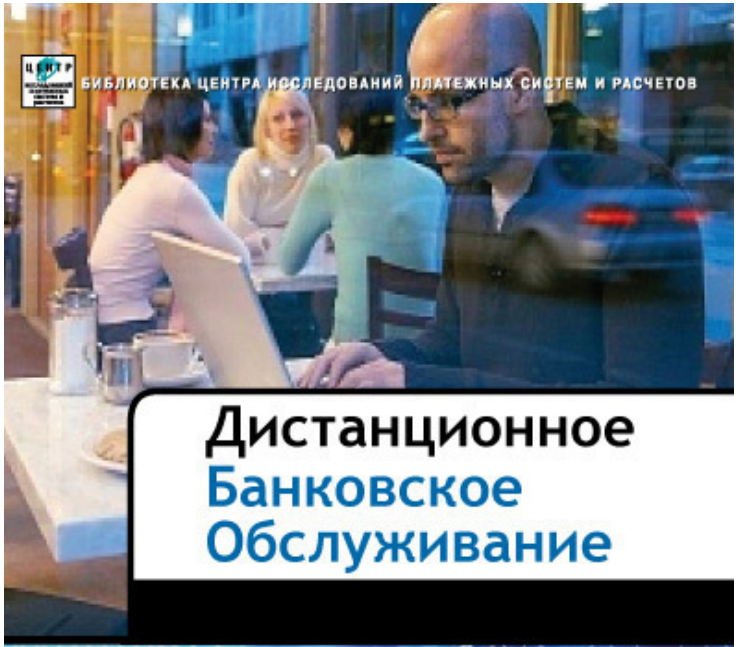

Дистанционное Банковское Обслуживание

КНОРУС

Коллектив авторов

Дистанционное банковское обслуживание

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=5019355
Дистанционное банковское обслуживание / кол. авторов.: КНОРУС : ЦИПСиР,; Москва; 2010
ISBN 978-5-406-00350-3

Аннотация

Банковское обслуживание стремительно приближается к потребителям, выходя за пределы банковских офисов. Очень большое количество финансовых продуктов и услуг можно получить, не посещая банк, а используя домашний компьютер, телефон или терминал около дома. Именно этому сегменту – дистанционному банковскому обслуживанию или дистанционному банкингу, посвящено данное издание. Книга охватывает почти все сегменты дистанционного банкинга, от традиционных систем клиент-банк, до инновационных продуктов, таких, как электронные деньги и наиболее популярные у населения устройства – платежные терминалы. Описаны способы продвижения, конкурентная ситуация, процедуры управления, взаимодействие с потребителями дистанционного банкинга, но при этом большое внимание уделено вопросам

безопасности, риск-менеджмента и регулирования этого перспективного рынка.

Можно с уверенностью утверждать, что данное издание является энциклопедией дистанционного банкинга.

Содержание

Дистанционное банковское обслуживание

Введение

Современный этап развития банковской деятельности в России, а это последние 10–12 лет, и в особенности начало XXI в., отмечен лавинообразным распространением технологий дистанционного банковского обслуживания (ДБО), объединяемых также понятием «электронный банкинг». Существует уже десятка полтора основных вариантов ДБО на основе различных телекоммуникационных систем или информационно-телекоммуникационных сетей, если использовать терминологию Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», начиная с многофункциональных банкоматов и POS-терминалов и заканчивая интернет-банкингом и технологиями мобильного банкинга, использующими беспроводной доступ к Всемирной сети посредством WAP-, SMS-, GPRS-, Wi-Fi– и т. п. «банкинга» [1]. Тенденция к трансформации банковской деятель-

[1] 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 карт. WAP

ности в немалой степени обусловливает усложнение ее содержания; отход от ее традиционной интерпретации как только совершения банковских операций и сделок неизбежно происходит вместе с внедрением кредитными организациями наиболее современных банковских информационных технологий, видов и способов предоставления банковских услуг. Именно виды и способы информационного взаимодействия кредитных организаций с их клиентами в процессе банковского обслуживания наряду с новыми условиями, в которых это взаимодействие реализуется, стали спецификой ДБО.

Одним из важнейших следствий распространения ДБО является необходимость совершенствования корпоративного управления в кредитных организациях, напрямую связанного с интенсивным внедрением новых технологий банковского обслуживания клиентов.

Возникновение дополнительных источников и факторов

(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 между собой, а также с информационными системами разного назначения. 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. WiFi *(Wireless Fidelity)* – обозначение некоторых типов беспроводных локальных вычислительных сетей (WLAN), в которых используются спецификации семейства 802.11.

банковских рисков вызывается внедрением информационных технологий, основанных на распределенных компьютерных системах, нередко использующих к тому же принципы «открытых систем» и универсальных протоколов сетевого и межсетевого взаимодействия. Поэтому при использовании технологий электронного банкинга в кредитных организациях, а особенно – банковских, целесообразно пересматривать внутрибанковские процессы с тем, чтобы управление и контроль в таких организациях, во-первых, были явно ориентированы на подобные технологии, во-вторых, оставались адекватны пруденциальным принципам банковской деятельности и, в-третьих, оставались эффективными. 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. То же самое относится и к защите интересов клиентов кредитных организаций и к выполнению последними взятых на себя конкретных обязательств (обеспечение доступности дистанционных сервисов, «обещанной» клиентам в договорах на обслуживание, полнофункциональности, своевременности предоставления услуг, информационной безопасности и т. д.). Наконец, внедрение в банковскую практику систем ДБО не должно приводить к нарушениям полноты и целостности функций внутреннего контроля в кредитных организациях и аудита (как внутреннего, так

и внешнего), равно как не должно создавать дополнительных проблем органам банковского (в общем случае – финансового) контроля.

Необходимо осознание того, что если содержание банковского дела с внедрением новых технологий банковского обслуживания в основном остается неизменным, то способы и условия осуществления банковской деятельности могут измениться в современных условиях радикально. В целом ряде случаев, как показывают исследования, проведенные за последние несколько лет в российском банковском секторе, для решения таких задач требуются и новые подходы, подкрепленные методологическими и организационно-техническими инновациями. Сегодня радикальные перемены назрели и в столь традиционно «консервативной» сфере, какой является банковский сектор. Наиболее серьезные изменения связаны с внедрением в практику управления и контроля банковской деятельности риск-ориентированного и процессного подходов, которым посвящен специальный раздел этой книги. Очевидной стала потребность в пересмотре парадигмы управления деятельностью кредитных организаций и контроля над ее осуществлением. Новые подходы позволяют наиболее успешно реализовать концепции клиент-ориентированного бизнеса и управления по целям (результатам) и являются эффективным средством решения стратегических задач, стоящих перед конкретным банком и банковской системой в целом.

Неизбежным следствием этих инноваций становится модернизация внутрибанковской деятельности, т. е. организация новых процессов и адаптация уже действующих к происходящим изменениям. Однако совершенно очевидно (и практика подтверждает это), что сама собой такая модернизация произойти не может. Вместе с принятием решения о переходе к ДБО целесообразно принятие адекватных мер по адаптации внутрибанковских процессов управления и контроля к новым условиям банковской деятельности. Для этого (как, впрочем, при внедрении любой новой технологии) требуется некая идеология, принятая на уровне кредитной организации в целом и реализуемая ее органами управления при каждом технологическом (и техническом) «перевооружении» организации. Это своего рода метапроцесс циклической адаптации основных внутрибанковских процессов, цикличность которой определяется темпами технологических и технических нововведений. В отсутствие соответствующего методологического подхода вновь внедряемые технологии могут неожиданно стать серьезной проблемой как для операционных и обеспечивающих подразделений кредитной организации, так и для ее руководства.

Изменение используемых кредитной организацией технологии банковского обслуживания требует радикальных инноваций сначала в «осознании» сути происходящего, а затем – в содержании и организации внутрибанковских процессов. При этом оказывается необходимой разработка со-

вершенно новых процессов, которых ранее просто не существовало. Безусловно, определяющим фактором при этом должно являться сохранение управляемости и контролируемости банковской деятельности, невзирая на ее переход в виртуальное пространство. Вопрос заключается в том, какие именно управленческие процессы необходимо разработать, внедрить, сопровождать и контролировать в таких условиях. Примером может служить целесообразность организации новых и адаптации действующих внурибанковских процессов при внедрении технологии интернет-банкинга: требуется целая совокупность новых внутрибанковских процедур только для того, чтобы организовать, сопровождать, вести, модернизировать и контролировать web-сайты, используемые кредитной организацией в качестве своих информационных, коммуникационных или операционных представительств в Сети. Причем состав этих процедур, их содержание и специфика различаются при размещении web-сайта в самой кредитной организации, на аппаратно-программных комплексах его разработчика, у интернет-провайдера и в других вариантах. То же самое можно сказать о внедрении технологий мобильного банкинга и мобильных платежей.

Эти проблемы в течение длительного времени не считались актуальными, поскольку компьютеризация банковской деятельности на системном уровне вообще не воспринималась как процесс превращения этой деятельности в преимущественно информационную. Причиной этого стал, вероят-

нее всего, принципиальный разрыв между привычным содержанием традиционной банковской деятельности и ее новыми формами, вызванными к жизни техническим прогрессом и конкуренцией в банковском секторе. Поэтому осознание значимости происходящих в этой деятельности перемен хронически запаздывало по сравнению с темпами внедрения в кредитных организациях информационных технологий и реализующих их автоматизированных систем, построенных на основе интернет-технологий).

Внедрение в финансовой сфере новых способов и условий осуществления банковской деятельности показало, особенно в последние годы, что профили риска кредитных организаций претерпевают существенное смещение вместе с переводом этой деятельности, как иногда говорят, в «киберпространство». Принципиальная причина этого заключается в невозможности для человека непосредственно наблюдать и контролировать процессы, происходящие в компьютеризованной среде. К сожалению, явление это общее, и общим же его следствием явились значительные ежегодные финансовые потери различных сообществ и граждан, обусловленные недостаточной надежностью различных компьютерных систем, инцидентами в сфере информационной безопасности и недостаточной квалификацией участников банковской деятельности, несовершенством ее технологического и технического обеспечения и другими подобными причинами.

Внедрение технологий электронного банкинга (практиче-

ски независимо от их общего количества и функциональных особенностей) требует изменений в организационно-штатной структуре кредитной организации. С приходом отрытых компьютерных систем требуется перераспределение ответственности, обязанностей, прав, полномочий, подконтрольности и подотчетности конкретных руководителей и исполнителей различных уровней в структуре организации. Это касается целого ряда специальных служб: прежде всего подразделения, отвечающего за информационные технологии и (или) автоматизацию, внутренний контроль, обеспечение информационной безопасности и финансовый мониторинг. Перемены охватывают и документарное обеспечение их деятельности. Такие изменения инициируются, как правило, органами управления организации и реализуются соответствующими (достаточно специфическими) внутрибанковскими процессами и процедурами.

На сегодняшний день полнота, адекватность и качество бизнес-процессов в кредитной организации фактически начинают определяться новым принципом: «знай свои технологии»[2]. Без преувеличения можно сказать, что большинство внутрибанковских процессов реализуется в современных условиях не столько персоналом кредитной организации, сколько ее внутрибанковскими автоматизированными системами. Да и сам банк с точки зрения собственно выполнения банковских операций «и других сделок», о которых

[2] По аналогии с принципами «знай своего клиента» и «знай своего работника».

сказано в ст. 5 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности», в значительной своей части представлен теперь не зданием с соответствующей вывеской и персоналом, а банковской автоматизированной системой (БАС) и хранилищем данных, доступ к которым обеспечивают как раз системы ДБО. В такой ситуации банк оказывается не более чем «кирпичным интерфейсом» для клиента, служащим для оформления и инициации доступа к автоматизированной системе, которая, собственно, и выполняет все банковские операции «и другие сделки» (причем не обязательно в самой кредитной организации). Мало того, и сам доступ клиент осуществляет, выступая фактически в роли «операциониста», работающего с этой автоматизированной системой удаленно, что радикально меняет и характер взаимодействия кредитной организации с ним, и состав так называемых «зон ответственности» кредитной организации, и ее «периметр безопасности». Эти наблюдения тем более справедливы, что по состоянию на февраль 2009 г. многие кредитные организации применяют от двух до десяти систем ДБО различного или вариативного функционального назначения.

Сказанное относится к внесению изменений в любые банковские информационные технологии (внедрение новых или модификация действующих). Дело здесь не только в технологиях электронного банкинга, но и, что не менее важно, в тех информационных системах, которые используются орга-

нами управления кредитной организации для принятия решений. Что касается технологий именно ДБО, то их применение предполагает прежде всего учет тех особенностей, которые сопутствуют или же могут сопутствовать их внедрению и применению, начиная с понимания сути происходящего во вновь формируемом виртуальном пространстве вместе с организацией управления не всегда очевидными процессами взаимодействия с клиентами (а это – изменение бизнес-модели как таковой) и заканчивая полнотой, своевременностью и адекватностью контроля над использованием новых технологий. Недостаточное осознание этой специфики может привести к возникновению проблем у кредитной организации в случаях массового дистанционного обслуживания с применением так называемой «сквозной обработки» *(straight-through processing)* при необходимости выявления «на лету» операций, подлежащих обязательному контролю (так называемых «подозрительных») и т. п.

Новые опасности связаны с использованием высоких технологий, в том числе и электронного банкинга, для противоправной деятельности. Достаточно напомнить, что в последние три года за нарушения законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма более ста отечественных кредитных организаций лишились лицензий на осуществление банковских операций, что явно свидетельствует о смещении профиля риска кредитной организации

и о том, что оценки кредитного, рыночного и других рисков, принимаемых ею, уже никого не интересуют. При этом любая кредитная организация, дистанционно предоставляющая банковские услуги, может оказаться вовлеченной в подобную противоправную деятельность только из-за того, что ее руководство недостаточно адекватно представляет себе возможные осложнения при использовании новых технологий.

Уместно отметить такие 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 реализуется «электронный банкинг» в каждом из уже достаточно многочисленных своих вариантов и как реализующие его процессы могут сказаться на итогах и эффективности банковской деятельности в целом. В результате органы управления кредитной организации не имеют необходимой информации как о собственно той или иной технологии ДБО (а такая информация, как правило, 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 вопросам может оказаться критическим для приня-

тия эффективных решений.

В результате внедрение технологий ДБО стало приводить к неконтролируемому смещению профилей ряда типичных банковских рисков – операционного, правового, репутационного, ликвидности (который ввиду специфики денежного обращения в условиях ДБО преобразовался в риск неплатежеспособности[3]) и стратегического. При этом причины смещения профилей рисков оказываются далеко не всегда очевидны для специалистов в области банковского дела, поскольку являются в основном технологическими и техническими, а содержание смещений далеко не всегда очевидно для технических специалистов, отвечающих за технологическое и техническое обеспечение. Поэтому 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 нередко используют одновременно несколько достаточно разнородных, хотя и технологически схожих систем ДБО (интернет-банкинг, интернет-трейдинг, мобильный банкинг и т. п.), что предполагает также комплекс-

[3] Наиболее явно этот риск проявляется в тех случаях, когда клиенты кредитной организации оказываются перед неработающим банкоматом, сообщающим, что «к сожалению, обслуживание невозможно» или «с вашим банком нет связи».

ный анализ влияния потенциально сопутствующих каждой из этих систем ДБО негативных факторов (источников риска) на банковскую деятельность кредитных организаций.

Практически любая система ДБО представляет собой своего рода «виртуальные ворота» к информационно-процессинговым ресурсам кредитной организации. Поэтому система ДБО должна гарантировать уверенность, что доступ к ресурсам имеет только, и исключительно, легитимный (известный, официально зарегистрированный) клиент или другой пользователь (оператор), действующий в рамках строго определенных для него прав и полномочий. Как показывает практика, без понимания этого уровни банковских рисков, принимаемых на себя кредитной организацией, могут неоправданно повышаться.

