
БИБЛИОТЕКА ЦЕНТРА ИССЛЕДОВАНИЙ ПЛАТЕЖНЫХ СИСТЕМ И РАСЧЕТОВ
Применение технологий электронного банкинга: риск-ориентированный подход
Л.В. Лямин
VALID THRU
CREDIT PILOT
ЮНИСТРИМ
КНОРУС

Леонид Витальевич Лямин

Применение технологий электронного банкинга: риск-ориентированный подход

http://www.litres.ru/pages/biblio_book/?art=5020395
Л.В. Лямин. Применение технологий электронного банкинга: риск-ориентированный подход:
КНОРУС, ЦИПСиР; Москва; 2011
ISBN 978-5-406-00978-9

Аннотация

Эта книга содержит анализ недостатков в использовании кредитными организациями электронного банкинга, на основе которого предлагается новый подход к обеспечению их технологической надежности. Современная банковская деятельность полностью зависит от распределенных компьютерных систем, в состав которых все чаще входят системы электронного банкинга.

В то же время недостатки российского гражданского, финансового и, в том числе банковского законодательства ставят высокотехнологичные кредитные организации в сложные условия в плане обеспечения надежности предоставления банковских услуг и защиты интересов клиентов. Использованный в книге риск-ориентированный подход позволяет исключить негативное влияние таких недостатков на организацию дистанционного банковского обслуживания с учетом рекомендаций зарубежных органов банковского регулирования и надзора.

Книга может быть полезна представителям высшего руководства и менеджерам среднего звена кредитных организаций, а также студентам и аспирантам, интересующимся современными подходами к управлению банковскими рисками в условиях электронного банкинга.

Содержание

Л.В. Лямин
Применение технологий электронного банкинга: риск-ориентированный подход

Мнение автора является экспертной точкой зрения и может не совпадать с официальной позицией Банка России

Принятые сокращения

DFD *(Data Flow Diagram)* – диаграмма потоков данных

DMZ *(DeMilitarized Zone)* – демилитаризованная зона

FFIEC – Федеральный совет по проверкам финансовых учреждений США OCC Управление контролера денежного обращения США SLA *(Service Level Agreement)* соглашение об уровне обслуживания VPN *(Virtual Private Network)* виртуальная частная сеть

АПО – аппаратно-программное обеспечение

АРМ – автоматизированное рабочее место

АС – автоматизированная система

АСП – аналог собственноручной подписи

БАС – банковская автоматизированная система

БКБН – Базельский комитет по банковскому надзору

ВА – внутренний аудит

ВК – внутренний контроль

ГК РФ – Гражданский кодекс Российской Федерации

ДБО – дистанционное банковское обслуживание

ЖЦ – жизненный цикл

ЗВС – зональная вычислительная сеть

ЗСК – знай своего клиента

ИБ – интернет-банкинг

ИСУ – информационная система управления

ИТ – информационные технологии

ЛВС – локальная вычислительная сеть

НСД – несанкционированный доступ

ОИБ – обеспечение информационной безопасности

ОЭСР Организация экономического сотрудничества и развития ПИО программно-информационное обеспечение

ПОД/ФТ – противодействие отмыванию денег и финансированию терроризма

ППР – поддержка принятия решений

ПСИ – приемо-сдаточные испытания

РМВ – реальный масштаб времени

СБ – служба безопасности

СБР – системный банковский риск

СВК – служба внутреннего контроля

СОР – система оценивания рисков

СЭБ – система электронного банкинга

ТБР – типичный банковский риск

ТЭБ – технология электронного банкинга

ТЭО – технико-экономическое обоснование

УБР – управление банковскими рисками

УРСИТ – универсальная рейтинговая система для информационных технологий

ФМ – финансовый мониторинг

ЭБР – элементарный банковский риск

Введение
Актуальность и проблематика электронного банкинга

Если вы не знаете как это делать, не делайте этого.
Б. К. С. Айенгар

Во всем мире кредитные организации сталкиваются с двумя принципиальными проблемами, которые им приходится решать при разработке и реализации своих стратегических и бизнес-планов, а именно:

– снижение себестоимости банковской деятельности;

– занятие лидирующих позиций на финансовых рынках.

Поскольку набор финансовых услуг, предоставляемых кредитными организациями, всегда строго регламентируется национальным банковским законодательством, а операционные нововведения быстро становятся общедоступными, получить конкурентные преимущества за счет варьирования состава, расширения или модернизации банковских услуг оказывается затруднительным. В публикациях, относящихся к вопросам современного финансового обслуживания, часто отмечается, например, что «компании, которые хотят выжить в современном мире, должны стремиться к использованию новых технологий для достижения конкурентных преимуществ»[1]. К тому же в условиях российского банковского законодательства, которое до сих пор остается в стадии становления, такие нововведения могут неожиданно выйти за границы так называемого «правового поля», а это чревато финансовыми потерями не только из-за их возможной нерентабельности (население в большинстве своем либо насторожено относится к нововведениям, либо не обладает необходимой компьютерной грамотностью), но также из-за возрастания уровня правового риска (непосредственного и опосредованного – через другие банковские риски). Поэтому в настоящее время кредитные организации в конкурентной борьбе на рынках предоставления финансовых услуг фактически вынуждены внедрять все новые банковские компьютерные (информационные) технологии, что в условиях функционирования российского банковского сектора практически всегда означает внедрение новых технологий *дистанционного банковского обслуживания,* или, иначе говоря, технологий «электронного банкинга», – этот англоязычный термин стал общепринятым. В итоге к концу первого десятилетия XXI в. это направление банковской деятельности включило уже около двух десятков вариантов такого предоставления банковских услуг, о чем свидетельствуют результаты первого сплошного анкетирования в этой области, проведенного Банком России[2]. Также к этому времени не осталось сомнений в том, что основной функцией кредитных организаций постепенно становится преимущественно *дистанционное* финансовое посредничество.

Следует сразу отметить то, что в *собственно* банковскую деятельность кредитных организаций в ее операционном понимании электронный банкинг изначально ничего нового не внес. Однако в том, что касается *способов* и *условий* осуществления этой деятельности, особенно в части организации реализующих и обеспечивающих ее технологических процессов (внутрибанковских и внешних), их аппаратно-программного обеспечения (как самих кредитных организаций, так и их контрагентов), состава факторов и источников банковских

---

[1] *Coderre D.* Internal Audit. Efficiency through automation. John Wiley&Sons Inc., Hoboken, NJ, USA, 2009.

[2] Сводная информация приведена в пресс-релизе Банка России, размещенном на его официальном web-сайте по адресу http://www.cbr.ra/press/Archive_get_blob.asp?doc_id=090313 1311401.htm.

рисков, а следовательно, содержания управления этими рисками, произошли *радикальные* изменения. Изучению этих изменений и подходам к их учету руководства кредитных организаций при определении им содержания и реализации внутрибанковских процессов (прежде всего управления банковскими рисками), составляющих их процедур и функций, а также взаимосвязей между ними в условиях применения электронного банкинга, посвящена эта книга.

Одно из главных отличий применения кредитными организациями технологий рассматриваемого типа от традиционных подходов к организации банковского обслуживания клиентов заключается в том, что клиенты, которые переходят к использованию таких технологий, после заключения ими договора банковского счета с кредитной организацией, дополнительного соглашения к этому договору о дистанционном банковском обслуживании и получения средств удаленного доступа к ее информационно-процессинговым ресурсам могут уже не являться в ее головной или дополнительный офисы (филиалы) для того, чтобы получить какую-либо банковскую информацию, или за выполнением требуемых им банковских операций, а работать

в условиях, так сказать, «домашнего банка». По сути, удаленно взаимодействующие с кредитной организацией клиенты «превращаются» в своего рода разновидности банковских операционистов. Такие возможности для них создают новые банковские автоматизированные системы, реализующие технологии электронного банкинга, предлагая реальным и потенциальным клиентам кредитных организаций нетрадиционные варианты и возможности их внеофисного обслуживания или предоставления банковских услуг.

Обеспечиваемые при этом пользователям систем электронного банкинга удобства и гибкость получения ими банковских услуг привели к широкому распространению во всем мире таких технологий, как *мобильные платежи* и *мобильный банкинг*[3], и, естественно, российский банковский сектор не является исключением. Напротив, за последние несколько лет наблюдается «бум» внедрения технологий такого рода отечественными кредитными организациями, причем развитие их непосредственно следует за достижениями в области технологий компьютерной связи, – так появились, к примеру, системы Wi-Fi-банкинга. Фактически ни одно из подобных технологических и технических достижений современности не остается без внимания банковского сообщества, что не удивительно, учитывая обострение борьбы за клиентуру и рынки сбыта финансовых продуктов. Вместе с тем следует отметить, что большинство кредитных организаций не ограничивается лишь одним каналом дистанционного банковского обслуживания, наращивая «технологические мышцы» и вводя в эксплуатацию одну систему такого рода за другой.

Типичными примерами, судя по результатам анкетирования Банка России, уже стали кредитные организации, предлагающие по 3 – 4 варианта этих систем для юридических и физических лиц, для клиентов, предпочитающих мобильный банкинг или предоставление банковских услуг через Интернет (так называемый «интернет-банкинг»), для пользователей «наладонных» компьютеров, коммуникаторов или PDA[4] (для которых организуются также специальные web-сайты) и т.п. Использование разнообразных телекоммуникационных сетей и систем вызвало к жизни управляемые через сеть Интернет (далее – Сеть) банкоматы, разнообразные системы мобильного (WAP-, SMS-, GSM-, GPRS-) и Wi-Fi-банкинга, POS-терминалы[5], и процесс этот, судя по всему, не прекратится до тех пор, пока существуют

---

[3] См., например, исследование: *Boyd C, Jacob K.* Mobile Financial Services and the Underbanked: Opportunities and Challenges for M-banking and M-payments. The Center for Financial Services Innovation, Chicago, Il, April 2007.

[4] PDA = *Personal Digital Assistant* – тип сверхлегкого миниатюрного персонального компьютера.

[5] WAP = *Wireless Application Protocol* – протокол беспроводного взаимодействия, служит для обеспечения беспроводного доступа к сервисам Интернет с помощью мобильного телефона. SMS = *Short Message Service* – служба коротких сообщений, позволяющая пользователям мобильных телефонов осуществлять двусторонний обмен текстовыми сообщениями

кредитные организации, конкуренция в банковской сфере, да и так называемый «научно-технический прогресс».

В то же время на мощной волне использования в банковской деятельности достижений в областях компьютерных и телекоммуникационных технологий существенно меняются *способы* и *условия* осуществления банковской деятельности. Речь, конечно, не идет о том, что применение таких технологий изменяет сущность банковской деятельности: в конце концов под электронным банкингом понимается не более чем некий новый «транспорт», обеспечивающий доступ клиента к вполне традиционным банковским продуктам и услугам, однако особенности этого транспорта таковы, что меняется *характер* банковского обслуживания, а отчасти и его *содержание*. То и другое в свою очередь существенно изменяет состав факторов и источников рисков, связанных с банковской деятельностью, из-за чего происходит смещение профилей риска кредитных организаций.

Необходимо отметить, что как отечественные, так и некоторые зарубежные кредитные организации, даже крупные, нередко демонстрируют недостаточное осознание этих изменений, придерживаясь своего рода «традиционных подходов» к пониманию содержания банковской деятельности, не замечая при этом, что времена уже наступили другие, а вместе с ними изменилось и само содержание. Этому, по-видимому, способствует и достаточно консервативный характер банковского сообщества в целом, в котором традиционно считается, что для высшего руководства кредитных организаций квалификация в области информационных технологий является лишь факультативной. Кстати сказать, во многих случаях отсутствие или неполнота осознания «нового времени» фактически закреплены в законодательстве, регламентирующем банковскую деятельность, и российское банковское (и в широком смысле финансовое) законодательство в этом смысле также не является исключением.

В российских условиях наиболее близким примером является, естественно, Федеральный закон от 2 декабря 1990 г. № 395-I «О банках и банковской деятельности». В его содержании отсутствует то, о чем сказано в его названии, а именно – в нем нет определения банковской деятельности как таковой. Вместо этого в ст. 5 перечислены «банковские операции и другие сделки», к которым фактически сведено понятие «деятельности», т.е. изначально неясно, что именно следует понимать под *банковской* деятельностью. Можно заметить, что с содержательной точки зрения все кредитные организации (или хотя бы те, которые определяются как универсальные) выполняют примерно одни и те же операции и предоставляют сходные банковские услуги, однако способы осуществления и результаты их банковской деятельности могут оказаться принципиально различными (вплоть до отзыва лицензии на это осуществление). Таким образом, дело заключается не столько в операциях, сколько в способах и условиях их совершения, которые определяет руководство кредитной организации, и применение технологий электронного банкинга это подчеркивает (в основном именно за счет смещения профилей риска кредитных организаций).

Указанное недоразумение, на первый взгляд не очень важное, на практике приводило и приводит к возникновению немалого количества новых источников банковских рисков, которые традиционно с этой деятельностью не связывались, – в сфере технологий электронного банкинга это проявляется наиболее наглядно. Внедрение систем электронного банкинга всегда приводит к такому не всегда заметному смещению профилей рисков кредитных

между собой, а также с информационными системами разного назначения. GSM = *Global System for Mobile communications* – глобальная система мобильной связи. GPRS = *General Packet data Radio Service* – общая служба радиопередачи пакетированных данных, предназначенная для осуществления экономичного обмена данными с помощью мобильного телефона, включая обеспечение WAP-доступа к Интернету. Wi-Fi = *Wireless Fidelity* – обозначение некоторых типов беспроводных локальных вычислительных сетей (*Wireless Local Area Network* – WLAN), в которых используются спецификации протокола семейства 802.11. POS = Point-Of-Sale – пункт продаж, место продавца (кассира). POS-терминал – устройство, предназначенное для дистанционного проведения расчетов за покупки в торговых предприятиях с использованием банковских пластиковых карт.

организаций, к чему многие из них на практике оказываются не готовы. Ситуация усугубляется еще и тем, что зачастую банковская деятельность (в широком смысле, как будет показано ниже) оказывается зависимой от сторонних компаний – провайдеров, о компьютерных и телекоммуникационных системах которых специалисты кредитных организаций могут не иметь необходимых для их надежного функционирования сведений. Следствием этого становятся крупные потери кредитных организаций и их клиентов из-за компьютерных мошенничеств и хищений, сетевых и вирусных атак, ошибок и инцидентов информационной безопасности, нарушений законодательства и других негативных явлений. Кроме того, коль скоро банковская деятельность во многом уходит в «виртуальное киберпространство», могут обостриться и все аналогичные проблемы с инсайдерами кредитной организации, которые лучше всех информированы об особенностях функционирования ее автоматизированных систем. Поэтому разработка подходов к обеспечению надежной банковской деятельности в условиях применения кредитными организациями технологий электронного банкинга стала весьма актуальной, о чем также говорит эта книга.

Фактически системы электронного банкинга появились в российском банковском секторе довольно давно, еще в начале 90-х гг. прошлого века, только назывались они тогда системами «Банк – Клиент» и не имели разновидностей[6]. Практически во всех случаях это были системы с так называемым «толстым клиентом», под которым понималось некое автоматизированное рабочее место с установленным на нем специализированным программным обеспечением для доступа к информационно-процессинговым ресурсам кредитной организации, служебными базами данных, средствами криптозащиты трафика, ограничения физического и логического доступа и т.д. Вопросы относительно банковских рисков, связанных с такими системами, как правило, не поднимались, поскольку все рисковые компоненты оставались на стороне клиента (естественно, юридического лица), и вообще в то время эти темы не обсуждались, потому что случаев несанкционированного доступа к упомянутым ресурсам было довольно мало.

За почти два прошедших десятилетия ситуация изменилась кардинальным образом и прежде всего потому, что акценты в финансовом обслуживании стали смещаться в сторону клиентов – физических лиц. Вследствие этого актуальны стали уже системы дистанционного банковского обслуживания с так называемым «тонким клиентом» – в предельном варианте, в случае банковского обслуживания через Интернет, – это обычный интернет-браузер типа Microsoft Explorer, Netscape Navigator, Mozilla, Opera и пр., через который можно получить доступ к диалоговым средствам интерфейса с процессингом кредитной организации. Одновременно возникли факторы риска, связанные с трафиком через не только локальные, но также зональные и глобальные сетевые структуры. Однако их наличие не остановило кредитные организации, стремящиеся за счет увеличения масштабов и количества вариантов дистанционного предоставления банковских услуг охватить как можно большее число клиентов, ценящих оперативность и удобство банковского обслуживания.

Как показывает изучение предложений компаний – разработчиков банковского программного обеспечения, в настоящее время в области удаленного автоматизированного (компьютеризованного) банковского обслуживания наблюдаются следующие четыре тенденции:

1) агрегация требований клиентуры кредитных организаций, их самих и корпоративных структур;

2) сочетание возможностей корпоративного и розничного банковского обслуживания;

3) создание корпоративных систем и модульная технология «Plug-and-Play»;

---

[6] Любые технологии электронного банкинга реализуются распределенными автоматизированными компьютерными системами, относящимися к системам «Банк – Клиент»; тем не менее для удобства классификации в главе 1 будет рассмотрена соответствующая обобщенная схема деления этих технологий, используемая в интересах банковского надзора, в частности, Банком Германии («Дойчебундесбанком»).

4) комбинация в системах дистанционного банковского обслуживания возможностей «толстого» и «тонкого» клиента.

Вместе с тем предлагаются варианты централизованного, распределенного и комбинированного построения систем дистанционного банковского обслуживания на основе локальных и зональных вычислительных сетей.

Можно отметить, что уже несколько лет российский банковский сектор основной акцент делает на внедрении и развитии многоканального дистанционного банковского обслуживания с интеграцией разнородных информационных технологий, при этом стараясь повысить эффективность способов и средств выполнения банковских операций и сделок, а также снизить уровни банковских рисков. Последнее, к сожалению, удается далеко не всегда, поскольку встречается немало примеров внедрения кредитными организациями недостаточно апробированных и защищенных компьютерных технологий (в широком смысле), несоответствия условий, в которых применяются технологии электронного банкинга, принципам обеспечения надежной банковской деятельности. Разного рода «деклассированные элементы» отечественного социума также быстро обучаются использованию систем электронного банкинга в противоправных целях, из-за чего достаточно серьезные финансовые потери несут и сами кредитные организации, и их клиенты. За последние три года число таких случаев выросло в несколько раз, так что суммарные финансовые потери российских кредитных организаций (и их клиентов) оцениваются уже десятками и сотнями миллионов рублей.

Такие потери свидетельствуют как о недопустимо высоких уровнях банковских рисков, принимаемых на себя кредитными организациями в процессе развития и увеличения масштабов дистанционного банковского обслуживания, так и об «эффективной» реализации источников этих рисков в отсутствие пруденциальных условий применения новых банковских информационных технологий. Это в свою очередь обусловлено наличием значительного количества *недостатков* в организации их применения в целом и использования конкретных систем электронного банкинга, причем как самими кредитными организациями, так и их клиентами. Ответственность за это лежит на руководстве и персонале кредитных организаций (а не на клиентах, как часто считается), поскольку и банковские автоматизированные системы, и клиенты, и контрагенты относятся к их так называемым «зонам ответственности». На самом деле ничего сверхъестественного в смысле организации надежных условий использования любых технологий дистанционного банковского обслуживания нет. Дело вовсе не в технологиях как таковых, или в банковских автоматизированных системах, или их локальных либо зональных вычислительных сетях и т.п., а в том, в каких целях и *как именно* все эти системы применяются. Определение же условий применения этих средств является прерогативой в первую очередь *руководства* высокотехнологичных кредитных организации, их исполнительных органов и менеджмента на разных уровнях внутрибанковской иерархии, вследствие чего в подавляющем большинстве случаев проблемы, возникающие у кредитных организаций в рассматриваемой предметной области, непосредственно увязываются с такими недостатками в их корпоративном управлении, что оно и корпоративным-то может считаться только с серьезной натяжкой.

Происходит это потому, что специфика новых банковских информационных технологий и их значимость для современной кредитной организации и ее клиентов недостаточно оцениваются и осознаются ее руководителями (исполнительными органами). При этом специфика применения соответствующих банковских автоматизированных систем должна в оптимальном варианте прямо отражаться в специальных условиях, в которых они применяются и которые организуются исходя из требований снижения влияния сопутствующих их особенностям угроз надежной банковской деятельности, т.е. уровней *рисков.* По многочисленным наблюдениям и публикациям в средствах массовой информации управление банков-

скими рисками в отечественных кредитных организациях оставляло и до сих пор оставляет желать лучшего, и особенно это относится к управлению такими рисками, уровни которых непосредственно зависят от, так сказать, «степени пруденциальности» условий применения новых банковских информационных технологий. Как ни странно, многочисленные случаи реализации этих рисков именно по технологическим и техническим причинам редко приводят к улучшению корпоративного управления.

Очевидно, что традиционная интерпретация банковской деятельности как только лишь совершения банковских операций не только устарела, но принципиально *неприемлема,* т.е. вместе с внедрением кредитными организациями новых банковских информационных технологий, видов и способов предоставления банковских услуг требуется «новое мышление» их руководства и осознание влияния изменения способов и условий банковской деятельности на ее содержание и характеристики. Специфическими особенностями современного банковского обслуживания стали именно способы дистанционного информационного взаимодействия между кредитными организациями и их клиентами в *информационном контуре банковской деятельности,* который создается новыми технологиями. Это новое явление и новое понятие, вошедшие в банковскую деятельность, и одним из важнейших следствий этого стала необходимость изменения подходов к корпоративному управлению в кредитных организациях, а именно адаптации его к тем технологиям и системам электронного банкинга, которые внедряют эти организации, – тоже как следствие корпоративных решений о переходе к дистанционному банковскому обслуживанию. Вместе с тем принципиально важной становится и оценка обеспеченности кредитной организации ресурсами, необходимыми для надежного банковского обслуживания в этом контуре: оборудованием, персоналом, квалификацией и т.д.

