

МОСКОВСКИЙ ЭКОНОМИЧЕСКИЙ журнал 3/2016

УДК 336.717



УПРАВЛЕНИЕ РИСКАМИ В УСЛОВИЯХ ЭЛЕКТРОННОГО БАНКИНГА

Risk management in the conditions of electronic banking

Мальшева Вера Васильевна, студентка

Российский экономический университет им. Плеханова

Malysheva Vera, student

Russian University of Economics named after Plekhanov

Аннотация. В современных условиях инновационное развитие банков в первую очередь связано с трансформацией каналов продаж банковских услуг, переходом от традиционного обслуживания клиентов через филиалы/отделения к альтернативным, основанным на широком использовании технологий дистанционного банковского обслуживания, то есть удаленного банкинга, который считается наиболее распространенной инновацией и становится основной функцией банков. На сегодня ни один банк не может считать себя конкурентоспособным при отсутствии эффективных систем электронного банкинга. В Западной Европе, по оценкам экспертов, к 2020 году клиентура ДБО будет составлять 60% от общего количества, по нашим оценкам, в Российской Федерации по оптимистическому прогнозу – 15-20%. В то же время, предоставляя банкам широкие

операционные возможности, удаленный банкинг приводит к росту рисков в банковской деятельности.

Annotation. In modern conditions of development of innovative banks in the first place associated with the transformation of banking sales channels, the transition from the traditional customer service through affiliates / branches to alternative, based on extensive use of remote banking technology, t. N. remote banking, which is considered the most common innovation and becomes the primary function of banks. At present, no bank can not consider themselves competitive in the absence of effective systems of electronic banking. In Western Europe, according to experts, by 2020. Clientele RBS will be 60% of the total, according to our estimates in the Russian Federation according to the optimistic forecast – 15-20%. At the same time, giving banks broad operational capabilities of the remote banking leads to increased risks in banking.

Ключевые слова: *дистанционное банковское обслуживание, риск, управление, структура, система.*

Keywords: *remote banking services, risk, management, structure, system.*

Внедрение инновационных систем электронного банкинга позволяет банкам повысить конкурентоспособность, увеличить объемы высокотехнологичных банковских услуг и получить дополнительные доходы. Вместе с тем использование технологий дистанционного банкинга связано с рисками, может оказать негативное влияние на поступление и капитал банка. Не меняя сущность традиционных рисков, интернет-технологии модифицируют характер традиционных рисков и вносят изменения в структуру и профиль рисков, требуют от банков создания современных систем управления рисками электронного банкинга с соблюдением международных стандартов.

Целью статьи является обоснование теоретических основ и научно-практических рекомендаций по повышению эффективности

управления рисками электронного банкинга и финансового мониторинга онлайн-операций банков.

На сегодня существуют различные варианты электронного банкинга и не имеет принципиального значения, какой именно вариант использует банк. Впрочем, как отмечает Д. Коддере, если компания не следует тенденции рыночных, финансовых и технологических условий, то она недолго останется в бизнесе. А это значит, что в современных условиях банк не может быть конкурентоспособным и предоставлять современные качественные услуги, если не обеспечивает надежное дистанционное обслуживание клиентов. Речь должна идти не об отдельных банковских операциях, а о радикальной перестройке организации всей банковской деятельности [4].

Заметим, что до сих пор нет четкого понимания содержания электронного банкинга. Чаще всего используется такое базовое определение электронного банкинга: «обеспечение возможностей для клиентов банков получать удаленный доступ к своим банковским счетам через информационно-телекоммуникационные системы и, как минимум, осуществлять переводы денежных средств между ними». Итак, дистанционным обслуживанием банка правомерно называть предоставление банковских продуктов/услуг по запросу клиента без непосредственного взаимодействия клиента с сотрудником банка. Иногда такой вид деятельности называют еще системой удаленного доступа, а получаемые клиентами услуги – ONLINE услугами.