Акцент на внутрибанковских процессах и на среде, в которой они реализуются, не случаен. Результаты банковского надзора в области электронного банкинга свидетельствуют, что эффективность применения сложных современных технологий банковского обслуживания, основанных на распределенных компьютерных системах, сети Интернет, мобильных компьютерных системах и т. д., равно как и парирование новых, связанных непосредственно с такими способами обслуживания клиентов кредитных организаций факторов банковских рисков, непосредственно зависит от условий, в которых применяются указанные технологии. Тем более что, как свидетельствует практика, далеко не все кредитные ор-

ганизации осознают и учитывают возможное влияние технологий ДБО на принимаемые и поддерживаемые ими бизнес-модели и стратегические планы. Отсутствие такого учета может обусловить воплощение банковских рисков в реальные финансовые потери (если в кредитной организации относятся к своим компьютерным технологиям без должного внимания).

В условиях всеобщей компьютеризации банковской деятельности велика опасность образования разрывов в общих процессах управления и контроля кредитной организации, использующей разные варианты ДБО, каждому из которых сопутствуют те или иные специфические источники и факторы риска. При этом как состав, так и содержание управленческой информации, которая может потребоваться на разных уровнях менеджмента кредитной организации, зачастую определяется применяемыми банковскими технологиями. Изменения во внутрибанковских процессах и составляющих их процедурах неразрывно связаны с внедрением новых технологий банковской деятельности. В еще большей степени это верно для применения технологий электронного банкинга и реализующих их банковских автоматизированных систем.

1. Классификация технологий дистанционного банковского обслуживания

1.1. Классификация электронного банкинга по технологиям предоставления услуг

Дистанционное банковское обслуживание (дистанционный банкинг) можно разделить по клиентскому сегменту на две категории:

1) розничный дистанционный банкинг *(consumer-banking*), ориентированный на обслуживание физических лиц;

2) корпоративный дистанционный банкинг *(business-banking*), ориентированный на обслуживание корпоративных клиентов (юридических лиц).

Обе эти категории используют сходные или аналогичные условия предоставления дистанционных банковских услуг по технологии доступа и по оператору их предоставления. Услуги дистанционного банкинга как в России, так и в остальном мире предоставляются не только банковскими ор-

ганизациями, несмотря на наличие слова «банкинг». Вообще термин «дистанционный банкинг», например С GAP, трактуется более широко, чем предоставление дистанционных услуг банком. Например, как «инновационное использование информационных и коммуникационных технологий для предоставления финансовых услуг посредством каналов, альтернативных традиционным банковским филиалам и банкоматам»[4]. Более того, мировой опыт показывает, что лидерами большинства проектов мобильного банкинга являются операторы сотовой связи, а не финансовые учреждения. В свою очередь это подтверждает и российский опыт в сфере так называемых «электронных денег»[5], а также в развитии сетей платежных терминалов, где лидерами выступают организации, не являющиеся банками. Хотя при этом и электронные деньги, и получение возможности проводить платежи через терминалы можно отнести к услугам дистанционного банкинга.

В этой связи дистанционное банковское обслуживание можно разделить по оператору предоставления услуг:

- банковский дистанционный банкинг;
- небанковский дистанционный банкинг.

---

[4] Building Financial Systems for the Poor. Международный опыт применения дистанционного банкинга: Первые итоги. Ольга Томилова, С GAP, Всемирный Банк, Москва, 20 ноября 2008 г., Российский Микрофинансовый Центр: VII Ежегодная конференция.

[5] В законодательстве Российской Федерации отсутствует понятие электронных денег.

Дистанционный банкинг можно разделить на две категории по характеру предоставления услуг, в зависимости от того, ведет ли использование системы к выполнению финансовой транзакции или нет. Эта классификация представлена на рис. 1.1.

Рис. 1.1. Структура дистанционного банкинга

Информационный банкинг направлен на предоставление пользователям финансовой информации, например получение выписки, получение информации о последних операциях, SMS-информирование о каждой транзакции и т. п. Транзакционный банкинг позволяет проводить финансовые транзакции, в результате которых происходит зачисление или списание реальных денежных средств, например платежи, переводы со счета или без открытия счета, управление счетом и т. п.

1.1.1. Информационный банкинг

Информационный банкинг может быть классифицирован по технологии предоставления услуг. Наиболее часто можно

встретить пять основных каналов получения пользователем информации, хотя на самом деле их может быть больше, все ограничено только возможностями банка или иной финансовой организации (рис. 1.2).

Рис. 1.2. Виды информационного банкинга

SMS – наиболее часто встречающаяся технология предоставления клиенту финансовой информации. Мобильный телефон стал действительно повсеместно используемым устройством, а самое главное, он всегда находится у клиента. Обычно посредством SMS передается информация о выполнении (невыполнении) финансовой транзакции, а также другая информация, не требующая подробного описания, так как эта технология технически ограничена небольшим количеством символов.

E-mail – эта технология обычно сопровождает финансовые услуги, предоставляемые посредством сети Интернет. Посредством электронного письма можно передавать практически любую информацию о финансовых услугах, и что немаловажно – представлять ее в более «красивом виде». Но при этом, в связи с огромным количеством спама, не факт,

что клиент получит и прочитает письмо, а не удалит его как очередную рекламную рассылку.

Интернет – наиболее интерактивный вид информационного банкинга, позволяющий, в отличие от других, обеспечить обратную связь с клиентом в режиме онлайн. В свою очередь эта технология информационного банкинга разделяется на *общедоступную* финансовую информацию (услуги, тарифы, условия обслуживания и т. п.) и *персональную* финансовую информацию (остаток счета, выписка по счету и т. п.). В этой связи для предоставления клиенту персональной информации требуется его идентификация на сайте, что чаще всего происходит путем присвоения клиенту логина и пароля, посредством которых он получает доступ в «личный кабинет», где ему предоставляется нужная информация.

Телефон – так же, как и SMS, – наиболее доступный вид информационного банкинга для любых клиентов, но в отличие от последнего намного менее удобный и более затратный. Посредством звонка в call-центр клиент может получить как общедоступную финансовую информацию (услуги, тарифы, условия обслуживания и т. п.), так и персональную (остаток счета, информацию о проведенных операциях и т. п.). Так же, как и для предыдущей технологии, получение доступа к персональной информации требует идентификации клиента, что достигается обычно с помощью пароля. В свою очередь технология предоставления информационного банкинга посредством телефона может предполагать как ис-

пользование автоматического режима, так и беседу с оператором.

Доставка бумажного документа, несмотря на явный архаизм технологии и ее дороговизну, остается достаточно востребованной. Многие клиенты просят присылать им ежемесячные выписки по почте, организации присылают по почте информацию о новых услугах и тарифах. В отличие от SMS или электронного письма классический бумажный конверт является более весомым инструментом взаимодействия с финансовой организацией.

1.1.2. Транзакционный банкинг

Транзакционный банкинг также может быть классифицирован по технологии предоставления услуг, основные из которых представлены на рис. 1.3.

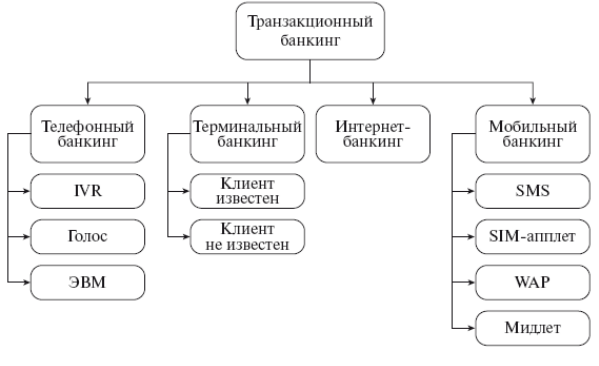

Рис. 1.3. Виды транзакционного банкинга

С точки зрения технологии предоставления услуг можно выделить четыре вида дистанционного банкинга: телефонный банкинг, терминальный банкинг, интернет-банкинг, мобильный банкинг.

Телефонный банкинг – предоставление дистанционных финансовых услуг посредством обычного телефонного подключения. Несмотря на то что в качестве клиентского устройства может выступать мобильный телефон, эта технология все равно остается телефонным банкингом до тех пор, пока не используются специфические технические решения, свойственные мобильному банкингу, о чем будет рассказано далее. Телефонный банкинг также подразделяется по технологии организации взаимодействия на три основные составляющие.

IVR (interactive voice response) – интерактивная информационная система, используемая для обработки обращений клиентов. Функционал IVR позволяет как предоставлять информацию в режиме реального времени, так и производить обработку команд (распоряжений) клиентов. Инструментом введения команд, как правило, является кнопка тонового набора на телефонном аппарате. Нажатие определенных комбинаций клавиш в режиме тонового набора позволяет вводить цифровые команды в ответ на голосовые подсказки системы дистанционного телефонного обслуживания.

Голос (голосовой банкинг) – устаревшая система взаимо-

действия финансовой организации и клиента, предполагающая «живой» диалог. В то же время продолжается ее использование во многих организациях, наиболее часто клиент может ее встретить при блокировке утерянной платежной карты. Для идентификации клиента в большинстве случаев используется словесный пароль, называемый клиентом и проверяемый оператором, также могут использоваться и дополнительные идентификаторы, например данные документа, удостоверяющего личность, адрес и т. п. Для большей защиты от несанкционированного доступа клиент может быть ограничен телефонным номером, с которого он может дать распоряжение банку. Номер проверяется автоматическим определителем номера или обратным звонком оператора клиенту. Еще буквально десяток лет назад, до развития интернет-трейдинга, этот вид дистанционного обслуживания был практически единственным для работы на фондовом рынке, и клиенты отдавали распоряжения своим брокерам по телефону.

ЭВМ (системы «клиент – банк») – еще один вид дистанционного обслуживания, теряющий свои позиции под напором интернет-технологий, в частности проигрывая интернет-банкингу. Системы «клиент – банк» предполагают прямую связь компьютера клиента и сервера банка, например, посредством модемной связи. С развитием широкополосного доступа в Интернет клиенты в массовом порядке переходят на системы интернет-банк. Так как системы «кли-

ент – банк» в основном используют юридические лица, а их пользователями выступают бухгалтерские подразделения, во многом достаточно консервативные, это дает возможность системам «клиент – банк» существовать еще какое-то время. Эти системы продолжают достаточно активно использоваться в регионах, где широкополосный доступ в Интернет пока еще не стал стандартом. В целом проблемы с внедрением разнообразных форм дистанционного банковского обслуживания скорее субъективны, что подтверждается исследованиями НАФИ (телефонное интервью в 22 городах-миллионниках по 2500 предприятиям малого и среднего бизнеса, из которых 55 % относятся к сфере малого бизнеса). С результатами опроса можно ознакомиться на рис. 1.4[6].

[6] Национальное агентство финансовых исследований. Опрос «Пользование и удовлетворенность услугами ДБО предприятиями малого бизнеса», проведенный в июле – сентябре 2008 г.

Рис. 1.4. Отношение к использованию ДБО со стороны 2500 предприятий малого и среднего бизнеса

Терминальный банкинг – вид дистанционного банкинга, наиболее широко используемый населением. Трудно встретить человека, который хоть раз не оплачивал мобильную связь через платежные терминалы. Эти устройства расставлены по территории России уже сотнями тысяч и добрались туда, где нет и в ближайшее время не будет банковских отделений. Сейчас на рынке со значительным отрывом преобладают небанковские платежные терминалы, хотя многие банки начинают собственные проекты по установке устройств самообслуживания. При этом банки часто ориентируются не на простейшие устройства, позволяющие произвести платеж наличными за различные услуги, а устанавливают многофункциональные банкоматы. Такие банкоматы позволяют получить наличные по карте, обменять валюту, осуществить различные платежи как наличными, так и с помощью платежной карты, отправить перевод с карты на карту и т. п.

Клиент известен (произведена предварительная идентификация клиента) – эта разновидность дистанционного банкинга чаще всего используется банками в устройствах самообслуживания и предполагает наличие счета клиента в банке и идентификацию владельца счета. В этом случае клиент при помощи своей идентификационной карты, роль которой может выполнять и обычная платежная карта, и спе-

циального ПИН-кода получает доступ к управлению счетом. Наличие карты не является обязательным условием, так как клиент может иметь только логин и пароль для доступа к управлению счетом. То, что клиент идентифицируется банком, позволяет ему не только управлять своим счетом, но и осуществлять платежи, внесенные наличными деньгами, по различным адресам, в том числе вводя произвольные банковские реквизиты. Также клиент может обменять практически любые суммы иностранной валюты, выполнить денежные переводы в пользу других физических лиц и произвести другие финансовые операции. Клиент, чья идентификация не была произведена, ограничен в операциях согласно п. 1.1 и 1.2 ст. 7 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон о противодействии легализации доходов, полученных преступным путем):

«1.1. Идентификация клиента – физического лица, установление и идентификация выгодоприобретателя не проводятся при осуществлении организациями, осуществляющими операции с денежными средствами или иным имуществом, операций по приему от клиентов – физических лиц следующих платежей, если их сумма не превышает 30000 рублей либо сумму в иностранной валюте, эквивалентную 30000 рублей:

1) связанных с расчетами с бюджетами всех уровней бюджетной системы Российской Федерации (включая предусмотренные законодательством Российской Федерации о налогах и сборах федеральные, региональные и местные налоги и сборы, а также пени и штрафы);

2) связанных с оплатой услуг, оказываемых бюджетными учреждениями, находящимися в ведении федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления;

3) связанных с осуществлением платы за жилое помещение, коммунальные услуги, с оплатой услуг по охране квартир и установке охранной сигнализации, а также с осуществлением платежей за услуги связи;

4) связанных с уплатой взносов членами садоводческих, огороднических, дачных некоммерческих объединений граждан, гаражно-строительных кооперативов, оплатой услуг платных автомобильных стоянок;

5) связанных с уплатой алиментов.

1.2. При осуществлении физическим лицом операции по покупке или продаже наличной иностранной валюты на сумму, не превышающую 15 000 рублей либо не превышающую сумму в иностранной валюте, эквивалентную 15 000 рублей, идентификация клиента – физического лица, установление и идентификация выгодоприобретателя не проводятся, за исключением случая, когда у работников организации, осу-

ществляющей операции с денежными средствами или иным имуществом, возникают подозрения, что данная операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма».

Клиент неизвестен (не произведена предварительная идентификация клиента) – большинство платежей в платежных терминалах производится без идентификации клиента. Учитывая, что подавляющее большинство операций – это пополнение счета мобильного телефона на сумму около 100 руб., такая ситуация не вызывает удивления. Как было указано ранее, без идентификации клиента можно производить достаточно ограниченный круг операций, хотя небанковские сети платежных терминалов с успехом обходят такого рода ограничения.

Интернет-банкинг – наиболее интересный сегмент дистанционного банкинга, позволяющий производить практически неограниченный спектр безналичных операций; к этому же сегменту можно отнести все системы электронных денег на базе интернет-сетей. Родоначальником систем интернет-банков являются системы «банк – клиент», которые первоначально были в основном предназначены для корпоративных клиентов. На компьютере пользователя устанавливалось специальное программное обеспечение, которое имело связь с банком, например, по модему. Интернет-банк в ос-

новном используют технологию «тонкого» клиента, т. е. для работы с этой программой достаточно стандартного браузера и любого компьютера в любой точке мира, подключенного к Интернету. Благодаря использованию этой технологии себестоимость удаленного обслуживания стремится к нулю, и системы интернет-банков используются в настоящее время не только юридическими лицами, но и частными клиентами. Как правило, для пользования интернет-банкингом пользователю необходимо иметь логин и пароль, а также компьютер для доступа в Интернет.