В первую очередь важно *осознание* высшими руководителями и менеджерами, входящими в исполнительные органы кредитных организаций, того, что реализация всех технологий электронного банкинга базируется на *распределенных* компьютерных системах. Это в свою очередь приводит к тому, что зоны ответственности кредитной организации существенно расширяются и даже такие традиционные из них, как клиентская или внутрисистемная, радикально видоизменяются (в плане содержания указанной ответственности). Современные универсальные протоколы сетевого взаимодействия и организация телекоммуникационных сетей по так называемому «принципу открытых систем» приводят к возникновению новых факторов, обусловливающих возникновение нетипичных (и непривычных) источников компонентов банковских рисков. В настоящее время нет необходимости в пропагандировании мультикомпонентности, комплексного характера типичных банковских рисков[7], однако в отечественных кредитных организациях традиционно принято уделять содержанию процесса управления банковскими рисками лишь формальное внимание, что в условиях применения технологий электронного банкинга означает гарантированное наличие непредвиденных и некомпенсируемых рисковых компонентов.

Поэтому, исходя из значимости новых факторов и источников банковских рисков, возникающих в указанных условиях, основная часть этой книги начинается именно с рассмотрения явления информационного контура банковской деятельности при электронном банкинге и обусловленных этим факторов риска системного характера, наличие которых целесообразно учитывать в интересах обеспечения надежности этой деятельности. Изложение ведется во многом с использованием материалов Базельского комитета по банковскому надзору и органов банковского регулирования и надзора США, поскольку они наиболее полно характеризуют рисковую обстановку в условиях применения технологий электрон-

[7] Использована формулировка из Указания оперативного характера Банка России от 23 апреля 2004 г. № 70-Т «О типичных банковских рисках».

ного банкинга. С учетом условий российского банковского сектора, в котором действует ряд специфических ограничений, выделяются и анализируются с аналогичных позиций лишь несколько типичных банковских рисков. Главный проблемный вопрос для кредитных организаций при принятии решений относительно применения тех или иных технологий заключается в убеждении, что получаемые от этого выгоды заведомо будут больше, чем возможные потери из-за затрат на внедрение и эксплуатацию банковских автоматизированных систем, реализующих такие технологии, и на компенсацию реализации компонентов банковских рисков, связанных с ведением бизнеса в «киберпространстве».

Речь не случайно идет об использовании риск-ориентированного подхода при анализе проблем, сопутствующих внедрению технологий электронного банкинга. Необходимо подчеркнуть, что в современных российских условиях с почти полным отсутствием законодательных и других нормативных актов, относящихся к области так называемых «электронных финансов» или, как иногда говорят, «предоставления финансовых услуг в электронной форме», пустота этого сегмента правового поля оказывает крайне *негативное* влияние на обеспечение надежности банковской деятельности, практически полностью зависящей от функционирования банковских автоматизированных систем и условий их использования прежде всего из-за отсутствия соответствующих точно определенных и установленных ориентиров. Из-за этого и наибольшая часть практических решений оказывается прерогативой вовсе не высшего руководства кредитных организаций, а менеджмента среднего звена, а то и просто персонала исполнительского уровня (что будет показано при рассмотрении процессного подхода). В рамках же риск-ориентированного подхода акцент делается на выявлении и устранении или, как минимум, ослаблении потенциального влияния источников компонентов банковских рисков (или хотя бы его хеджировании), а значит, и повышении этой надежности в корпоративном плане.

Риск-ориентированный подход весьма эффективен именно в приложении к анализу информационного контура банковской деятельности и вообще автоматизации внутрибанковских процессов в силу своей универсальности: он служит защите кредитных организаций и их клиентов от любых угроз их интересам или негативных явлений независимо от степени развития законодательной базы банковской деятельности. Очевидно, что все нюансы технологического и технического обеспечения этой деятельности никакими нормативными правовыми актами предусмотреть невозможно в силу того, что оно изначально не может регламентироваться в соответствии с действующим банковским законодательством. Из-за этого оказывается невозможно зафиксировать упомянутые ориентиры ни на федеральном, ни на отраслевом или ведомственном уровне. Впрочем, зарубежный опыт банковского регулирования и надзора показывает, что в этом нет необходимости (если, конечно, имеется развитая законодательная база, содержащая описания как порядка, так и характеристик банковской деятельности). Но тогда единственным вариантом содействия обеспечению надежности высокотехнологичных кредитных организаций остается разработка рекомендаций, основанных на *здравом смысле,* с указанием тех недостатков (не нарушений!), о которых лучше знать заранее и которые целесообразно устранять (лучше же – не допускать их появления), чтобы надежность банковской деятельности не снижалась независимо от того, какие именно автоматизированные системы внедряет кредитная организация. Здесь имеется в виду, что риск-ориентированный подход вполне был бы пригоден даже в условиях полного отсутствия (если можно такое представить) регламентации банковской деятельности со стороны государства (из состава банковских рисков исчез бы лишь правовой риск) для выработки рекомендаций по повышению ее технологической надежности.

Далее акцент делается на уже достаточно широко известном у нас так называемом процессном подходе, использование которого оказывается весьма желательным именно при переходе кредитной организации к дистанционному банковскому обслуживанию и его даль-

нейшем развитии. Как правило, такие организации, внедрившие и апробировавшие один из вариантов электронного банкинга, на достигнутом не останавливаются (к этому их подталкивает и конкуренция) и продолжают развивать это направление банковской деятельности, расширяя спектр предоставляемых клиентам сервисов и внедряя новые банковские информационные технологии и автоматизированные системы. Вследствие этого, помимо жизненного цикла таких систем, оказывается целесообразным говорить и о *жизненном цикле внутрибанковских процессов.* К сожалению, как свидетельствует опыт изучения деятельности российских кредитных организаций, такой подход все еще остается делом будущего (хотя автор обоснованно является его убежденным сторонником).

В свою очередь реализация такого подхода в новых условиях банковской деятельности, сущность которых определяется теми информационными технологиями, которые внедряет кредитная организация, невозможна без пересмотра организации и содержания прежде всего общих внутрибанковских процессов управления и контроля, которые в таких организациях приобретают заметную специфику. Особенности корпоративного управления в условиях применения технологий электронного банкинга заключаются в его четкой ориентации, во-первых, на учет особенностей самих технологий такого рода, реализующих их автоматизированных систем и информационного контура банковской деятельности, во-вторых, на обеспечение соответствия их применения принципам или стандартам «пруденциальной» банковской деятельности (хотя в российском банковском секторе подобная терминология пока не является общепринятой) и, в-третьих, на своевременную и адекватную адаптацию внутрибанковских процессов при внедрении и развитии дистанционного банковского обслуживания. Принципиально важным здесь является то, что, какими бы ни были технологические нововведения в обеспечении банковской деятельности, они не должны негативно влиять на выполнение кредитными организациями своих обязательств перед клиентами (имея в виду защиту их интересов) и контролирующими банковскую деятельность государственными органами. Кроме того, в современных условиях повышается важность обеспечения предоставления последним полной, своевременной и адекватной информации о банковской деятельности в целом и об операциях, совершаемых кредитными организациями по ордерам удаленных клиентов.

Отдельная глава посвящена специфической проблематике управления web-отношениями кредитной организации – актуальная тема в условиях использования представительств в Сети подавляющим большинством отечественных кредитных организаций. Несмотря на то что, к примеру, технология интернет-банкинга используется в российском банковском секторе уже достаточно давно (с 1997 – 1998 гг.), вопросам риск-ориентированного анализа отношений, возникающих в Сети между разными агентами сетевого и информационного взаимодействия, внимания в литературе до последнего времени не уделялось. Однако исследования, проводимые зарубежными органами банковского регулирования и надзора, свидетельствуют о наличии ряда достаточно «тонких» аспектов такого взаимодействия, за которыми в отсутствие их учета также скрываются источники компонентов банковских рисков, так как само наличие web-отношений оказывается своеобразным фактором риска как для кредитной организации, так и для ее клиентов. Обусловлено это преимущественно спецификой проявления виртуальных эффектов Сети как открытой информационной системы.

Главное же заключается в осознании необходимости модернизации ряда действующих внутрибанковских процессов, имеющих непосредственное отношение к дистанционному банковскому обслуживанию с учетом особенностей упоминавшихся *новых* условий банковской деятельности, а также формирования новых *процессов* (например, управления отношениями с провайдерами, web-отношениями и т.п.). Такое осознание логично связывается с разработкой своего рода новой *идеологии* управления и контроля, которая инициируется советом директоров кредитной организации, а затем реализуется ее исполнительными

органами и менеджерами разных уровней. В связи с этим в изложении введено понятие внутрибанковского «мета-процесса», управляющего циклической адаптацией отдельных процессов, которая сама определяется темпом нововведений по направлениям применения компьютерных информационных технологий. Отсутствие соответствующего «руководящего подхода» к внедрению новых средств компьютеризации банковской деятельности вместо ожидаемых выгод может стать причиной непредсказуемого возникновения и реализации источников компонентов банковских рисков. В ситуации, когда банковская деятельность сама стала во многом информационной дисциплиной, такие компоненты могут оказаться весьма существенными и для кредитной организации, и для ее клиентов. Поэтому наиболее важным аспектом адаптации оказывается обеспечение сохранения *управляемости* и *контролируемости* банковской деятельности, переходящей при электронном банкинге в виртуальное пространство.

Содержание этой книги опирается на материалы зарубежных и международных органов банковского регулирования и надзора (в том числе представленных на ряде международных семинаров по тематике электронного банкинга), мнения зарубежных специалистов по вопросам обеспечения надежности высокотехнологичной банковской деятельности, опыт изучения организации применения технологий электронного банкинга отечественными кредитными организациями и зарубежными коммерческими банками, а также их дочерними банками, работающими на территории России. Несмотря на то что кредитных организаций, полностью свободных от недостатков, пока не выявлено (это не означает, что их не существует, – просто любой человеческий опыт имеет вполне понятные ограничения!), что и неудивительно, учитывая сложность и относительную новизну рассматриваемой тематики, все-таки результаты изучения зарубежного опыта свидетельствуют о желательности следования ему в отечественном банковском секторе, поскольку даже в отсутствие должным образом развитого финансового и, в частности, банковского законодательства использование так называемой «лучшей практики»[8] способно существенно снизить уровень ряда типичных банковских рисков (имея в виду те риски, уровни которых прямо зависят от банковских информационных технологий и реализующих их внутрибанковских процессов, процедур и автоматизированных систем).

Базельский комитет по банковскому надзору уделяет в ряде своих публикаций серьезное внимание вопросам управления рисками в условиях применения технологий электронного банкинга и корпоративному управлению в кредитных организациях. Следование его рекомендациям позволяет повысить надежность банковской деятельности в целом за счет снижения уровней рисков, которым подвергаются кредитные организации и их клиенты, а значит, обеспечить лучшую защиту их интересов.

[8] Общепринятый термин в материалах зарубежных органов банковского регулирования и надзора.

Глава 1
Понятие и специфика технологий электронного банкинга

Любая достаточно развитая технология неотличима от магии.
Артур Кларк

Независимо от того, какого рода система дистанционного банковского обслуживания (ДБО) внедряется кредитной организацией, такая система фактически становится для нее своеобразными «виртуальными воротами», которые открывают доступ из «киберпространства» локального, зонального или глобального сетевого взаимодействия к информационно-процессинговым ресурсам и информационным а по сути, – к финансовым активам этой организации. Надежность банковской деятельности, которая осуществляется через такое пространство, *непосредственно* зависит от того, насколько организация способна управлять происходящими в нем и значимыми для нее (и ее клиентов) процессами и контролировать их течение. Очевидно, что специфика такой деятельности изначально находится в противоречии между обеспечением доступа к упомянутым ресурсам только и исключительно для легитимных пользователей (официально зарегистрированных клиентов, операторов, операционистов и т.п.), действующих в пределах точно установленных для них прав и полномочий, и технологиями, предполагающими реализацию принципов открытых систем и универсальных протоколов сетевого взаимодействия, составляющих базис большинства вариантов ДБО. Если руководство кредитной организации, внедряющей систему электронного банкинга (СЭБ), недостаточно полно представляет себе особенности проблематики ДБО с точки зрения вариативности состава компонентов типичных банковских рисков, принимаемых на себя кредитной организацией, то уровни этих рисков будут заведомо (и неоправданно) повышаться, а сами эти компоненты – реализоваться, что всегда приводит к финансовым потерям.

До настоящего времени в российском банковском секторе внедрение и применение банковских информационных технологий в целом не считается чем-то значимым с точки зрения изменения характера банковской деятельности. В подавляющем большинстве кредитных организаций этот процесс не предваряется и не сопровождается *адекватным* анализом состава сопутствующих таким технологиям компонентов банковских рисков. Из-за этого как сами кредитные организации, так и их клиенты оказываются подвержены новым специфическим угрозам надежности банковской деятельности. С этими угрозами кредитные организации далеко не всегда справляются, о чем свидетельствует, к сожалению, уже достаточно обширная статистика финансовых потерь этих организаций и их клиентов. При этом собственно технологический аспект оказывается в значительной степени «вторичным»: к примеру, не столь важно, каким именно путем похищаются финансовые средства – с помощью банкоматного мошенничества, через систему интернет-банкинга, за счет применения какого-то варианта фишинга, фарминга или вишинга и т.п., – важно то, что деньги исчезают именно в информационном контуре ДБО по причинам недостаточно полного учета новых факторов источников типичных банковских рисков и управления ими в кредитной организации.

Вследствие этого рассматриваемая ниже классификация технологий или вариантов ДБО может варьироваться без ущерба для общности рассмотрения этой предметной области. Она введена в основном для того, чтобы можно было выделить те особенности каналов и сред информационного взаимодействия между кредитными организациями и их клиентами, которые желательно учитывать в случаях комплексного внедрения соответствующих систем

ДБО. В настоящее время компании, разрабатывающие системы такого рода, или кредитные организации, осуществляющие их самостоятельные разработки, все больше стремятся к многоканальности предоставления банковских услуг, объединяющей его варианты. Вместе с тем это, как правило, не приводит к организации *комплексного* анализа всей совокупности источников банковских рисков, сопутствующих каждому из каналов ДБО, а следовательно, новые источники рисков остаются «скрытыми» для кредитной организации, так что воздействие на них (т.е. собственно управление рисками) начинается нередко лишь тогда, когда они реализуются в виде финансового ущерба.

1.1. Классификация технологий электронного банкинга

На сегодняшний день единой, устоявшейся классификации технологий электронного банкинга еще не существует. Поскольку любые технологии такого рода используются для обеспечения удаленного информационного взаимодействия между кредитными организациями и их клиентами, с наиболее общей точки зрения можно полагать, что все они в совокупности охватываются одним общим понятием систем типа (или класса) «Банк – Клиент». В то же время исторически сложившиеся этапы развития способов и средств этого взаимодействия привели к тому, что под системами «Банк – Клиент» до настоящего времени понимаются преимущественно такие программно-технические комплексы, для функционирования которых на стороне клиента необходимо создание специализированного автоматизированного рабочего места (АРМ) на базе персонального компьютера, установка на нем специализированного программно-информационного обеспечения ДБО, задействование тех или иных выделенных каналов связи (на основе кабельных или релейных линий), а также введение на стороне кредитной организации шлюзов для передачи потоков данных (модемных пулов, маршрутизаторов, коммутаторов и т.п.).

Такие достаточно «тяжеловесные» и дорогостоящие системы получили условное название систем «с толстым клиентом»[9]. Эти системы характеризуются достаточно обширными функциональными возможностями в части ограничения прав доступа к информационно-процессинговым ресурсам клиента и кредитной организации, использования служебных баз данных и баз нормативно-справочной информации, криптозащиты сетевого трафика, а также сохранения так называемой «сеансовой информации», сопровождающей двусторонний информационный обмен (что принципиально важно для обеспечения юридической силы так называемых «электронных документов», парирования случаев «отказа от операций», разрешения спорных ситуаций и т.п.). За все эти возможности приходится, естественно, немало платить, что могут себе позволить в основном юридические лица.

В отличие от этих систем для обслуживания физических лиц гораздо удобнее и дешевле системы с так называемым «тонким клиентом», использование которых не связано с необходимостью установки на АРМ клиента специального программно-информационного обеспечения, да и само стационарное АРМ на его стороне зачастую не требуется. В наиболее «тонком» случае могут использоваться обычный браузер или система меню, что типично для технологий мобильного и интернет-банкинга. Однако в этих случаях осложняется решение всех перечисленных выше вопросов с точки зрения функциональных возможностей той или иной технологии электронного банкинга (ТЭБ) и реализующей эту технологию СЭБ. Эта книга преимущественно посвящена тому, чем приходится «платить» кредитным организациям и их клиентам за удобства оперативного доступа к информационно-процессинговым ресурсам, обеспечивающим банковскую деятельность.

Вместе с тем каждый из способов ДБО и каждая используемая для его реализации банковская автоматизированная система (БАС) могут иметь ряд принципиальных отличий (прежде всего в части каналов связи и среды взаимодействия), равно как и множество особенностей, из-за чего объединение их в один класс существенно затрудняет анализ состава компонентов банковских рисков, угроз банковской деятельности, лежащих в их основе, и причин возникновения этих угроз. Для такого анализа наиболее удобна простая классифика-

[9] Системы электронного банкинга такого рода в зависимости от их сложности, архитектуры, многоканальности и т.п. характеристик могут стоить от тысяч до миллионов условных единиц. Учет этого фактора с позиций риск-ориентированного подхода важен с точки зрения оценки потенциального стратегического риска.

ционная схема, используемая специалистами Департамента банковского надзора Банка Германии (рис. 1.1)[10]:

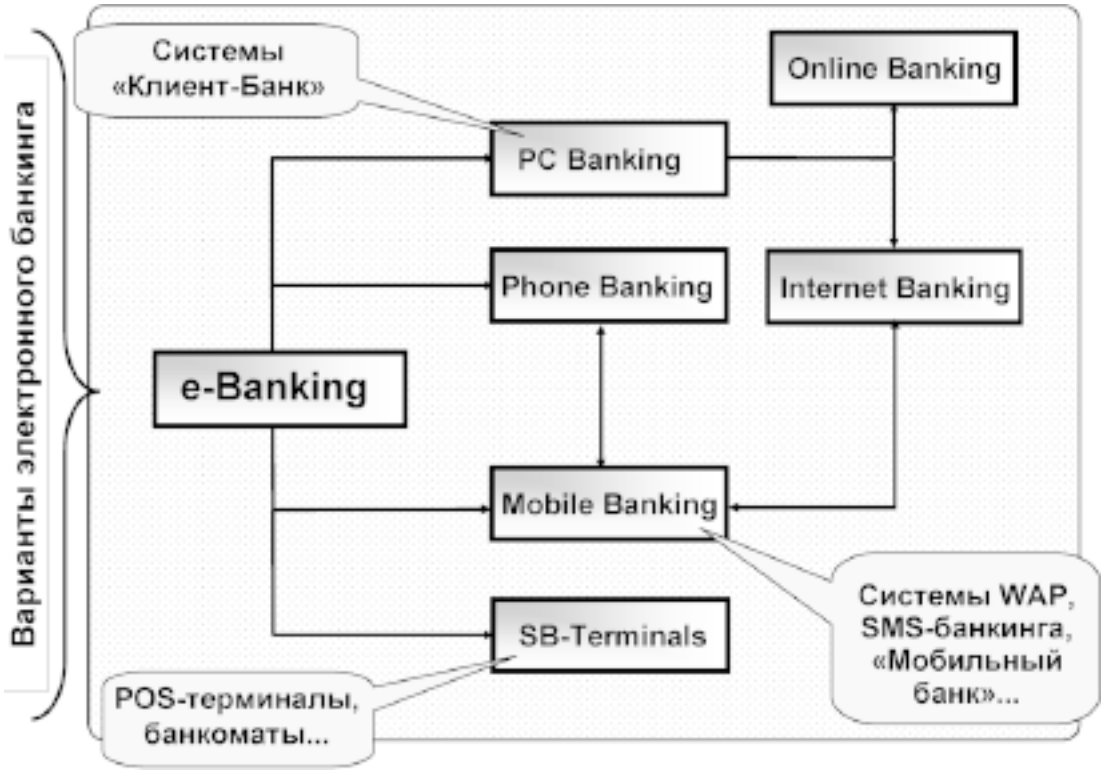

Рис. 1.1. Укрупненная классификация вариантов электронного банкинга

На этой схеме отсутствует деление отдельных «ветвей», учитывающее специфические детали, свойственные различным технологиям электронного банкинга, поскольку для последующего изложения это не принципиально, к тому же такие варианты ДБО, как использование, скажем, систем Wi-Fi, в отечественной банковской практике еще не стали распространенными. Кроме того, не имеет принципиального значения и конкретный вариант ДБО, выбираемый кредитной организацией: важно лишь то, что «если компания не следует тенденциям изменяющихся рыночных, финансовых и технологических условий, то она недолго останется в бизнесе»[11]. В современном банковском бизнесе кредитные организации, если они не хотят потерять конкурентные преимущества, по существу, «вынуждены» переходить к дистанционному предоставлению банковских услуг, а следовательно, «радикально перестраивать» организацию своей банковской деятельности. В этой ситуации принципиально важным становится то, что речь идет именно о *деятельности* кредитной организации в целом, а не только о выполнении «банковских операций» и «других сделок».

Необходимо отметить также, что *адекватного* понимания содержания электронного банкинга до настоящего времени тоже еще не сложилось. Об этом свидетельствуют многие документы, разработанные зарубежными органами банковского регулирования и надзора, в которых приводятся определения содержания этого явления и формируется рабочий понятийный аппарат. Если попробовать сформулировать своего рода «базовое» определение электронного банкинга по таким материалам[12], то оно будет выглядеть следующим обра-

[10] По материалам семинара по надзору в области электронного банкинга, проведенного «Дойчебундесбанком» для специалистов Банка России в 2002 г. Приведенная схема используется в надзорных целях до настоящего времени.

[11] *Coderre D.* Internal Audit. Efficiency through automation. John Wiley & Sons Inc., Hoboken, NJ, USA, 2009.

[12] См., например, Risk Management Principles for Electronic Banking. Basel Committee on Banking Supervision, Bank for International Settlements, Basel, July 2003; Internet-Banking. Comptroller's Handbook. I – IB. Office of the Comptroller of the

зом: «обеспечение возможностей для клиентов кредитных организаций получать удаленный доступ к своим банковским счетам через информационно-телекоммуникационные системы и, как минимум, осуществлять переводы финансовых средств между ними».

