

## 5. БАНКОВСКИЙ АУДИТ

### 5.1. ВЛИЯНИЕ ВНЕДРЕНИЯ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ НА БАНКОВСКИЕ РИСКИ

Школин М.В., аспирант кафедры менеджмента Московской академии предпринимательства при Правительстве г. Москвы;

заместитель начальника отдела планирования и анализа деятельности банка Финансового департамента Банка «Возрождение»

В данной статье мы рассмотрим риски, существующие у банка при традиционном банковском обслуживании (физическое посещение офиса). Попытаемся определить, на какие риски влияют технологии дистанционного банковского обслуживания и какие новые риски при этом возникают.

В любой хозяйственной деятельности всегда существует опасность потерь, вытекающая из специфики хозяйственных операций. Опасность таких потерь представляет собой коммерческий риск. Ведущим принципом в работе коммерческих банков в условиях перехода к рыночным отношениям является стремление к получению как можно большей прибыли, оно ограничивается возможностью понести убытки<sup>1</sup>.

Понятие риска связано с невозможностью прогнозировать будущее с вероятностью 100%. Риски присутствуют во всех сферах человеческой деятельности. Однако определение риска во многом зависит от сферы деятельности.

Понятие «риск» имеет достаточно длительную мировую историю, но наиболее активно начали изучать различные аспекты риска в конце XIX – начале XX века. Для отечественной экономики проблема риска и его оценки не является новой. В 20-х годах нашего столетия был сформулированы юридические предпосылки учета хозяйственных рисков<sup>2</sup>.

В соответствии письмом ЦБ от 23.06.2004 №70-т «О типичных банковских рисках» – под банковским риском понимается присущая банковской деятельности возможность (вероятность) понесения кредитной организацией потерь и (или) ухудшения ликвидности вследствие наступления неблагоприятных событий, связанных с внутренними факторами (сложность организационной структуры, уровень квалификации служащих, организационные изменения, текучесть кадров и т.д.) и (или) внешними факторами (изменение экономических условий деятельности кредитной организации, применяемые технологии)<sup>3</sup>. При этом риск означает вероятность наступления события, которое может неблагоприятно сказаться на прибыли банка или на его капитале. Под потерями понимаются прямые убытки или частичная утрата основного капитала, неполучение прибыли, а также отток клиентов, потеря доли рынка, утрата положительного имиджа банка.

Источником возникновения внешних рисков является внешняя среда по отношению к банковской структуре. Банк не может оказывать на них влияние, он может только предвидеть и учитывать их в своей деятельности. Можно сказать, что к внешним относятся риски, непосредственно не зависящие от деятельности банка. Например, непредвиденные изменения законодательства, регулирующего банковскую деятельность; неустойчивость политического режима в стране и т.д.

Источником возникновения внутренних рисков является сама банковская структура. Например, к числу внутренних рисков можно отнести неэффективность менеджмента, ошибочную маркетинговую политику, ресурсную политику.

По мнению автора, в состав внешних рисков входят следующие риски:

- страновой риск;
- валютный риск;
- налоговый риск;
- системный риск;
- риск конкуренции;
- репутационный риск;
- правовой риск;
- кредитный риск;
- риск несоответствия условиям государственного правового регулирования.

В состав внутренних входят следующие риски:

- стратегический риск;
- технологический риск;
- операционный риск;
- риск ликвидности;
- процентный риск;
- риск упущенной финансовой выгоды.

Мы рассмотрели риски, существующие при традиционном банковском обслуживании, теперь перейдем к рассмотрению рисков, возникающих при дистанционном банковском обслуживании.

Электронные банковские услуги (дистанционные банковские услуги) – это не экзотический финансовый инструмент и не дополнительное направление банковской деятельности, а новый способ осуществления банковской деятельности только с помощью интернет-системы. Интернет-система включает в себя: прямые подключения модемной связи, частные и сети общего пользования, интернет, телевидение (кабельное телевидение), мобильные устройства и телефоны. Электронные банковские услуги делают возможным предложить банковское обслуживание по всему миру 24 часа в сутки 7 дней в неделю.