Мобильный банкинг – этот вид дистанционного банкинга, учитывая количество мобильных телефонов на руках населения, по праву может считаться наиболее перспективным на текущий момент. Найти сейчас человека, не имеющего мобильного телефона, так же трудно, как и не видавшего телевизор. Мобильная связь проникла во все уголки России, произведя телефонизацию всей страны. Но несмотря на это пока телефоны в своей основной массе используются для передачи голосового трафика, все остальные услуги, за исключением, пожалуй, SMS, занимают незначительную долю. Мобильный телефон в качестве терминала для доступа к дистанционным банковским услугам используется в четырех основных технологиях:

SMS (SMS-банкинг) позволяет проводить финансовые транзакции посредством команд, переданных при помощи SMS. Это наиболее простая система, совместимая со все-

ми моделями телефонов и работающая везде, где есть мобильная связь. При этом для клиента использование SMS-банкинга не самая удобная форма доступа к финансовым услугам из-за необходимости набирать большой объем текстово-цифровой информации, а также запоминать условные обозначения команд.

SIM-апплет – при использовании этого вида дистанционного банкинга платежное приложение записывается непосредственно на SIM-карту телефона и позволяет достаточно безопасно производить финансовые транзакции. Для использования этой технологии клиенту необходимо предварительно приобрести новую SIM-карту с установленным платежным приложением.

Мидлет – платежное JAVA-приложение, работающее в памяти мобильного устройства и позволяющее проводить финансовые транзакции в защищенном режиме. В отличии от предыдущей технологии менять SIM-карту не нужно, но при этом JAVA-приложение работает не на всех моделях мобильных телефонов.

WAP – по сути это интернет-банкинг для мобильного устройства, так как позволяет получить доступ к интернет-сайту финансовой организации, адаптированному для отображения на небольшом экране мобильного телефона. Работа с этим сайтом аналогична обычному интернет-банкингу с помощью компьютера.

Классифицировать все технологии дистанционного бан-

кинга практически невозможно из-за их постоянного развития и быстрого появления новых технологий. Развитие технологий вызывает изменение традиционных видов предоставления банковских услуг, а также появление инновационных как по форме, так и по сути финансовых продуктов.

1.2. Анализ применения технологий дистанционного банковского обслуживания

В III квартале 2008 г. Банк России провел анкетирование кредитных организаций по вопросам применения технологий дистанционного банковского обслуживания[7].

По данным, подготовленным Департаментом банковского регулирования и надзора и опубликованным Департаментом внешних и общественных связей Банка России, в анкетировании участвовали 1090 кредитных организаций из 77 регионов России. Результаты анкетирования свидетельствуют о том, что на практике применяются около 20 вариантов организации дистанционного банковского обслуживания. При этом различные технологии электронного банкинга используют 1042 кредитные организации (95,6 % принявших участие в анкетировании, т. е. абсолютное большинство). Не применяют ДБО только 48 кредитных организаций (4,4 %).

Подавляющее большинство кредитных организаций при-

---

[7] Анкетирование проводилось на основании п. 76 «Стратегии развития банковского сектора Российской Федерации на период до 2008 года», принятой Правительством РФ и Центральным банком РФ, и на основании письма Банка России от 1 августа 2008 г. № 94-Т в продолжение работы по созданию системы мониторинга использования кредитными организациями современных технологий дистанционного банковского обслуживания (ДБО).

меняют широкий спектр технологий электронного банкинга. В 743 организациях (77,4 %) в эксплуатации находятся от 2 до 5, а в 71 (6,5 %) – от 6 до 10 разновидностей систем ДБО. Распределение кредитных организаций по числу таких технологий приводится на рис. 1.5.

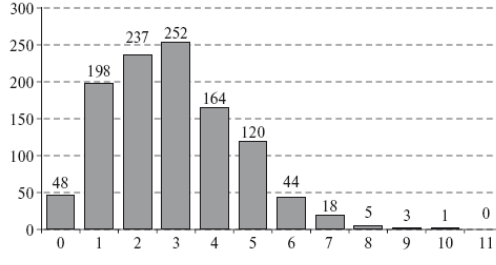

Рис. 1.5. Распределение кредитных организаций по количеству используемых ими технологий дистанционного банковского обслуживания

Наибольшее распространение получили следующие варианты ДБО (рис. 1.6):

– с использованием систем «банк – клиент» – 1023 организации (94 %);

– с использованием систем денежных переводов без открытия банковского счета – 713 организаций (65 %);

– с применением программно-технических устройств, предназначенных для осуществления операций с использованием платежных карт, – 632 организации (58 %).

Что касается использования web-сайтов, то, по данным

регламентной банковской отчетности (форма 0409070), кредитные организации используют в своей банковской деятельности от 2 до 12 web-сайтов различного функционального назначения, ориентированных также на различные группы клиентов (юридических или физических лиц, осуществляющих операции интернет-банкинга и с ценными бумагами, пользователей мобильного банкинга через портативные средства компьютерной связи – палмбуки или карманные персональные компьютеры, мобильные телефоны, коммуникаторы и т. п.).

Рис. 1.6. Результаты I этапа анкетирования кредитных организаций по вопросу применения технологий ДБО

2. Дистанционное предоставление банковских услуг

2.1. Интернет-банк

Дистанционное банковское обслуживание через Интернет, или так называемый интернет-банкинг (ИБ), появившееся в российском банковском секторе более десяти лет назад, стало сегодня одним из наиболее интересных и динамичных современных направлений развития банковских технологий. За последние годы ИБ превратился в средство массового удаленного предоставления банковских услуг российскими кредитными организациями. Вместе с этим в несколько раз выросло как число организаций – разработчиков специализированного программно-информационного обеспечения (ПИО) ДБО, так и количество внедренных ими такого рода проектов. При этом целый ряд кредитных организаций реализовал собственные проекты, в том числе систем ИБ.

Направление интернет-банкинга появилось и начало развиваться с 1995 г. в США. Его возникновение было обусловлено преимущественно действующими в этой стране ограничениями на открытие коммерческими банками своих филиалов в разных штатах. Первым коммерческим банком, ко-

торый начал обслуживать своих клиентов через Сеть, был *Security First Network Bank*. Эта идея довольно быстро нашла отклик в Европе, а затем банковский интернет-сервис появился и в Российской Федерации. Это произошло в 1997 г. благодаря Гута-банку, хотя внедренная этой кредитной организацией система интернет-трейдинга еще не представляла собой полнофункциональное ДБО. Следующим лидером среди коммерческих банков в области клиентского интернет-обслуживания с 1998 г. стал Автобанк, так что указанный год можно считать отправным для ИБ. Дальнейший лавинообразный рост числа систем ИБ и пользующейся этой технологией клиентуры кредитных организаций привел к введению Банком России специальной формы банковской отчетности 0409070 и дополнению данными о ДБО формы 0409251. По данным первой из этих форм, количество программно-информационных комплексов ИБ росло быстро, и очень скоро рынок «насытился»: общее число таких комплексов достигло 100[8] и начиная с 2006 г. незначительно колеблется около этого значения (1–2 системы теряют популярность, вместо них появляется столько же или чуть больше новых), что отражено на рис. 2.1 (два значения слева получены, соответственно, из публикаций средств массовой информации и по данным сплошного анкетирования, про-

[8] Около половины из них разработаны самими кредитными организациями (т. е. являются совершенно уникальными), остальные – различными компаниями, действующими на рынке банковского программного обеспечения.

водившегося Банком России в 2001 г.):

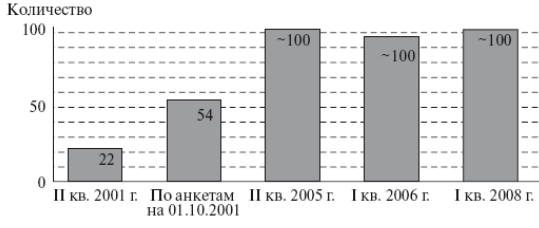

Рис. 2.1. Динамика количества программных комплексов интернет-банкинга в российских кредитных организациях

В настоящее время число кредитных организаций, внедривших и внедряющих у себя этот вид обслуживания, перевалило за 950 (с учетом тех, которые не используют для предоставления услуг ИБ специализированные web-сайты), их число тоже не постоянно, поскольку время от времени некоторые из организаций теряют лицензию на осуществление банковских операций или проходят процедуры слияния с другими кредитными организациями, другие же вводят эту технологию в конкурентной борьбе и т. п. Количество клиентов ИБ для разных кредитных организаций варьируется очень широко: от нескольких сотен до 200 тыс., но в целом эта разновидность ДБО стала совершенно типичной для российского банковского сектора. Что касается общемировой практики, то, по оценкам зарубежных экспертов, к 2020 г. в Западной Европе 60 % клиентов кредитных организаций будут пользоваться технологией ИБ (сейчас это зна-

чение характерно в среднем только для наиболее «продвинутых» коммерческих банков), а в США этот уровень уже достигнут.

Российские кредитные организации достаточно долго экспериментировали с разными формами оперативного удаленного банковского обслуживания, которые объединялись понятием «*on-line banking*». Как эксперименты, так и стационарное обслуживание осуществлялись преимущественно в «закрытых системах», в которых клиенты коммерческих банков получали доступ к банковским функциям при помощи так называемых «толстых клиентов» (специализированных программно-информационных модулей, устанавливаемых на персональные компьютеры клиентов), телефонного набора или разновидностей кабельных соединений. Любые системы такого рода неизбежно и существенно «ограничивают» реальную и потенциальную клиентскую базу кредитных организаций. Для доступа к нужной кредитной организации клиентам, находящимся вне региона ее дислокации, приходится либо становиться абонентами конкретной кабельной системы, либо оплачивать телефонные счета за дистанционные соединения; кроме того, несмотря на применение современных технологий банковского обслуживания, к которым относится и ДБО, кредитные организации вынуждены при этом на самом деле проявлять индивидуальный подход к каждому клиенту.

В настоящее время в области удаленного автоматизиро-

ванного или компьютеризованного банковского обслуживания можно наблюдать следующие четыре тенденции:

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

• сочетание возможностей корпоративного и розничного банковского обслуживания;

• создание корпоративных систем и модульная технология *Plug-and-Play*;

• комбинация в системах ДБО возможностей «толстого» и «тонкого» клиента.

Развиваясь в этих направлениях, кредитные организации рассчитывают расширить как состав и способы предоставления банковских услуг, так и клиентуру ДБО.

Основными факторами, действующими в условиях применения технологии ИБ и повышающими уровни банковских рисков и смещающими их профили для кредитных организаций, являются:

1) «виртуальный» характер дистанционных банковских операций;

2) общедоступность «открытых» телекоммуникационных систем;

3) чрезвычайно высокая скорость выполнения транзакций;

4) глобальные масштабы межсетевого операционного взаимодействия;

5) участие фирм-провайдеров в проведении операций;

6) возможность скрытой противоправной деятельности в Интернете.

Очевидно, что при изучении и анализе рисков, связанных с банковской деятельностью в современных технологически насыщенных условиях, необходимо учитывать все компоненты среды, через которые проходят банковские данные кредитной организации и информация ее клиентов. Каждый из этих компонентов в той или иной мере может оказаться фактором риска.

При общем развитии и распространении интернет-технологии как таковой клиенты кредитных организаций могут воспользоваться значительным числом банковских услуг – от получения выписок по счетам до совершения большинства расчетно-платежных, конверсионных и фондовых операций в любом месте мира, причем используя всего лишь ПИО самого «тонкого клиента», какой только возможен при ДБО, т. е. интернет-браузера. Чтобы получить доступ к компьютерной сети какой-либо кредитной организации, в настоящее время требуется только автоматизированное рабочее место (персональный компьютер), с которого можно выйти в Сеть. В итоге Интернет стал представлять собой такую обеспечивающую технологию, которая сделала банковские услуги и обслуживание доступными для огромного числа клиентов кредитных организаций и устранила барьеры, обусловленные географическим положением, фактором времени и правами собственности на телекоммуникационные системы.

При наличии такого расширенного рынка отечественные кредитные организации могут получить весьма широкие возможности распространения или модификации своих услуг и предложений, а также значительного сокращения затрат на обслуживание своей филиальной сети и административных расходов. Технологические затраты, правда, при этом возрастают, но считается, что они могут быстро окупиться: еще на начальных этапах исследований применения технологии ИБ предполагалось, что эти затраты будут снижаться (менее 1 цента на транзакцию), и это подтвердилось. Сейчас некоторые кредитные организации предлагают своим VIP-клиентам услуги ИБ бесплатно (скорее, правда, условно-бесплатно).

В то же время выяснилось, что технология ИБ изначально придает отношениям между банком и клиентом своеобразную анонимность, поскольку фактически клиент работает с банком виртуально. К сожалению, следствием этого явились факты противоправного использования технологии ИБ для легализации доходов, полученных незаконным путем, совершения других экономических преступлений, а также для финансирования деятельности террористических организаций.

За последние 2–3 года в материалах зарубежных органов банковского надзора и в средствах массовой информации появился целый ряд публикаций по этой тематике. Для отмывания денег, как выясняется, по всему цивилизованно-

му миру фактически используются технологии электронного банкинга с учетом предоставляемых ими анонимных возможностей. В последние 5—б лет в зарубежных публикациях, относящихся к сфере финансового контроля, отмечается, что неизбежное отставание законодательной базы от практики, регулирующей новые интернет-технологии и финансово-технические, если можно так выразиться, инструменты, создает идеальные условия для их незаконного использования в целях отмывания денег. Этому способствует то обстоятельство, что многие электронные платежные инструменты отличаются предельно высокой скоростью транзакций, анонимностью, сочетаемостью с другими платежными системами, обеспечиваемой всемирными телекоммуникационными системами глобальностью и автоматизированностью, применением так называемых «безлюдных» технологий.

Перечисленные особенности снижают эффективность традиционных методов борьбы с отмыванием денег в виде требования предоставления банку определенной информации, отслеживания и анализа содержания операций, а также установления личности клиента и, на чем принято делать акцент в последнее время, выгодоприобретателя. Технология ИБ оказалась привлекательной для многих мошенников, так что кредитные организации, не обеспечивающие адекватного контроля за использованием систем ИБ, рискуют оказаться вовлеченными незаметно для самих себя в противоправ-

ную деятельность. Надо отметить, что во всем мире в борьбе с незаконным использованием автоматизированных систем предоставления финансовых услуг делаются попытки адаптации существующих методов и процедур к электронной торговле и платежным инструментам, например устанавливаются требования увеличения объема необходимых данных (особенно при карточных операциях), обеспечения доступа к источникам клиентской информации, комплексного анализа ДБО через разные телекоммуникационные сети, а также совершенствуются методы проведения расследований, «интернационализируется» банковский контроль и т. д.

Очевидно, что проблемы противоправного использования кредитных организаций, например, в качестве «механизмов» отмывания денег не новы, и технологии ДБО лишь обеспечили новый «транспорт» для этого. Однако руководству кредитных организаций целесообразно адекватно учитывать новые факторы риска такого рода при внедрении и развитии ИБ.

Проведенные исследования свидетельствуют, что можно определить три основные разновидности или варианта ИБ, которые реально применяются в настоящее время, различаются масштабом и содержанием банковской деятельности с использованием Интернета, а также составом компонентов типичных банковских рисков, которые сопутствуют применению кредитными организациями технологии ИБ. В основном этот состав определяется наличием (или отсутствием)

непосредственных, физических связей между используемыми web-ресурсами и банковской автоматизированной системой (БАС) кредитной организации.

В число наиболее распространенных вариантов ИБ входят следующие.

1. Информационный вариант – это базовый уровень ИБ. В обобщенной терминологии электронных банковских систем ему соответствуют так называемые системы 1-го уровня. Как правило, кредитная организация при этом дает на обособленном сервере маркетинговую информацию относительно банковских услуг и обслуживания, свои реквизиты, тарифы и пр. Соответствующий совокупный риск считается относительно низким, поскольку БАС кредитной организации обычно не имеет непосредственной связи с таким сервером, и внутренняя вычислительная сеть этой организации недоступна для проникновения извне. В то же время соответствующий сервер или web-сайт может оказаться уязвимым для внешних воздействий прежде всего в части нарушения его функционирования, намеренного искажения, уничтожения представляемой на нем информации или размещения антирекламы, информации, негативно влияющей на имидж кредитной организации (сомнительных баннеров или ссылок на порносайты и т. п.). Поэтому руководству кредитной организации целесообразно предусмотреть внедрение эффективных средств контроля для предотвращения таких несанкционированных воздействий.