В этом определении можно увидеть своего рода «операционный» акцент, появление которого объясняется исторически сформировавшимся «примитивным» подходом к интерпретации содержания банковской деятельности и который существенно *сужает* подмножество факторов, обусловливающих возникновение новых источников компонентов банковских рисков, подлежащих учету и анализу в кредитной организации при переходе ее к ДБО. На самом деле при выборе той или иной ТЭБ руководству, исполнительным органам и специалистам кредитной организации всегда следовало бы анализировать особенности этой технологии с целью выявления и описания сопутствующих ей факторов риска, а также оценивать свои возможности в части управления конкретной ТЭБ и контроля ее использования с учетом специфики формируемого ею так называемого «информационного контура банковской деятельности» – нового явления в сфере банковской деятельности.

Функционирование современной кредитной организации отличается в первую очередь тем, что традиционный подход к анализу содержания банковской деятельности оказывается *принципиально* непригодным: он приводит к тому, что большое количество новых, нетипичных для традиционной банковской деятельности источников компонентов банковских рисков упускается из вида со всеми вытекающими отсюда негативными последствиями для кредитных организаций и их клиентов. Те и другие в такой ситуации оказываются незащищенными от новых угроз, которые вполне можно парировать при пруденциальной[13] организации этой деятельности в новых технологических условиях. Помимо этого, конкурентные условия могут способствовать и тому, что окажутся внедренными недостаточно надежные, проверенные и «отработанные» технологии электронного банкинга и реализующие их банковские автоматизированные системы из-за того, что сложность таких систем не согласуется с интервалом времени, выделяемым на их освоение и запуск в эксплуатацию. Что уж говорить о том, что дополнительной и непростой особенностью организации применения практически любой ТЭБ оказывается необходимость учета недостаточной квалификации клиентов кредитной организации в областях компьютерных и телекоммуникационных технологий.

В итоге руководству кредитной организации, принимая решение о переходе к ДБО, необходимо заранее определить круг потенциальных проблем, с которыми может быть связано такое обслуживание, и новых вопросов, которые придется решать в целях обеспечения и поддержания надежности банковской деятельности (в широком смысле имея в виду выполнение всей совокупности принимаемых на себя этой организацией обязательств как перед клиентами, так и перед теми или иными контролирующими органами). Поэтому целесообразно добиваться наиболее полного охвата предметной и одновременно проблемной области новых *способов* и *условий* осуществления банковской деятельности. Прежде всего логично достичь полного осознания *модификации* ролевой функции кредитной организации, внедряющей ТЭБ, предложив, к примеру, такое определение электронного банкинга: «совокупность всех организационно-технических мероприятий, реализуемых кредитной организацией с помощью технологий дистанционного банковского обслуживания для обслуживания своих клиентов (реальных и потенциальных) при выполнении этой организацией функций дистанционного финансового посредника».

Currency, Washington, DC, USA, October 1999; E-Banking. Federal Financial Institutions Examination Council, Washington, DC, USA, August 2003.

[13] Пруденциальный (англ. *prudential* от лат. *prudens)* – разумный, осторожный, отказывающийся от риска.

В этом случае речь не идет о создании исчерпывающего понятийного аппарата высокотехнологичной банковской деятельности, тем более что в наше время «технический прогресс» продолжает видоизменять банковскую деятельность. Просто необходимо подчеркнуть, что собственно появление «дистанционности» действительно *радикально* меняет характер банковской деятельности. До сих пор руководство многих кредитных организаций не осознает этих изменений, так что принятие мер по приведению организации внутрибанковских процессов и составляющих их процедур (вплоть до отдельных функций) в соответствие с новыми способами и условиями банковской деятельности, формируемыми такими технологиями, начинается только после того, как новые, нетипичные (и неосознававшиеся до последнего времени) угрозы ее надежности реализуются, а сами эти организации и их клиенты потеряют немалые денежные средства.

В то же время адекватный *превентивный* анализ состава компонентов типичных банковских рисков, действующих в условиях применения технологий и систем электронного банкинга, гарантировано позволяет избежать неприятностей такого рода за счет заблаговременного внесения изменений во внутрибанковские процессы и процедуры, с ориентацией их на выявление, учет (мониторинг, анализ) и парирование потенциальных угроз надежности банковской деятельности. Но для этого в высокотехнологичной кредитной организации неизбежно должны произойти изменения в содержании корпоративного управления, причем каждая процедура в составе этого процесса оказывается «привязана» к особенностям вновь образуемых *зон концентрации* источников компонентов банковских рисков и одновременно *зон ответственности* кредитной организации. Эти понятия также не являются новыми, однако в условиях применения технологий электронного банкинга они приобретают новую актуальность и содержательно заметно усложняются.

1.2. Информационный контур банковской деятельности и новые факторы банковских рисков

Внедрение технологий ДБО привело к образованию принципиально нового явления в банковской деятельности, которое можно определить понятием «информационный контур банковской деятельности» (ИКБД)[14]. В общем случае если бы о возникновении, специфике функционирования и особенностях проявления этого контура *заблаговременно* задумывались в каждой кредитной организации, переходящей к ДБО, то тематика анализа банковских рисков, сопутствующих внедрению новых технологий такого рода, быстро себя исчерпала бы. Как раз этого и не происходит прежде всего в силу новизны технологий как таковых и неразвитости законодательной базы банковской деятельности. Впрочем, если все, что связано в кредитной организации с ДБО, делать правильно, то ничего страшного или неприятного, связанного с новыми банковскими технологиями, для нее не происходит

Несколько упрощенная, но тем не менее достаточная для предварительного анализа схема ИКБД, предназначенная для обоснования концептуальных положений описываемого ниже подхода, приведена на рис. 1.2. На ней условно показаны две кредитные организации в «киберпространстве».

Прежде всего целесообразно обратить внимание на основные, своего рода «системные» факторы, обусловливающие возникновение новых источников компонентов банковских рисков, – таковых можно выделить как минимум три (о других, хотя и не новых, но также принципиально важных факторах риска, сопутствующих электронным банковским технологиям как таковым, будет сказано в следующей главе). Эти факторы в первую очередь логично учитывать при организации управления рисками.

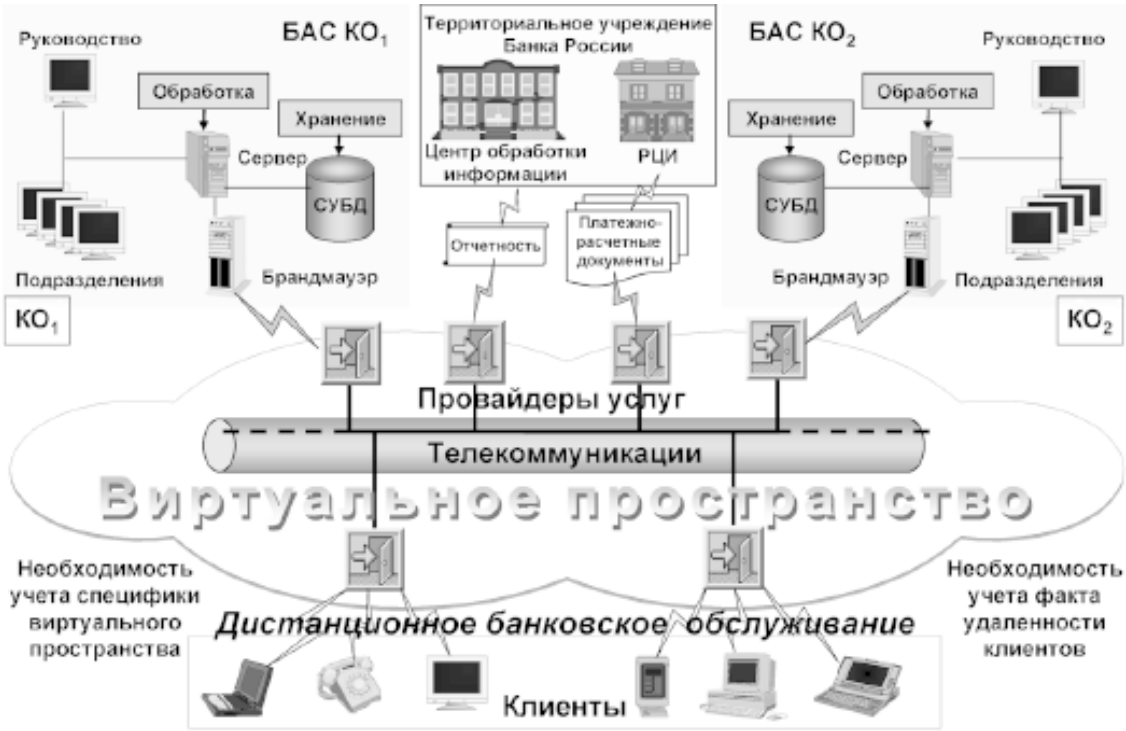

Рис. 1.2. Информационный контур банковской деятельности и новые факторы банковских рисков

[14] *Лямин Л.В.* Анализ факторов риска, связанных с интернет-банкингом // Расчеты и операционная работа в коммерческом банке. 2006. № 5. С. 52 – 63; № 6. С. 43 – 54; № 7 – 8, С. 37-54.

Первый фактор заключается в возникновении для кредитной организации клиентов *нового* типа, которые зачастую фактически сами играют роли операционистов или близкие к ним. Очевидно, что вместе с переходом кредитной организации к ДБО, т.е. к такому варианту предоставления банковских услуг, когда в течение сеанса информационного взаимодействия клиент ей «не виден» и работает с ней «из-за горизонта», эта организация теряет своего рода «линию обороны» от клиента. Если в условиях традиционной организации банковской деятельности клиент должен взаимодействовать с операционным сотрудником, который не позволяет ему совершать ошибки при оформлении своих операций, создавать инциденты информационной безопасности, осуществлять противоправную деятельность и т.п., то в новых условиях предоставления банковских услуг клиенту ничто не может помешать этим заниматься. Столь же очевидно, что чем бо$льшую свободу действий кредитная организация предоставит клиенту в рамках ДБО и чем менее жесткие условия обслуживания для него создаст, тем больше проблем такой клиент создаст самой кредитной организации, существенно усложнив для нее сначала создание доказательной базы электронного банкинга, а затем и претензионную работу, и разбор конфликтных ситуаций. Поэтому в содержании договоров с клиентами относительно ДБО (или дополнительных соглашений к договорам банковского счета) кредитной организации необходимо учитывать те особенности удаленного взаимодействия, которые при неблагоприятном стечении обстоятельств *могут* негативно сказаться на выполнении ею принимаемых на себя обязательств, но не по ее вине, а по вине клиента (который, кстати, далеко не всегда это осознает).

Справедливости ради надо отметить, что и сами клиенты, взаимодействующие с кредитными организациями с помощью различных систем электронного банкинга, также не защищены от воздействия рассматриваемого фактора риска – на этом эффекте основан целый ряд мошеннических технологий, упомянутых в начале этой главы, и вариантов их реализации. Результативность атак такого рода в последнее время привела к тому, что Банком России была начата разработка специальных тематических рекомендаций для кредитных организаций, которые ориентируют их на обеспечение *дополнительной* защиты интересов клиентов[15]. Имеется в виду, что в условиях применения этими организациями так называемых «высоких технологий» целесообразно вместе с внедрением той или иной ТЭБ формировать *специальные* процедуры, ориентированные на защиту интересов клиентов ДБО и учитывающие особенности конкретной технологии и реализующей ее СЭБ (прежде всего в плане отличия от уже освоенных банковских информационных технологий). Такие процедуры разрабатываются исходя из полного понимания высшим менеджментом кредитной организации специфики ТЭБ и соответствующих средств, применяемых для обеспечения ДБО, и архитектуры ее банковских автоматизированных систем.

Эти соображения становятся основанием для пересмотра формирования политики установления взаимоотношений кредитных организаций с клиентами по предоставлению им вариантов ДБО. При этом затрагивается достаточно много аспектов, начиная с содержания договоров на конкретный вид обслуживания и заканчивая пересмотром подходов к осуществлению финансового мониторинга (ФМ), имея в виду в первую очередь мероприятия, необходимые для парирования эффектов взаимной анонимности. В частности, в содержании договоров на ДБО становится необходимо предусматривать специальные соглашения и условия относительно использования средств так называемых аналогов собственноручной подписи, применение которых допускается Гражданским кодексом Российской Федерации

[15] Письма Банка России от 7 декабря 2007 г. № 197-Т «О рисках при дистанционном банковском обслуживании»; от 30 января 2009 г. № 11-Т «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга» и др.

(ГК РФ)[16], систем ДБО или, как иногда говорят иначе, – «электронного документооборота» и обеспечения юридической силы электронных документов, расследования спорных (конфликтных) ситуаций, включая создание тех или иных согласительных и технических комиссий, и т.п.

Что касается процесса ФМ, то Банк России со своей стороны уже неоднократно обращал внимание кредитных организаций на наличие таких эффектов и необходимость принятия *специальных* мер по учету их в процедурах, составляющих внутрибанковский процесс[17]. Сложность ситуации с разработкой документов такого рода обусловлена в первую очередь тем, что каждая кредитная организация, внедряющая какую-либо ТЭБ, даже если эта технология хорошо известна и апробирована в банковском секторе, уникальна в смысле архитектуры своих распределенных компьютерных систем, локальных или зональных вычислительных сетей (охватывающих ее филиалы или дополнительные офисы), квалификации персонала, состава провайдеров и т.д. Поэтому формирование детальных рекомендаций по организации и содержанию процесса ФМ в условиях ДБО (как, впрочем, и многих других внутрибанковских процессов) просто невозможно, а поэтому кредитные организации по существу оказываются вынуждены самостоятельно приспосабливать этот процесс (равно как и составляющие его процедуры) к своим информационным технологиям, специфическим (зачастую уникальным) архитектурам сетевых структур и каждого ИКБД в целом, особенностям построения их банковских автоматизированных систем и т.п., на что целесообразно обращать внимание их руководству.

Вместе с тем осознание необходимости пересмотра организации и содержания процесса ФМ становится в последние годы все более актуальным в связи с теми возможностями, которые высокие технологии, включая технологии электронного банкинга, могут предоставлять для разного рода противоправной деятельности: легализации доходов, полученных преступным путем (так называемого «отмывания денег»), финансирования терроризма, хищений денежных средств, мошенничеств и т.п. При этом необходимо иметь в виду, что незаметное вовлечение кредитной организации в противоправную деятельность может привести к лишению ее лицензии на выполнение банковских операций и судебному преследованию в соответствии с законом. Поэтому руководству кредитной организации целесообразно четко осознавать возможные направления смещения уровней банковских рисков в условиях ДБО, поскольку в случае реализации компонентов правового риска такого рода оценки принимаемого ею кредитного, рыночного и других рисков теряют значение. Очевидно, что любая кредитная организация, дистанционно предоставляющая банковские услуги, может оказаться заподозренной в участии в ускользнувшей от внимания ее сотрудников противоправной деятельности лишь из-за того, что ее высший менеджмент неадекватно представляет себе профиль риска, сопутствующий использованию новых банковских информационных технологий. Это в свою очередь вызывается тем, что условия для осуществления ДБО, которые само руководство и должно подготовить, оказываются неподходящими, почему

[16] Статья 160 ГК РФ.

[17] См., например, такие документы, как Положение Банка России от 19 августа 2004 г. № 262-П «Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»; письма Банка России от 13 июля 2005 г. № 99-Т «О Методических рекомендациях по разработке кредитными организациями правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»; от 30 августа 2006 г. № 115-Т «Об исполнении Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем…» в части идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)»; от 5 апреля 2007 г. № 44-Т «О проверке осуществления кредитными организациями идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)»; от 27 апреля 2007 г. № 60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)».

важно помнить о необходимости создания специальных условий пруденциальной банковской деятельности в условиях ДБО, а специфика эта определяется применяемыми технологиями.

В то же время для клиента, пользующегося СЭБ для получения банковских услуг, особенно операционного характера, принципиально значимым системным фактором риска становится то, что в условиях ДБО он не имеет возможности *непосредственного* контроля над получением и выполнением кредитной организацией ордеров, отправляемых им через ИКБД[18]. Эта ситуация радикально отличается от непосредственного «физического» взаимодействия клиента с операционистом или кассовым работником кредитной организации – первым для него служит интерфейс с СЭБ или в более общем смысле системой типа «Банк – Клиент», вторым, в случае получения наличных денег, – банкомат, в случае платежа – POS-терминал или его аналог. При этом необходимо подчеркнуть, что никаких теоретических разработок относительно клиентских рисков до настоящего времени не существует, мало того, во всех публикациях по рассматриваемой тематике речь практически всегда идет только о рисках банковской деятельности, хотя сами эти риски зачастую непосредственно зависят от условий, в которые кредитная организация ставит клиента ДБО. Как будет показано ниже, условия эти должны быть максимально жесткими в смысле ограничения количества «степеней свободы», которыми может воспользоваться клиент ДБО во время сеанса связи.

По существу во время сеанса ДБО клиент полностью зависим от кредитной организации (функционирования ее автоматизированных систем) и от провайдеров, которые выполняют свои функции в ИКБД между ним и кредитной организацией. К сожалению, общая «культура» банковской деятельности в российском банковском секторе до последнего времени такова, что клиент ДБО в соответствии с договором, заключаемым им с кредитной организацией, и в силу недостаточной технической квалификации и отсутствия юридической подготовки не обладает почти никакими правами, тогда как обязанностей на него налагается немало (при этом многие клиенты вообще не читают тексты договоров на ДБО). В оптимальном варианте организации договорных отношений такого рода кредитным организациям следовало бы *детально* знакомить своих клиентов, использующих такое обслуживание, с угрозами, которым «подвергаются» их интересы во время сеансов информационного взаимодействия с ней, причем не «по доброте душевной», а имея в виду снижение для самой себя уровней потенциально возникающих компонентов банковских рисков, о чем уже говорилось, но это, по-видимому, дело будущего (если обратиться к материалам судебных исков последних лет).

Второй фактор системного характера состоит в том, что в процесс современной банковской деятельности в условиях ДБО оказываются вовлечены третьи стороны, которые ранее к ней отношения преимущественно не имели. К их числу относятся провайдеры кредитных организаций, обеспечивающие формирование и поддерживающие функционирование ИКБД в каждом отдельном случае. Конкретные виды, состав и функции провайдеров кредитной организации определяются тем, какая именно ТЭБ и в каких целях внедряется ею, какая СЭБ реализует эту технологию, а также какие среды передачи данных и каналы (линии) связи при этом задействуются (включая интернет-провайдеров, операторов мобильной связи, платежные системы и т.п.). Очевидно, что если в процессе удаленного информационного взаимодействия сеанс ДБО окажется прерван или подвергнется другому негативному воздействию не по причинам, возникшим в кредитной организации, а из-за проблем, имевших место на территории провайдера, то клиент этой организации, интересы которого

[18] Понятие «ордер клиента» введено и определено в Письме Банка России от 31 марта 2008 г. № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга».

пострадали вследствие такого прерывания, обратится с претензиями именно к ней, а не к неведомому ему провайдеру, тем более что в общем случае и сам клиент может находиться в произвольном месте земного шара, где доступно использование какого-либо средства компьютерной связи. Дальнейшие последствия для кредитной организации будут зависеть от того, какой конкретно ущерб был нанесен интересам клиента ДБО, особенно в тех ситуациях, когда речь идет о невыполнении им своих финансовых обязательств перед другими сторонами.

От содержания и организации аутсорсинга такого рода[19] прямо зависят и те варианты *зависимости* надежности банковской деятельности кредитной организации от провайдеров, в которые неизбежно попадает эта организация вместе со своими клиентами ДБО. Вариантов здесь достаточно много – начиная с обеспечения физической связи со средой информационного взаимодействия и заканчивая обеспечением резервных маршрутов (или каналов) такого взаимодействия при возникновении аварийных ситуаций. Эта множественность вынуждает руководство и специалистов кредитной организации внимательно относиться к содержанию контрактов на аутсорсинг, тщательно анализировать варианты распределения обязанностей и ответственности за уровень обслуживания, возникающие в виртуальном пространстве, включая уровень *банковского* обслуживания (что, как правило, в таких контрактах просто не учитывается). Независимо от выбранной ТЭБ и состава поддерживающих ее использование провайдеров руководству кредитной организации целесообразно предусмотреть однозначные семантические связи между содержанием контрактов на аутсорсинг и договоров с клиентами на ДБО в части обязанностей и ответственности сторон.

Это может оказаться не такой простой задачей, как нередко считается в отечественных кредитных организациях, причем сложность ее обратно пропорциональна качеству решений, принимаемых в части совершенствования управления банковскими рисками в условиях ДБО. Ничего *принципиально* невозможного в учете источников компонентов банковских рисков, вновь возникающих из-за действия рассматриваемого фактора риска, нет – проблема заключается в полноте анализа состава ИКБД и ролевых функций составляющих его элементов (что требует понимания сути ТЭБ). Однако ситуация существенно осложняется тем, что результаты «выяснения» правовых отношений, возникающих между агентами удаленного информационного взаимодействия, почти полностью зависят от высоких технологий, а специалисты в сфере таких технологий и в области правового обеспечения банковской деятельности до сих пор говорят, как известно, «на разных языках».

Третий фактор связан с возникающей в условиях открытых систем и универсальных протоколов сетевого взаимодействия потенциальной доступностью банковских автоматизированных систем и других информационно-процессинговых ресурсов кредитных организаций, а также устройств, используемых их клиентами при ДБО, для несанкционированного доступа и сетевых атак. Угрозы такого рода появились вместе с возникновением банковских автоматизированных систем. Постоянной остается проблема возможных злонамеренных действий со стороны инсайдеров кредитной организации (в широком смысле). Технологии электронного банкинга наряду с выгодами для кредитных организаций и удобствами для их клиентов существенно *расширили* спектр потенциальных угроз, которые могут быть реализованы извне этих организаций и при этом настолько «дистанционно», что локализовать источник этих угроз оказывается очень непросто (в том числе ввиду слабой регламентации функционирования провайдеров кредитных организаций и контроля над ними). Вследствие

[19] В этой книге понятие аутсорсинга интерпретируется в наиболее широком смысле, а не в традиционном понимании, как передача кредитной организацией сторонней организации выполнения каких-либо функций, которые она могла бы выполнять сама, но ей самой невыгодно это делать по соображениям, например, финансового плана. Тем самым, по мнению автора, обеспечивается наиболее полный охват вариантов зависимости банковской деятельности от сторонних организаций, которые подлежат учету в управлении рисками банковской деятельности.