В зависимости от возможности осуществления банковских операций дистанционное банковское обслуживание банка можно разделить на 3 уровня.

- информационный – это основной уровень. как правило, банк имеет рекламную информацию о банковских продуктах и услугах, событиях в деятельности банка, сосредоточенную на специально выделенном сервере;
- частично деловой – этот уровень допускает ограниченное взаимодействие между банковскими системами и клиентами;
- деловой – позволяет клиентам выполнять банковские операции.

По данным Базельского комитета по банковскому надзору, из-за быстрых изменений в информационных технологиях никакой список рисков не может быть исчерпывающим. Хотя основные виды рисков, возникающих в процессе электронных банковских операций, в принципе

<sup>1</sup> Жуков Е.И. Банки и банковские операции, М. 1997, с. 207.

<sup>2</sup> Разработка управленческих решений: курс лекций, Титова Н.Л., М. 2004.

<sup>3</sup> Центральный Банк РФ, Письмо №70-Т от 23.06.2004 г. «О типичных банковских рисках».

не новы, все же анализ обстоятельств возникновения некоторых из таких рисков и степени их влияния на банки может быть полезен банкам и их руководству<sup>4</sup>.

Следует выделить операционный риск, риск для репутации банка и юридический риск, являющиеся важнейшими видами рисков при проведении большинства электронных банковских операций. Такие риски особенно угрожают диверсифицированным международным банкам, и в трех последующих подпунктах мы подробнее рассмотрим такие виды рисков. Есть ряд специфических проблем, связанных со всеми группами рисков сразу. Например, взлом системы безопасности, открывающий несанкционированный доступ к информации клиента, может быть классифицирован как операционный риск. Но такое событие влечет для банка как юридический риск, так и риск для репутации этого банка. Хотя эти три разных вида риска могут порождаться одной проблемой, для нейтрализации каждого из рисков могут потребоваться сразу несколько мер защиты. Ниже мы рассмотрим другие риски, которыми могут сопровождаться некоторые формы электронных банковских операций и работа с электронными деньгами. Обсудим и риски, связанные с пересечением границы.

### Операционный риск

Операционные риски возникают из потенциального ущерба, вызванного ненадежностью систем защиты от несанкционированного доступа. Безопасность системы является крайне важным условием, поскольку банки могут оказаться объектом внешнего или внутреннего вторжения с угрозой системам и продуктам. Операционный риск может быть следствием злоупотребления клиента, неадекватно спроектированной или внедренной системы электронных расчетов и электронных денег. Чаще всего риски возникают именно в этой операционной сфере.

Кроме вторжений извне в систему электронных банковских операций, банки подвергаются операционному риску из-за жульничества своих сотрудников, имеющих возможность тайно получить аутентификационные данные для доступа к счетам клиентов или украсть хранящиеся в банке кредитные карточки. Могут скомпрометировать банки и ошибки сотрудников, допущенные по небрежности или невнимательности.

Особую тревогу вызывают подделки преступниками электронных денег, число которых будет расти, если банки не примут адекватных мер защиты, способных выявить фальсификаты. Банкам угрожает операционный риск от подделок, поскольку банк несет ответственность в каждом случае фальсификации баланса электронных денег. Кроме того, приходится нести расходы на восстановление системы, допустившей несанкционированный доступ.

Банки всегда рискуют, если выбранные им системы имеют проектные недостатки или внедрены недостаточно профессионально. Например, банк рискует столкнуться с перебоями в работе системы, если выбранные им системы электронных операций несовместимы с требованиями пользователя.