2. Коммуникационный вариант описывается как использование «банковской электронной системы» 2-го уровня, что позволяет реализовать некоторые виды информационного взаимодействия между БАС кредитной организации и ее клиентами. В зависимости от состава сетевых связей такое взаимодействие может быть ограничено электронной почтой, запросами форм документов и справок о счетах, заявками на ссуды, обновлением стандартных файлов (изменение реквизитов клиента и т. д.). Сопутствующий риск при такой конфигурации выше, чем в первом случае, уже только из-за возможного наличия непосредственных физических связей между web-ресурсами и БАС кредитной организации, равно как и увеличения числа технических средств, вовлекаемых в процесс предоставления банковских услуг. Поэтому кредитной организации требуются адекватные средства контроля для предотвращения и мониторинга любых попыток неавторизованного доступа к своим внутренним сетям и компьютерным системам и вирусного контроля, а также оповещения руководства о таких попытках и принятия парирующих мер.

3. Операционный (или транзакционный) вариант реализуется системами 3-го уровня, позволяющими клиентам опосредованно или непосредственно (при автоматизированной работе с бэк-офисом) выполнять транзакции. Поскольку при этом обычно существуют физические связи систем ИБ с внутренней вычислительной сетью кредитной организации или обслуживающего ее провайдера, такой архитектуре со-

путствует наивысший риск (наиболее сложный состав источников риска), и поэтому должны существовать адекватные средства контроля, учитывающие все угрозы, возникающие в отношении этой организации и интересов ее клиентуры. Одновременно требуются сложные средства обеспечения защиты и безопасности информации, выявления и контроля источников рисков, оповещения руководства о подозрительных действиях и неблагоприятных ситуациях, а также развитые планы действий на случай чрезвычайных обстоятельств.

Потенциальные угрозы для кредитных организаций и их клиентов существуют во всех перечисленных вариантах, почему и не следует при анализе факторов и источников банковских рисков ограничиваться только операционными составляющими ИБ (что типично). Чем сложнее состав технических средств, с помощью которых осуществляется обслуживание клиентов, и разнообразнее используемые каналы прохождения информации (включая системы провайдеров), тем больше источников риска, связанных с различными информационными системами, приходится учитывать при выявлении, оценивании, анализе банковских рисков и организации управления ими.

Это не означает, что банковское обслуживание через Интернет заведомо связано с повышенными рисками для кредитных организаций и их клиентов – просто необходимо четко представлять себе тот информационный контур банковской деятельности (ИКБД), который формируется каж-

дой системой ИБ, возможные источники рисков, связанные с ним, и подход к управлению типичными банковскими рисками, требуемый в каждом конкретном случае для обеспечения полного контроля над смещением профиля риска кредитной организации, применяющей такую технологию электронного банкинга. В зависимости от конкретного варианта реализации источники риска могут варьироваться; базовыми факторами при этом являются организация:

• внутрибанковского процесса обеспечения ДБО в части рабочих процедур и распорядительных документов;

• отношений с клиентами кредитной организации, пользующимися системами ИБ, на основе договоров на ДБО;

• взаимодействия с клиентами ДБО через «киберпространство» (виртуальное пространство Сети и БАС);

• обеспечения информационной безопасности в отношении отдельных систем ИБ или в их комплексе;

• внутреннего контроля над применением технологии ИБ, включая осуществление финансового мониторинга;

• отношений с провайдерами, от которых зависит надежность ДБО через Интернет;

• выявления, оценки, мониторинга источников специфических банковских рисков, специфических для ИБ, и управления ими[9].

---

[9] По этому вопросу см. письмо Банка России от 31 марта 2008 г. № 36-Т «О Рекомендациях по управлению рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга».

Упрощенная структура ИКБД ИБ показана на рис. 2.2.

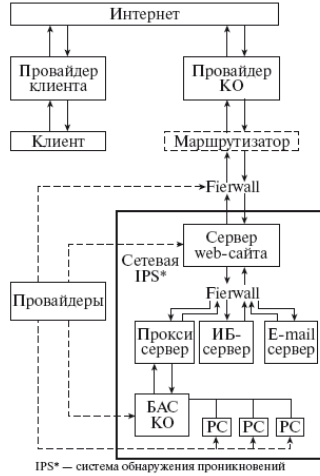

Рис. 2.2. Обобщенное представление структуры информационного контура банковской деятельности (ИКБД)

Одним из важных аспектов ИБ является организация web-сайтов, которые нередко используются как своего рода «виртуальные ворота» к информационно-процессинговым ресурсам кредитной организации. С точки зрения общепринятых требований органов банковского надзора (как за рубежом, так и в России) любые информационные материалы, публикуемые кредитными организациями, в том числе в Сети, должны способствовать формированию у реальных и потенциальных клиентов этих организаций полного и точно-

го представления о характере, показателях и специфике деятельности этих организаций[10]. Фактически при переходе к ИБ для создания, ведения и сопровождения используемых web-сайтов в кредитной организации целесообразно сформировать и в дальнейшем, по мере развития ДБО адаптировать специальный внутрибанковский процесс[11]. Это следует делать во избежание появления дополнительных источников (компонентов) правового и репутационного рисков, связанных с возможными неточностями маркетинговой информации и несоответствием требованиям законодательства, касающимся защиты прав потребителя.

Последнее непосредственно относится к организации web-сайтов и web-порталов, используемых в банковской деятельности. Оформление и распределение информации на web-страницах, фреймах, баннерах и посредством гиперссылок должно быть четким и однозначным, не оставляющим

[10] Полная регламентация порядка создания, архитектуры и содержания web-сайтов кредитных организаций невозможна и не нужна, но, исходя из необходимости защиты интересов клиентов кредитных организаций, в том числе потенциальных, и повышения «транспарентности» этих организаций, Банк России пришел к заключению о необходимости подготовки Указания оперативного характера от 3 февраля 2004 г. № 16-Т «О Рекомендациях по информационному содержанию и организации web-сайтов кредитных организаций в сети Интернет» (в настоящее время подготовлена к выпуску его новая редакция).

[11] Подробно об этом и других аспектах процессного подхода к применению технологий электронного банкинга см.: *Лямин А.В.* Процессный подход к применению технологий электронного банкинга с позиций риск-фокусированного надзора/ Управление в коммерческом банке. 2006. № 6. С. 83–94; 2007. № 1. С. 57–68; № 2. С. 66–74; № 3. С. 53–70.

сомнений в источниках и условиях предоставления услуг.

Не менее важна правильная организация так называемых «демилитаризованных зон», изолирующих БАС кредитной организации и ее внутреннюю сетевую структуру (локальную или зональную вычислительную сеть) от внешней сетевой среды, равно как и их административно-технического обеспечения. Для этого специалистам кредитной организации необходимо разрабатывать модели угроз, которые могут быть связаны с технологией ИБ, и сценарии их возможного развития. Это в свою очередь требует анализа архитектуры каналов информационного взаимодействия, которые в общем случае начинаются с сетевых экранов (брандмауэров), web-серверов и прокси-серверов. Речь идет как о сохранении конфиденциальности банковской и клиентской информации, так и о защите от хакерских, крэкерских, фишерских, фармерских и т. п. атак[12], а также от проникновения вирусных программ, которых сегодня развелось великое множе-

[12] Соответственно, речь идет о несанкционированном проникновении в локальные вычислительные сети кредитных организаций, взломе их компьютерных систем (с целенаправленным разрушением средств защиты, баз данных и пр.), перехвате данных персональной идентификации и фальсификации доменных имен с целью совершения хищений финансовых средств со счетов клиентов (пользователей Интернета) и др. Количество web-сайтов, с которых можно свободно «скачать» программное обеспечение для взлома компьютерных систем, атак на организации и их клиентов, а также получить информацию о недостатках в защитных средствах операционных систем, прокси-серверов, сетевых экранов и т. п., исчисляется многими тысячами (по информации web-сайта www.antiphishing.org, знакомство с содержанием которого полезно специалистам кредитных организаций).

ство. Поэтому грамотно составленная и реализованная политика информационной безопасности, включающая антивирусное направление, в кредитных организациях (с доведением соответствующих требований и до клиентов, обслуживаемых дистанционно) стала необходимым условием обеспечения надежности современной банковской деятельности.

Наконец, если говорить о наиболее важных технологических и технических аспектах надежности банковской деятельности в целом, следует помнить, что современная кредитная организация полностью зависит от надежности своих распределенных компьютерных систем и от надежности аналогичных систем своих провайдеров. Очевидно, что прерывание ДБО «по техническим причинам», нарушение функциональности (или искажение контента) web-сайта, с которым взаимодействует клиент, могут вызвать негативную общественную реакцию в отношении ИБ и ДБО. Поскольку абсолютно надежных компьютерных и телекоммуникационных систем не существует, специалистам кредитных организаций (включая службы информатизации, безопасности, внутреннего контроля и др.) целесообразно организовать, реализовать и при необходимости адаптировать следующие внутрибанковские процедуры:

• оценку и расчет характеристик надежности используемого аппаратно-программного обеспечения (АПО) ИБ, включая сегменты ИКБД, находящиеся вне самой организации (каналы связи, маршруты взаимодействия с клиентами,

каналы ДБО и пр.);

• резервирование АП О и массивов банковских и клиентских данных (в части как «горячего», так и «холодного» резервов[13]) с учетом необходимости перехода на резервные каналы взаимодействия с клиентами и восстановления («отката») сеансов связи в рамках ИБ;

• тестирование функциональности, надежности, защищенности и устойчивости АП О ИБ как кредитной организации, так и ее провайдеров, включая планы действий при чрезвычайных обстоятельствах, возможную компрометацию АПО, а также хранение и восстановление сеансовой информации.

Весь комплекс надежности целесообразно оценивать в направлениях выполнения кредитной организацией своих обязательств перед клиентами, контролирующими и правоохранительными органами, начиная с документарного обеспечения банковской деятельности по ДБО в рамках ИБ, положений о подразделениях кредитной организации, имеющих какое-либо отношение к его обеспечению[14], и заканчивая

---

[13] Имеются в виду такие разновидности резервирования, при первой из которых резервные системы (серверы, автоматизированные рабочие места, устройства копирования данных и т. п.) работают одновременно с основным оборудованием (в «горячем» режиме), а при второй – резервное оборудование выключено, так что для его инициации требуется некоторое время (прогрев, загрузка программного обеспечения, считывание резервных массивов данных и т. д.).

[14] Это следующие основные подразделения кредитной организации: информационных технологий (ИТ или информатизации автоматизации), внутреннего контроля, обеспечения информационной безопасности, финансового монито-

должностными инструкциями ответственных менеджеров и исполнителей, непосредственно управляющих применением технологии ИБ и контролирующих использование соответствующих автоматизированных систем.

Важным аспектом является учет взаимной анонимности кредитной организации и ее клиента, возникающей при ДБО через Интернет, поскольку для идентификации и аутентификации сторон чаще всего используются средства аналогов собственноручной подписи. Недостатки в организационно-техническом и программноалгоритмическом обеспечении применения таких средств могут негативно сказаться на формировании доказательной базы и обеспечении юридической силы «электронных документов», гарантий невозможности отказа от операции (с обеих сторон), предотвращении возможной противоправной деятельности и управлении рисками банковской деятельности, принимаемыми на себя как кредитной организацией, предлагающей услуги ИБ, так и ее клиентами. Руководству и специалистам кредитной организации следует учитывать накопленный за годы применения технологии ИБ в банковском секторе негативный опыт мошенничеств и хищений с помощью систем ДБО, осложняемый недостатками в организации и содержании претензионной работы с клиентами ИБ.

ринга (в рамках внутреннего контроля или как обособленное), правового обеспечения, предоставления корпоративных и (или) розничных услуг, сервис-центр. Конкретный состав определяется структурой кредитной организации и распределением ответственности в ней в части поддержки ИБ.

Специфика сетевого взаимодействия в условиях открытых информационных систем (к которым относится и интернет-взаимодействие) предполагает учет дополнительных факторов риска, связанных с широко распространенным хакерством. Под такого рода учетом понимается организация и адаптация ряда специализированных внутрибанковских процедур, относящихся к основным внутрибанковским процессам и подразделениям, ответственным за их реализацию, а именно:

• выявление недостатков в организации и содержании внутрибанковских процессов (как следствие прежде всего неполной их адаптации к новым банковским информационным технологиям);

• выявление недостатков во внутрибанковских документах (обусловленных отставанием соответствующей регламентации от развития ИБ) по всей иерархической структуре кредитной организации;

• выявление и принятие мер по парированию новых угроз в ИКБД ИБ (в том числе за счет отслеживания «успехов» хакерского сообщества и приемов противоправной деятельности);

• выявление и оперативная замена АП О и ПИО, «пробитых» хакерами (а также другими «деклассированными» элементами, действующими в киберпространстве Интернета);

• выявление недостатков в работе провайдеров, входящих в ИКБД ИБ (в части несоответствия требуемому уровню об-

служивания и в плане коррекции недостатков в организации контрактных отношений[15]).

Процедурами управления и тщательного контроля в кредитной организации, предоставляющей услуги ИБ, желательно охватывать[16]:

- дизайн, контент и хостинг web-сайтов;
- конфигурацию сетевых экранов;
- системы предотвращения и обнаружения вторжений[17];
- сетевое администрирование;
- управление информационной безопасностью;
- сервер ИБ;
- прикладное программное обеспечение (расчетов, платежей и пр.);
- внутренние серверы;
- АПО бэк-офиса;
- служебное ПИО;
- автоматизированные системы поддержки принятия ре-

---

[15] В российском банковском секторе уже накоплено немало примеров, связанных с проблемами функционирования АП О провайдеров разного рода, из-за чего оказывалось невозможным выполнение кредитными организациями своих обязательств перед клиентами, с сетевыми атаками через системы провайдеров или их пассивностью в содействии парирования таких атак на кредитные организации, несоответствием уровня обслуживания и т. п.

[16] E-Banking. IT Examination Handbook, Federal Financial Institutions ExaminationCouncil. Washington, DC, USA, August 2003.

[17] *Intrusion Prevention System* (IPS) и *Intrusion Detection Systems* (IDS), размещаемые как в локальной вычислительной сети, так и на хостах кредитной организации.

шений[18].

Все эти компоненты фактически входят в единый ИКБД, обеспечивающий ДБО в рамках ИБ (несмотря на то что часть из них входит также и в другие информационные контуры в кредитной организации, связанные между собой разнообразными информационными сечениями), и каждый из них следует охватить внутрибанковскими процедурами управления и контроля. Помимо этого все «чувствительные» к возможному переходу в нештатные режимы функционирования компоненты (что может быть обусловлено отказами или сбоями АПО и ПИО кредитной организации, вирусными атаками, несанкционированным доступом, ошибками персонала и клиентов и т. п.), должны быть упомянуты в таких внутрибанковских документах, как «Положение об управлении рисками банковской деятельности», «Положение об информационной безопасности» и «Положение о внутреннем контроле» (о системе или службе внутреннего контроля).

Несмотря на кажущуюся сложность внедрения и применения технологии ИБ, практика свидетельствует, что при правильной организации внутрибанковских процессов и составляющих их процедур удается исключить влияние подавляющего большинства факторов и источников банковских рисков, сопутствующих применению технологии ИБ как таковой. Для российских условий типичными банковскими рисками, которые характеризуются наличием компонентов

[18] Иногда называемые также информационными системами управления (ИСУ).

технологического и технического характера, являются следующие пять рисков: стратегический, операционный, правовой, репутационный и ликвидности (неплатежеспособности).