появления ДБО БАС кредитной организации перестает быть «вещью в себе» и при наличии недостатков в сетевой защите и «дыр» в периметре безопасности кредитной организации оказывается доступна для вирусных, хакерских, крэкерских и прочих атак, «достижение целей» которых означает реализацию всех банковских рисков, связанных с этим вариантом банковской деятельности.

Широкое распространение интернет-технологий наряду с интенсивным использованием для банковской деятельности сети Интернет и предоставляемых в связи с этим сетевых ресурсов породило новое направление исследований, относящееся к компонентам банковских рисков, возникающими из-за так называемых web-отношений[20]. Их анализу будет посвящен специальный раздел настоящей книги. Эти отношения возникают при внедрении кредитной организацией такого варианта ДБО, как интернет-банкинг, и требуют в общем случае существенного дополнения процесса управления банковскими рисками новыми процедурами (которые при развитии этой ТЭБ практически составляют новый внутрибанковский процесс, в котором целесообразно согласованное участие нескольких структурных подразделений кредитной организации).

Из дальнейшего изложения можно будет выделить еще несколько менее существенных факторов возникновения источников рисков, образующих соответствующие подмножества для каждого из рассматриваемых типичных банковских рисков, однако все три перечисленных основных фактора системного плана как минимум не должны ускользать от внимания руководства кредитной организации, переходящей к ДБО. Такое понимание *значимости* кратко рассмотренных выше факторов в современных условиях может стать одной из наиболее важных характеристик качества корпоративного управления в высокотехнологичной кредитной организации. Необходимо отметить, что при этом изменения происходят не только в технологическом и техническом обеспечении банковской деятельности, они в оптимальном варианте должны были бы происходить и в ряде основных бизнес-процессов кредитных организаций (или в *подлежащих* реализации). В книге рассматриваются возможные подходы к *оптимизации* способов и условий банковской деятельности при внедрении и применении кредитными организациями новых технологий электронного банкинга, их совершенствовании и комплексном развитии.

Следует специально подчеркнуть, что все процессы информационного взаимодействия в киберпространстве принципиально характеризуются анонимностью агентов этого взаимодействия и установить, кто именно в конкретный момент времени «держал палец на кнопке», с полной уверенностью невозможно. В каждом случае передачи и обработки данных, которые так или иначе связаны с какими-либо активами кредитной организации (являясь либо собственно записями о них или командами на изменения их значений), любой такой процесс существует *только* в отдельные кванты времени в электронных устройствах или каналах связи. По завершении такого управляющего процесса от него может не оставаться никаких следов, кроме изменения значений полей в записях баз данных, почему и становятся принципиально важными файлы так называемых «компьютерных журналов», фиксирующих события, происходящие в банковских автоматизированных системах (в зависимости от назначения и содержащихся в них данных их часто называют «системными логами» и «аудиторскими трейлами»). Это в свою очередь означает, что *традиционные* процессы управления банковской деятельностью и контроля над ней в высокотехнологичных кредитных организациях заведомо не могут считаться эффективными – эти процессы целесообразно *адаптировать* к применяемым банковским информационным технологиям и системам на основе

[20] WEBLINKING: Identifying Risks and Risk Management Techniques. Interagency Guidance. Federal Deposit Insurance Corporation, National Credit Union Administration, Office of Thrift Supervision, Office of the Comptroller of the Currency, Washington, DC, April 23, 2003.

риск-ориентированного анализа, который тоже следует адаптировать к специфике таких технологий.

Указанный анализ также целесообразно строить на изучении состава и структуры ИКБД, образуемого ТЭБ, внедряемой кредитной организацией. Даже если такая организация использует две-три однородные системы разного целевого назначения (по функциям, группам клиентуры и т.п.), схожесть процессов информационного взаимодействия в них не должна вводить в заблуждение. В этом случае лучше потратить дополнительное время и силы на аналогичный анализ, но с уверенностью избежать неожиданного негативного проявления какого-либо изначально незамеченного «мелкого» источника риска. Такой подход требует, естественно, подготовки соответствующих руководящих решений и распорядительных документов, что целесообразно предусмотреть заранее, до *практического* начала ДБО клиентов[21], особенно физических лиц, поскольку, как показывает практика, принципиальное отсутствие корпоративной культуры создает почву для возникновения новых инцидентов информационной безопасности и неправильного использования компьютерных и телекоммуникационных технологий.

Предваряя последующее изложение, можно сделать еще несколько замечаний. Прежде всего любой вновь внедряемой технологии предоставления банковских услуг и осуществления банковской деятельности в целом сопутствует увеличение числа внутрибанковских процессов или хотя бы процедур, составляющих такие процессы. Если этого не происходит, то, как свидетельствует практика, негативные события в жизни кредитной организации и ее клиентов неизбежны из-за непредвиденных ситуаций, которые вполне можно было бы прогнозировать и зачастую просто исключить их возникновение.

Далее приходится также пересматривать уже существующие в кредитной организации процессы с точки зрения их адаптации к новым способам и условиям банковской деятельности в рамках ДБО. Как говорится в уже цитировавшемся источнике, «мы слишком часто обнаруживаем себя ограниченными ментальными барьерами, создаваемыми нами самими. Методы, хорошо работавшие в прошлом, внедрились в наше мышление… если полагаться только на прошлый опыт, то следствием будут попытки применить привычные решения к непривычным проблемам либо не будут найдены новые эффективные подходы к старым проблемам»[22]. Стереотипы руководящего мышления в новых условиях банковской деятельности, формируемых применением технологий электронного банкинга, могут оказаться серьезным дополнительным источником для компонентов *всех* типов банковских рисков просто потому, что содержание таких технологий сложно для понимания, а из-за этого в свою очередь руководством кредитных организаций не модернизируются своевременно внутрибанковские процессы управления и контроля, в первую очередь процесс управления банковскими рисками. Для этого процесса ресурсная база, существовавшая в кредитной организации до внедрения ТЭБ, оказывается заведомо недостаточной (также в первую очередь), однако это не замечается или замечается слишком поздно для парирования уже реализовавшихся банковских рисков.

Еще одним принципиальным аспектом внутрибанковского управления и контроля в условиях лавинной компьютеризации банковской деятельности становится увеличение опасности возникновения разрывов в этих процессах, особенно если кредитная организация использует разные варианты ДБО, каждому из которых сопутствуют уникальные подмножества источников риска. Поэтому изменения в содержании внутрибанковских процессов и входящих в их состав процедур целесообразно синхронизировать с *каждым* решением о развитии банковской деятельности в рамках ДБО и каждым фактом внедрения новой тех-

---

[21] Internet-Banking. Comptroller's Handbook. I – IB.

[22] *Coderre D.* Internal Audit. Efficiency through automation.

нологии электронного банкинга. Этому вопросу будет уделено особое внимание, поскольку речь пойдет о подходе к согласованной модернизации тех внутрибанковских процессов, от которых непосредственно зависит надежность такой банковской деятельности. Говорить об этом нужно потому, что качество корпоративного управления определяется в современных кредитных организациях и новых условиях ДБО тем, насколько *реально* управляемыми и контролируемыми являются банковские автоматизированные системы.

Наконец, в ходе дальнейшего развития ДБО, без чего конкурентоспособным кредитным организациям, по-видимому, не обойтись, придется вносить существенные адаптационные изменения в свои бизнес-модели. Такие изменения обычно затрагивают стратегическое планирование и работу многих структурных подразделений кредитной организации, распространяясь по ее иерархии после внедрения первой же ТЭБ и соответствующей СЭБ. В дальнейшем этот процесс неизбежно станет повторяющимся при каждом следующем «витке» спирали технического прогресса в отечественном банковском секторе. Поэтому руководителям высокотехнологичных кредитных организаций логично привыкать к «новому мышлению» в связи с применением ДБО, которое будет служить оптимизации корпоративного управления, сохранению надежности и устойчивости этих организаций, равно как и выполнению ими обязательств перед своими клиентами и контролирующими органами.

Глава 2
Типичные банковские риски, ассоциируемые с применением технологий электронного банкинга

Не то важно, может что-либо произойти или не может, – все может произойти. Важно значение происходящего.
Суфийская мудрость

Проблематика банковских рисков привлекает внимание органов банковского регулирования и надзора разных стран уже довольно давно, и попытки их подробного описания и анализа имели место задолго до начала эры ДБО. Значимость потенциальных угроз надежности банковской деятельности в целом осознавалась в банковском сообществе, что выражалось, к примеру, даже в таких оригинальных формулировках, как «банковское дело – это принятие на себя риска с получением компенсации за него»[23], однако, как это ни парадоксально, до настоящего времени в публикациях, посвященных банковскому делу и сопутствующим рискам, отсутствует *единый* теоретический подход к определению, интерпретации и практическому применению даже базовых понятий, связанных с этой теорией. Внедрение в банковскую деятельность технологий и систем ДБО усугубило ситуацию в том плане, что на этой волне стали возникать как бы все новые и новые виды банковских рисков, из-за чего и без того не законченная методология, охватывающая выявление, оценивание, анализ, мониторинг банковских рисков и управление ими, стала размываться, затрудняя ее практическое использование.

Оборот «как бы» употреблен здесь не случайно. Несмотря на то что теоретические разработки в области рисков банковской деятельности ведутся уже более 20 лет (первые публикации систематического характера относительно отдельных компонентов таких рисков относятся еще ко второй половине 80-х гг. прошлого века), законченной или даже сколько-нибудь полной «теории» этих рисков до настоящего времени не создано – проработаны только отдельные направления. В основном такие разработки были посвящены кредитному, процентному, ценовому, валютному рискам или совокупности последних, определяемых как рыночный риск, а также риску ликвидности. Мало того, практически каждый из зарубежных органов банковского регулирования и надзора[24] до последнего времени формировал свою собственную теорию, причем общее число банковских рисков варьировалось от полутора десятков до одного (операционного, поглощавшего все остальные). Одна из таких теоретических разработок Базельского комитета по банковскому надзору (БКБН) нашла отражение в упомянутом ранее Указании оперативного характера Банка России от 23 июня 2004 г. № 70-Т «О типичных банковских рисках». В этом материале фигурируют следующие 11 банковских рисков: кредитный, страновой, рыночный, фондовый, валютный, процентный, ликвидности, операционный, правовой, потери деловой репутации и стратегический. Между тем, с течением времени и развитием банковских информационных технологий этим дело не ограничилось, поскольку возникли новые компоненты банковских рисков, уже технологического характера, которые стали вносить существенные коррективы в теоретические подходы к анализу рискованности банковской деятельности.

---

[23] Guiding Principles in Risk Management for U.S. Commercial Banks. The Financial Services Roundtable, A Report of the Subcommittee and Working Group on Risk Management Principles; Washington, DC, USA, June 1999.

[24] Автор располагает материалами таких учреждений только из США, Канады, Западной Европы и Великобритании, а также Сингапура и Южной Кореи, однако это не умаляет общности рассмотрения.

Вследствие этого в последних по времени выпуска материалах БКБН, посвященных основным принципам управления рисками в условиях применения электронного банкинга[25], стали фигурировать еще и такие риски, как:

– деловой;
– безопасности;
– хищений идентификационных данных;
– мошеннических действий со счетами;
– отмывания денег;
– обезличивания индивидуальности;
– отрицания транзакций,

несмотря на то что в этой же работе отмечалось «отсутствие возникновения принципиально новых рисков» и что «деятельность в области электронного банкинга не приводит к возникновению рисков, которые не были бы уже идентифицированы в предыдущих работах Базельского Комитета». Вместе с тем было также указано, что фундаментальные характеристики ДБО и факторы, которые ассоциируются «с видами обслуживания в рамках электронного банкинга… увеличивают и модифицируют некоторые из традиционных рисков, связанных с банковской деятельностью, в особенности стратегический, операционный, правовой и репутационный риски, тем самым влияя на общий профиль риска в банковском деле». Мало того, в некоторых других материалах БКБН говорится еще и о так называемых рисках, «характеризующих электронную обработку данных в банках», а именно:

– риск непредусмотренного раскрытия информации;
– риск ошибок;
– риск мошенничества;
– риск прерывания операций;
– риск неэффективного планирования;
– риски, связанные с действиями клиентов.

В более ранних документах БКБН, посвященных типичным банковским рискам и считавшихся основополагающими в этой области, перечисленные выше разновидности рисков не упоминались и не рассматривались. Также в этих документах отсутствуют указания на совокупности «новых» банковских рисков как на *компоненты* типичных банковских рисков, а это, с точки зрения автора, неточность, имеющая *принципиальный* характер. Очевидно, что нагромождение дополнительных разновидностей банковских рисков может привести только к размыванию границ методологии, которую вряд ли когда-нибудь можно будет считать законченной.

Не лучше, чем в этом общеевропейском методическом органе банковского регулирования и надзора, обстоят дела с теоретическими исследованиями в области банковских рисков в условиях электронного банкинга и в отдельных странах. Чтобы не перегружать изложение, уместно ограничиться только двумя примерами попыток преодоления ограничений, свойственных традиционному подходу к описанию банковских рисков при переходе к анализу их специфики, обусловленной эффектами виртуального пространства, в котором осуществляется современная банковская деятельность.

В частности, Банк Нидерландов в рассматриваемом отношении выделяет следующие «нетрадиционные» риски[26]:

– риск управляемости (обусловленный недостаточной гибкостью и обеспечением банковских информационных технологий);

---

[25] Например, Risk Management Principles for Electronic Banking.

[26] Цитируются материалы семинара, проводившегося для специалистов Банка России в 2004 г.

– риск эксклюзивности (обусловленный недостаточной защитой против несанкционированного доступа к банковским автоматизированным системам и отдельным средствам в их составе);

– риск целостности (обусловленный неточностью, неполнотой банковской информации или несвоевременностью ее поступления);

– риск контролируемости (обусловленный недостаточными функциональными характеристиками средств контроля);

– риск непрерывности (обусловленный возможной недостаточной доступностью для работы самих информационных технологий);

– риск пользователя (обусловленный возможным неправильным использованием информационных технологий).

Легко заметить некорректность приведенных формулировок, которые семантически должны были бы строиться совершенно иначе, учитывая, что при рассмотрении рисков речь всегда идет о возможности наступления событий, характеризуемых неким *негативным* влиянием на результаты той или иной деятельности. Эти же формулировки должны были бы строиться, например, таким образом:

– риск неуправляемости (или потери управляемости);

– риск потери конфиденциальности (или несанкционированного доступа);

– риск нарушения целостности (или искажения данных);

– риск неконтролируемости (или потери контроля);

– риск недоступности (или прерывания функционирования) и т.п.

Важно подчеркнуть, что подобные отмеченные семантические смещения во внутрибанковских документах, относящихся к организации и содержанию управления банковскими рисками, и проистекающие из общепринятого подхода, выражаемого словами «все все понимают», *недопустимы,* так как «затуманивают» существо негативного явления. Следствием этого, как правило, становятся просчеты в содержании составляющих данный процесс процедур, а также пробелы в их понимании, организации и выполнении.

Наконец, в материалах одного из основных органов банковского регулирования и надзора США и старейшего из них, созданного еще в середине XIX в. – Управления контролера денежного обращения[27], – такие банковские риски определяются как «ключевые риски, связанные с электронными банковскими операциями», а именно это:

– риски, связанные с зависимостью от поставщиков и провайдеров;

– риски, связанные с обеспечением безопасности, целостности и конфиденциальности банковских данных;

– риски, связанные с авторизацией, аутентификацией и подтверждением достоверности и прав пользователя;

– риски, связанные со стратегией ведения бизнеса и деловыми операциями;

– риски, связанные с планированием непрерывности деловых операций;

– риски, связанные с допустимостью проведения тех или иных операций и правовыми вопросами;

– риски, связанные с компьютерными преступлениями и отмыванием денег.

При этом в более ранних и также считающихся базовыми материалах ОСС, посвященных организации банковского регулирования и надзора на основе рисков[28], перечисляются 9 банковских рисков (совпадающих с формулировками БКБН за исключением странового

[27] *Office of the Comptroller of the Currency* – ОСС, в составе которого служба банковского инспектирования была создана еще в 1863 г., а в 1874 г. – банковский надзор, этой истории посвящена книга *Robertson R.M.* The Comptroller and Bank Supervision. OCC, Washington, DC, USA, 1995.

[28] В терминологии документов ОСС.

и фондового)[29], к которым только что перечисленные риски *как будто* никакого отношения не имеют.

Очевидны как сходство, так и различия в интерпретации аналогичных угроз надежности банковской деятельности, осуществляемой с использованием кредитными организациями новых компьютерных информационных технологий. Кстати, можно заметить, что при анализе рисков электронного банкинга зарубежные специалисты исключают из ИКБД собственно банковские автоматизированные системы (причем это свойственно специалистам и США, и некоторых стран Западной Европы)[30]. В трактовке систем электронного банкинга как виртуальных «ворот», открывающих доступ к информационно-процессинговым ресурсам кредитной организации, такой подход представляется в значительной мере упрощенным, поскольку все подверженные влиянию источников риска ресурсы такого рода сконцентрированы в так называемом «бэк-офисе» кредитной организации. Вследствие этого и анализ содержания компонентов банковских рисков логично осуществлять на всем протяжении ИКБД, который замыкается в хранилище банковских и клиентских данных, используемых для операционной и информационной деятельности кредитной организации, включающей также предоставление информации ее клиентам по счетам и операциям, равно как и подготовку регламентной банковской отчетности для контролирующих органов.

В российской литературе, посвященной рискам банковской деятельности, также часто встречаются «новые» банковские риски, упоминаемые в связи с разными сторонами информатизации этой деятельности. Наиболее «популярными» из них стали «информационные», «технологические», «технические» риски (или их комбинации) и некоторые другие. Дело не в новых названиях как таковых, а в том, что предметная область банковских рисков как бы становится шире вместе с каждой новой банковской информационной технологией, а значит, размывается и становится безграничной и соответствующая методология (как область знаний); вместе с тем она постоянно устаревает, вследствие чего использовать ее на практике почти невозможно. На самом деле новые технологические и технические решения сами собой не приводят к возникновению *новых* видов банковских рисков, которые необходимо учитывать в процессе управления ими (кстати, традиционно считается, что в него входят также процедуры выявления, анализа, мониторинга и оценки уровней этих рисков) и в «изобретении» этих видов рисков необходимости нет. Противоречия, подобные приведенному, свидетельствуют, по мнению автора, о неперспективности такого «экстенсивного» подхода к описанию и анализу банковских рисков. Понимая, что увеличение «множественности видов» банковских рисков препятствует поддержанию целостности и обеспечению преемственности методологии анализа банковских рисков с течением времени и технического прогресса, логичнее было бы более детально изучать и анализировать их структуру. Следовательно, имея в виду возможное развитие их с течением времени, все перечисленные выше новые риски целесообразно интерпретировать как *компоненты* типичных банковских рисков, уделяя им внимание при внедрении каждой новой ТЭБ.

С одной стороны, наличие некоторого хаоса в рассматриваемой области неудивительно, поскольку осознание рассматриваемых рисков оказалось непосредственно и почти исключительно связано с долгим эмпирическим путем развития и освоения банковского дела как такового. С другой стороны, быстрое внедрение и распространение банковских информационных технологий привело к таким системным изменениям в банковской сфере, которые создали условия для неожиданных и крупных трансформаций профилей рисков, обусловленных *варьирующимися* факторами риска как для отдельных кредитных органи-

---

[29] Large Bank Supervision. Comptroller's Handbook. EP-LB. Office of the Comptroller of the Currency, Washington, DC, USA, May 2001.

[30] По информации, полученной автором на ряде международных семинаров по вопросам обеспечения надежности банковской деятельности, проводившихся под эгидой органов банковского регулирования и надзора.

заций, независимо от их размеров, так и для финансовых систем в разных странах (в силу эффекта лавинного распространения рисков). Поэтому понятие риска как вероятности каких-либо потерь (включая упущенную выгоду) повсеместно становится предметом изучения и с эвристических, и с математических позиций[31], а для высокотехнологичных кредитных организаций отсутствие единой теории банковских рисков создает дополнительные проблемы с учетом их специфических компонентов, вносимых ДБО, в процессе управления банковскими рисками (УБР).

Анализ причин возникновения технологических и технических компонентов типичных банковских рисков приводит к выводу, что основным фактором для этого (опять-таки системного характера) является превращение банковской деятельности в своего рода «информационную дисциплину», которая в современном мире естественным образом оказалась «замкнута» на компьютерные технологии и вычислительные сети. Это означает, что все угрозы надежности банковской деятельности, порождающие источники указанных компонентов, можно свести в два небольших перечня:

1) данные (банковские и клиентские), передаваемые, обрабатываемые и хранимые в ИКБД, могут быть:

– похищены,

– изменены,

– уничтожены,

2) операции, совершаемые с этими данными, могут быть:

– имитированы,

– искажены,

– блокированы.

Поэтому становится необходимым постоянное обеспечение кредитной организацией авторизации, верификации и контроля получаемых, передаваемых и обрабатываемых финансовых и других (банковских, клиентских) данных, равно как и операций, осуществляемых с этими данными. Для этого в условиях применения электронного банкинга требуются дополнительные специальные процедуры, необходимости в которых при традиционной банковской деятельности не было в силу отсутствия такого явления, как ИКБД.

Эта проблематика до сих пор не считалась значимой и актуальной, по-видимому, из-за того, что автоматизация деятельности кредитных организаций, включая ДБО, не воспринималась как системный *феномен,* влияющий на эффективность и качество данной деятельности и превративший эти организации в аппаратно-программные комплексы информационных систем, состоящие из двух основных частей: БАС (в широком смысле) и хранилища банковских данных. Одновременно изменился и характер целого ряда типичных банковских рисков, в которых все более значимую роль стали играть их компоненты технологического и технического характера. Отсутствие такого восприятия объясняется, вероятно, несоответствием традиционного, устоявшегося понимания содержания банковской деятельности ее радикально изменившемуся характеру, обусловленному возникновению новых вариантов ДБО. Из-за этого в кредитных организациях возникли многочисленные недостатки в осуществлении УБР, негативное влияние которых на характеристики банковской деятельности и интересы клиентов этих организаций усугубляются опережающими темпами внедрения новых банковских информационных технологий и систем электронного банкинга по сравнению с совершенствованием процесса УБР.

