей репутации не меньше, чем о прибылях, маркетинге и качестве обслуживания клиентов.

Топ-менеджерам кредитных организаций необходимо хорошо представлять, что клиенты коммерческих банков, использующие для выполнения своих операций системы электронного банкинга и занимающиеся противоправной деятельностью, могут не только нанести удар по репутации банка, но и создать для него серьезные осложнения во взаимоотношениях с регулирующими органами, вплоть до отзыва лицензии на осуществление банковских операций.

Еще одна проблема связана с совершенствованием профессиональной подготовки персонала банка (включая сотрудников служб внутреннего контроля кредитных организаций) по вопросам обеспечения информационной безопасности[12]. Учитывая заметное увеличение источников банковских рисков, основу которых составляют особенности функционирования систем электронного банкинга, специалистам коммерческих банков, в чьи функции входит управление рисками, необходимо иметь не только экономическое или юридическое, но и техническое образование, позволяющее достаточно уверенно ориентироваться в особенностях функционирования различных технологий ДБО.

Ненадлежащее обеспечение информационной безопасности систем электронного банкинга (в частности, продажа населению слабозащищенных финансовых услуг) ведет к созданию предпосылок для хищения денежных средств и финансирования криминала. Существующая динамика развития современных процессов, связанная с ростом технических возможностей, способна многократно увеличить объемы финансирования криминала. Если допустить рост уровня хищений в больших объемах (соизмеримый с госсектором), это может быть серьезной угрозой экономической безопасности страны (см. таблицу).

Итак, рассмотренные проблемы имеют в первую очередь практическое значение, так как направлены на решение важной задачи для российского банковского бизнеса – повышение доверия клиентов кредитных организаций к технологиям ДБО, включая системы электронного банкинга.

По итогам проведенного анализа выявлено, что наряду с очевидными преимуществами применение систем электронного банкинга привело к значительному расширению профиля операционного риска, активизации деятельности киберпреступников и использованию данного вида ДБО для легализации преступных доходов.

Своевременное принятие регулирующими органами нормативных документов в области применения электронного банкинга (по четырем рассмотренным направлениям) будет способствовать

[12] О целесообразности проведения подготовки/переподготовки работников кредитной организации, ответственных за работу с клиентами – пользователями систем дистанционного банковского обслуживания по вопросам защиты от воздействий вредоносного кода, было указано в письме Банка России от 24.03.2014 № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности» (п. 4.3).

Актуальные направления регулирования для банковского сектора

Направления регулирования в условиях электронного банкинга	Задачи регулятора	Задачи банка
Повышение качества управления операционным риском в банках	Разработать и выпустить рекомендации для кредитных организаций по управлению операционным риском в целях минимизации последствий проявления источников операционного риска, связанных с особенностями функционирования систем электронного банкинга (как на стороне банка, так и на стороне клиента)	Внедрить в системы управления рисками в банке дополнительные меры по минимизации последствий проявления источников операционного риска в условиях электронного банкинга. Адаптировать методики проверок риск-подразделений и службы внутреннего контроля к условиям электронного банкинга
Противодействие киберпреступлениям, направленным на банки и на их клиентов, использующих системы электронного банкинга	Разработать и выпустить рекомендации для кредитных организаций по снижению рисков, связанных с возрастанием активности киберпреступников, чьи действия направлены на кражи денежных средств как банков, так и их клиентов; Усилить взаимодействие с правоохранительными органами для выработки наиболее действенных мер по предотвращению подобных преступлений. Создать центр по противодействию киберугрозам в банковской сфере	Внедрить дополнительные меры защиты информации для систем электронного банкинга, основываясь на риск-ориентированном подходе. Использовать «лучшую практику» в банке (основываясь на зарубежном и отечественном опыте) по предотвращению киберпреступлений
Использование систем электронного банкинга в схемах, направленных на легализацию преступных доходов	Внести необходимые изменения в нормативные акты в целях повышения «прозрачности» операций клиентов банков в условиях ДБО, включая системы электронного банкинга. Разработать и выпустить рекомендации для кредитных организаций по выявлению «сомнительных» операций, выполняемых с использованием систем электронного банкинга	Внедрить меры идентификации клиентов, использующих для выполнения своих операций системы электронного банкинга. Расширить перечень признаков «сомнительных» операций, выполняемых с использованием систем электронного банкинга
Недостаточная подготовка сотрудников риск-подразделений банка по тематике применения технологий ДБО (включая системы электронного банкинга)	Разработать и выпустить рекомендации для кредитных организаций, направленные на повышение качества подготовки специалистов риск-подразделений, служб внутреннего контроля и подразделений финансового мониторинга по вопросам возникновения дополнительных источников рисков, связанных с особенностями функционирования систем электронного банкинга	Внедрить мероприятия по повышению уровня подготовки специалистов риск-подразделений, служб внутреннего контроля и подразделений финансового мониторинга по вопросам, связанным с особенностями функционирования систем электронного банкинга. Это могут быть дополнительные курсы по особенностям функционирования применяемых систем, переподготовка «рисковиков», имеющих только экономическое и/или юридическое образование по программам технического образования

Источники: [2, 3, 6, 7, 9, 10, 11, 14, 16].