За рубежом, где в составе банковской деятельности могут допускаться варианты взаимодействия с клиентами, отличные от указанных условий (например, дистанционное открытие банковских счетов с установленным интервалом идентификации, ряд операций кредитования и др.), учету, как правило, подлежат все типичные банковские риски[19]. В то же время очевидно, что выгоды от применения технологии ИБ намного выше, чем затраты как на первичное внедрение соответствующего АП О и адаптацию внутрибанковских процессов, так и на хеджирование сопутствующих компонентов банковских рисков (и их возможную последующую компенсацию в случае реализации). Наилучшим свидетельством наличия этих достоинств является широкое распространение технологии ИБ в российском банковском секторе.

[19] См., например: Internet Banking, Comptroller's Handbook, I–IB, Office of the Comptroller of the Currency, Washington, DC, October 1999.

2.2. Мобильный банк: теоретические возможности и практическая необходимость

Разговор о мобильном банкинге должен начаться с определения терминологии. На практике очень часто встречаются словосочетания «мобильный банкинг» и «SMS-банкинг». Если с мобильным банкингом все более или менее понятно, – это предоставление банковских услуг через мобильный телефон, то под SMS-банкингом некоторые банковские специалисты подразумевают только информационные сервисы – SMS-уведомления, а др. – и активные операции со стороны клиента (запросы информации, SMS-команды на совершение операций). Единой трактовки этого термина пока не сложилось. Понятие SMS-банкинга правильнее использовать в том случае, если интерфейсом взаимодействия клиента с банком являются SMS-команды и SMS-сообщения, которые клиент сам читает и набирает. Таким образом, SMS-банкинг – это просто технически более простая и для клиента менее удобная концепция обслуживания с использованием мобильного телефона. Мобильный же банк – это более общее понятие. Мобильный банк может взаимодействовать с клиентом с помощью как SMS, так и специального программного интерфейса мобильного телефона, который орга-

низует более удобное представление информации, иерархию меню и поддерживает связь с банковским сервером посредством любого канала (SMS, GPRS, Wi-Fi, транспорт тут не принципиален) или отображение специализированного сайта (WAP).

Какие же технические реализации мобильного банка существуют и чем они отличаются?

1. *SMS-банкинг,* в рамках которого все взаимодействие с клиентом строится на уровне SMS-сообщений. SMS-банкинг может быть *пассивным,* когда клиенту предоставляются только информационные сервисы (информация о совершенных операциях, начисленных процентах, информирование об истечении срока действия договора, карты и т. п.), и *активным,* когда посредством SMS-команд клиент может совершать какие-то операции (запрашивать информацию, проводить платежи и т. п.). Технически это самая простая реализация мобильного банка, которая совместима совершенно со всеми мобильными телефонами, и все доработки касаются только серверной части банка, которая должна уметь отправлять, получать и соответствующим образом обрабатывать SMS-команды. К ее достоинствам стоит отнести и то, что SMS-банкинг будет работать везде, где работает сам мобильный телефон. Активные операции через SMS-банкинг для клиента неудобны, так как ему нужно запоминать и правильно набирать условные наименования команд (например: *Inf* – информация по счету, *pay* – оплатить) и их реквизиты

(номер счета, сумму, валюту и т. п.). Чтобы облегчить клиенту жизнь, можно построить интерактивную систему взаимодействия с клиентом, в рамках которой на любую неправильную SMS-команду клиенту будет возвращаться сообщение с полным списком команд в системе, а в случае частичного набора команды система будет сама додумывать ее за клиента (например, сообщение <P> или <PA>, при условии, что в системе нет других команд, начинающихся с этой буквы однозначно может идентифицироваться как <PAY>, а в случае если есть несколько команд, начинающихся с этих символов, клиенту будет отправлен список этих команд для уточнения).

2. *SIM-апплет* – это приложение, записанное непосредственно на SIM-карту. Первоначально записывать приложения непосредственно на SIM-карту могли только в момент ее выпуска, и для того чтобы прописать апплет на старую карту, необходимо ее заменить в офисе оператора. Сейчас стали появляться карты, на которые апплеты можно загружать в любой момент, в том числе дистанционно. SIM-апплет позволяет обеспечить наиболее серьезную криптографию, но использование этой технологии сдерживается тем, что владельцам старых SIM-карт необходимо их физически заменить.

3. *Мидлет* – загружаемое приложение на JAVA, которое функционирует в памяти мобильного телефона так же, как игры или программки типа ICQ-клиента JIMM, Яндекс-кар-

ты и т. п. Преимуществом этой технологии является достаточно высокая совместимость с различными моделями телефонов (но не стопроцентная, например, знаменитый iPhone до сих пор не поддерживает JAVA, а на некоторых моделях телефонов могут все-таки возникать проблемы с запуском приложения) и независимость от SIM-карт.

4. *WAP-сайт* – специальным образом кастомизированный для отображения на маленьком экране телефона интернет-сайт. Просмотр его осуществляется встроенным браузером телефона.

SIM-апплеты и мидлеты в качестве транспорта могут использовать любой канал – SMS, GPRS/EDGE. GPRS/EDGE-транспорт является предпочтительным для клиента, так как обеспечивает передачу большего объема информации за меньшие деньги. Однако при этом нужно учитывать особенности тарификации операторами сотовой связи услуги передачи данных. Например, компания МТС округляет любой пакет обмена данными до 100 КБ и поэтому множественные короткие соединения получаются крайне затратными, кроме того, даже при отсутствии трафика тарифицируется каждый час соединения, так что долго поддерживать связь без обмена данными также не имеет смысла. В роуминге МТС округляет уже до 60 КБ, которые стоят 30 руб., т. е. практически на порядок дороже. Поэтому приложение мобильного банка, использующее этот канал, должно иметь настройки, позволяющие пользователю задавать параметры разрыва

соединения и возможность ограничения услуги в роуминге. Также стоит отметить, что WAP-трафик стоит дороже, чем обычное GPRS-соедининение.

В настоящее время на рынке представлены реализации мобильного банка как интегрированные с различными банковскими системами (процессинговые системы, автоматизированные банковские системы), так и независимые, которые по крайней мере потенциально интегрируются с любыми банковскими системами. Независимые приложения наиболее интересны, так как продуктовый ряд большинства банков разнесен по нескольким банковским системам, разработанным зачастую разными производителями (карточная система, розничная банковская система, кредитный бэкофис), с которыми мобильный банк должен взаимодействовать, чтобы обеспечить клиентам максимальный набор сервисов. Из независимых приложений стоит отметить следующие реализации:

• компания «Интервейл» (www.intervale.ru), на технологиях которой построены проекты Сбербанка РФ, Народного Банка Казахстана, МТС-Pay. В качестве транспорта апплеты «Интервейл» используют SMS, которые проходят через сервер компании и основная стоимость этой технологии для банка определяется именно тарификацией SMS-трафика клиентов, а не приобретением собственно сервера приложений и лицензий на количество апплетов. Решения «Интервейл» могут использовать технологию безопас-

ной аутентификации 3D-Secure международных платежных систем VISA и MasterCard;

• продукт BARS (Bank Remote Service) компании «Оникс-Капитал» (www.oncsoft.com), который базируется на JAVA-мидлете и использует в качестве транспорта GPRS;

• мобайл-клиент от компании BSS (www.bssys.com), базирующийся на JAVA-мидлете и использующий GPRS. Также BSS предлагает специальные версии клиентов для КПК и смартфонов и WAP-банкинг. Из интересных особенностей стоит отметить приложение MobiPass для генерации аналога собственноручной подписи с помощью мобильного телефона.

Достаточно часто банки с сильной IT-командой идут по пути собственной разработки мобильного банка.

При выборе технологической платформы для реализации мобильного банкинга стоит обратить внимание на унификацию идентификации клиента в системах мобильного банка и интернет-банка. Не стоит усложнять клиенту жизнь и заставлять его запоминать два комплекта идентификаторов и паролей.

Теоретически мобильный банк может предоставить клиенту все те возможности, которые предоставляет и интернет-банк. Мобильный телефон накладывает ограничения на предоставление информации для клиента, связанные с небольшим экраном телефона, поэтому сложные или объемные экранные формы необходимо специальным образом оп-

тимизировать, масштабировать, разбивать, переносить. Работа с клавиатурой телефона также далеко не так комфортна для клиента, как с клавиатурой компьютера, но в принципе позволяет ввести все те же символы. Однако на практике самой востребованной услугой мобильного банкинга является SMS-информирование – им пользуются сотни тысяч, если не миллионы клиентов российских банков. Банкиры, реализовавшие полноценный мобильный банк с управлением счетами и платежами, часто жалуются, что клиенты еще не готовы к его использованию – они немногочисленны и используют лишь малую часть предлагаемых им возможностей системы мобильного банковского обслуживания.

В современных условиях оптимальный набор услуг с помощью мобильного телефона выглядит примерно следующим образом:

• *SMS-информирование:* это не только сообщения картхолдерам о совершенных транзакциях, но и возможность, по желанию клиента, получать информацию о зачислении средств на текущие счета, начислении процентов по вкладам, работе длительных поручений (регулярные платежи и переводы), информации о кредитной задолженности, завершении срока действия различных договоров (карта, депозит, ячейка и т. п.);

• *запросы в банк:* это может быть заявка на перевыпуск карты в ответ на уведомление об окончании срока действия карты, просьба предоставить информацию по продуктам или

детальную информацию о конкретном продукте или просьба call-центру банка связаться с клиентом;

• *платежи и переводы:* вот тут стоит крепко задуматься над объемом предоставляемых услуг, чем больше свободы мы предоставляем клиенту в совершении активных операций, тем сложнее и дороже как система обеспечения безопасности, так и интеграция с другими банковскими системами.

Сомнительно, что кому-то из клиентов банка действительно нужно оперировать ценными бумагами, открывать договора или совершать сложные и разнообразные платежи именно с помощью мобильного телефона. С мобильного телефона имеет практический смысл совершать какие-то неотложные операции, а для всех остальных случаев существует интернет-банк, который клиенту уже привычнее (его пользователей гораздо больше, чем пользователей мобильного банка, хотя и не так много, как хотелось бы), несравненно удобнее в использовании и защищеннее. Трудно себе представить ситуацию, в которой кому-то нужно срочно оплатить коммунальные услуги, открыть депозит или купить (продать) акции. Эти операции всегда терпят несколько часов, до того времени, как человек попадет на работу, домой, в интернет-кафе и совершит их через интернет-банк. Владельцы ноутбуков благодаря технологиям мобильного Интернета и активно развивающимся беспроводным сетям вообще не привязаны к какому-либо месту и практически в

любой момент могут выйти в Интернет и совершить необходимые операции, тем более что сейчас появился целый класс сверхкомпактных ноутбуков, так называемых нетбуков, которые не только имеют малые габариты и низкий вес, но и дешевы (зачастую дешевле самого простого смартфона). Для особо нетерпеливых существуют смартфоны (доля которых на рынке устройств для мобильной связи неуклонно растет). Задача банка заключается только в том, чтобы адаптировать сайт интернет-банка для использования через небольшие экраны смартфонов и не добиваться обязательной аутентификации, требующей подключения к компьютеру различных токенов.

Набор платежей, которые у среднестатистического человека может возникнуть потребность сделать неотложно, достаточно ограничен, это:

• пополнение баланса телефона не только своего, но и чужого, например: необходимо срочно связаться с абонентом, номер которого отключен за неуплату, или пополнить телефон членов семьи, друзей. Даже без серьезной криптографии риски при совершении таких операций минимизируются лимитами и тем, что в конце концов получатели средств известны – в базе оператора есть данные всех абонентов;

• пополнение счета у интернет-провайдера, который отключил за неуплату домашний Интернет;

• перевод денег между своими (!) счетами. Это актуально в ситуации, когда человек в магазине вдруг захотел ку-

пить что-то дорогостоящее, а денег на карте не хватает и он переводит на нее часть средств с депозита. В случае новых кризисов можно представить себе ситуацию, когда паникующий клиент по нескольку раз на дню переводит деньги между разновалютными счетами, пытаясь догнать колебания валютных курсов;

• очевидно, возможны еще несколько видов платежей, которые действительно актуально делать срочно и именно в режиме реального времени: для таких случаев можно предусмотреть возможность создания шаблонов платежей, которые сам клиент сможет создавать через интернет-банк или в отделении банка.

Все эти сервисы можно реализовать и на технологии SMS-банкинга. Таким образом, выбранная технология реализации мобильного банкинга скорее вопрос удобства использования для клиента и стоимости взаимодействия, чем функциональной наполненности сервиса.

Отдельно стоит упомянуть о сервисах мобильного банкинга, которые с середины 2008 г. запустили крупнейшие российские сотовые операторы: «МТС-Pay» от МТС, «Мобильный платеж» от Билайна и «Мобильные платежи» от Мегафона. Сервисы Билайна и Мегафона практически идентичны и позволяют совершать платежи с лицевого счета абонента который можно пополнить (в том числе автоматически, при снижении баланса) с банковской карты. МТС предлагает более «продвинутый» сервис, в рамках которого все

операции совершаются со счета банковской карты, зарегистрированной в системе. По сути, сотовые операторы вступили в конкуренцию с банками, предоставляя своим клиентам банковские услуги (платежи и переводы), и, возможно, в дальнейшем проникновение сотовых операторов в платежные технологии будет только увеличиваться – в мировой практике уже есть реализованные проекты, в которых сотовый телефон служит средством совершения платежей в торговых точках. Банки, если они не хотят потерять этот рынок, должны активно участвовать в развитии своих технологий мобильного обслуживания.

Если попытаться заглянуть в будущее мобильного банковского обслуживания, то технологический прогресс, очевидно, в недалеком будущем приведет к смыканию продуктового ряда смартфонов и нетбуков. Функции мобильного телефона и мобильного компьютера сольются в одном удобном для пользователя устройстве. В этом случае уже сейчас близкие по своей сути каналы обслуживания (мобильный банк и интернет-банк) сольются в единую сущность. Эта тенденция должна учитываться при проектировании системы мобильного банковского обслуживания.

2.3. Мобильный банкинг-банковская практика

При рассмотрении вопроса о переходе параллельно с другими технологиями ДБО к мобильному банкингу или независимо от них нельзя забывать, что потенциальные клиенты любого нового варианта ДБО – это люди, привыкшие к использованию наличных денег, поэтому для перехода на новый вид обслуживания им необходимо убедиться не просто в том, что оно «работает», но в том, что оно лучше привычных схем платежей. Безусловными признаками такого обслуживания являются *удобство* (включая оперативность) и *универсальность* (включая повсеместность) осуществления платежей. При этом принципиально важно то, что клиенты сделают выбор в пользу новой системы или технологии осуществления платежей только тогда, когда:

1) она будет характеризоваться очевидными преимуществами по сравнению с имеющимися в настоящее время вариантами;

2) они почувствуют доверие к новой системе на основе точного понимания сопутствующих ей потенциальных рисков.

Новые формы электронных платежей помимо дебетовых карт не могут быть просто привнесены на рынок волной высоких технологий, реализуемых смарт-картами и мобильны-

ми устройствами, если они не будут связаны с экономическими выгодами для их покупателей и продавцов одновременно с надежностью и удобством использования, которыми характеризуются привычные формы платежей. Еще не создано такой платежной схемы, которая сочетала бы возможности ввода, хранения, обработки и передачи данных с использованием каналов мобильной связи таким образом, чтобы обеспечивалось повсеместное использование и тиражируе-мость. Тем более что клиентуре трудно оценить, насколько безопасна (или небезопасна) может быть новая система и насколько ей можно доверять.