Чтобы не «нагромождать» все новые и новые риски в ситуациях применения кредитными организациями разнородных технологий электронного банкинга, предлагается простая модификация традиционного подхода, ориентированная на анализ *состава компонен-*

[31] Guiding Principles in Risk Management for U.S. Commercial Banks. June 1999.

тов типичных банковских рисков, который неизбежно усложняется за счет возникновения их дополнительных источников, обусловленных в свою очередь действием рассмотренных выше новых факторов риска в ИКБД. Таким образом, в предлагаемой методологии риск-ориентированного подхода постулируется, что **внедрение кредитными организациями новых информационных технологий, в том числе технологий электронного банкинга, не приводит к возникновению новых видов банковских рисков, но расширяет состав факторов и порождаемых ими источников компонентов типичных банковских рисков и вызывает смещения профилей рисков, сопутствующих банковской деятельности.**

Здесь уместно также подчеркнуть различие между традиционными системами «Банк – Клиент» так называемого «закрытого» типа, которые предлагались только для юридических лиц и оказывались удобны лишь в тех случаях, когда «точка входа» в такую систему оставалась стационарной (в виде АРМ), и быстро распространяющимися системами ДБО с вариативным доступом к ним. Их разновидности продолжают появляться, что связано преимущественно с развитием мобильных средств связи и сопутствующих им компьютерных систем, а значит, возникают *специфические* для последних источники компонентов банковских рисков, которые существенно отличают их от систем со стационарными автоматизированными рабочими местами для ДБО. В свою очередь общность рассмотрения данной предметной и проблемной области предполагает ее *инвариантность* к особенностям среды информационного взаимодействия, в которой действуют элементы ИКБД.

В число основных факторов системного уровня, которые принципиально повышают уровни ряда типичных банковских рисков при использовании технологий электронного банкинга, входят также следующие:

– «виртуальный» характер дистанционных банковских операций;

– доступность «открытых» телекоммуникационных систем;

– чрезвычайно высокая скорость выполнения транзакций в виртуальном пространстве;

– глобальный характер межсетевого операционного взаимодействия;

– участие компаний-провайдеров в реализации банковского обслуживания;

– возможности использования систем электронного банкинга для противоправной деятельности.

Недостатки в учете этих факторов при внедрении технологий электронного банкинга приводят к росту вероятностей реализации компонентов банковских рисков как для кредитных организаций, так и для их клиентов. В свою очередь необходимость учета этих факторов в УБР приводит к требованию уточнения понятия и содержания собственно «банковской деятельности».

Это понятие стало существенно шире за последние годы, охватывая процесс применения банковских информационных технологий, а также новые способы и средства информационного взаимодействия кредитных организаций со своими клиентами и контрагентами. Соответственно в процессе УБР необходимо учитывать это расширение, поскольку результаты банковской деятельности стали в значительной мере, если не полностью, зависеть от того, могут ли считаться условия применения таких технологий *пруденциальными* и каким образом обеспечивается и гарантируется технологическая и техническая надежность кредитных организаций, равно как и эффективность процессов управления и контроля в них.

2.1. Особенности риск-ориентированного подхода к внедрению и применению технологий электронного банкинга

Как показывает анализ изменений, происходящих в составе и содержании банковских бизнес-процессов (в оптимальном варианте подлежащих внесению кредитными организациями вместе с внедрением ими технологий электронного банкинга – независимо от их общего количества и функциональных особенностей), вслед за такими изменениями могут (а лучше бы *должны)* следовать и изменения в организационно-штатной структуре кредитной организации. Фактически подразумевается требование *адаптации* распределения функциональных ролей, ответственности, обязанностей, прав, полномочий, подконтрольности и подотчетности конкретных руководителей и исполнителей на различных уровнях иерархии управления этой организации к новым банковским технологиям. Это положение относится к целому ряду специальных служб в структуре кредитной организации. Прежде всего к подразделениям, отвечающим за процесс УБР, применение информационных технологий (ИТ) и (или) автоматизацию, внутренний контроль и финансовый мониторинг (в настоящее время эти два процесса нередко реализует одно подразделение), обеспечение информационной безопасности, ведение претензионной работы, а также сервис-центр и некоторые другие. Вместе с тем все сопутствующие и адекватные складывающейся в кредитной организации ситуации изменения должны коснуться и документарного обеспечения деятельности перечисленных подразделений. Такие изменения инициируются, как правило, органами управления этой организации и реализуются соответствующими (достаточно специфическими по сути) внутрибанковскими процессами и процедурами.

На сегодняшний день полнота, адекватность и качество бизнес-процессов в кредитной организации фактически стали определяться соответствием их новому, к сожалению, не получившему пока правильного осознания принципу: «Знай свои технологии»[32]. Без преувеличения можно сказать, что большинство процедур, входящих в состав внутрибанковских процессов, реализуется в современных условиях не столько персоналом кредитной организации, сколько ее банковскими автоматизированными системами. Да и сама кредитная организация, если говорить о собственно выполнении банковских операций «и других сделок», о которых сказано в ст. 5 Федерального закона от 2 декабря 1990 г. № 395-I «О банках и банковской деятельности», в значительной своей части представлена теперь не зданием с обозначающей ее вывеской, а БАС и хранилищем данных, доступ к которым во все большем числе случаев обеспечивают системы ДБО[33]. Таким образом, привычный «Банк» оказывается для клиента кредитной организацией не более чем «кирпичным интерфейсом», служащим для официального оформления и инициации доступа к той БАС, которая выполняет все банковские операции и совершает другие сделки (причем не обязательно в самой кредитной организации). В дополнение к этому клиент может в ряде случаев осуществлять доступ к бэк-офису кредитной организации через ИКБД, выступая фактически в роли «операциониста», взаимодействующего с ее БАС удаленно, что *радикально* меняет и характер отношений с ним кредитной организации, и состав так называемых «зон ответственности» этой орга-

[32] По аналогии с принципами «Знай своего клиента» и «Знай своего работника», которые часто фигурируют в литературе в связи с исследованиями банковских рисков.

[33] Это тем более справедливо в ситуациях территориального разнесения официально зарегистрированной кредитной организации или ее филиала и процессингового центра, а также в условиях так называемого «оффшоринга» – трансграничного аутсорсинга процессинга.

низации, и ее «периметр безопасности»[34]. Приведенные наблюдения оказываются тем более справедливыми, что по состоянию на февраль 2009 г. большинство кредитных организаций применяет от двух до десяти систем ДБО разного или вариативного функционального назначения (пик соответствующей диаграммы приходится на 3 – 4 системы такого рода). Одновременно, как правило, задействуются и 2 – 4 web-сайта (по той же статистике – даже до 12!).

Внедрение любых технологий электронного банкинга *не должно* негативно сказываться на надежности и устойчивости высокотехнологичных кредитных организаций, т.е. уровень совокупного или агрегированного банковского риска[35] повышаться не должен. Это означает, что изменения в структурах профилей отдельных типичных банковских рисков должны происходить таким образом, чтобы профиль агрегированного риска, пусть даже меняясь, оставался *контролируемым* в смысле установленных для его компонентов пределов с учетом их возможного взаимного влияния. При этом подразумевается, что в кредитной организации существует описание этих компонентов в форме определений основных типичных банковских рисков, имеющих компоненты технологического и технического характера, причем в эти описания своевременно (в оптимальном варианте) вносятся коррективы, определяемые особенностями вновь внедряемой ТЭБ и реализующей ее СЭБ.

В этой книге используется иерархическая модель для профилей банковских рисков, представленная на рис. 2.1, которая была апробирована в процессе проводившихся в течение нескольких лет исследований организации банковской деятельности, осуществляемой технологиями электронного банкинга. В ней фигурируют три уровня: помимо уровня известных типичных банковских рисков (ТБР) рассматриваются также нижележащий уровень так называемых «элементарных» банковских рисков (ЭБР) и вышележащий уровень «системных» банковских рисков (СБР). Это в известной степени условные понятия, призванные лишь подчеркнуть различия между уровнями анализа состава компонентов агрегированного банковского риска: каждый ЭБР соответствует некоему недостатку в формировании организационно-технической базы банковской деятельности или, иначе, «просчету» в управлении рисками банковской деятельности в смысле превентивного воздействия на потенциальные источники компонентов этих рисков. Каждый СБР характеризует возможные последствия влияния неконтролируемого изменения профиля и повышения отдельного ТБР или их совокупности, что в итоге может привести к негативным событиям системного характера[36]: отзыву лицензии на осуществление банковских операций, банкротству, ограничению выполняемых операций и т.п. На средней условной плоскости ТБР показан профиль риска в форме Пентагона с указанием уровней пяти типичных банковских рисков.

[34] Эти понятия подробно поясняются ниже.

[35] Large Bank Supervision.

[36] Имея в виду интерпретацию банковского сектора страны как некой системы, состоящей из взаимодействующих кредитных организаций, их клиентов и контрагентов, функции которых известны и унифицированы за счет регламентации, которая, впрочем, охватывает лишь часть банковской деятельности.

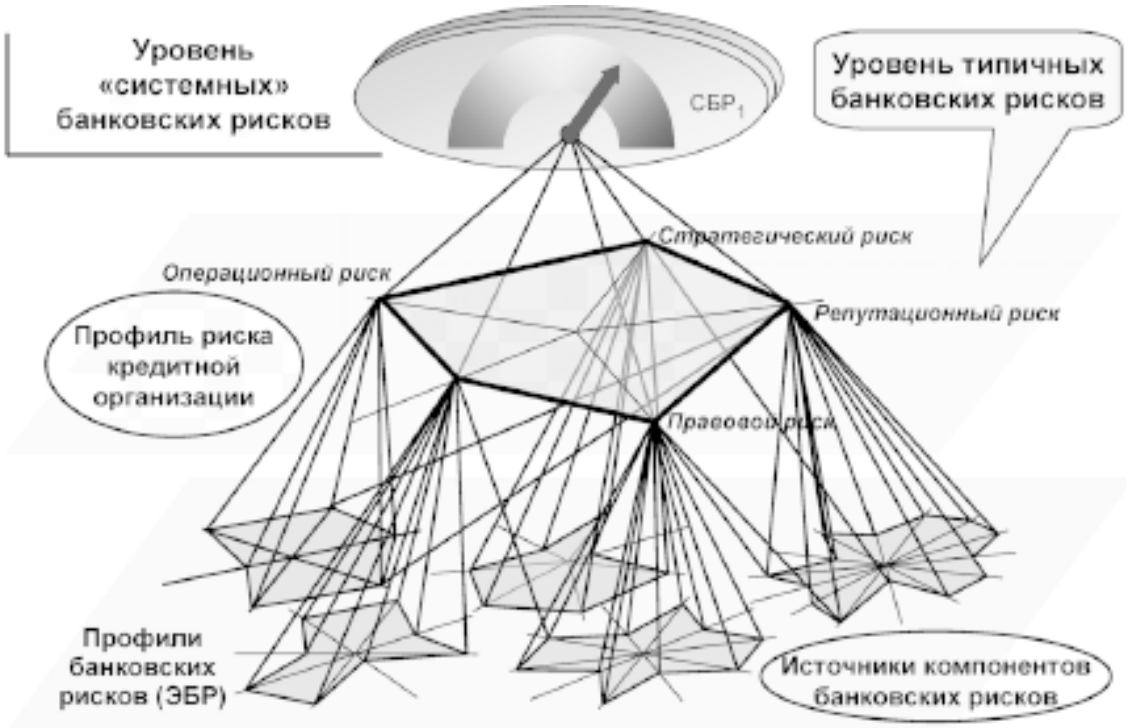

Рис. 2.1. Пример профиля банковских рисков при использовании иерархического подхода

Чтобы удерживать уровни банковских рисков в допустимых пределах, необходимо осуществлять выявление их компонентов, анализировать причины их возникновения – источники указанных компонентов, определять меры воздействия на эти источники (осуществлять собственно УБР) и контролировать результаты такого воздействия. В свою очередь для эффективной организации и реализации перечисленных процедур в составе процесса УБР целесообразно учитывать уже разработанные и апробированные подходы к его формированию, кратко рассматриваемые ниже.

В одном из основных материалов БКБН, посвященных проблематике УБР в новых условиях[37], отмечается: «При выборе технологии электронного банкинга руководству кредитной организации следует анализировать сопутствующие ей факторы и источники рисков, а также оценивать возможности управления данной технологией и контроля ее использования». При этом специально в отношении ДБО через Интернет, учитывая способность технологий такого рода стимулировать взаимную *анонимность* кредитных организаций и их клиентов (скрытых средой информационного взаимодействия), говорится, что «предоставление финансовых услуг через Интернет может существенно изменить и (или) даже увеличить традиционные банковские риски (например, стратегический, репутационный, операционный, кредитный и ликвидности)». На самом деле состав банковских рисков, на изменение профилей и уровней которых влияют технологии электронного банкинга, непосредственно зависит от особенностей банковского законодательства, действующего в той или иной стране. Поэтому перечни банковских рисков, приводимые в различных руководствах зарубежных органов банковского регулирования и надзора, отвечают условиям *только* конкретной страны (или так называемой «объединенной Европы»), а в широком смысле они, конечно, вариативны. Кроме того, в этом же смысле рассматриваемый риск-ориентированный подход не ограничивается только рисками, которые принимают на себя кредитные орга-

[37] Risk Management Principles for Electronic Banking.

низации, а распространяется и на их клиентов, что в условиях электронного банкинга приобретает, так сказать, «особую значимость», потому что риски, которым подвергаются такие клиенты, могут непосредственно преобразоваться в компоненты типичных банковских рисков (о чем чаще всего просто забывают).

В число основных характеристик современных условий осуществления банковской деятельности (которые целесообразно учитывать при стратегическом планировании использования электронного банкинга) входят:

– активная разработка и внедрение новых вариантов банковского обслуживания и сопутствующих им новых банковских технологий;

– внесение изменений в законодательство, ориентированных на повышение надежности и транспарентности банковской деятельности[38];

– дефицит специалистов в области технологий электронного банкинга на фоне их быстрого развития и распространения;

– многообразныезависимости эффективности банковскойдеятельности от сторонних организаций (разного рода аутсорсинга);

– усложнение контроля над процессами, протекающими в виртуальном пространстве банковской деятельности («киберпространстве»).

При этом наблюдается принципиальное противоречие между темпами развития банковских информационных технологий и законодательной базы осуществления банковской деятельности и ее обеспечения. Эти условия никак не зависят от кредитных организаций, поэтому учитывать их целесообразно как факторы возникновения потенциальных проблем, с которыми вполне вероятно им придется столкнуться при внедрении ТЭБ. Здесь уместно сделать краткое отступление, чтобы отметить некоторые особенности проявления таких факторов, о которых целесообразно подумать еще *до* начала этого внедрения при принятии решения относительно выбора конкретной технологии.

Прежде всего руководству кредитной организации уместно оценить, насколько хорошо известна, распространена и апробирована предлагаемая ТЭБ, поскольку история развития банковского дела знает немало примеров использования недостаточно хорошо освоенных технологий и систем такого рода, что всегда приводило к реализации компонентов всех имеющих отношение к делу типичных банковских рисков. «Пробелы» в законодательстве обычно приводят к несовпадениям в интерпретации правил и условий использования ДБО разными сторонами, оказывающимися в спорных ситуациях, связанных с недостатками в организации условий применения конкретной ТЭБ (в самом широком смысле), равно как в содержании обязанностей и ответственности лиц, от которых оно зависит, и определении степени ответственности сторон – участников конфликта. Здесь следует отметить и то, что российским кредитным организациям до настоящего времени приходится самим парировать недостатки отечественного финансового, и в частности банковского законодательства, что относится в значительной мере к содержанию текстов договоров с клиентами ДБО и контрактов с провайдерами, действующими в соответствующем ИКБД: положения этих документов подвергаются наиболее тщательному анализу в арбитражных судах.

В более узком смысле для того чтобы руководству кредитной организации определить состав факторов риска, способных негативно повлиять на процесс и результаты банковской деятельности, удобно разбить ИКБД на так называемые «зоны концентрации источников риска» (как минимум – известные специалистам кредитной организации и предполагаемые ими) и проанализировать особенности каждой из них. Первой такой зоной является клиент ДБО, последней – компоненты локальной вычислительной сети (ЛВС) этой организации,

[38] В качестве примера можно привести принятый еще в 1962 г. Федеральный закон США «О компаниях, обслуживающих банки», в котором речь идет о контроле над провайдерами кредитных организаций.

между которыми располагаются зоны, относящиеся к ее провайдерам, телекоммуникационным системам и пр., включая зональные вычислительные сети (ЗВС) в распределенных или многофилиальных структурах крупных кредитных организаций. Затем, при необходимости, отдельные факторы или источники рисков можно сгруппировать по признакам их возможного проявления в тех или иных типичных банковских рисках. Это может оказаться полезным, например, при организации управления банковскими рисками по их типам: операционный, правовой, репутационный и др. Как бы то ни было, указанные зоны подлежат описанию во внутренних документах кредитной организации, относящихся к управлению банковскими рисками, вместе с общими мерами по парированию их потенциального влияния.

В связи с этим можно определить основные подлежащие оперативному решению проблемы, связанные с новыми факторами, повышающими уровни банковских рисков при использовании технологий электронного банкинга, с чем сталкиваются соответствующие кредитные организации при создании *пруденциальных* условий банковской деятельности (с учетом всех зон ответственности и концентрации источников компонентов банковских рисков):

для кредитных организаций:

а) возможно снижение надежности (а вслед за этим и устойчивости) банковской деятельности из-за неадекватного учета новых факторов и источников банковских рисков, обусловленных спецификой новой ТЭБ и сложностью контроля реализующих их внутрибанковских и системных процессов;

б) из-за различий в практической реализации кредитными организациями технологии электронного банкинга возникает необходимость в точном учете конкретного состава реально действующих факторов риска в каждом отдельном случае (варианте архитектуры БАС и систем электронного банкинга);

для клиентов кредитных организаций:

а) возможен ущерб их интересам из-за реализации неизвестных или малоизвестных им факторов и источников банковских рисков при отсутствии у них достаточной квалификации в части ТЭБ (включая понимание функционирования конкретного ИКБД в выбранном ими варианте ДБО);

б) освоение выбранной СЭБ может оказаться серьезно затруднено из-за несоответствия характеристик собственной личности (возраст, социальное положение, образование, сфера деятельности и т.п.), следствием чего станет повышение уровней принимаемых на себя «клиентских» рисков.

Поэтому, в частности, в ряде своих материалов БКБН отмечает необходимость разработки кредитными организациями «эффективной внутрибанковской политики и практики управления проектами, жизненным циклом систем, контроля над изменениями и гарантией обеспечения требуемого качества банковской деятельности и обслуживания клиентов»[39]. Одновременно подчеркивается, что план внесения адаптационных изменений в перечисленные компоненты банковской деятельности (и внутрибанковские процессы) высшему руководству кредитных организаций целесообразно составлять еще *до* перехода к практической эксплуатации систем ДБО. Причем план этот должен «эффективно доводиться» до всех менеджеров структурных подразделений кредитной организации, которые будут иметь отношение к использованию новой банковской технологии.

Наиболее значимой особенностью организации процесса УБР в условиях электронного банкинга является вариативность ИКБД, компоненты которого и их потенциальное негативное влияние необходимо учитывать. При этом приходится помнить о том, что каждая

[39] Risk Management Principles for Electronic Banking.

ТЭБ и реализующая ее СЭБ создают свой *собственный* контур такого рода, и эти информационные контуры могут не только не совпадать (даже при использовании однородных технологий электронного банкинга), но и существенно различаться подмножествами источников компонентов риска, концентрирующихся в тех или иных зонах. Сами эти зоны также могут оказаться *неявно* выраженными, скажем, в случаях использования кредитной организацией так называемых «виртуальных частных сетей»[40], формирующих в общедоступных сетях передачи данных защищенные «туннели» передачи информации, сетевых экранов (брандмауэров) и прокси-серверов, требующих весьма тщательной настройки своего программно-информационного обеспечения, с помощью которого организуется сетевая защита. Недостатки в организации применения информационных технологий такого рода, которые известны, как правило, только узким специалистам, могут оказаться теми «виртуальными воротами» к информационно-процессинговым ресурсам бэк-офиса кредитной организации, на которые обычно нацелены хакерские, вирусные и прочие сетевые атаки.

Очевидно, что риск-ориентированный подход требует не только составления схем ИКБД, определения и описания зон концентрации источников компонентов банковских рисков, но и *комплексного* анализа их потенциального влияния на указанные ресурсы. При этом важно постараться охватить процессом УБР все каналы информационного взаимодействия кредитной организации с клиентами или, при неблагоприятном стечении обстоятельств, – со злоумышленниками, имея в виду, что в условиях развитых филиальных структур необходима организация мониторинга влияния источников компонентов банковских рисков во всей структуре подразделений кредитной организации и для всех ее систем электронного банкинга (особенно в ситуациях, когда услуги электронного банкинга предоставляются филиалами), охватывая также и БАС (о чем нередко забывают).

[40] *Virtual Private Network* – VPN.

2.2. Классификация банковских рисков и их компонентов

Основной акцент при рассмотрении факторов и источников компонентов банковских рисков необходимо делать на выполнении кредитной организацией своих обязательств перед клиентами ДБО и на защите их интересов. Безусловно, это не означает, что кредитные организации забудут о своих коммерческих интересах, но, с точки зрения автора, риск-ориентированное рассмотрение проблематики ДБО может считаться полноценным *только* в том случае, если оно одновременно и «клиент-ориентированное». В банковской сфере сосредоточены интересы огромного числа клиентов кредитных организаций, которые всегда будут оставаться зависимыми от *доверия* к ним со стороны таких клиентов. Отсутствие доверия, как справедливо подчеркивается в материалах БКБН, способно вызвать кризисные явления в этой сфере. Достаточно заметить, что количество клиентов ДБО у разных кредитных организаций, действующих на территории Российской Федерации, варьируется от нескольких сотен до нескольких сотен тысяч, так что процессы УБР и претензионной работы целесообразно рассматривать как *не менее* важные, чем собственно операционная деятельность кредитных организаций (к сожалению, такой подход пока еще нельзя считать распространенным в отечественном банковском секторе).