Многие банки полагаются на внешних провайдеров услуг и внешних специалистов для внедрения, применения электронных банковских операций. Такая зависимость оправдана: она позволяет банку передать на

условиях аутсорсинга обеспечение операций электронных расчетов и электронных денег, которые банк по экономическим причинам не способен реализовать самостоятельно. Однако расчет на аутсорсинг подвергает банк операционным рискам. Провайдеры услуг могут не иметь необходимого опыта предоставления услуг, на которые рассчитывает банк, или оказаться неспособными регулярно обновлять свои технологии. Предоставленные провайдером услуги могут оказаться неэффективными при выходе системы из строя или из-за финансовых проблем, подрывающих способность банка предоставлять услуги и продукты.

Быстрое развитие и совершенствование информационных технологий ставит перед банками проблему старения компьютерных систем. Например, программное обеспечение, обслуживающее электронные банковские операции, требует постоянного обновления, но каналы распространения обновленных версий программного обеспечения могут тоже таить в себе опасность для банков, если преступникам или злоумышленникам придет в голову перехватить и модифицировать программное обеспечение. Кроме того, быстрое развитие технологий может представлять проблему для сотрудников банка, не способных полностью освоить характер новой технологии, принятой банком. Это приведет к сбоям в работе с новыми или обновленными системами.

Другим источником операционного риска может стать нарушение клиентом (случайное или преднамеренное) правил пользования услугами банка. Такой риск становится более вероятным, если клиентам не объяснили профилактических мер безопасности. В отсутствие адекватных мер контроля за банковскими операциями клиенты могут отказаться признать ранее утвержденные ими сделки, что принесет банку существенные финансовые потери. Клиенты, использующие персональные данные (код идентификации, номера кредитных карт или банковских счетов) в не защищенном электронном трафике, могут позволить преступникам получить доступ к счетам клиента. Соответственно банк понесет финансовый ущерб, поскольку перевод денежных средств не был санкционирован клиентом. Еще одним поводом для беспокойства является практика отмывания денег.

### Репутационные риски

Репутационный риск приводит к негативному имиджу банковского учреждения в глазах общественности, недоверию ко всем его финансовым операциям, в том числе к способности банка поддерживать нормальные деловые взаимоотношения с клиентами. Репутационный риск может возникнуть, если какие-либо действия банка провоцируют утрату общественного доверия к способности банка осуществлять свои прямые функции. Репутационный риск может быть следствием деятельности самого банка, но может быть инициирован и третьей стороной. Возросший репутационный риск может быть прямым результатом нарастания других рисков, особенно, операционного риска.

Ошибки, должностные преступления служащих и злонамеренные действия третьей стороны могут также угрожать репутации банка. Репутационный риск может возникнуть и из значительных проблем в коммуникационных сетях, затрудняющих доступ клиентов к своим счетам, особенно в тех случаях, когда у них нет альтернативного варианта доступа. Существенные по-

<sup>4</sup> <http://www.bis.org/>.

тери, вызванные ошибками другого банковского учреждения при реализации электронных банковских операций, могут побудить клиентов относиться с подозрением к услугам и продуктам банка, даже если у банка в этом смысле нет никаких проблем. Репутационный риск может возникнуть в результате спланированных атак на банк. Хакер, взломавший веб-сайт банка, способен намеренно внести искажения в информацию о банке или его продуктах.

Репутационный риск может быть опасен не только для какого-то одного конкретного банка, но и для всей банковской системы в целом. Если, например, репутация крупного международного банка окажется под угрозой из-за его неспособности защитить свои электронные операции, под вопросом окажется надежность систем безопасности и других банков. Такая ситуация, сложившаяся в экстремальных обстоятельствах, способна привести к системному разрушению банковской системы в целом.

### **Правовой риск**

При относительно новой практике проведения электронных операций права и обязанности сторон в подобных сделках в некоторых случаях остаются не регламентированными. Например, в некоторых странах меры защиты клиента при проведении электронных операций могут оставаться для него неясными. Кроме того, правовой риск может возникнуть из-за неопределенностей, которые содержатся в тексте договоров и соглашений, заключенных с помощью электронных средств.