Вместе с тем у мобильного телефона есть свойства, как правило, не учитываемые при решении упомянутого вопроса, – это его «персональность» и точно такое же ощущение «мгновенной реакции», возможности его использования «здесь и сейчас», как в случае применения для ДБО технологии и системы интернет-банкинга. Клиенту необходимо при этом понимать, что проблема перехода на новую разновидность банковского обслуживания заключается не в применении какой-то принципиально новой технологии, а в изменении его отношения к технологии, которая уже им уверенно освоена. Это задача маркетингового подразделения кредитной организации или подразделения по внешним связям или аналогичного, включая информирование в офисах и на web-сайтах вместе с демонстрационным представлением. Ну и наконец, принципиальным удобством является возможность

автоматического подключения к сети связи в любом месте, где имеется соответствующая зона охвата. При этом интересным, хотя и неисследованным, аспектом мобильного банкинга является возможность получения координат (позиционирование) мобильного телефона и виртуальной кредитной карточки в процессе сеанса ДБО.

Мобильный телефон вообще можно рассматривать в узком смысле как своего рода виртуальную банковскую карту, т. е. запоминающее устройство, принадлежащее клиенту и идентифицирующее как его самого, так и учреждение, в котором хранятся деньги клиента (записи об остатках на счетах). При таком использовании мобильный телефон исключает необходимость затрат на выпуск пластиковых карт для клиентов кредитной организации и сопутствующих использованию этих карт проблем. По сути устройство идентификации клиента в GSM-телефонах (SIM-карта) – это та же банковская смарт-карта со встроенным чипом, просто имеющая непривычный вид или интерпретируемая как «виртуальная банковская карта». Понятно, что на такой карте (как и в запоминающем устройстве телефонного аппарата) могут быть записаны и PIN-код клиента, и номер счета, и дополнительное банковское программное обеспечение, и т. п.

В дополнение к этому кредитные организации могут оперативно рассылать своим клиентам мобильного банкинга как общие, так и индивидуальные сообщения, что уже реализуется в системах SMS-банкинга. При этом клиенты полу-

чают возможность контроля состояния своих счетов и истории банковских операций. Поскольку обеспечиваются возможности двустороннего общения, клиенты могут запросить повышение установленного предела кредитования с оперативным ответом от кредитной организации или отслеживать ситуации снижения остатков на счетах ниже установленного контрольного предела, а также необычные операции, что позволяет самим клиентам предотвращать мошенничества с их счетами (либо оперативно уведомлять кредитную организацию о такой подозрительной деятельности). Это дает клиентам ощущение контроля над ситуацией.

Программное обеспечение может использоваться для придания мобильному телефону функций POS-терминала в пункте торговли: наличие дисплея и клавиатуры вместе с процедурами считывания реквизитов клиента с SIM-карты (для идентификации его и его счета), а также защищенной при этом линии связи (трафика). Если же телефонная карта не может служить в качестве виртуальной банковской карты, то к мобильному телефону придется подключать карт-ридер, что, естественно, менее удобно. В принципе мобильный телефон может служить и в качестве «виртуального банкомата», если это принципиально позволяют условия использования POS-терминалов в пункте торговли.

Учитывая возможность реализации интернет-банкинга через средства мобильной связи, мобильный телефон может играть роль интернет-банка как одной из его разновидностей

в зонах, где обеспечивается доступ к Интернету. Однако для российских условий существуют определенные проблемы с инфраструктурой, из-за которых мобильный банкинг может оказаться предпочтительнее. Тем не менее внедрение технологии Wi-Fi может способствовать решению этой проблемы, создавая тем самым для клиентов кредитных организаций дублирующие (резервные) маршруты доступа к информационно-процессинговым ресурсам этих организаций, требуемым для удаленного выполнения банковских операций и получения сопутствующей информации.

Запоминающее устройство SIM-карты может хранить таких три существенных компонента дистанционного информационного взаимодействия, как меню пользователя, ключевую информацию, защищающую клиентский трафик, и специализированное программное обеспечение мобильного банкинга. К двум последним компонентам произвольный доступ в общем случае невозможен, потому что он контролируется соответствующими операторами (мобильной связи или кредитной организации). Поэтому можно считать, что хотя в совокупности мобильный телефон все равно будет уступать компьютерам, банкоматам и POS-терминалам, содержимое его SIM-карты, необходимое для осуществления ДБО, лучше защищено от постороннего вмешательства.

Одним из примеров развития этого направления является внедренная кредитной организацией Сити-банк система Citi Mobile, которая рекламируется как «уникальный, пол-

нофункциональный, весьма безопасный вид банковского обслуживания прямо вам в руки, в любое время, в любом месте». Для регистрации в Citibank® Online клиентам нужен только мобильный телефон; после регистрации на телефон клиента передается подтверждение. Далее следует загрузка: чтобы получить программное обеспечение, клиенты выбирают гиперссылку в полученном сообщении (в ряде случаев клиенты могут загрузить Citi Mobile непосредственно от оператора связи). При активации клиент запускает приложение Citi Mobile по телефону и соединяется, вводя свой код телефонного доступа. Надо отметить, что на web-сайте Сити-банка приведена информация только об удобствах для клиентов, в распоряжении которых имеется мобильный телефон или iPhone, но не об источниках банковских рисков, которые могут сопутствовать этой новой схеме мобильного банкинга.

Внедрение мобильного банкинга может служить целям сохранения и расширения клиентской базы за счет индивидуализации услуг в отношении наиболее ценных клиентов. При этом типовые банковские услуги могут предоставляться таким образом, что уникальным станет клиентский опыт за счет адресного предложения кредитной организацией новых услуг своим клиентам по всему ассортименту именно в текущей «мобильной» среде. Мобильный банкинг вовсе не вытесняет привычные каналы предоставления кредитной организацией банковских услуг, но позволяет охватывать до-

полнительные слои населения или условия, в которых могут оказаться клиенты (например, при нахождении в отпуске, командировке и т. п.). Замечено также, что такой вид ДБО весьма активно используется гастарбайтерами в Западной Европе и США, которые формируют с его помощью весьма значимые финансовые потоки[20] (а в Российской Федерации дела с гастарбайтерами обстоят особенно «хорошо»).

Для мобильного банкинга существуют такие принципиальные ограничения, как двусторонняя конвертация наличности и «электронных денег» в отличие от виртуального перевода или преобразования финансовых средств. Поэтому стратегия мобильного банкинга неизбежно должна предполагать создание сети пунктов, обеспечивающих такую конвертацию, хотя в той или иной форме такие сети во многих городах уже существуют и проблемы «ликвидности» электронных денег тем самым решена. При этом необходимо учитывать, что люди, живущие в условиях экономики с превалирующим наличным денежным обращением (а это как раз российские условия) и получающие перечисления на некие отчуждаемые средства платежа (социальные карты и т. п.), обычно испытывают желание убедиться в возможности конвертации записей о соответствующей платежеспособности в наличные средства сразу по их перечислении. Для

---

[20] *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.

систем мобильного банкинга и внедряющих такие системы кредитных организаций такие условия могут оказаться критичными в части реализации соответствующего компонента стратегического риска. При прямых электронных переводах необходимость в конвертации отпадает, так что не исключено, что в перспективе упомянутые конвертационные пункты окажутся не нужны, но если это и произойдет, то, безусловно, не завтра.

Вместе с тем остается проблема определения, какие именно товары и услуги (в широком смысле – потребности клиента) можно оплачивать с помощью мобильных транзакций и с какими ограничениями. Поскольку законодательной базы так называемых «электронных финансов» в российских условиях практически не существует, то кредитным организациям целесообразно ориентировать работу своих подразделений правового обеспечения, информационной безопасности, внутреннего контроля, управления рисками банковской деятельности и информационных технологий на исключение потенциально возможных компонентов правового, стратегического и репутационного рисков.

Если коснуться основных технических вопросов, которые необходимо решить при организации мобильного банкинга, то в качестве таковых можно выделить следующие три:

1) *способ* передачи данных с мобильного телефона и на него;

2) *обеспечение* информационной безопасности передачи

данных;

3) *организация* информационного взаимодействия с клиентом.

Выбор канала передачи данных определяет несколько важных параметров ДБО в варианте мобильного банкинга, а именно:

• *скорость,* которая зависит от пропускной способности канала и задержек приема, обработки, передачи;

• *надежность,* которая зависит от технических средств, формирующих канал информационного взаимодействия, с учетом их устойчивости к перегрузкам трафика, а также их защищенности (информационной безопасности);

• *стоимость,* которая зависит от используемых сетевых ресурсов и тарифов тех или иных операторов связи. Информационная безопасность передачи данных, от которой прямо зависит степень доверия со стороны клиента к мобильному банкингу, равно как и уровень отдельных компонентов стратегического, операционного, репутационного и правового рисков, в свою очередь зависит от применяемых стандартов шифрования. Это безопасность двоякого рода, которая связана с шифрованием исключительно канала передачи данных и сквозным шифрованием. В первом случае сервис мобильного банкинга зависит от оператора сотовой связи, поскольку в его сетевых структурах существует потенциальная угроза информационной безопасности (можно руководствоваться брендом компании, но это не гарантирует отсут-

ствия человеческого фактора в ней самой). Во втором случае безопасность обеспечивается на всем маршруте между мобильным телефоном и сервером кредитной организации (за счет использования ключевой информации на обеих сторонах) независимо от носителя потоков данных, поскольку оператор мобильной связи не имеет доступа к их содержанию.

Говоря об обеспечении информационной безопасности в системах мобильного банкинга, необходимо отметить, что решения, не основывающиеся на SIM-картах, менее безопасны. Для кредитной организации этот факт прямо связан с решениями в отношении контроля ее зон ответственности (и зон концентрации факторов и источников риска). Например, решения на основе WAP *(Wireless Application Protocol)* по своей сути аналогичны предоставлению банковских услуг через Интернет, поэтому кредитной организации, внедряющей такое решение, следует распространить меры по обеспечению информационной безопасности при взаимодействии с клиентами через Интернет и на среду мобильного банкинга. В общем случае чем ниже информационная безопасность технологической платформы, тем больше кредитной организации придется использовать дополнительных мер предотвращения возможности инцидентов с информационной безопасностью[21].

---

[21] Используется терминология Стандарта Банка России СТО БР ИББС– 1.0 «Обеспечение информационной безопасности организаций банковской системы

Информационное взаимодействие между кредитной организацией и ее клиентом в ряде отношений зависит от выбранной технической платформы (так называемой «среды приложения»), поскольку она определяет удобство пользования мобильным банкингом для клиента в части:

• *эргономичности* интерфейса – простоту и интуитивность использования;

• *времени* доступа – ожидание загрузки данных и обновления меню;

• *сложности* установки – требования квалификации клиента и его адаптации;

• *простоты* обновления – установка новой версии или добавление сервисов.

При этом возможна ориентация как на клиента кредитной организации, так и на сеть связи. В первом случае реализацией банковской услуги управляет прикладная программа, загруженная в мобильный телефон, что снижает затраты времени на работу с меню (в том числе за счет интеграции в него новых функций) и подготовку данных к передаче, однако от клиента может потребоваться дополнительная «сноровка» при запуске новых «приложений». Во втором случае прикладные программы не загружаются, а услуга предоставляется непосредственной отправкой с сервера на телефон, что может замедлить работу из-за пересылок из сети и в сеть, однако по ряду причин упрощает поддержку мобиль-

---

Российской Федерации. Общие положения».

ного банкинга со стороны провайдера. Наиболее дорогостоящим оказывается вариант голосовой связи, следующий по стоимости – вариант с использованием SMS, а наиболее дешевый – сеанс на основе передачи данных; при этом услуги, ориентированные на сеть, дороже, чем ориентированные на клиента.

Выбор технологии непосредственно влияет на содержание взаимоотношений кредитной организации с ее провайдерами, особенно в плане наличия или отсутствия необходимости ее поддержки с их стороны. Например, услуги мобильного банкинга, предоставляемые на основе собственных SMS-, WAP– или JAVA-разработок, такой поддержки не требуют и могут предлагаться клиентам кредитной организации без ведома оператора. В противном случае возрастают требования к содержанию договоров с провайдерами, поскольку усложняется решение вопросов обеспечения надежности рассматриваемого вида ДБО в целом, его информационной безопасности, организации и содержания внутреннего контроля в соответствующей части, а также стоимости предоставляемых услуг в целом.

Кредитная организация может рассчитывать на некую «интегрируемую платформу безопасной связи», оставляя за собой решение «чисто банковских» вопросов. В этом случае оператор управляет всем процессом связи от клиента (SIM-карты) до сервера кредитной организации. Тем самым провайдеру передается решение всех вопросов связи. Возможен

вариант с размещением всей «платформы мобильного банкинга» у провайдера. При этом клиентские счета управляются банком, но система мобильного банкинга в целом обеспечивается и управляется оператором мобильной связи. Могут реализоваться и другие модели, но в любом случае их выбор определяется стратегией и ресурсами кредитной организации, тем, насколько глубоко она собирается внедрять услуги мобильного банкинга в свою банковскую деятельность, и ее способностью самостоятельно внедрять технологии ДБО и сопровождать жизненный цикл соответствующих автоматизированных систем.

Варианты такого рода не запрещаются российским банковским законодательством, но могут привести к возникновению сомнений в обеспечении конфиденциальности банковской и клиентской информации. Во всех вариантах следует помнить, что в случае сбоев в работе системы мобильного банкинга клиенты скорее будут обращаться с претензиями в кредитную организацию, чем к провайдеру. Поэтому подобные сценарии целесообразно предусмотреть и в договорах с клиентами на ДБО, и в работе сервис-центра организации, во многом полагающейся на провайдеров, и в ее внутрибанковских процессах.

Здесь также возможны варианты организации взаимодействия между кредитной организацией и ее провайдерами[22] в

[22] Одним из примеров могут являться организация отношений между коммерческим банком «Таврический» и оператором мобильной связи «Билайн»: кре-

части:

• совместного маркетинга мобильного банкинга;

• продвижения и оформления банковских услуг через агентов провайдеров;

• распределения функций и ответственности в решении проблемных ситуаций;

• комбинации продаж оптовых и розничных мобильных услуг;

• поддержки и сопровождения систем мобильного банкинга.

Необходимо учитывать, что чем больше функций кредитная организация отдает на аутсорсинг, тем больше внимания ей придется уделять контролю за провайдером, его финансовым состоянием, технологиями и системами, обеспечением информационной безопасности и т. д. В случае мобильного банкинга это неизбежно. В российских условиях провайдеры нередко закрыты от кредитных организаций и уж тем более от их клиентов, хотя по мере роста числа организационных и технологических предложений и появления возможностей выбора для кредитных организаций ситуация понемногу начинает меняться. В то же время структуры, которые придерживаются принципа открытости в совместном бизнесе и идут друг другу навстречу в решении организационно-технических вопросов, очень быстро начинают ощу-

---

дитная организация использует для оплаты услуг дистрибьюторскую сеть провайдера.

щать финансовые выгоды такого подхода.

Как свидетельствует практика, чем сложнее оказывается в организационном или техническом плане работа с системой мобильного банкинга, тем менее охотно клиенты ею пользуются. Известны случаи, когда кредитным организациям приходилось сворачивать дорогостоящие проекты, имевшие множество достоинств в части надежности и информационной безопасности, из-за того что клиентам не нравились те или иные сложности. В этом заключается зависимость от компонентов операционного, репутационного и стратегического рисков. В то же время кажущиеся более неудобными варианты организации отношений с клиентами, при которых они вынуждены время от времени являться в кредитную организацию для обновления банковского программного обеспечения, замены SIM-карт или каких-либо других средств идентификации, могут оказаться все-таки желательны с точки зрения процедур финансового мониторинга. В первую очередь это относится к программам внутреннего контроля кредитной организации, связанным с осуществлением противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ)[23]. В частности, речь идет о «Программе идентификации кредитной организацией своих клиентов, установ-

[23] См. письмо 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».

ления и идентификации выгодоприобретателей» и о «Программе по организации в кредитной организации работы по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», которые, очевидно, должны предусматривать специальные дополнительные процедуры в отношении любых клиентов ДБО.