Как бы то ни было, кредитным организациям, переходящим к ДБО, целесообразно осуществлять *упреждающий* анализ влияния описанных выше основных факторов возникновения новых компонентов банковских рисков на эффективность банковской деятельности в целом. Типичные банковские риски, в составе которых имеются сопутствующие ДБО компоненты административно-организационного, технологического и технического характера, перечислены в упоминавшемся ранее Письме Банка России от 31 марта 2008 г. № 36-Т (далее – Письмо 36-Т). То, что акцент в этом документе сделан на технологии интернет-банкинга, не сказывается на общности рассмотрения, поскольку практически все изложенное в этом документе можно непосредственно соотнести со всеми остальными технологиями ДБО. К числу банковских рисков, с которыми ассоциируются указанные компоненты, в Письме 36-Т отнесены: стратегический, операционный, правовой, репутационный риски и риск ликвидности (который в условиях электронного банкинга модифицируется в риск неплатежеспособности[41]).

Прежде чем перейти к дальнейшему изложению, следует сделать некоторые пояснения относительно отбора типичных банковских рисков для последующего анализа. Дело в том, что из общего числа этих рисков в зависимости от особенностей действующего банковского законодательства некоторые себя *никак* не проявляют, тем не менее это не означает, что с внесением изменений в законодательство они не заявят о себе в будущем. Поэтому ниже приводятся выдержки из материала Управления контролера денежного обращения США (OCC)[42], в котором рассматриваются все классифицированные этой организацией банковские риски, рассматриваемые на примере ДБО в варианте интернет-банкинга и приводимые здесь в качестве наиболее полного варианта анализа такого рода. Эти выдержки (как, впрочем, и сам цитируемый документ) могут оказаться полезными при принятии в кредитной организации руководящих решений относительно содержания ДБО и организации *пруденциальных* усло-

[41] Как ни странно, в обширной литературе, посвященной банковским рискам, автору не удалось найти упоминания весьма важного акцента, значительно отличающего практическую интерпретацию понятия ликвидности в новых, высокотехнологичных условиях банковской деятельности от традиционно принятой.

[42] Internet-Banking. Comptroller's Handbook.

вий его применения. В этих рекомендациях речь идет о следующих девяти (основных?) банковских рисках[43]:

– кредитном;
– операционном;
– ценовом;
– ликвидности;
– процентном;
– валютном;
– правовом;
– репутационном;
– стратегическом.

Затем кратко излагаются описания факторов возможного повышения уровней каждого из перечисленных банковских рисков (свойственные, естественно, американской действительности).

В качестве причин повышения уровня **кредитного** риска в рассматриваемом материале упоминаются следующие: «Отсутствие личного контакта с клиентами при взаимодействии через Интернет может привести к возникновению проблемы верификации истинности личностей клиентов и в дальнейшем к ошибочным решениям в части кредитования. Могут возникнуть трудности при подтверждении залога и выполнении соглашений по обеспечению безопасности совершения операций интернет-банкинга.

При отсутствии правильного управления [кредитованием][44] использование интернет-банкинга может привести к концентрации кредитов у заемщиков или кредитов в отдельной отрасли производства.

Возможно недостаточное осознание советом директоров и руководством [кредитной организации] дополнительных факторов кредитного риска в связи с применением технологии интернет-банкинга».

Очевидно, что в российских условиях приведенные соображения пока еще не стали актуальными в силу известных законодательных ограничений.

В отношении **операционного** риска в цитируемом материале ОСС отмечается, что «возможны ошибки при выполнении и (или) отказы в предоставлении услуг интернет-банкинга в связи со сбоями в функционировании системы или программного обеспечения. Клиенты, осуществляющие деловые операции через Интернет, скорее всего не потерпят ошибок или промахов со стороны финансовых учреждений, которые не обладают специальными средствами внутреннего контроля для управления проведением операций в рамках интернет-банкинга. Подобным образом клиенты ожидают непрерывной доступности конкретной услуги и web-страниц с простой навигацией (ориентацией) по ним.

В дополнение к операционному риску ошибки в клиринге могут повысить репутационный риск, риск ликвидности и кредитный риск».

Здесь следует отметить, что в условиях электронного банкинга операционный риск характеризуется существенно большей *вариативностью,* нежели предусмотрено в материале ОСС, поскольку в его состав входят компоненты, относящиеся ко всему ИКБД, включая не только web-сайты кредитных организаций, но и разнообразные каналы (линии) связи, системы основных и суб-провайдеров, возможные сетевые атаки, а также самих клиентов

[43] Здесь излагается подход только одного органа банковского регулирования и надзора. Позиции других аналогичных по функциям учреждений США от этого подхода несколько отличаются как по количеству учитываемых банковских рисков, так и по составу их компонентов.

[44] Здесь и далее в квадратных скобках приводятся слова, поясняющие контекст, поскольку полные переводные выдержки из текста документа, которые содержат необходимые в каждом случае пояснения, заняли бы слишком много места.

указанных организаций, о чем в рассматриваемом материале вообще не упоминается (возможно, в силу более высокой компьютерной грамотности населения США, хотя это в данном случае не принципиально).

О **ценовом** риске сказано следующее:

«Банки могут оказаться подвержены ценовому риску, если они начинают или расширяют депозитный брокеринг, торговлю кредитами или программу страхования от риска в результате деятельности в рамках интернет-банкинга. При осуществлении интенсивного трейдинга активов возможно наличие недостатков в действующих системах управления для измерения и мониторинга ценового риска, а также управления им».

Этот риск для отечественных кредитных организаций, применяющих технологии электронного банкинга, пока что не актуален.

В части риска **ликвидности** отмечается только то, что: «Возможно значительное увеличение изменчивости в депозитах, поступающих от клиентов, которые держат свои счета только из соображений [наиболее выгодных] ставок или сроков.

Системы управления активами/пассивами и кредитным портфелем должны соответствовать услугам, предлагаемым в рамках интернет-банкинга».

Надо отметить, что с понятием «ликвидность» здесь связан лишь традиционный смысл, т.е. используемая семантика не учитывает давно уже ставших традиционными проблем не столько с *наличием* у кредитной организации финансовых средств (ликвидных активов), сколько с их *получением* клиентами в требуемые им моменты времени. Это актуально во всех случаях так называемых «электронных переводов»[45], в том числе когда клиентами кредитной организации являются не только физические лица, но и юридические, включая другие кредитные организации. Об этом подробнее будет сказано ниже при рассмотрении полных формулировок банковских рисков и «заложенных» в этих формулировках причинно-следственных связей между негативными событиями и их последствиями для кредитных организаций, предлагающих ДБО, и соответствующих клиентов.

Учет особенностей изменения **процентного** риска также представляется пока что не актуальным, однако в интересах полноты изложения следует привести относящуюся к нему цитату: «Интернет-банкинг может способствовать формированию депозитных, кредитных и других отношений с более широким кругом потенциальных клиентов, чем другие формы маркетинга. Доступ более широкого круга клиентов, заинтересованных преимущественно в наиболее высоких процентных ставках или сроках, усиливает потребность руководства [кредитной организации] в поддержании на должном уровне систем управления активами/пассивами, включая способность быстрого реагирования на изменяющиеся рыночные условия».

Также в плане ДБО пока неактуально повышение уровня **валютного** риска, о причинах которого сказано, что: «Возможны недостатки в системах контроля для приема депозитов от клиентов-нерезидентов или открывающих счета, номинированные в валютах, отличных от доллара США».

Что касается **правового** риска, то его возникновение связывается с такими проблемами, как «недостаточно развитая нормативная база, применимая к операциям электронного финансового обслуживания, включая интернет-банкинг. Возможны недостатки в контроле над выполнением требований, применимых к электронному обслуживанию и предоставлению услуг через Интернет или отсутствие такого контроля. Возможно невыполнение правила "знай своего клиента" и нарушение запретов, наложенных на некоторых из них».

Сказанное здесь вполне справедливо, но это не все, что желательно учитывать в процессе УБР: практика свидетельствует, что структура этого риска значительно усложняется.

---

[45] В зарубежной терминологии – *Electronic Funds Transfer.*

То же самое относится к **репутационному** риску (или, иначе, риску потери деловой репутации[46]), причем он оказывается тесно связан с правовым и операционным банковскими рисками. Относительно него сказано, что «репутации банка может быть нанесен ущерб при обслуживании в рамках интернет-банкинга, если оно плохо организовано, не соответствует требованиям рынка или как-то иначе отталкивает клиентов и общественность».

Наконец, в части **стратегического** риска акцент сделан на том, что «возможно недостаточное осознание руководством рисков, связанных с применением интернет-банкинга, до принятия решения о внедрении этого вида деятельности. Возможно несоответствие технологии внедрения системы интернет-банкинга деловым целям в стратегическом плане и установленным границам для рисков. Возможны недостатки в уровне развития технологий и информационных систем управления для внедрения системы интернет-банкинга. Возможен недостаток ресурсов в банке для идентификации, мониторинга и контроля рисков в деловых операциях интернет-банкинга и нехватка квалификации персонала. Требуется учет изменений, которые электронные финансовые технологии, такие как интернет-банкинг, вносят в конкуренцию».

Необходимо заметить, что анализ этого банковского риска также не совсем полон, тем более что из-за взаимного влияния рисков он также связан с другими: операционным, правовым и репутационным. Кроме того, акцент на технологии интернет-банкинга представляется несколько устаревшим, тем более что и во время выхода рассмотренного материала применялись разнообразные системы электронного банкинга; тем не менее все цитированное в американских условиях своей актуальности не утратило, а в отечественных такая актуальность постепенно возникает.

Возвращаясь к Письму 36-Т, надо сказать, что оно является первым документом, в котором проведен детальный анализ как собственно типичных банковских рисков, явно связанных с ДБО, так и подхода к организации ряда внутрибанковских процессов, не только непосредственно имеющих отношение к управлению рисками, но подлежащих модернизации в связи с изменениями в профиле риска кредитной организации, обусловленными ее переходом к ДБО. Вместе с тем этот документ являет собой первый пример того, как проблематика ДБО фактически вынуждает российские кредитные организации учитывать *смещение* своих профилей рисков, чтобы удерживать эти риски в допустимых пределах и тем самым предотвратить возможное негативное влияние их реализации на выполнение обязательств перед своими клиентами и Банком России как органом банковского регулирования и надзора. В этом документе выделены пять типичных банковских рисков, в структуре которых явно присутствуют компоненты технологического и технического характера, которые целесообразно учитывать в процессе УБР:

– операционный;
– неплатежеспособности (ликвидности);
– правовой;
– репутационный;
– стратегический.

Следует заметить, что этот перечень справедлив на время написания настоящей книги, и практические исследования подтвердили его адекватность ситуации, складывающейся в отечественном банковском секторе вместе с интенсивным внедрением и развитием кредитными организациями технологий электронного банкинга, однако он вполне может оказаться недостаточным по мере развития банковских информационных технологий.

[46] Как это определено в Письме Банка России от 30 июня 2005 г. № 92-Т «Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах».

К примеру, в число подлежащих дополнительному анализу типичных банковских рисков может войти *страновой* риск, если речь зайдет о трансграничном банковском обслуживании или так называемом оффшоринге. В одном из своих материалов БКБН делает на этом специальный акцент, хотя по состоянию на сегодняшний день только определена собственно предметная область, вследствие чего говорить о каких-либо конкретных рекомендациях пока еще преждевременно, за исключением таких, как определения базовых принципов, служащих наиболее общими ориентирами[47]:

«Принцип 1: до того как начать деятельность в рамках трансграничного электронного банкинга, кредитной организации следует провести должное оценивание риска и принимаемых на себя обязательств, в результате которого в ней будет внедрена эффективная программа управления рисками данной деятельности.

Принцип 2: кредитной организации, собирающейся приступить к обслуживанию в рамках трансграничного электронного банкинга, следует разместить на своем web-сайте информацию, достаточную для того, чтобы ее потенциальные клиенты могли получить достоверные сведения об этой организации как юридическом лице, включая страну дислокации и лицензионные данные».

В основном в материалах такого рода обсуждаются вопросы учета несоответствия содержания законов о банковской деятельности разных государств, проблемы расследования подозрительной банковской деятельности, в которой участвуют коммерческие банки разных стран, и вопросы международного взаимодействия органов банковского надзора.

В любом варианте электронного банкинга, чтобы исключить факторы повышения уровней банковских рисков и неконтролируемые смещения их профилей из-за влияния на банковскую деятельность особенностей виртуального киберпространства, которое служит средой взаимодействия кредитных организаций со своими клиентами и контрагентами, в кредитных организациях целесообразно *адекватно* модифицировать подходы к управлению этими рисками. Это означает учет прежде всего невозможности непосредственного контроля человеком процессов, происходящих в любой компьютеризованной среде (включая телекоммуникационные системы), и отсутствия разработанного законодательства, которое регламентировало бы предоставление финансовых услуг в электронной форме, т.е. основных принципиальных проблем УБР, сопутствующих эксплуатации систем ДБО. Однако помимо них имеется еще значительное число проблемных вопросов, которые хотя и не являются принципиальными в условиях пруденциальной организации применения кредитными организациями ДБО, но *становятся* таковыми при отсутствии указанных условий, приводя к возникновению отнюдь не неизбежных источников компонентов банковских рисков.

В то же время эффективное УБР вряд ли возможно без полного понимания изменений, которые могут происходить в структурах типичных банковских рисков, и вызывающих их причин. Соответствующие описания целесообразно включать в такой внутрибанковский документ, как «Положение об управлении банковскими рисками» или аналогичный ему. Ниже приводятся с учетом положений Письма 36-Т некоторые соображения о том, с какими изменениями в указанных структурах могут сталкиваться кредитные организации, переходящие к ДБО.

[47] Management and Supervision of Cross-Border Electronic Banking Activities. Basel Committee on Banking Supervision, BIS, Basel, July 2003.

2.3. Изменение профиля стратегического риска

Наиболее серьезные негативные последствия для кредитной организации, внедряющей какую-либо ТЭБ и соответствующую СЭБ, связаны с реализацией компонентов стратегического риска. Это нисколько не противоречит тому факту, что многие организации российского банковского сектора успешно прошли этапы внедрения и опытной эксплуатации систем ДБО, которые стали для них весьма прибыльными. Другое дело, что неудачные проекты, естественно, не приобретают известности, а не окупившиеся затраты на разработку сложных и дорогостоящих систем электронного банкинга становятся физической оценкой этого вида риска.

В общем случае компоненты стратегического риска связаны с возможными текущими и перспективными финансовыми потерями, обусловленными неправильными бизнес-решениями и (или) несоответствующей реализацией ключевых решений такого рода в кредитной организации, что приводит к невозможности достижения ею своих бизнес-целей и (или) чрезмерным затратам на внедрение и сопровождение используемых банковских технологий и автоматизированных систем. К ним относятся также неправильное распределение ресурсов, ошибки в выборе (способах, комбинации) видов предоставляемых банковских услуг, неадекватные принятым или планируемым бизнес-моделям технологические и организационно-технические решения, а также неоправданные вложения крупных средств в неперспективные проекты или банковские автоматизированные системы, ошибки, допущенные в маркетинговой, рыночной, конкурентной, технической политике и т.п. Важно учитывать также, что с этим видом банковского риска могут быть связаны все остальные четыре риска, которые рассматриваются здесь в приложении к технологиям электронного банкинга.

Такие связи неизбежно возникают и между компонентами стратегического риска, относящимися к ошибочным решениям. Тогда их негативный эффект может усилиться, поскольку сделанные в рамках проекта СЭБ затраты могут недостаточно контролироваться, особенно в тех случаях, когда неудачный проект затрагивает *несколько* внутрибанковских процессов и соответствующих структурных подразделений кредитной организации. Поэтому даже в тех случаях, когда преимущества нового бизнес-направления очевидны, нецелесообразно отказываться от типовых этапов внедрения автоматизированных систем, важнейшим из которых является подготовка и обсуждение технико-экономического обоснования (ТЭО). Тем не менее зачастую этот и другие связанные с ним документы в кредитных организациях просто отсутствуют, так что даже удачный проект может оказаться связан в итоге с существенными непредвиденными дополнительными расходами.

В зарубежной практике банковского регулирования и надзора считается уместным контролировать не только содержание планов информатизации (автоматизации) банковской деятельности, но также достаточность их обоснования и ход поэтапного выполнения, включая связанные с ними процедуры. Например, вновь внедряемая технология должна быть ориентирована на совершенно *конкретную* клиентуру, которая по данным, скажем, маркетинговых исследований воспользуется новыми сервисами, предлагаемыми кредитной организацией и реализуемыми с помощью той или иной СЭБ. Вместе с этим должны быть четко определены порядок ее внедрения, взаимодействия тех или иных специалистов кредитной организации с клиентами ДБО, вопросы поддержки со стороны сервис-центра, содержание возможной претензионной работы и т.д. Если речь идет о предполагаемом массовом продукте, то необходимо рассчитывать производительность СЭБ и БАС, организовать процедуры контроля динамики развития новых сервисов, роста клиентской базы и количества ордеров, поступающих в кредитную организацию, и пр.

Следует специально отметить, что при внедрении проектов электронного банкинга необходимо уделять внимание взаимным связям между внутрибанковскими процессами, без учета которых реализуются такие компоненты стратегического риска, которые нередко считаются косвенными или просто не учитываются. Например, внедрение СЭБ, реализующей принципы открытых систем и универсального протокола сетевого взаимодействия, приводит к необходимости пересмотра периметра безопасности кредитной организации, который заметно расширяется и вместе с клиентом ДБО «уходит за горизонт» и принятию серьезных *новых* мер по его защите, а также по контролю использования ТЭБ. На том и другом всегда делается акцент зарубежными органами банковского регулирования и надзора[48], о чем пойдет речь в параграфе, посвященном адаптации УБР. Между тем вносить изменения в связанные внутрибанковские процессы следует *согласованно* и не упуская из виду суть происходящих изменений, поскольку неадекватность организации процесса ФМ может привести к тому, что внедрение дорогостоящей СЭБ негативно скажется на «имидже» кредитной организации в глазах правоохранительных органов и неожиданно окажется стратегической ошибкой.

Уже этих примеров достаточно для того, чтобы охарактеризовать многообразие проявлений стратегического риска, особенно в связи с другими банковскими рисками. В этом плане недостаточная, с точки зрения клиентов кредитной организации функциональность банковских автоматизированных систем и (или) систем электронного банкинга, равно как неудобство в работе с ними, приводит, как правило, к негативной реакции пользователей СЭБ, которые либо отказываются от предлагаемых сервисов, либо переходят на обслуживание в другую кредитную организацию. Это приводит к неокупаемости такой автоматизированной системы по причинам репутационного плана, но результат всегда один, и только в лучшем случае он связан для кредитной организации с упущенной выгодой.

В российской практике электронного банкинга, пусть и не такой продолжительной, уже было немало случаев просчетов даже по приведенному выше небольшому перечислению проблемных вопросов. Типичная ситуация, связанная с реализацией компонентов стратегического риска, может развиваться как неумышленная атака типа «наводнение» *(flood-attack),* при этом ее причинами становятся и недостаточная производительность БАС и СЭБ, и отсутствие контроля характеристик динамики ДБО, и ошибки в расчетах требуемой пропускной способности каналов (линий) связи.

В качестве одного из примеров такого рода можно привести историю, произошедшую не так давно с российской кредитной организацией, в свое время являвшейся одним из лидеров ДБО: после того как в какой-то момент времени к ее системам электронного банкинга одновременно подключились около тысячи клиентов, направляемые ими ордера вызвали перегрузку производственных мощностей и организация была вынуждена остановить ДБО. Следствием этого, также непредвиденным, стало массовое обращение клиентов в ее сервис-центр, который не был рассчитан на такую нагрузку, так что получить объяснения относительно прерываний в обслуживании большинству клиентов оказалось невозможно. Этой кредитной организации пришлось в авральном порядке несколько дней заниматься техническим перевооружением, чтобы избежать реализации правового и репутационного рисков, но компоненты стратегического риска уже реализовались в незапланированных расходах на осуществление технической реорганизации. Всего этого можно было бы избежать, если бы в организации были бы заблаговременно приняты организационно-технические меры по оперативному (или, если не в режиме реального времени, то регламентному) контролю производительности банковских автоматизированных систем и приведению ее в соответствие с потребностями клиентов ДБО.

[48] Risk Management Principles for Electronic Banking.

Аналогичная ситуация, но связанная уже с компонентами правового риска, возможна, если функциональные характеристики СЭБ и поддерживающей ее БАС недостаточны для гарантированного обеспечения информационной безопасности. При этом просчеты нередки не только из-за того, что имеются неконтролируемые информационные сечения между теми или иными системами и подсистемами в кредитной организации или в ИКБД, но часто из-за того, что не прогнозировались ошибки, допускаемые клиентами.

Руководству кредитной организации, принимая решение о переходе к ДБО через открытые системы (в том числе – через Интернет), целесообразно, по сути, провести некоторые специализированные исследования, в том числе в части оценки зависимости этой организации от «третьих лиц», присутствующих в ИКБД, прежде всего от провайдеров разного рода. Организация отношений с ними также может относиться к стратегическим решениям, так как известно, скажем, немало примеров сетевых атак, ориентированных на финансовые учреждения, но осуществлявшихся через компьютерные системы других компаний. Такая атака типа «распределенный отказ в обслуживании»[49] имела место и в отношении уже упоминавшейся кредитной организации, причем обращение ее специалистов к провайдерам с просьбой помочь парировать ложный трафик нашли отклик далеко не у всех таких компаний. Те, кто отказался помочь, ссылались на контрактные обязательства, которые касались только обеспечения конкретных каналов (линий) связи, их пропускной способности, поддержки серверов и т.п., но не содействия в организации сетевой защиты и участия в ней. В итоге этой кредитной организации пришлось пересматривать, а точнее, строить заново свою «политику отношений» с провайдерами. Кстати, это до настоящего времени «больной» вопрос для многих кредитных организаций, особенно тех, кто работает в условиях недостаточно развитой региональной инфраструктуры и отсутствия конкуренции между различными провайдерами (но тем не менее берется за ДБО!).