не только развитию данного вида ДБО, но и повышению стабильности банковской системы России.

Предложенные авторами подходы к регулированию ЭБ направлены:

– на минимизацию последствий появления новых источников операционного риска в условиях электронного банкинга, причинами чего являются надежность аппаратно-программного обеспечения данного вида ДБО и надежность различного рода провайдеров услуг (интернет-провайдеров для систем интернет-банкинга и операторов сотовой связи для систем мобильного банкинга);

– на противодействие киберпреступлениям в кредитно-финансовой сфере, так как киберпреступность

является одним из основных сдерживающих факторов развития электронного банкинга в России;

– на снижение риска использования данного вида ДБО в схемах, предназначенных для легализации преступных доходов, за счет принятия дополнительных мер по идентификации клиентов, применяющих для выполнения своих операций системы электронного банкинга;

– на повышение профессионального уровня персонала кредитных организаций, обслуживающего системы электронного банкинга.

Список литературы

1. *Гренъ И.В*. Компьютерная преступность. Минск: Новое знание, 2007. 413 с.

2. *Генкин А., Суворова Е*. Электронные платежи: будущее наступает сегодня. М.: Альпина Паблишер, 2011. 284 с.

3. Дистанционное банковское обслуживание. М.: КноРус, 2010. 328 с.

4. Интернет-технологии в банковском бизнесе: перспективы и риски: учебно-практическое пособие. М.: КноРус, 2014. 318 с.

5. *Кинг Б*. Банк 3.0. Почему сегодня банк – это не то, куда вы ходите, а то, что вы делаете. М.: Олимп-Бизнес, 2014. 520 с.

6. *Криворучко С.В., Лопатин В.А*. Национальная платежная система: структура, технологии, регулирование: международный опыт, российская практика. М.: КноРус, 2013. 456 с.

7. *Коржов В*. Современные DDoS-атаки. URL: http://www.osp.ru/lan/2014/09/13042710/.

8. *Логинов Е.Л*. Отмывание денег через интернет-технологии. М.: ЮНИТИ-ДАНА, 2005. 208 с.

9. Основные тенденции использования электронного банкинга. URL: http://ac.gov.ru/files/publication/a/1153.pdf.

10. Платежные карты / под ред. А.С. Воронина. М.: КноРус, 2014. 560 с.

11. *Ревенков П.В*. Дистанционное банковское облуживание: актуальные направления регулирования // Банковское дело. 2012. № 9. С. 57–62.

12. *Ревенков П.В., Бердюгин А.А*. ДБО: Интернет создает новых клиентов и расширяет профили рисков // Банковское дело. 2013. № 12. С. 64–67.

13. *Скиба В.Ю., Курбатов В.А*. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008. 320 с.

14. *Скобелев А*. Рэнкинг российских интернет-банков 2014 // Банковские технологии. 2014. № 4. С. 54–58.

15. Форензика – компьютерная криминалистика / под ред. Н.Н. Федотова. М.: OneBook, 2012. 420 с.

16. Электронные платежи: специфика, регулирование, технологии: практическое пособие. М.: Регламент-Медиа, 2013. 245 с.

17. Risk Management Principles for Electronic Banking. July 2003. URL: http://www.bis.org/publ/bcbs98.htm.

18. Risk Management Principles for Electronic Banking. May 2001. URL: http://www.bis.org/publ/bcbs82.htm.

19. Management and Supervision of Cross-Border Electronic Banking Activities. October 2002. URL: http://www.bis.org/publ/bcbs93.htm.

20. Risk Management for Electronic Banking and Electronic Money Activities. March 1998. URL: http://www.bis.org/publ/bcbs35.pdf.

21. Electronic Banking Group Initiatives and White Papers. October 2000. URL: http://www.bis.org/publ/bcbs76.htm.

Finance and Credit
ISSN 2311-8709 (Online)
ISSN 2071-4688 (Print)

REGULATING ELECTRONIC BANKING: CURRENT ISSUES

Pavel V. REVENKOV,
Aleksei L. POSPELOV

Abstract

Subject The article considers the banking system of the Russian Federation and emphasizes the urgent issue of electronic banking regulation.

Objectives The study aims at identifying the most important areas of banking regulation in electronic banking.

Results The basis of e-banking is Internet banking (management of bank accounts and bank cards through the Internet and web-browser in on-line mode) and mobile banking (management of bank accounts and bank cards from laptops, PDAs, smartphones and other similar devices). However, apart from obvious advantages, e-banking brought additional risks into banking. To be more precise, the amount of bank risks remained the same, but their technical component has increased significantly. The risk level was impacted by the extension of the operational risk profile; a significant increase in the number of cybercrimes in the financial sector; the use of electronic banking systems in the schemes aimed at money laundering; lack of commercial bank employee training in information security management and associated risks inherent in electronic banking. We have analyzed each of the four causes of additional sources of risk and emphasized the most urgent tasks for regulators and credit institutions to minimize the risks arising in electronic banking.