Кредитным организациям, переходящим к мобильному банковскому обслуживанию клиентов, целесообразно помнить о наличии у них обязательств не только перед клиентами, но и перед контролирующими органами. Основные обязательства такого рода связаны с предоставлением и подтверждением ряда гарантий:

• сохранения банковской тайны (обеспечения конфиденциальности банковской и клиентской информации);

• предоставления сведений, требуемых контролирующим органам о клиентах и совершаемых им операциях;

• соблюдения правил осуществления бухгалтерского учета и подготовки регламентной банковской отчетности;

• адаптации программ внутреннего контроля и реализации мер, относящихся к ПОД/ФТ;

• соблюдения лицензионных требований, начиная с содержания банковской деятельности и заканчивая использованием средств криптозащиты.

В условиях мобильного банкинга, при котором задействуются провайдеры, образуются специфические конфи-

гурации информационного контура банковской деятельности и информационные сечения в нем, могут потребоваться нетривиальные организационно-технические решения, к принятию которых руководству кредитной организации необходимо быть готовым заранее, до начала практического использования технологии ДБО. В противном случае не исключено такое неприятное для кредитной организации событие, как существенная реализация компонентов стратегического риска.

Возможности мобильных телефонов, вполне вероятно, приведут к радикальному изменению характера отношений между кредитными организациями и их клиентами, прежде всего потому, что это повсеместно используемая технологическая база. Мобильные телефоны можно обнаружить практически повсюду, в сельской местности и даже в относительной «глуши» труднодоступных регионов. Мобильный банкинг поэтому может стать популярным у людей, для которых по каким-либо причинам нецелесообразно приобретение компьютера. Все соображения такого рода прямо относятся к технико-экономическому обоснованию проектов мобильного банкинга и подлежат учету при принятии соответствующих решений руководством кредитной организации. Некоторые зарубежные исследования предполагают возможность существенного сокращения организационно-технических и операционных расходов кредитных организаций и их клиентов в случае внедрения рассмотренных или аналогич-

ных им схем ДБО[24]. Тем не менее в любом случае мобильный банкинг должен соответствовать стратегии, принятой кредитной организацией, ее бизнес-планам и наличным ресурсам, предусматривающим внедрение технологии ДБО и сопровождение автоматизированных систем, реализующих эту технологию.

Из приведенного анализа видно, что специалистам кредитной организации и ее руководству целесообразно принимать решения по широкому кругу вопросов при переходе к мобильному банковскому обслуживанию. Практика свидетельствует, что грамотный и тщательный подход к этому гарантирует исключение подавляющего большинства факторов и источников банковских рисков, сопутствующих применению технологии и систем мобильного банкинга.

[24] См., например: C GAP (Консультационная группа помощи бедным) Focus Note № 48. Washington, DC, June 2008.

3. Проблемы конкуренции на рынке банковской розницы

Исторически вся банковская система постсоветских государств начала свое развитие с обслуживания корпоративных клиентов. Услуги для физических лиц ограничивались набором из депозитов, банковских карт (в основном в рамках «зарплатных» проектов), переводов и обмена валют. Однако рано или поздно почти все банки вышли на розничный рынок. На постсоветском пространстве розничная экспансия началась в разное время и с разных сегментов, но итог везде одинаков – конкуренция на розничном рынке растет с каждым днем.

При этом конкуренция на корпоративном и розничном рынке существенно различается. На корпоративном рынке количество потенциальных клиентов значительно меньше, а их обороты, потребность в банковских продуктах и, как результат, потенциальный доход – существенно выше. Таким образом, прибыль с каждого клиента достаточно велика и оправдывает установление персональных отношений практически с каждым из них. Личные отношения на этом рынке решают многое – не секрет, что большинство мелких и средних предприятий привязаны не столько к банку, сколько к конкретному менеджеру, который обеспечивает им ком-

фортные условия сотрудничества с банком. И зачастую, когда клиентский менеджер меняет место работы, значительная часть его клиентской базы «уходит» вместе с ним в новый банк. На массовом рынке обеспечить персональные отношения с каждым клиентом практически невозможно.

Кроме того, многие банки предлагают очень похожие, практически идентичные розничные продукты, что усложняет их дифференциацию в глазах клиента.

В этой ситуации очевидным решением проблемы борьбы за клиента является ценовая конкуренция, и банки наперебой увеличивают ставки по депозитам, снижают – по кредитам, продляют *grace*-период и т. п. Но снижение цен не может быть бесконечным. Рано или поздно будет достигнута точка безубыточности, и наиболее слабые игроки начнут разоряться. Но даже те финансовые «монстры», которые могут позволить себе работать некоторое время в убыток и вытеснят с рынка мелкие и средние банки, продолжат конкурировать между собой, балансируя на грани рентабельности. Общеизвестно, что снизить цены легко, гораздо сложнее потом их снова поднять.

Гораздо эффективнее конкурировать не по цене, а по продукту. Лучшее предложение клиенту позволяет обосновать более высокую по сравнению с конкурентами цену, а активно растущий в последние годы средний класс, представляющий самую интересную для коммерческих банков часть розничной аудитории, менее чувствителен к цене.

Несмотря на обостряющуюся конкуренцию, значительная часть населения все еще не охвачена банковскими услугами (согласно докладу Merrill Lynch, в начале 2007 г. лишь каждый пятый житель России имел банковский счет). Это связано как с низкой финансовой грамотностью, так и с отсутствием банковских отделений в пределах досягаемости конкретного гражданина. Причем речь идет не о сельском населении и жителях небольших городов, где банковских отделений, кроме Сбербанка, обычно не бывает. Уровень доходов жителей глубинки и их финансовая грамотность делает их идеальными клиентами сберкасс: коммерческим банкам они не доверяют, да и потребности в банковских услугах почти не испытывают. Речь о жителях крупных и средних городов, которые работают, получают стабильный доход и достаточно адаптировались к новой экономике, чтобы быть активными потребителями банковских услуг. Тем не менее существующие банковские отделения мало подходят для обслуживания этих клиентов. Все банковские отделения открываются в основном в деловых районах городов и работают в обычном графике (с 9—10.00 до 18–19.00 с перерывом на обед). Такое расположение и график работы ориентированы на корпоративных клиентов, представители которых, вполне естественно, посещают банки в свое рабочее время, так как делают это «по службе». Обычный же гражданин может посетить отделение банка только в перерыв или после окончания рабочего дня, но большинство отделений банков в это

время также не работают – их график совпадает с графиком работы большинства населения! Даже если отделение работает в обеденный перерыв или его рабочий день на час длиннее обычного, то там клиента встречают очереди. Розничные торговые сети давно адаптировались к требованиям клиентов, поэтому повсеместно открываются круглосуточно работающие торговые центры, в спальных районах появился новый формат магазинов – «магазин шаговой доступности». Среди банков таких примеров пока немного – первым на круглосуточный режим работы в январе 2004 г. перешли отделения Екатеринбургского Банка24.ру (и в 2007 г. в период с 21.00 до 9.00 в его девяти круглосуточных отделениях осуществляется в среднем одна операция каждые 4 мин), а в «шаговой доступности» в большинстве спальных районов крупных городов по-прежнему – только Сбербанк. Таким образом, банковский продукт должен быть не только лучшим, он должен быть еще и доступным для клиентов.

Проблема доступности банковских услуг для розничных клиентов усугубляется еще и тем, что практически все маркетинговые коммуникации с розничным клиентом ориентированы на «ковровую» обработку потенциальных клиентов (газеты, телевидение, радио, рекламные щиты). Клиент, узнав об интересном для себя предложении, должен отыскать банковское отделение, в котором сможет получить более подробную информацию, и совершить покупку. Согласно исследованиям М. Дымшица (см. статью «Для большин-

ства банков реклама – просто бесполезная трата денег», журнал «Банковское обозрение» за март 2007 г.), эффективная зона распространения банковской рекламы составляет всего 800 метров. Однако отделений-то у банков как раз и не хватает: согласно данным программы «Национальная банковская система России в 2010–2020 годах», количество банковских отделений в расчете на 100000 жителей составляет всего 3,2, что примерно в 10 раз меньше, чем в США, и в 20 раз меньше, чем в Германии (по более свежим данным АРБ, на октябрь 2007 г. их было уже 14 на 100000 жителей). Клиент, заинтересовавшийся предложением, вынужден тратить время на поиск отделения нужного банка. Многих клиентов не устраивает сама необходимость тратить время на поиск отделения, некоторые в процессе поиска могут передумать или найти другой банк. Даже достигнув своей цели, клиенты имеют большие шансы обнаружить если не закрытые двери, то, как минимум, длинную очередь из других желающих во внерабочее время воспользоваться банковскими услугами.

Создание необходимой сети отделений даже в масштабах отдельного региона – задача, требующая значительных капиталовложений и, главное, времени. Даже при наличии огромного количества денег банку потребуется много времени на то, чтобы найти подходящее помещение, договориться о его покупке или аренде, обустроить его в соответствии с жесткими требованиями регулирующих органов, набрать и обучить персонал. А в течение этого времени более расторопные

конкуренты будут увеличивать свое присутствие и долю на рынке. Да и догнать по количеству точек обслуживания наиболее разветвленные банковские сети (не говоря о наследии Сбербанка СССР) практически невозможно. Даже при наиболее быстром способе наращивания сети присутствия – поглощении других банков – количество отделений будет расти, но концентрироваться они будут по-прежнему в тех же самых местах, не увеличивая доступность банковских услуг для населения.

А тут еще кризис некстати грянул – кончились дешевые и длинные западные деньги. В этих условиях рост сетей банковских отделений если не остановится вовсе, то существенно замедлится.

3.1. Технологические решения проблем конкуренции

Дистанционное банковское обслуживание может решить проблемы развития банковской розницы и сделать массовые продукты удобнее и доступнее для клиента. Значительная доля банковских операций может совершаться клиентом самостоятельно.

Операции с наличными в банковском офисе самообслуживания могут совершаться через банкомат с функцией приема наличных и опционально платежного терминала. Такие офисы самообслуживания могут создаваться достаточно быстро, на небольших площадях, не требуют персонала и стоят значительно дешевле, чем полноценные отделения банка. Безналичные операции могут совершаться клиентом прямо из дома или офиса через Интернет или с помощью мобильного телефона, а также в устройствах самообслуживания: банкоматах и информационных терминалах.

Таким образом, проблемы организации массового обслуживания физических лиц (и доступности банковских услуг вообще) могут быть решены с помощью современных банковских технологий. Они позволяют связать между собой все банковские продукты, и это будет удобно для клиента, создаст весомое конкурентное преимущество. Таким образом, ценовая война трансформируется в войну технологий.

В этой ситуации поставщики IT-решений и грамотная собственная команда IT-специалистов становятся важнейшим ресурсом современного розничного банка.

Ключевым моментом в реализации концепции дистанционного банковского самообслуживания клиентов становится тесная интеграция разнородных банковских систем (CRM, учетная система, карточная система, интернет-банк) и обеспечение круглосуточного и унифицированного доступа клиентов к банковским услугам по различным каналам обслуживания. Банку остается выбрать, на базе какой системы и какого банковского продукта строить дистанционное обслуживание.

Пластиковые карты изначально создавались как банковский продукт, предназначенный для дистанционного и круглосуточного доступа клиента к своему счету в банке. Поэтому с момента появления на свет это был самый высокотехнологичный банковский продукт, а карточная система (процессинговый центр) до сих пор в подавляющем большинстве банков является единственной, работающей в режиме 24 ч в сутки 365 дней в году. Любая другая банковская система, работающая со счетами клиентов, имеет регламентную процедуру закрытия дня, во время которой подавляющее большинство из них недоступно из внешней среды. Кроме того, в процессе своего развития карточные продукты обрастали дополнительными высокотехнологичными сервисами, а процессинговая система, которая их обслуживала, соответ-

ственно и наращивала каналы взаимодействия с клиентом (мобильный телефон, интернет-банк и т. п.). К настоящему времени современные процессинговые системы поддерживают практически все существующие электронные каналы взаимодействия с клиентом.

Кроме круглосуточной доступности по различным каналам для клиента важна полнота предоставляемых услуг. Он должен иметь возможность воспользоваться максимально возможным для каждого канала количеством банковских продуктов и услуг. Поэтому встает вопрос интеграции с различными банковскими и внешними информационными системами. Со стороны современной процессинговой системы не возникает особых трудностей в налаживании *online* или квази-*online* взаимодействия с различными системами как внутри, так и за пределами банка, и выбор конкретной реализации интерфейса *(online,* квази-*online)* целиком определяется возможностями той системы, с которой осуществляется интеграция. Практика показывает, что в той или иной степени *online*-интерфейс обмена данными можно создать практически с любой информационной системой.

Таким образом, процессинговая система становится единым центром управления различными каналами обслуживания, обмениваясь необходимой информацией с внешними системами (которые могут добавляться в схему взаимодействия постепенно, расширяя набор сервисов и объектов, доступных клиенту). При этом добавление нового канала об-

служивания никак не будет усложнять работу существующих банковских систем, ведь вся логика взаимодействия с каналом обслуживания замыкается на уровне процессингового центра, выполняющего функции *«channel management»*. Обобщая, можно отметить следующие плюсы такого решения:

- круглосуточная доступность процессинговой системы;
- существующая поддержка всех электронных каналов обслуживания;
- унифицированный объем услуг, предоставляемых по всем каналам обслуживания. Подключая новый канал взаимодействия с клиентом, мы имеем в нем все сервисы, уже доступные клиентам по существующим каналам (за исключением тех, на которые накладываются технические ограничения конкретного канала);
- подключение новой информационной системы делает ее сервисы доступными по всем каналам взаимодействия с клиентами;
- централизация обслуживания розничных операций в процессинговой системе позволяет использовать средства мониторинга и обеспечения безопасности, которые уже функционируют в процессинговом центре для обеспечения безопасности операций с банковскими картами.

3.2. Возможности дистанционного банковского обслуживания

Изюминка стратегии розничного бизнеса, основанного на концепции дистанционного банковского самообслуживания, заключается в том, что клиенту достаточно один раз посетить отделение банка, чтобы заключить договор и получить средства идентификации (банковскую карту, токен или идентификатор для интернет-банка и т. п.). В дальнейшем пользоваться услугами банка и приобретать новые продукты он может дистанционно. Это позволяет банкам сделать свои продукты не только удобными, но и доступными для клиентов, вне зависимости от совпадения географии и времени работы отделений с режимом жизни и работы клиента. Для первого и, возможно, единственного «живого» контакта банка с клиентом достаточно небольшой точки продаж (в этом плане идеально работает концепция «*in-store banking*») или даже свободно перемещающегося по городу продавца банковских услуг (например, в Казахстане до кризиса активно развивалась продажа банковских услуг агентами).

На сегодняшний день в процесс обслуживания клиентов могут быть вовлечены следующие каналы взаимодействия:

• традиционные «карточные» банкоматы и POS-терминалы, которые в последнее время существенно расширили спектр своих возможностей;

• информационные и платежные киоски;
• интернет-банк;
• телефонный банк;
• мобильный банк;
• call-центр.

Каждый из этих каналов обеспечивает различный набор услуг и возможностей.

POS-терминал:

• традиционная оплата товаров и услуг в точке продаж;
• покупка различного рода скретч-кодов;
• взнос наличных на банковский счет;
• пополнение счетов (сотовые телефоны, интернет-провайдеры и т. п.).