Таким образом, возможны существенно различные сценарии возникновения угроз надежной банковской деятельности в части компонентов стратегического риска, связанных с применением ДБО, и такие сценарии целесообразно рассматривать, разрабатывая модели потенциальных угроз эффективной реализации ключевых решений, принимаемых руководством кредитной организации по направлению внедрения информационных технологий. Тем более принятию недостаточно продуманных руководящих решений в части перехода к ДБО должно препятствовать ТЭО (почему это в основном и важно). Впрочем, следует заметить, что разработка систем поддержки принятия решений или, как иногда говорят, информационных систем управления[50] пока не стала распространенной практикой в российском банковском секторе.

[49] Наиболее «популярный» в последние годы вид сетевых атак – *Distributed Denial of Service* (DDoS), представляющий расширенный вариант DoS-атаки за счет задействования компьютеров, находящихся в сетевых структурах сторонних организаций за счет «заражения» их специальными вирусами-червями (см. ниже).

[50] Decision Support System/Management Information System.

2.4. Изменение профиля операционного риска

Причины, приводящие к возникновению компонентов операционного риска при ДБО, наиболее разнообразны по сравнению с другими видами банковских рисков. От них зависят возможные текущие и перспективные финансовые потери, обусловленные ошибками при выполнении банковских операций (что может привести к неправильной реализации учетных и расчетных процедур), мошенническими действиями в отношении кредитной организации (включая несанкционированные транзакции, хищения финансовых средств в электронной форме и пр.), нарушением непрерывности (доступности) и (или) переходом автоматизированных систем кредитной организации, используемых для осуществления банковской деятельности, в «нештатные» режимы функционирования (вследствие возможных аварий, отказов и сбоев оборудования как самой кредитной организации, так и ее провайдеров, в каналах связи и т.п., из-за чего возможны потери клиентских транзакций, данных и невыполнение ею обязательств перед своими клиентами). К этому же примыкают случаи несанкционированного сетевого доступа злоумышленников к информационно-процессинговым ресурсам кредитной организации.

Независимо от того, что именно является причиной нарушения штатного функционирования банковских автоматизированных систем кредитной организации и ее систем электронного банкинга, результатом этого всегда будет являться невыполнение ею тех или иных взятых на себя перед клиентами ДБО обязательств, т.е. снижение ее *надежности* по причине невыполнения положений соответствующих договоров. Базовых обязательств такого рода пять – они относятся к следующим понятиям:

– доступность обслуживания (непрерывности функционирования);

– состав функций («полнофункциональность»);

– финансовые операции (денежные обязательства);

– временные характеристики (своевременность обслуживания);

– конфиденциальность информации (информационная безопасность).

Только выполнение *всех* перечисленных обязательств без каких-либо отклонений от установленных договорами уровней обслуживания (в отношении клиентов) при дистанционном предоставлении банковских услуг свидетельствует о *надежности* как банковской деятельности, осуществляемой кредитной организацией, так и ее самой (впрочем, как показывает практика, в текстах таких договоров подобное перечисление можно встретить крайне редко). Речь здесь идет, естественно, о технологической и технической стороне понятия надежности[51].

Вследствие этого наличие или отсутствие разнообразных источников компонентов операционного риска зависит и от того, как кредитная организация решает «типовые» вопросы обеспечения надежности функционирования компьютерного оборудования, и от решения ею специфических для ДБО вопросов. В различных источниках, отечественных и зарубежных, приводятся статистические данные относительно влияния угроз штатному функционированию компьютерных систем на этот показатель банковской деятельности: в среднем можно считать, что 60% случаев прерываний бизнеса обусловлено сбоями в работе автоматизированных систем организаций. При этом наиболее частой общей причиной сбоев в их работе считаются внедрение или изменение информационных технологий и (или) программных приложений, которые не были:

– правильно спланированы (включая «откат» в исходное штатное состояние);

[51] Интерпретируемой как свойство сохранять значения установленных параметров функционирования в определенных пределах, соответствующих заданным режимам и условиям в течение установленного времени.

– полностью протестированы (включая модели и сценарии развития угроз).

Прерывания функционирования автоматизированных систем в целом обусловлены различными ошибками/сбоями в соотношении:

– технологические сбои – 20%;

– ошибки процессов – 40%;

– ошибки персонала – 40%.

Все перечисленное здесь наглядно характеризует степень зависимости результатов современной банковской деятельности от надежности компьютерных систем кредитной организации, что должно полностью *осознаваться* ее руководством и *адекватно* учитываться при распределении ресурсов. Для многих средних и небольших организаций выделение достаточных ресурсов на обеспечение надежности внедряемых банковских информационных технологий становится непростой задачей, если такие технологии, как ДБО, внедрялись недостаточно обоснованно, или в силу недостаточного осознания значимости указанных технологий и реализующих их автоматизированных систем финансирование осуществляется по «остаточному принципу».

Ошибки при выполнении банковских операций – явление уже относительно редкое, в этом случае имеются в виду преимущественно неточности, связанные с информационными сечениями ИКБД, в которых происходит какой-то перенос данных из одной среды хранения в другую (ошибки операционистов кредитной организации или клиентов при заполнении интерфейсных полей, преобразование форматов, переписывание из одной базы данных в другую и пр.). Тем не менее если СЭБ и БАС совместно с ней не подвергаются тщательным испытаниям (включая результаты неправильных действий пользователей), то все непроверенные варианты будут «проверены» уже в реальной эксплуатации этих систем[52], что приведет к неизбежным дополнительным затратам на поиск пропавшего контента ордеров клиентов, отладку программно-информационного обеспечения этих систем, лишней претензионной работе и т.д. Во многих российских кредитных организациях подобные ситуации не редкость, особенно когда речь заходит о противоправной деятельности, связанной с искажениями в полях записей баз данных кредитной организации или хищением средств со счетов клиентов, что обычно происходит из-за недостатков в обеспечении информационной безопасности.

Последнее может иметь место в тех случаях, когда в СЭБ и (или) БАС остаются «лазейки», позволяющие осуществлять несанкционированный доступ (НСД) к массивам данных и банковскому программному обеспечению. В ряде практических случаев такого рода операторы, находящиеся в информационных сечениях между СЭБ и БАС, располагают возможностями, к примеру, подмены реквизитов платежных документов клиентов ДБО или имитации поступления от них соответствующих ордеров[53] и т.п. Кстати, даже такой НСД к информационно-процессинговым ресурсам кредитной организации, который не приводит к чьим-либо финансовым потерям, вполне может обернуться утечкой конфиденциальной информации, а прямым следствием этого станут опять-таки хищения денежных средств, возникновение возможностей для шантажа клиентов или более серьезные последствия для них, поскольку в условиях криминализованной экономики сведения о банковских операциях «и других сделках» могут оказаться более значимыми, чем суммы денег, фигурировавшие в скомпрометированных транзакциях.

Что касается нарушений непрерывности функционирования (доступности) автоматизированных систем кредитной организации и (или) переходов в «нештатные» режимы функционирования, а также сбоев в каналах (линиях) связи, то следствием их могут являться и

---

[52] Это касается и практики так называемых «заплаток» *(patches)* для программного обеспечения.

[53] Это понятие определено Банком России в упоминавшемся ранее Письме № 36-Т.

прерывания сеансов ДБО с потерей или искажением клиентской информации, и невозможность выполнения финансовых и других обязательств кредитной организацией перед клиентами, и в наихудшем случае несанкционированные списания средств с их счетов и другие негативные явления. То же самое с учетом вирусных, сетевых и хакерских атак[54] можно отнести к распределенным компьютерным системам провайдеров кредитной организации и т.п.

Последние годы характеризуются множеством случаев разнообразных атак на системы электронного банкинга и банковские автоматизированные системы кредитных организаций. Упоминавшаяся выше атака типа «отказ в обслуживании» изначально организовалась с помощью программ, осуществлявших генерацию очень большого количества запросов, передаваемых через вычислительные сети на сервер – объект атаки, обычно в короткие интервалы времени. Тем самым превышалась производительность сервера и он прекращал функционирование, «не в силах» справиться с таким количеством запросов[55]. В современных условиях применяется «распределенный» вариант этой атаки, осуществляемой через промежуточные сетевые компьютерные системы с целью многократного усиления негативного эффекта (повышения «мощности атаки»). Для этого могут использоваться ложные сетевые обращения *(ping*[56]*),* программы-черви *(worm),* распространяющиеся по вычислительным сетям и инсталлирующиеся на каждом доступном АРМ, чтобы в заданный момент времени начать генерацию ложных запросов, и пр. Это происходит в фоновых режимах, почему задействованные компьютеры иногда называются «зомби», а сеть, которая из них состоит, – «ботнет»[57]. На рисунке 2.2 показана общая схема сетевых атак рассматриваемого типа (представляющая собой модифицированный рисунок из книги *Crume J.* Inside Internet Security).

Рис. 2.2. Инициация атаки типа DDoS

[54] Приведенное разделение несколько условно, оно основано на различиях в моделях соответствующих угроз для БАС кредитной организации.

[55] *Crume J.* Inside Internet Security. Addison-Wesley, Pearson Education Ltd., 2000.

[56] От термина *Packet Internet Groper.*

[57] Комбинация из английских слов *robot* и *net.*

Возвращаясь к проблемам применения кредитными организациями информационных технологий (ИТ), надо отметить, что нередко незначительным или даже не существующим источником компонентов операционного риска их специалисты считают процедуры оперативного внесения небольших по масштабам изменений в программно-информационное обеспечение ДБО и БАС (упоминавшихся выше «заплаток»). Такая необходимость возникает обычно в тех случаях, когда:

– клиенты кредитной организации совершают действия, непредусмотренные алгоритмами, реализованными в автоматизированной систем, что приводит к непредсказуемым результатам («зависанию» и пр.);

– функционирование принятой в эксплуатацию автоматизированной системы не совпадает с ее техническим проектом, так что требуется оперативная доработка отдельных функциональных модулей;

– выявляются ошибки в проекте автоматизированной системы и требуется ее временный вывод из эксплуатации (отключение сервисов) для перепрограммирования, перенастройки отдельных модулей и т.п.;

– автоматизированная система оказывается скомпрометирована сетевыми или вирусными атаками, действиями хакеров или инсайдеров кредитной организации, из-за чего требуется ее усовершенствование.

Все перечисленные причины, за исключением последней, служат, как правило, признаками недостаточно полного тестирования БАС и СЭБ. Однако, поскольку сложившуюся ситуацию всегда необходимо оперативно исправлять, специалисты кредитной организации вынуждены принимать экстренные меры по устранению недостатков, внедряя в автоматизированную систему программные или библиотечные модули, нередко написанные наспех, не прошедшие типовых процедур проверки и приемо-сдаточных испытаний и содержащие ошибки, потому что отсутствие оперативности играет в таких случаях *негативную* роль. Для кредитной организации следствием такого «подхода», не соответствующего принятой инженерной практике разработок, всегда становятся новые источники компонентов этого риска.

Любое упомянутое выше мошенничество, несанкционированное вмешательство, функциональный сбой или отказ (т.е. нарушение штатного режима работы) компьютерных систем (неважно по какой причине) повлекшие за собой невозможность получения клиентом установленного договором на ДБО сервиса или выполнения им своих финансовых обязательств перед третьими сторонами, связано с возникновением компонентов как минимум правового и репутационного рисков, а в некоторых случаях риска неплатежеспособности и стратегического риска (имеется в виду негативная общественная реакция). Реализация компонентов операционного риска изначально становится возможна преимущественно (хотя и не только) по причине несоблюдения установленных когда-то государственными стандартами (начиная с ГОСТ 34.602-89) порядков разработки автоматизированных систем – неважно, банковских или нет, а потребовать этого (и проследить за исполнением) в кредитной организации оказалось некому, и это становится для нее еще одним существенным фактором операционного риска. Кстати, такие стандарты утверждались как раз для того, чтобы автоматизированные системы работали так, как требуется, а не так, как получится.

2.5. Изменение профиля правового риска

Повышение уровня правового риска приводит к возможным финансовым потерям, являясь следствием возможных нарушений кредитной организацией положений нормативно-правовых документов, которые регламентируют банковскую деятельность, и (или) законодательной неопределенности отдельных аспектов предоставления банковских услуг. Реализация компонентов этого риска имеет форму санкций, которые могут быть наложены на кредитную организацию за нарушение ею правил выполнения банковских операций, несоответствие требованиям ведения бухгалтерского учета и, как следствие, недостоверность банковской отчетности, за потерю значимых банковских данных, утечку конфиденциальной банковской и (или) клиентской информации, включая нарушение банковской тайны, возможную скрытую противоправную деятельность, в которую оказывается вовлечена кредитная организация из-за слабого контроля использования ее СЭБ, а также за недостатки, обусловленные несовершенством организационно-технического, аппаратно-программного или же программно-информационного обеспечения банковской деятельности, как самой кредитной организации, так и ее провайдеров, что может вызывать претензии со стороны клиентов ДБО.

Первой же задачей, подлежащей решению при внедрении кредитной организацией любой ТЭБ, становится серьезное усиление «общебанковских» функций управления и контроля с тем, чтобы особенности СЭБ, реализующей конкретную технологию, не вызвали сомнений у контролирующих органов в выполнении правил бухгалтерского учета и подготовке регламентной отчетности (в широком смысле). Кредитной организацией должна быть гарантирована фиксация в базах данных и правильная обработка всех ордеров клиентов, которые имеют отношение к этим процедурам, независимо от канала ДБО и информационных сечений между системами электронного банкинга и БАС кредитной организации. К отмеченному тесно примыкают проблемы обеспечения доказательной базы электронного банкинга и обеспечения юридической силы так называемых «электронных документов», которые в традиционной форме не существуют, а их распечатки также требуют удостоверения подлинности (эта проблематика еще будет подробно обсуждаться в других разделах, в том числе в плане организации последующей претензионной работы в части ДБО).

Далее целесообразно предусмотреть возможности нарушения непрерывности функционирования ИКБД (неожиданное прекращение сеанса ДБО) в плане вероятных правовых последствий реализации соответствующих компонентов операционного риска (еще одного варианта проявления взаимного влияния банковских рисков). Здесь возникает несколько основных вопросов, подлежащих рассмотрению специалистами кредитной организации:

– организация оперативного предоставления клиенту другого маршрута или варианта ДБО (в случае недоступности системы или прерывания сеанса, к примеру, интернет-банкинга это может быть другой web-сайт или вообще другая СЭБ);

– оперативная реализация соответствующего ситуации раздела плана действий на случай чрезвычайных (иногда говорят «непредвиденных») обстоятельств, для чего требуется наличие схем резервирования и резервных ресурсов, отработанное распределение обязанностей и т.п.;

– включение в текст договора с клиентом на ДБО положений, определяющих порядок действий сторон в форс-мажорных обстоятельствах, их обязанности, ответственность, порядок разрешения спорных ситуаций и компенсации потенциального ущерба интересам клиента и т.п.;

– организация оперативного восстановления массивов банковских и клиентских данных, целостность которых может оказаться нарушенной из-за прерывания сеанса ДБО,

для чего требуется формирование и поддержание соответствующего архива и порядок его использования;

– включение в текст контрактов с провайдерами, от которых зависит непрерывность функционирования ИКБД, положений, устанавливающих порядок действий сторон в форс-мажорных обстоятельствах, их обязанности, ответственность, порядок разрешения спорных ситуаций и компенсации ущерба.

Точный перечень указанных вопросов, связанных с компонентами правового риска, как и для операционного риска, определяется специалистами кредитной организации с учетом специфики ее БАС, систем электронного банкинга, видов провайдеров, состава услуг, предоставляемых в рамках ДБО, возможных сетевых и вирусных атак, средств защиты от них и т.п.

Потенциальное влияние тех компонентов правового риска, которые сопутствуют компрометации банковских информационных ресурсов, обусловлено недостатками в обеспечении информационной безопасности кредитной организации. Они могут иметь место из-за новизны/сложности ТЭБ или недостаточного освоения внедренной в ней СЭБ. На практике его причины кроются в неполноте предусмотренных моделей и сценариев развития угроз, предполагаемых для конкретного ИКБД, связанного с этой технологией. Одним из наиболее серьезных факторов риска при этом является квалификационный «разрыв» между специалистами подразделений ИТ и обеспечения информационной безопасности кредитной организации: первые отвечают за непрерывность и функциональность БАС и СЭБ и могут не располагать полным знанием сопутствующих последней из них угроз, последние же могут не полностью представлять технические механизмы реализации этих угроз. Результатом становятся «дыры» в периметре безопасности кредитной организации, который, кстати, в условиях электронного банкинга может приобретать весьма сложную форму – если эксплуатируется несколько разнородных систем ДБО и имеется несколько видов пользователей их и БАС.

Действие упомянутого разрыва проявляется не только в несоответствии квалификаций. Часто во избежание этого в условиях бюджетных и ресурсных ограничений практически все полномочия системного уровня вынужденно концентрируются в подразделении ИТ кредитной организации. Это относится к таким специализациям, как администрирование банковских автоматизированных систем и систем ДБО, локальных вычислительных сетей, баз данных и информационной безопасности. Тем самым создается опасность чрезмерной концентрации системных полномочий в руках очень небольшого контингента высококвалифицированных специалистов. Подобная ситуация осложняется тем, что контролировать возможные негативные проявления так называемого «человеческого фактора» при этом становится практически невозможно (в организации отсутствуют независимые специалисты с сопоставимой или более высокой квалификацией в области ИТ, чем у таких «супер-администраторов»), так что не может идти и речи о выполнении принципа «четырех глаз»[58]. В условиях осуществления банковской деятельности в виртуальном пространстве это может оказаться весьма серьезным фактором и операционного, и правового, и репутационного, а вслед за ними и стратегического рисков (а для клиентов такой организации, как следствие, – риска неплатежеспособности по их счетам в какой-то момент).

Проблемы организационно-технического плана, приводящие к реализации компонентов правового риска в условиях ДБО, также разнообразны и варьируются от невыполнения клиентом платежей из-за того, что, как говорят, «платежка не прошла», до невозможности оплаты покупок через POS-терминал или получения денег через банкоматы из-за непола-

[58] Под этим понимается осуществление двойного параллельного независимого контроля (в том числе при принятии «ответственных» решений, т.е. значимых для финансового состояния кредитной организации).

док в обеспечивающей их функционирование ЗВС, к последнему варианту относятся также разнообразные «банкоматные» мошенничества с пластиковыми картами и несвоевременное денежное подкрепление. Причиной возникновения перечисленных угроз надежности банковской деятельности является недостаточный контроль со стороны специалистов кредитной организации работоспособности или безопасности обслуживаемых ею удаленных специализированных банковских терминалов. В свою очередь изначальным фактором риска может быть отсутствие адекватного потребностям ДБО внутреннего порядка в кредитной организации или контроля его выполнения.

К проблематике правового риска могут примыкать прямые или косвенные санкции со стороны тех учреждений, которые контролируют отдельные стороны банковской деятельности, не имеющие непосредственного отношения к выполнению банковских операций и не связанные с возникновением компонентов правового риска до внедрения технологий ДБО. Имеется в виду, что для защиты трафика между клиентом и кредитной организацией используются разнообразные средства криптозащиты. Не касаясь вопросов их достоинств, недостатков и надежности, следует отметить, что их использование (включая распространение среди клиентов ДБО) требует получения специальных разрешений у компетентных органов и сертификации. В последние годы активность проверок по указанным вопросам выросла и они оказались связаны для кредитных организаций с новыми компонентами правового риска. То же самое относится к проведению проверок соблюдения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2.6. Изменение профиля репутационного риска

Следствиями повышения репутационного риска являются возможные финансовые потери, обусловленные формирующимся негативным общественным мнением в отношении кредитной организации из-за невыполнения (нарушения) ею обязательств перед клиентами, что приводит к их потере, оттоку заемных средств и упущенной выгоде, судебным искам, появлению общедоступных сведений о нарушениях банковской тайны (конфиденциальности информации) и т.п. Причинами этого становятся недоступность, неработоспособность, неполная функциональность, ненадежность, небезопасность автоматизированных систем кредитной организации, включая хакерские воздействия на используемые ею web-сайты. Из-за реализации перечисленных угроз и связанных с ними компонентов банковских рисков происходят потеря (искажение) банковских и (или) клиентских данных (в том числе из-за отказов аппаратно-программного обеспечения как самой кредитной организации, так и ее провайдеров), компьютерные преступления, сетевые атаки.

Сказанное во многом относится к проявлениям операционного, правового и стратегического рисков, о чем уже говорилось выше и что характеризуется как взаимное влияние рисков, однако с репутационным риском связан еще один существенный аспект, обусловленный сложностью практического освоения технологий и систем электронного банкинга. Когда-то среди американских работников рекламы бытовала поговорка «А теперь давайте встанем на четвереньки и посмотрим на проблему с позиции клиента». Если привыкший к традиционному обслуживанию в операционном зале «средний» клиент ДБО не разберется с функционированием интерфейса предоставляемой ему СЭБ кредитной организации, не сможет управлять сеансом информационного взаимодействия (например в рамках интернет-банкинга), не получит требуемой ему информации или, что хуже всего, из-за своих ошибок потеряет какие-то денежные средства (в том числе и из-за нарушений информационной безопасности), то он, как правило, выскажет свои претензии в адрес кредитной организации, а то и доведет их до судебного разбирательства. При этом клиенту вряд ли придет в голову мысль, что он в чем-то не прав, невзирая на текст договора на ДБО.

Поэтому, если при заключении договора на ДБО сотрудники кредитной организации не потрудятся убедиться в понимании клиентом содержания этого документа (а другого ГК РФ, вообще говоря, не предусматривает), в том, что он понимает, допустим, как работает аналог собственноручной подписи (о котором сказано в ст. 160 ГК РФ, но требования к нему не определены, т.е. неясно, какое средство идентификации может считаться таковым, а какое нет), в освоении им интерфейса выбранной СЭБ, в понимании требований информационной безопасности и т.п., то впоследствии им придется выполнять существенно больший объем претензионной работы, чем в противоположном случае. Таким образом, речь идет о том, что об обеспечении необходимой и достаточной квалификации клиента можно не заботиться (что и встречается на практике), но тем самым кредитная организация только осложнит жизнь самой себе.