Conclusions The latest achievements in information and communication technologies on the basis of the global Internet and mobile communication capabilities have created ideal conditions for introducing the electronic banking technology, however, it is subject to proper regulation.

Keywords: electronic banking, regulation, operational risk, information security, money laundering

References

1. Gren' I.V. *Komp'yuternaya prestupnost'* [Computer crime]. Minsk, Novoe znanie Publ., 2007, 413 p.

2. Genkin A., Suvorova E. *Elektronnye platezhi: budushchee nastupaet segodnya* [Electronic payments: the future comes today]. Moscow, Al'pina Pablisherz Publ., 2011, 284 p.

3. *Distantsionnoe bankovskoe obsluzhivanie* [Remote banking service]. Moscow, KnoRus Publ., 2010, 328 p.

4. *Internet-tekhnologii v bankovskom biznese: perspektivy i riski* [Internet technologies in banking: prospects and risks]. Moscow, KnoRus Publ., 2014, 318 p.

5. King B. *Bank 3.0. Pochemu segodnya bank – eto ne to, kuda vy khodite, a to, chto vy delaete* [Bank 3.0: Why Banking Is No Longer Somewhere You Go But Something You Do]. Moscow, Olimp-Biznes Publ., 2014, 520 p.

6. Krivoruchko S.V., Lopatin V.A. *Natsional'naya platezhnaya sistema: struktura, tekhnologii, regulirovanie: mezhdunarodnyi opyt, rossiiskaya praktika* [National payment system: structure, technologies, regulation: international experience, Russian practice]. Moscow, KnoRus Publ., 2013, 456 p.

7. Korzhov V. *Sovremennye DDoS-ataki* [Modern DDOS-attacks]. Available at: http://www.osp.ru/lan/2014/09/13042710/. (In Russ.)

8. Loginov E.L. *Otmyvanie deneg cherez internet-tekhnologii* [Money laundering through Internet technologies]. Moscow, YUNITI-DANA Publ., 2005, 208 p.

9. *Osnovnye tendentsii ispol'zovaniya elektronnogo bankinga* [Major trends in using the electronic banking]. Available at: http://ac.gov.ru/files/publication/a/1153.pdf. (In Russ.)

10. *Platezhnye karty* [Payment cards]. Moscow, KnoRus Publ., 2014, 560 p.

11. Revenkov P.V. Distantsionnoe bankovskoe obsluzhivanie: aktual'nye napravleniya regulirovaniya [Online banking: urgent areas for regulation]. *Bankovskoe delo = Banking*, 2012, no. 9, pp. 57–62.

12. Revenkov P.V., Berdyugin A.A. DBO: Internet sozdaet novykh klientov i rasshiryaet profili riskov [RBS: The Internet creates new customers and expands risk profiles]. *Bankovskoe delo = Banking*, 2013, no. 12, pp. 64–67.

13. Skiba V.Yu., Kurbatov V.A. *Rukovodstvo po zashchite ot vnutrennikh ugroz informatsionnoi bezopasnosti* [Guidance on protection against internal threats of information security]. St. Petersburg, Piter Publ., 2008, 320 p.

14. Skobelev A. Renking rossiiskikh internet-bankov 2014 [Ranking of Russian Internet banks 2014]. *Bankovskie tekhnologii = Bank Technologies*, 2014, no. 4, pp. 54–58.

15. *Forenzika – komp'yuternaya kriminalistika* [Forensics is a science of computer crime detection]. Moscow, OneBook Publ., 2012, 420 p.

16. *Elektronnye platezhi: spetsifika, regulirovanie, tekhnologii: prakticheskoe posobie* [Electronic payments: specifics, regulation, technologies: a practical guide]. Moscow, Reglament-Media Publ., 2013, 245 p.

17. Risk Management Principles for Electronic Banking. July 2003. Available at: http://www.bis.org/publ/bcbs98.htm.

18. Risk Management Principles for Electronic Banking. May 2001. Available at: http://www.bis.org/publ/bcbs82.htm.

19. Management and Supervision of Cross-Border Electronic Banking Activities. October 2002. Available at: http://www.bis.org/publ/bcbs93.htm.

20. Risk Management for Electronic Banking and Electronic Money Activities. March 1998. Available at: http://www.bis.org/publ/bcbs35.pdf.

21. Electronic Banking Group Initiatives and White Papers. October 2000. Available at: http://www.bis.org/publ/bcbs76.htm.

Pavel V. REVENKOV
Odintsovo Humanities University, Odintsovo, Moscow Region, Russian Federation
pavel.revenkov@mail.ru

Aleksei L. POSPELOV
Odintsovo Humanities University, Odintsovo, Moscow Region, Russian Federation
pal@cbr.ru