Схемы электронных денег могут оказаться привлекательными для отмывания денег, если система предлагает свободный баланс и лимиты сделок и предусматривает ограниченный контроль за совершаемыми сделками. Применение закона об отмывании денег может оказаться неэффективным для некоторых форм электронных платежей, поскольку такие платежи производятся дистанционно, и для банков затруднительно применять традиционные методы для предотвращения и выявления преступных действий. Данный факт подтверждается в письме Ассоциации российских банков №А-02/1Е-517 от 16.10.2006 к Центральному банку России.

Банки, занимающиеся электронными операциями, могут оказаться перед лицом правовых рисков, связанных с сохранением конфиденциальности частной информации клиентов. Клиенты, не информированные должным образом о своих правах и обязанностях, могут по незнанию инициировать судебные иски к банку. А в некоторых странах к банкам, неспособным обеспечить конфиденциальность частной информации, применяются юридические санкции.

Банки, предпочитающие улучшить обслуживание клиентов путем связи с их сайтами в Интернете, тоже могут оказаться перед лицом правовых рисков. Хакер может использовать этот подключенный сайт для хищения денег со счета клиента, что для банка обернется судебным иском.

Электронная торговля все растет, и банки могут сыграть свою роль в системах электронной идентификации, как, например, с применением цифровых сертификатов. Но функция поддержки сертификации тоже может грозить банку правовыми рисками. Например, банк, гарантирующий сертификацию, может понести ответственность за финансовые потери сторон, свя-

занные с лицензией. Кроме того, правовые риски могут возникнуть в ситуации, когда банки участвуют в новых системах аутентификации, а права и обязанности сторон недостаточно четко прописаны в договорных документах.

### **Прочие риски**

Такие традиционные банковские риски, как кредитный риск, риск ликвидности, риск, связанный с процентной ставкой, и рыночный риск могут также проистекать из электронных банковских операций, хотя практические последствия таких рисков могут быть совсем другого уровня, чем последствия операционных, репутационных и правовых рисков. Особенно это касается банков, задействованных в широком диапазоне финансовой деятельности, в отличие от банков и их дочерних структур, специализирующихся на электронных операциях и электронных деньгах.

#### ***Кредитный риск***

Банки, задействованные в электронных банковских операциях, могут наращивать кредитную активность по нетрадиционным каналам и расширить их рынок за пределами традиционных географических границ. Малоэффективная система определения кредитоспособности заемщиков, обращающихся за получением кредита через посредство дистанционных банковских процедур, может увеличить кредитный риск для банков.

#### ***Риск ликвидности***

Риск ликвидности – риск, проистекающий из неспособности банка выполнить свои обязательства в назначенный срок. Риск ликвидности может оказаться значительным для банков, специализирующихся на электронных банковских операциях, если они неспособны убедить клиентов, что их фонды достаточны для погашения долга и производства платежей в любой конкретный промежуток времени.

#### ***Риск, связанный с процентной ставкой***

Риск, связанный с процентной ставкой, обусловлен финансовой устойчивостью банка к неблагоприятным изменениям процентной ставки. Значительному риску такого рода могут подвергнуться банки, специализирующиеся на работе с электронными деньгами, при неблагоприятном снижении процентной ставки, что снижает стоимость активов, на которые опирается система электронных денег.

По нашему мнению, при дистанционном банковском обслуживании у банка возникают 2 новых вида риска.

#### ***Внешний***

Рыночный риск – риск ущерба от нарушения баланса, вызванного изменением рыночных цен, включая изменение курса валют. Такому риску подвержены банки, принимающие платежи в иностранной валюте в качестве электронных денег.

#### ***Внутренний***

Риск внедрения новых продуктов и технологий – риск, возникающий в связи со сложностью расчета окупаемости затрат на внедрение новых технологий, и как следствие, возможностью потерь в случае неоправданных вложений банка.

### Оценочные риски

Оценочные риски типичны для нашего времени. Они обычно проходят три этапа.