К повышению уровня репутационного риска ведут любые неудобства, которые испытывают клиенты ДБО при работе с СЭБ, начиная с запутанного интерфейса систем интернет-банкинга или малофункционального меню системы мобильного банка и заканчивая несанкционированным снятием денег с их счетов через банкоматы посредством так называемого «белого пластика» и других мошеннических приемов. Разнообразие вариантов хищений привело к тому, в частности, что Банк России начал выпуск своего рода письма-предупреждения для кредитных организаций и их клиентов (например, Письмо от 7 декабря 2007

г. № 197-Т «О рисках при дистанционном банковском обслуживании»[59]). Негативная реакция клиентов на любой из таких вариантов может начинаться словами: «Почему вы меня не предупредили о том, что…» Можно привести и другие примеры, когда специалисты кредитной организации вынуждены объяснять клиенту, что его претензии относительно пропажи денег с его счета неосновательны, потому что он:

– не обеспечил должного ограничения доступа к своему АРМ, которое использовалось для ДБО, и с этого компьютера мог отправлять ордера кто угодно (а его идентификаторы могли быть написаны снизу на клавиатуре);

– хранил идентификационную информацию на жестком диске своего АРМ, с которого имеется доступ в Интернет, поэтому хакер смог осуществить взлом и скопировать ее, после чего похитил деньги со счета;

– сознательно перевел 500 000 руб. со счета, а не 5000 и не тому контрагенту, как утверждается в претензии, а то, что «залипла» клавиша или реквизиты платежа были подменены, – это не основания для возврата денег;

– передал свою пластиковую карту неустановленному лицу, которое вылетело в Лондон (Париж, Абу-Даби и т.п.) и там осуществило снятие денег через банкоматы и оплату покупок в дорогих бутиках, а сам ждал дома;

– скомпрометировал данные персональной идентификации, совершая покупки в интернет-магазинах, играя в интернет-казино или храня деньги в электронных кошельках;

– вообще сам во всем виноват и надо внимательно читать договор, в котором «русским по белому» написано, что PIN-код считается аналогом собственноручной подписи.

И тому подобное. При этом ни служба безопасности кредитной организации , ни специалисты по ИТ, ни сотрудники сервис-центра АРМ клиента никогда не видели, не знают, что он, допустим, доктор философии, а не компьютерщик, и оснований для возмещения исчезнувших средств, к сожалению, не имеется. Множество историй такого рода произошло с пользователями систем ДБО (www.banki.ru).

[59] *Лямин Л.В.* К вопросу о рисках, связанных с применением технологий дистанционного банковского обслуживания // Управление в кредитной организации. 2008. № 2. С. 20-31.

2.7. Изменение профиля риска ликвидности (неплатежеспособности)

Как уже кратко отмечалось ранее, риск ликвидности в условиях применения технологий электронного банкинга трансформируется в риск неплатежеспособности, приводящий к возможным финансовым потерям, обусловленным неспособностью кредитной организации своевременно и полностью выполнить свои финансовые обязательства перед клиентами из-за изменения характеристик управления ликвидностью в условиях открытого сетевого взаимодействия, проявления которого не всегда предсказуемы. Как правило, сам этот риск реализуется опосредованно через репутационный, правовой и стратегический риски, поскольку для него характерны такие явления, как непредвиденный отток средств, финансовые хищения в крупных размерах (включая несанкционированные переводы денежных средств), другие потери высоколиквидных активов, сбои и отказы в работе БАС, СЭБ и другого аппаратно-программного обеспечения, которое используется для осуществления банковского обслуживания как кредитной организации, так и ее провайдеров, «стоящих на пути» в ИКБД, а также недостатки организационно-технического характера, следствием которых становится невыполнение кредитной организацией своих обязательств перед клиентами.

Простейшим примером является невозможность получения наличных денег в банкомате по причинам, обсуждавшимся выше, т.е. кредитная организация сама по себе остается абсолютно «ликвидна» и денег на так называемой «зарплатной карте» достаточно, однако получить их невозможно, потому что на дисплее устройства высвечивается надпись: «С вашим банком нет связи» или еще проще: «Выполнение операции невозможно. Извините» либо «Банкомат не работает», – конечно, без каких-либо объяснений, но кредитная организация оказывается в глазах клиента фактически неплатежеспособна, а на ее деловую репутацию влияют обстоятельства, в которых находится клиент ДБО (сказанное относится и к POS-терминалам).

В условиях ДБО клиент может взаимодействовать с кредитной организацией лишь опосредованно, через ИКБД, который ему «не виден», поэтому установить, по какой именно причине «не проходят» финансовые операции, клиент не в состоянии (тем более что оперативно связаться с кредитной организацией не всегда возможно). Вследствие этого возникают дополнительные компоненты упомянутых рисков, непосредственно ассоциируемых с риском неплатежеспособности, без учета которых при организации ДБО (в связи с потенциальными проблемами: аварийными ситуациями, сбоями в работе программного обеспечения различных компьютерных систем, сетевыми атаками, перекрывающими каналы связи или «подавляющими» процессинговые мощности, и другими) претензии клиентов ДБО неизбежны. В то же время предвидеть их возникновение и возможные последствия (варианты ущерба), причем в связи с конкретными факторами возникновения этих компонентов, сложно в отсутствие заранее разработанных сценариев, так что такие компоненты этого риска реализуются.

2.8. Возможности учета компонентов типичных банковских рисков

Вопрос проведения расчетов уровней банковских рисков в условиях отсутствия законченной теории их определения и анализа также остается до настоящего времени дискуссионным[60], тем более проблематично доведение его решения до точного учета влияния технологий электронного банкинга. В классических определениях собственно понятия банковского риска, которые можно найти в публикациях зарубежных органов банковского регулирования и надзора, также наблюдается некоторое несоответствие. Если обобщить такие определения, то можно сформулировать два его «интегральных» варианта. Один из вариантов использует своего рода *абсолютное* исчисление, и в такой трактовке базовое определение выглядит следующим образом: **«Банковский риск – это возможный финансовый ущерб для капитала или доходов кредитной организации, который может иметь место вследствие ее банковской деятельности».**

В рекомендациях зарубежных органов банковского регулирования и надзора[61] для отдельных видов банковских рисков определения такого рода обычно уточняются за счет указания состава негативных внутренних факторов, действующих в кредитных организациях, которые вообще приводят к возникновению источников банковских рисков.

С другой стороны, принципиально важным является то, что одни и те же негативные последствия могут по-разному влиять на финансовое состояние кредитных организаций ввиду различий в их размерах, масштабах и специфике банковской деятельности, структуре финансовых ресурсов и технологическом обеспечении выполнения банковских операций. Проще говоря, один и тот же по *абсолютной* величине убыток один банк не заметит, другой сможет парировать, а третий банк «не переживет». Следовательно, подчеркивают специалисты упомянутых учреждений, необходимо оценивать уровни банковских рисков в терминах их *значимости* для конкретных коммерческих банков (кстати сказать, только тогда уместно использование определений качественного характера, относящихся к оценкам уровней банковских рисков). При таком подходе обобщенная формулировка понятия банковского риска может быть представлена в другом интегральном виде, предполагающем использование уже *относительной* шкалы: **«Банковский риск – это оценка значимости возможного ущерба финансовым ресурсам и доходам коммерческого банка, обусловленного применяемыми им способами ведения банковского дела».**

Интересно отметить, что в рассматриваемых зарубежных материалах для определения собственно риска в подавляющем большинстве случаев используется первая формулировка, однако, когда речь идет об *интерпретации* выявляемых факторов риска в приложении к оценке ситуации в кредитной организации, семантика выводов полностью относится ко второму варианту.

Суть подхода от описанных выше различий в классификации рисков не изменяется и заключается в попытках *качественного* оценивания, точнее сказать, описания степени или «серьезности» возможного финансового ущерба, который может быть нанесен коммерческому банку. При этом вводятся от трех до пяти градаций степени или уровня оцениваемого риска. Ниже приведена таблица определений уровней агрегированного риска, устанавливаемых в указанных источниках по двум «осям координат» – оценок уровней типичных банковских рисков и качества управления этими рисками (табл. 2.1).

---

[60] Guiding Principles in Risk Management for U.S. Commercial Banks.

[61] Large Bank Supervision; Community Bank Supervision. Comptroller's Handbook. EP-CBS. Office of the Comptroller of the Currency, Washington, DC, USA, July 2003.

Таблица 2.1
Оценки уровня агрегированного риска

Качество управления риском	Уровень риска		
	Низкий	Средний	Высокий
Низкое	«Умеренный»	«Высокий»	«Высший»
Удовлетво-рительное	«Низкий»	«Умеренный»	«Высокий»
Высокое	«Низший»	«Низкий»	«Умеренный»

В оригинале использованы понятия: Lowest, Low, Moderate, High, Highest

Для выбора подходящей оценки используются совокупности экспертных заключений по «параметрам» деятельности руководства кредитной организации по разным бизнес-направлениям, от которых зависят и состав подмножества источников, и влияние компонентов типичных банковских рисков[62].

Учет *всех* источников компонентов типичных банковских рисков при использовании кредитной организацией множественных систем электронного банкинга может оказаться невозможным в силу их разнообразия и сложности структур задействуемых ею ИКБД, ЛВС или ЗВС, что подразумевает чрезмерные затраты ресурсов этой организации. Вследствие этого ее руководство вполне может согласиться с существованием незначительных по уровню компонентов банковских рисков, потенциальный ущерб от реализации которых будет оцениваться в меньшую сумму, чем затраты на их мониторинг и парирование. В этом случае может оцениваться так называемый «чистый риск», определяемый как разница между неизбежным риском, присущим самой банковской деятельности, и корректирующим эффектом, достигаемым в рамках внутрибанковского мониторинга уровней типичных банковских рисков и УБР (в том числе сотрудниками служб внутреннего контроля и аудита).

Однако здесь следует проявлять известную осторожность: такой подход может быть оправдан только проведением тщательного анализа потенциальных последствий существования «остаточных рисков» в ИКБД. Следует, кстати, отметить возможность резкого роста *цены* любых, даже незначительных на первый взгляд, нарушений целостности банковских данных, которые могут лавинообразно тиражироваться в базах банковских данных и клиринговых системах. Важно отметить, что процедуры УБР осуществляются именно в отношении *источников* риска, а не самих рисков, поскольку в такой абстрактной формулировке

[62] *Лямин Л.В.* Принципы риск-ориентированного банковского контроля в области интернет-банкинга // Оперативное управление и стратегический менеджмент в коммерческом банке. 2003. № 5. С. 36 – 38; № 6. С. 35 – 49. Описанный подход справедлив для технологий электронного банкинга в целом.

исчезает физический смысл процесса, из-за чего и возникают разногласия между авторами публикаций по этой тематике.

Глава 3
Жизненные циклы банковских автоматизированных систем и внутрибанковских процессов

Все, что делалось до сих пор, было недоразумением.
С. Лем. «Звездные дневники Ийона Тихого»

Технологический и технический прогресс в сфере банковской деятельности, выражающийся во внедрении разнообразных технологий электронного банкинга, обусловливает тенденцию к их интенсивному развитию вследствие того, что:

■ удобство и оперативность получения банковских услуг, обеспечиваемые системами электронного банкинга, предполагают очень быстрое расширение клиентской базы ДБО и лавинный рост количества клиентских ордеров (на выполнение операций, получение информации и т.д.);

■ универсальные кредитные организации стараются охватить ДБО максимально возможное количество предлагаемых ими банковских услуг (с учетом ограничений, налагаемых законодательством и подзаконными актами, регламентирующими банковскую деятельность[63]);

■ условия конкуренции ориентируют кредитные организации на продолжение развития ДБО, внедрение новых его вариантов (многоканальных), предложение дополнительных видов банковских услуг и внедрение систем электронного банкинга, поддерживающих их предоставление.

Кроме этого, общий курс Правительства России на расширение обеспечения банковскими услугами населения страны, включая отдаленные регионы, будет одновременно способствовать внедрению и развитию все новых вариантов ДБО. Это в свою очередь потребует от высокотехнологичных кредитных организаций *углубленного* анализа потребностей своих реальных и потенциальных клиентов, меняющихся условий конкуренции, достоинств и недостатков банковских информационных технологий, а также сопутствующих им факторов и источников компонентов банковских рисков, которые подлежат учету во внутрибанковских процессах, начиная с процесса УБР.

Также следует отметить, что в Стратегии развития банковского сектора Российской Федерации на период до 2008 г. в качестве одной из основных задач было указано «развитие содержательных (риск-ориентированных) подходов, включающих оценку деятельности кредитных организаций и применение мер надзорного реагирования исходя прежде всего из содержания и реальной оценки рисков банковской деятельности с позиций их потенциального влияния на устойчивость кредитных организаций…» Решение этой задачи предполагало в том числе «совершенствование банковского надзора за деятельностью кредитных организаций… включая анализ рисков, возникающих у кредитных организаций в рамках взаимоотношений с юридическими и физическими лицами». В свою очередь в последние годы упомянутые взаимоотношения базируются и реализуются преимущественно на технологиях электронного банкинга, вследствие чего применение таких технологий стало требовать адекватного риск-ориентированного анализа[64].

---

[63] Например, в случае открытия банковского счета, оформления кредита, кассового обслуживания и др.

[64] *Лямин Л.В.* Анализ факторов риска, связанных с интернет-банкингом // Расчеты и операционная работа в коммерческом банке. 2006. № 5. С. 52 – 63; № 6. С. 43 – 54; № 7-8. С. 37-54.

Современные тенденции в развитии ДБО неизбежно окажут влияние на функционирование подавляющего большинства российских кредитных организаций, причем этот процесс на самом деле уже набирает силу, о чем свидетельствует статистика, получаемая по регламентной банковской отчетности[65]. Вследствие этого можно предположить, что технологии электронного банкинга начнут уже в ближайшем будущем превалировать на отечественном рынке финансовых услуг (подтверждением чему в свою очередь также стало широкое распространение разнообразных платежных систем и систем так называемых «электронных денег»), а значит, руководителям кредитных организаций скорее всего придется перестраивать свои бизнес-процессы с учетом этих перспектив. Впрочем, как будет показано ниже, это все равно практически необходимо для поддержания надежности и устойчивости[66] кредитных организаций, осваивающих ДБО, потому что его спецификой стали виды и способы *информационного* взаимодействия кредитных организаций с их клиентами в процессе банковского обслуживания наряду с новыми *условиями,* в которых это взаимодействие реализуется (имеется в виду ИКБД).

Сказанное выше относится к внесению изменений в любые банковские информационные технологии (в связи как с внедрением новых, так и с модификацией действующих). И дело здесь не только в электронном банкинге как таковом, но и, что не менее важно, в тех информационных системах, которые используются органами управления кредитной организации для принятия стратегических и тактических решений относительно предложения новых сервисов и расширения клиентской базы. Что касается именно ДБО, то применение соответствующих технологий предполагает прежде всего учет тех особенностей, которые сопутствуют или же могут сопутствовать их внедрению и применению в плане контроля над уровнями типичных банковских рисков. Для этого требуется понимание сути происходящего во вновь формируемом киберпространстве ИКБД вместе с организацией *управления* не всегда очевидными виртуальными процессами (а это изменение бизнес-модели как таковой) и обеспечением полноты, своевременности и адекватности *контроля* над использованием новых банковских информационных технологий и реализующих их автоматизированных систем.

Пересматривать внутрибанковские процессы при использовании технологий электронного банкинга целесообразно для того, чтобы управление и контроль, становящиеся в известной мере *специфическими,* во-первых, были явно ориентированы на технологии такого рода, во-вторых, оставались адекватны пруденциальным принципам банковской деятельности и, в-третьих, чтобы собственно банковская деятельность оставалась управляемой и подконтрольной. Принципиально важным является то, что, какими бы ни были технологические нововведения в банковской деятельности, они *не должны* оказывать негативного влияния на выполнение кредитными организациями банковских операций, равно как на надежность, устойчивость и безопасность этих организаций (в двояком смысле: как их самих, так и в отношении интересов их клиентов). То же самое относится и к защите интересов клиентов кредитных организаций, и к выполнению последними взятых на себя *конкретных* обязательств (доступность дистанционных сервисов, «обещанная» клиентам полнофункциональность, своевременность предоставления услуг, выполнение финансовых обязательств). Наконец, внедрение в банковскую практику тех или иных систем ДБО не должно приводить к нарушениям *полноты* и *целостности,* с одной стороны, функций внутреннего контроля в

[65] Это видно в первую очередь по данным, приводимым в формах банковской отчетности 0409070 «Сведения об использовании кредитной организацией интернет-технологий» и 0409251 «Сведения о счетах клиентов и платежах, проведенных через кредитную организацию (ее филиал)».

[66] По аналогии с упоминавшейся выше трактовкой понятия «надежность» устойчивость в традиционном понимании интерпретируется как способность восстанавливать свое состояние (режим) после какого-либо возмущения, проявляющегося в отклонениях значений параметров режима от исходных (начальных) значений (или от штатного функционирования).

кредитных организациях и аудита (как внутреннего, так и внешнего), с другой стороны, банковского (или в широком смысле – финансового) контроля над банковской деятельностью в киберпространстве.

Уместно отметить также существенные особенности в информационном обеспечении (или поддержке принятия) решений относительно внедрения и применения технологий ДБО. Зачастую представители высшего руководства кредитных организаций имеют достаточно отдаленное представление о том, как конкретно, технически реализуется «электронный банкинг» в каждом из уже достаточно многочисленных своих вариантов и как реализующие его процессы могут сказаться на результатах и эффективности банковской деятельности в целом. В итоге органы управления кредитной организации вынуждены работать в условиях отсутствия необходимой информации как о собственно той или иной технологии ДБО (а такая информация, как правило, вообще сложна для восприятия при отсутствии соответствующей ей специальной квалификации), так и о том, какие условия применения определенной технологии могут считаться *пруденциальными.* Очевидно, что дефицит информационного обеспечения управления кредитной организацией по этим двум главным вопросам может оказаться критическим для принятия эффективных решений, что особенно негативно может сказаться через далеко не всегда очевидные недостатки в организации и содержании УБР.

Результатом отмеченной неадекватности стало то, что внедрение технологий ДБО приводит к неконтролируемому, вообще говоря, смещению профилей ряда типичных банковских рисков, рассмотренных в предыдущей главе, и реализации их компонентов, связанной с нанесением ущерба кредитной организации и ее клиентам. При этом причины смещения профилей рисков, являясь преимущественно технологическими и организационно-техническими, оказываются далеко не всегда *очевидными* для специалистов в области банковского дела, а содержание смещений далеко не всегда *понятно* тем специалистам, которые отвечают за внедрение и развитие ИТ в кредитной организации (собственно за технологическое и техническое обеспечение банковской деятельности). Это первый из принципиально значимых квалификационных разрывов, которые негативно сказываются на технологической надежности кредитной организации при переходе ее к ДБО.

Здесь необходимо подчеркнуть, что в настоящее время без учета конкретных проявлений смещения профиля риска в условиях ДБО эффективное управление банковской деятельностью и контроль над ее осуществлением и результатами вряд ли возможны. Такой учет целесообразен в рамках процессного подхода в корпоративном плане, поскольку многие кредитные организации, как правило, поэтапно внедряют и одновременно (параллельно) используют по несколько достаточно разнородных, хотя и технологически схожих схем ДБО (интернет-банкинга, интернет-трейдинга, мобильного банкинга и т.п.), что предполагает также *комплексный* анализ влияния потенциально сопутствующих каждой из них негативных факторов (источников компонентов банковских рисков) на банковскую деятельность.

3.1. Процессный подход – базовые положения

Акцент на внутрибанковских процессах и на *условиях,* в которых они реализуются, не случаен: изучение использования кредитными организациями систем электронного банкинга свидетельствует, что результаты и эффективность применения новых, зачастую достаточно сложных технологий ДБО, которые базируются на распределенных компьютерных системах, сети Интернет, мобильных компьютеризованных устройствах, телекоммуникационных сетях и т.п., непосредственно зависят от условий, в которых технологии такого рода применяются. То же самое относится к парированию влияния источников банковских рисков, непосредственно связанных с такими способами обслуживания клиентов. Важно отметить также то, что при этом далеко не все руководители кредитных организаций осознают возможное влияние технологий ДБО на выполнение утверждаемых ими стратегических планов и поддерживаемые в этих организациях бизнес-модели, ибо новые технологии электронного банкинга способны *существенно* изменить условия их реализации, повышая уровни типичных банковских рисков. Поэтому при внедрении конкретного варианта ДБО целесообразно изначально определить его специфику именно из этих соображений, причем не просто как очередной новой технологии, реализуемой через компьютерные и телекоммуникационные системы нового поколения, но и переводящей банковскую деятельность в «виртуальное пространство» практически без каких бы то ни было ограничений. На этом целесообразно сделать акцент и при пересмотре подходов к модернизации процесса УБР, его описания и содержания, а также к распределению обязанностей и ответственности за его реализацию между исполнительными органами и рядом структурных подразделений кредитной организации, перечисляемых в параграфе 3.2.

Само отсутствие подобного учета может обусловить реализацию банковских рисков – вероятностных по сути событий – и обращение их в реальные финансовые потери, причем именно из-за неосознаваемого повышения этой вероятности (если в кредитной организации относятся к своим компьютерным технологиям без должного внимания). Поэтому руководству кредитной организации логично было бы при принятии решения о переходе к ДБО задумываться не только о ТЭО любого из возможных его вариантов (что само по себе в отечественном банковском секторе встречается нечасто), но и о ресурсной базе процесса УБР с точки зрения оценки ее достаточности. Не исключено, что ее негативная оценка окажется весомым аргументом в пользу либо отказа от такого решения, либо реализации его только после накопления *достаточных* ресурсов в части административных и организационно-технических решений, персонала подразделений кредитной организации, его совокупной квалификации и т.п. Впрочем, последние годы функционирования российского банковского сектора отмечены тенденцией как к повышению качества корпоративного управления в кредитных организациях, так и к поиску путей его дальнейшего совершенствования, что (как показывает и зарубежная практика) при использовании процессного подхода существенно облегчается.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.