Большинство банков применяют различные формы дистанционного банковского обслуживания, такие как интернет-банкинг, «Банк-клиент», «Теле-Банк», мобильный банкинг (WAP-, SMS-, GSM-, GPRS-), Wi-Fi- банкинг, POS-терминалы и другие, используя несколько вариантов этих систем для обслуживания юридических и физических лиц. При всех различиях системы электронного банкинга, они основаны на системах доступа и передачи информации по одному из каналов связи – компьютер, Интернет, стационарный или мобильный телефон, они имеют существенные преимущества перед традиционным обслуживанием [1].

Заметим, что при использовании технологий электронного банкинга возникает большое количество новых, нетипичных для традиционной банковской деятельности источников компонентов банковских рисков. Банки и клиенты в такой ситуации оказываются незащищенными от угроз, которые могут возникнуть из-за внедрения недостаточно надежных технологий электронного банкинга и банковских автоматизированных систем, которые реализуют. В связи с этим принято выделять три основных «системных» фактора, обуславливающих возникновение новых источников компонентов банковских рисков при внедрении систем электронного банкинга:

- появление в банке клиентов нового типа, которые часто фактически сами играют роль операционистов;
- привлечение третьей стороны, в том числе провайдеров, для обеспечения формирования и поддержания функционирования систем ДБО;
- потенциальная доступность банковских автоматизированных систем банков для несанкционированного доступа и сетевых атак.

К основным рискам, связанных с внедрением систем электронного банкинга, принято относить операционный, юридический, стратегический, репутационный и риск ликвидности. Источники угроз кроются как в программном обеспечении, так и в умышленном или непреднамеренном срабатывании человеческого фактора. Например, угрозы банковской информационной безопасности могут исходить от пользователей внешних сетей (атаки из Интернета, злонамеренное использование каналов дистанционного банковского обслуживания), от персонала банка (вследствие ошибочных действий или небрежности). В программном обеспечении, поддерживающем услуги интернет-банкинга, могут быть встроены подпрограммы разрушительного воздействия или компьютерные вирусы. Немалую угрозу несут в себе сбои в работе оборудования и программного обеспечения [3].

Базельский комитет по банковскому надзору определил принципы управления рисками при предоставлении банковских услуг в

электронном формате, которые включают:

- принципы для совета директоров и правления банка;
- принципы для выбора и адекватного функционирования средств обеспечения безопасности;
- принципы для повышения значимости управления рисками.

Первые три принципа управления рисками электронного банкинга определены в разделе «Наблюдение со стороны совета и руководства». Их суть заключается в том, что совет директоров и правление банка отвечают за разработку корпоративной стратегии банка и за организацию эффективного наблюдения за рисками. Предполагается, что они принимают четкие, обоснованные и формализованные стратегические решения относительно того, будет ли в будущем предоставлять банк услуги в рамках интернет-банкинга, и если да, то каким образом контролировать риски электронного банкинга.

Наблюдательный совет банка несет ответственность за политику управления рисками при осуществлении операций интернет-банкинга и за наличие контроля за безопасностью. В свою очередь, правление банка должно обеспечить надлежащее функционирование систем управления рисками электронного банкинга, что означает введение надлежащих правил авторизации и способов аутентификации, средств контроля логического и физического доступа, построение адекватной структуры безопасности для поддержания необходимых допусков и ограничений в части действий как внутренних, так и внешних пользователей, а также целостности транзакций, записей и информации [2].

Следующие семь принципов управления рисками Базельским комитетом определены в категории «Средства обеспечения безопасности». Такая категория представляет особую значимость вследствие повышенной сложности технологий, применяемых при операциях интернет-банкинга. Третья группа принципов управления рисками электронного банкинга включает рекомендации по управлению правовым и репутационным рисками. Их рост может

быть обусловлен различиями в законодательных актах стран, через которые осуществляются онлайн-операции, в обеспечении конфиденциальности информации и правилах защиты клиента, действующих на территориях этих стран.

При использовании метода ВИА размер капитала на покрытие операционного риска (Operational Risk Capital – ORC) рассчитывается по следующей формуле:

$$ORC = \alpha \times GI$$

где: $\alpha = 15\%$ – фиксированное значение, установленное Базельским комитетом; GI – среднегодовой валовой чистый доход за последние 3 года (валовой чистый доход = (+) процентный доход; (-) расходы на проценты, (+) – поступления от сборов и комиссий; (-) – расходы на сборы и комиссии, (+) – прибыль и/или ущерб от финансовой деятельности, (+) – прибыль от акций и долей, (+) – другие операционные доходы).