- Первый – банк может скрупулезно проанализировать риски и по возможности классифицировать их. Если риски не поддаются количественному измерению, руководство банка может идентифицировать вероятность возникновения таких рисков и принять меры к ограничению числа таких рисков. Менеджмент обязан разработать обоснованный и законный метод оценки степени каждого риска, влияния, которое этот риск окажет на деятельность банка (включая максимальный потенциальный ущерб) и оценить вероятность возникновения подобной ситуации.
- Второй этап в оценке риска – определение советом директоров или старшим менеджментом допустимого предела банковских рисков на основе анализа возможных потерь для банка при возникновении подобного рода проблемы. И последнее: руководство банка может сравнить допустимые пределы риска с вероятностью, что возникший риск не превысит этих пределов.

### ВЫВОД

Дистанционные банковские услуги оказывают влияние на внешние и внутренние риски банка, существующие при традиционном обслуживании клиентов банка, а также добавляют новые.

По мнению автора, в целях учета этих рисков и минимизации их влияния руководство банка должно разработать систему контроля управления банковскими рисками, которая предусматривает следующие уровни.

- Первый уровень. Контроль осуществляют руководители структурных подразделений банка, отвечающие за определенный бизнес. Первый уровень включает в себя:
  - организацию контроля выполнения работниками подразделений соответствующих процедур, предусмотренных стандартами конкретного бизнеса;
  - мониторинг адекватности параметров управления рисками конкретных инструментов внутри отдельного бизнеса конкретному состоянию;
  - предотвращение ухудшения состояния и размера соответствующего риска;
  - мониторинг количественного значения параметров управления определенными банковскими рисками.
- Второй уровень. Контроль осуществляют комитеты банка. Второй уровень включает в себя:
  - мониторинг состояния и размера определенных рисков;
  - недопущение существенного увеличения доли активов, качество которых заметно отличается от среднего по бизнесу и/или группе инструментов;
  - недопущение длительного ухудшения одного и/или нескольких параметров управления определенным риском;
  - контроль адекватности границ принятия решений для штатной ситуации и в случае кризисного состояния.
- Третий уровень. Контроль осуществляет правление банка. Третий уровень включает в себя:
  - прекращение деятельности подразделений банка, несущих чрезмерные риски;
  - контроль соответствия доходности определенного бизнеса уровню соответствующих рисков;
  - недопущение длительной несбалансированности пассивов и активов банка;
  - предотвращение использования инфраструктуры банка в целях легализации доходов, полученных преступным путем.

### Литература

1. Жуков Е.И. Банки и банковские операции, М. 1997, с. 207.
2. Разработка управленческих решений: курс лекций, Титова Н.Л., М. 2004.
3. Центральный банк Российской Федерации, Письмо №70-Т от 23.06.2004 «О типичных банковских рисках».
4. <http://www.bis.org/>.

*Школин Михаил Владимирович*

### РЕЦЕНЗИЯ

Актуальность проблемы. В статье рассматриваются риски, существующие у банка, как при традиционном обслуживании (т.е. клиенты физически посещают офис банка), так и при дистанционном, по новому производится их классификация в зависимости от факторов на них влияющих.

Научная новизна – заключается в разработке методики оценки влияния дистанционного банковского обслуживания на банковские риски.

Практическая значимость заключается в возможности применения в коммерческих банках, использующих технологии дистанционного банковского обслуживания, данной методики, что позволит не только улучшить финансовые показатели кредитных организаций, но и минимизировать влияние рисков на них.

Несмотря на сделанные замечания, данная статья заслуживает публикации.

*Журавлев П.В., д.э.н., профессор Российской экономической академии им. Г.В. Плеханова*

## 5.1. AGENCY OF A HEADING OF DISTANT BANKING SERVICING ON BANKING MARKS

M.V. Shkolin, the Post-graduate Student of Chair of Management of the Moscow Academy of Business at the Government of Moscow

Shkolin Michael Vladimirovich – the post-graduate student of the Moscow academy of business at the government of Moscow, the Deputy chief of the Department of planning and the analysis of activity of Bank of Financial department of Bank «Vozrozhdenie» (Open Society).