Заметим, что за последние годы электронные технологии, из-за возможности запутывания следов и потоков финансовых средств, стали достаточно активно использоваться для легализации доходов, полученных незаконным путем, и отмывание денег. Многими банковскими специалистами как отечественными, так и зарубежными отмечается отставание законодательной базы от практики, регулирующей новые банковские инструменты и технологии, которые могут использоваться для отмывания денег. Их анонимность используется для такой противоправной финансовой деятельности, где фигурируют фиктивные фирмы, подставные лица, то есть которые не существуют реально, а имитированы с помощью электронного документооборота и т.п. Угрозы для банков заключаются в том, что они могут незаметно быть привлечены к противоправной деятельности со всеми негативными последствиями реализации компонентов юридического, репутационного и стратегического рисков.

Определяющим направлением развития банков в современных условиях является активное использование инновационных систем

электронного банкинга как основной формы обслуживания клиентов, которая позволяет расширить и улучшить качество клиентской базы, результативные показатели деятельности, укрепить конкурентные позиции, повысить доступность банковских услуг в отдаленных регионах, а также положительно влияет на имидж банка, его позиционирование как высокотехнологичного финансового института.

Использование систем электронного банкинга, предоставляя определенные преимущества банкам, сопровождается ростом рисков. При таких условиях для банков актуальным является внедрение интегрированного подхода к управлению рисками, связанными с внедрением технологий электронного банкинга, основанного на принципах Базельского комитета, и предусматривают, чтобы каждый сотрудник банка был заинтересован в контроле и предупреждении рисков электронного банкинга, а также повышении ответственности руководства и обеспечении безопасности банка.

Важным является усиление контроля за системами электронного банкинга, в частности системами электронного финансового трансфера, что обусловлено различиями в технологических уровнях, нормах законодательства, требованиях регулирующих органов в разных странах. При таких условиях для контроля за электронными банковскими операциями целесообразно использовать современные интеллектуальные системы, включая эвристические методы, для выявления подозрительных онлайн-операций или финансовых потоков. В то же время регулятору необходимо требовать от банков наличия в них эффективных систем финансового мониторинга, адекватных способам и условиям осуществления ими банковской деятельности.

Список литературы

1. Азиева Н.Н. Дистанционное банковское обслуживание в России: современное состояние и управление рисками // Экономика. Бизнес. Банки. 2015. №3 (12). С. 85-95.
2. Гринько Е.Л., Леонтьева Е.М. Идентификация рисков

дистанционного банковского обслуживания // Актуальные проблемы экономики, социологии и права. 2016. № 1. С. 21-24.

3. Смагина М.Н., Сорина Е.И., Золотарева Г.М. Внутренний аудит и менеджмент операционных рисков системы дистанционного банковского обслуживания // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2015. № 8 (148). С. 38-44.
4. Шумилина О.В., Езангина И.А. Финансовая безопасность банка: риски ДБО // Научный альманах. 2016. № 2-1 (16). С. 392-396.

References

1. Azieva N.N. Distancionnoe bankovskoe obsluzhivanie v Rossii: sovremennoe sostojanie i upravlenie riskami // Jekonomika. Biznes. Banki. 2015. №3 (12). S. 85-95.
2. Grin'ko E.L., Leont'eva E.M. Identifikacija riskov distancionnogo bankovskogo obsluzhivanija // Aktual'nye problemy jekonomiki, sociologii i prava. 2016. № 1. S. 21-24.
3. Smagina M.N., Sorina E.I., Zolotareva G.M. Vnutrennij audit i menedzhment operacionnyh riskov sistemy distancionnogo bankovskogo obsluzhivanija // Vestnik Tambovskogo universiteta. Serija: Gumanitarnye nauki. 2015. № 8 (148). S. 38-44.
4. Shumilina O.V., Ezangina I.A. Finansovaja bezopasnost' banka: riski DBO // Nauchnyj al'manah. 2016. № 2-1 (16). S. 392-396.