Обычный банкомат:

• получение наличных;
• просмотр баланса счета и получение списка операций, включая внутрибанковские операции, путем обращения за актуальной выпиской непосредственно в учетную систему, ответственную за данный банковский продукт. В результате клиент может видеть полную информацию о движении денежных средств по своим счетам;
• переводы денег между своими счетами, в том числе с конвертацией различных валют;
• переводы по номеру карты, эмитированной данной платежной системой (P2P-переводы через инфраструктуру платежных систем VISA, MasterCard). Такие же переводы могут

быть доступны внутри банка или внутри ассоциации дружественных банков по любым картам вне привязки к платежной системе;

• отправка и получение денег из систем моментальных переводов и систем интернет-расчетов (Web-money, Яndex-деньги и т. п.);

• оплата счетов, консолидированных в EBPP-системе (Electronic Bill Presentment & Payment), примером такой системы является система «Город» компании ЦФТ;

• различные платежи по известным клиенту реквизитам (сотовый телефон, интернет, коммунальные услуги и т. п.), в том числе индивидуальные для каждого клиента (клиент может сам через Интернет-банк или по заявлению в банк создать свои собственные шаблоны);

• покупка скретч-кодов;

• продажа товаров. Украинский ПриватБанк практикует продажу в своей банкоматной сети различных телефонов, ноутбуков и прочей мелкой электроники, в том числе и с рассрочкой платежа. После того как клиент выбирает необходимый товар и оставляет свои координаты для связи, с ним связывается представитель са11-центра и решает вопросы доставки;

• генерация виртуальных карт для расчетов в Интернете. При этом клиент получает возможность задать срок действия карты, лимит на сумму авторизации, его возобновление, количество использований карты и в результате тут же

получить чек со всеми реквизитами карты, необходимыми для совершения операций в сети Интернет;

• различного рода заявки банку на продукты и услуги, например на перевыпуск карты, подписку на SMS-сервис, открытие депозита и т. п.;

• получение персональных сообщений от банка (персональное обращение, уведомление об очередном платеже по кредиту и т. п.) и адресной рекламы. Не перестает удивлять, как подавляющее большинство банков игнорирует возможности персонализации общения с клиентом через

банкомат. Персонализация может быть как на уровне обращения по имени к собственному клиенту и адресных предложений ему, так и предложений клиентам чужих банков, снимающим наличные или оплачивающим услуги (можно, например, в режиме ожидания показывать клиенту контекстную рекламу с предложением специальных условий и просьбой оставить номер своего телефона для связи). Большинство банков загружает в свои банкоматы общий сценарий для всех клиентов. В результате владельцы карт VISA или MasterCard вынуждены бесполезно тратить время и пролистывать экраны, информирующие о том, что по картам СТБ и Юнион Кард взимается дополнительная комиссия за получение наличных (хотя по префиксу карты можно определить, к какой платежной системе она относится, и обойти ненужную «ветку» сценария). Персонализация общения позволит не только укрепить отношения с собственными

клиентами и продать им дополнительные продукты, но и, возможно, привлечь часть клиентов от конкурентов, ведь можно легко определить, что карта «чужая», и направить диалог с клиентом конкурента по специальной ветке сценария;

• публичная реклама. Украинский банк «Надра» активно использует мультимедийные возможности своих банкоматов для привлечения к ним клиентов и даже придумал броское и забавное название для своей сети банкоматов «Cash a lot» (Кашалот).

Банкомат с cash-in предоставляет ряд дополнительных возможностей:

• внесение наличных на счет клиента как для пополнения текущих счетов, так и для погашения кредитов;

• платежи наличными без использования банковских карт;

• обмен валют с выдачей сдачи купюрами и монетами.

Последние два вида операций крайне важны, так как позволяют расширить клиентскую базу. Этими услугами могут пользоваться люди, которые еще не имеют банковской карты и, значит, с высокой долей вероятности, не являются клиентами какого-либо банка (ведь банковская карта – самый распространенный банковский продукт). Это «непаханое поле» клиентов, которых не надо переманивать у конкурента, до них просто нужно донести свое предложение.

Интернет-банк:

• получение любой информация по счетам и договорам. Это не только остатки на счетах и выписки, но и график погашения кредитной задолженности, изменившийся после досрочного погашения;

• управление лимитами и статусами карт и других объектов (блокировка, разблокировка, изменение лимита выдачи наличных и т. п.);

• генерация виртуальных карт для расчетов в сети Интернет. В интернет-банке это делать, несомненно, удобнее, чем в банкомате, и эта возможность решает проблему безопасных расчетов в сети Интернет. Сформировав заказ в интернет-магазин и узнав окончательную стоимость своей покупки, клиент может в режиме реального времени создать одноразовую виртуальную карту на необходимую сумму, расплатиться ею и забыть о ее существовании и проблемах с безопасностью у эквайера, которому стали известны реквизиты этой карты. Другие операции по одноразовой карте уже не пройдут;

• покупка скретч-кодов;

• переводы между своими счетами, в том числе с конвертацией валют;

• переводы по номеру карты (P2P);

• переводы со свободными банковскими реквизитами с предварительной проверкой всех реквизитов;

• платежи как по шаблонам (которые впоследствии будут доступны также и в банкоматах), так и со свободными реквизитами;

• создание планов платежей и переводов, т. е. возможность создания графика платежей, которые будут производиться автоматически в будущем в заданные даты или с заданной периодичностью (отсроченные и регулярные операции);

• отправка и получение денег из систем моментальных переводов и систем интернет-расчетов (Web-money, Яndex.Деньги и т. п.);

• оплата счетов, консолидированных в EBPP-системе (Electronic Bill Presentment & Payment), примером такой системы является система «Город» компании ЦФТ;

• различные платежи по известным клиенту реквизитам (сотовый телефон, Интернет, коммунальные услуги и т. п.), в том числе индивидуальные для каждого клиента (клиент может сам через интернет-банк или по заявлению, поданному в банк, создать свои собственные шаблоны);

• возможность формирования сложных заявок на продукты и услуги, из которых наиболее интересной является заявка на кредит, к которой прикладываются отсканированные копии необходимых для рассмотрения заявки документов;

• получение персональных сообщений от банка и адресной рекламы;

• переписка с банком.

Платежный киоск:

• может выполнять все те операции, что и банкомат с функцией приема наличных, кроме собственно операций, связанных с выдачей денег;

• из-за относительной дешевизны оптимален для создания сети массового погашения кредитов с небольшими суммами погашения или приема платежей. В России эти устройства изначально предназначались именно для обслуживания мелких платежей и развивались в основном как небанковские сети, а в Казахстане, где киоски появились совсем недавно, они, наоборот, сразу ориентировались на погашение кредитов и создавались чаще всего банками.

Информационный киоск:

• доступны все операции интернет-банка;

• дополняет банкомат для создания офиса самообслуживания.

Мобильный телефон:

• SMS-уведомления о совершаемых операциях или изменении состояния объектов (пополнение счета, блокировка карты);

• SMS-запросы (баланс счета, состояние объекта);

• управление статусами объектов (блокировка карты);

• SMS-платежи, например оплата того же сотового теле-

фона;

- покупка скретч-кодов;
- отправка заявок на услуги;
- персональные сообщения от банка и адресная реклама.

Обычный телефон (IVR):

- предоставление информации по счетам и договорам в автоматическом режиме;
- управление статусами объектов;
- заявки на услуги;
- персональные сообщения от банка и адресная реклама.

3.3. Практическое применение дистанционного банковского обслуживания

Реализовав хотя бы часть дистанционных сервисов, банк получает уникальное конкурентное преимущество, и тому есть несколько примеров успешной реализации современных интернет-технологий.

НОМОС-БАНК (Россия)

Корпоративный банк, который начал развивать розничный бизнес с расширения спектра продуктов, предлагаемых в рамках обычного зарплатного проекта. Депозит, управляемый банковской картой через банкомат, предоставил владельцам зарплатных карт уникальную и удобную возможность накопления средств. Банк нарастил депозитный портфель без каких-либо вложений в создание сети отделений и рекламные кампании. В дальнейшем банкомат с функцией приема наличных позволил гасить кредиты и пополнять счета (всем заемщикам выдается банковская карта), а информационный киоск дополнил функции банкомата для полноценного управления счетами. Интернет-банк с уникальной технологией аутентификации клиентов на базе стандартов Dual Passcode Autentification/Chip Autentification

Programme (с помощью EMV-карты платежных систем VISA или MasterCard, ее PIN-кода и криптокалькулятора, позволяющего создавать разовые пароли для входа в систему и подписывать операции) позволяет клиентам совершать банковские операции дома или в офисе и даже с помощью «наладонника». Особенностью этого проекта является то, что функции учетной системы для кредитных и депозитных договоров реализует карточный бэк-офис!

Банк «Финсервис» (Россия)

Совместный проект Собинбанка и сети «Седьмой континент» по первой в России реализации концепции *in-store banking*. Во всех магазинах сети «Седьмой континент» открывается миниотделение банка «Финсервис», состоящее из точки продаж и банкомата с функцией *cash-in* (только за первый год работы банк создал более 100 отделений и около 150 точек банковского самообслуживания). Банк с клиентом в точке продаж подписывает договор и выдает ему карту, а также пакет активации интернет-банка. В дальнейшем клиент может совершать все наличные операции в банкомате и активировать интернет-банк, через который совершать безналичные операции. Процессинговый центр интегрирован с двумя банковскими системами, из которых получает информацию по кредитным и депозитным договорам. Концепция *in-store banking* оказалась очень успешной: за год работы выдано более 250000 дебетовых карт, несколько десят-

ков тысяч потребительских кредитов, начат выпуск кредитных револьверных карт, а тысячный клиент интернет-банка появился через месяц после его запуска в эксплуатацию. Теперь банк «Финсервис» выходит за пределы торговой сети «Седьмой континент» и открывает свои офисы продаж и точки самообслуживания по всей Москве и в некоторых регионах.

4. Дистанционное предоставление финансовых услуг небанковскими организациями

4.1. Электронные деньги в российской платежной системе

Выяснению правового режима электронных денег в России следует предпослать краткую характеристику национальной платежной системы с указанием особенностей ее регулирования. Без этого, ввиду серьезного несовершенства и неполноты национального законодательства, оказывается чрезвычайно сложно разобраться, где заканчиваются телекоммуникационные, информационные, почтовые, агентские услуги и начинаются собственно финансовые или банковские операции, включая эмиссию и обращение электронных денег.

Обращение электронных денег осуществляется в сфере розничных платежей. Дополнительные сложности правового анализа вызваны тем, что формирование розничного сегмента в России происходило в ускоренном темпе и до сих пор не завершено, договорная база оперирующих здесь субъ-

ектов (за исключением банков) находится в стадии формирования и постоянно меняется, судебные прецеденты, позволяющие сделать выводы о позиции органов правосудия, отсутствуют, органы надзора и регулирования на финансовом рынке до недавнего времени практически не уделяли внимания небанковским платежным системам, имеющиеся в литературе исследования акцентированы на технологических и организационных аспектах построения таких систем, не уделяя внимания правовым вопросам.

4.1.1. Структура рынка и регулирование розничных платежей

В 2008 г. объем сегмента розничного платежного рынка оценивался в 35–40 млрд дол., из них за услуги связи – 15 млрд дол., коммунальные платежи – 12 млрд дол., возврат потребительских кредитов (погашаемых с использованием услуг третьего лица) – 10 млрд дол. Ежегодный рост этого сегмента составляет 15–20 % в год.

Оплата коммунальных услуг остается наиболее востребованной населением услугой. Основной объем платежей в этой сфере обрабатывается Сбербанком и Почтой России. Доля других коммерческих банков на рынке коммунальных платежей не превышает 2 %. В крупных городах подавляющую долю рынка (до 90–98 %) удерживает Сбербанк, а в сельской местности до 50 % платежей проходит через По-

чту России. В среднем рыночная доля Сбербанка составляет около 80 %, а Почты России – 15 %. Около 5 % платежей совершается непосредственно на предприятиях, оказывающих услуги.

Принципиально иная ситуация сложилась на рынке приема платежей за услуги мобильной связи. На долю кредитных организаций здесь приходится не более 10 % платежей, остальные платежи принимаются розничными агентами, представляющими операторов связи. Эти компании, возникшие в 1990-е гг., выступили инициаторами создания рынка приема платежей за услуги мобильной связи, предоставив своим агентам технологии и привлекательные коммерческие условия. Таким образом возникла в какой-то степени альтернативная банковской система приема платежей от населения. Первоначально операторы мобильной связи решали узкоспециальную задачу – упрощение процедуры оплаты услуг связи, что с учетом дистанционного и всеохватывающего характера самой услуги при крайне слабом региональном присутствии банков (особенно 10 лет назад) представляло собой нетривиальную задачу. По мере роста этой альтернативной (банковской) платежной системы выяснилось, что она носит универсальный характер и розничные агенты по приему платежей, изначально действующие от имени мобильных операторов, в принципе могут обрабатывать потоки микроплатежей для любого другого продавца. Кроме того, расширение перечня обрабатываемых платежей

существенно повышало эффективность (прибыльность) самой системы. Тем самым изначально закрытые агентские сети по сбору платежей начали превращаться в открытые электронные платежные системы. В их орбиту втягивались (либо создавали собственные платформы, основанные на использовании предоплаченных карт, представители интернет-индустрии и иные продавцы, оказывающие свои услуги дистанционно и регулярно (при незначительном размере единичной платежной транзакции).

Правовое регулирование банковской и внебанковской (альтернативной) розничных платежных систем принципиально отлично. Кредитные организации действуют и осуществляют банковские операции на основании лицензии, предоставляемой Банком России. К организациям, которые не являются кредитными, относятся организации почтовой связи; кредитные кооперативы; микрофинансовые организации; операторы мобильной связи, предоставляющие услуги по переводу денежных средств («мобильные» и иные кошельки); международные системы переводов; ломбарды, разнообразные розничные агенты-посредники и т. д. В отличие от кредитных организаций, предоставляющих клиентам самый широкий перечень интегрированных финансовых услуг, прочие поставщики действуют в ограниченных рыночных сегментах, осуществляя узкий перечень разрешенных законом (или явно не запрещенных) операций.

В небанковском сегменте услуг по переводу денежных

средств следует выделить Почту России, которая, по-видимому, является самой крупной розничной сетью в Российской Федерации. К услугам почтовой связи закон относит почтовый перевод денежных средств (услуга организаций федеральной почтовой связи по приему, обработке, перевозке, передаче, доставке, вручению денежных средств с использованием сетей почтовой и электрической связи). Помимо оказания услуг почтовой связи она в соответствии с законом вправе осуществлять оказание иных услуг почтовой связи, тарифы на которые не регулируются государством, а также осуществлять на договорной основе распространение печатных изданий, доставку и выдачу пенсий, пособий и других выплат целевого назначения, реализацию ценных бумаг, инкассацию и доставку денежной выручки, прием платы за коммунальные услуги, прием платы за товары (услуги), выплату наличных денежных средств с использованием пластиковых карт и иную деятельность, разрешенную законодательством Российской Федерации.

По агентскому договору с юридическими лицами или индивидуальными предпринимателями, имеющими соответствующую лицензию, организации федеральной почтовой связи могут выполнять отдельные технологические операции лицензируемого вида деятельности. Таким образом, Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи» наделяет Почту России правом осуществлять специальные финансово-почтовые операции по переводу денеж-

ных средств, которые по своему экономическому содержанию мало отличимы от банковских переводов без открытия текущего счета.

По итогам 2006 г. объем финансово-почтовых операций, проведенных Почтой России, составил около 1,3 трлн руб. Большая часть из них приходится на операции по доставке пенсий: Почта России контролирует более 60 % рынка доставки пенсий. Она занимает также значимую долю на рынке приема коммунальных платежей и платежей в адрес третьих лиц, что составляет примерно 14 % всех финансовых услуг, оказываемых Почтой России, и 25 % рынка коммунальных услуг Российской Федерации.

Еще несколько лет назад почтовые переводы денежных средств осуществлялись по так называемой бумажной технологии. Скорость прохождения денежных средств была невысока, и осуществление почтового перевода занимало примерно две недели. При таком уровне обслуживания Почта России не могла составить конкуренцию системе банковских переводов. С начала 2002 г. Почта России запустила систему электронных переводов – единую систему, на которой базируется оказание практически всех финансовых услуг. На конец 2007 г. около 35 % из 40 тыс. почтовых отделений имели выделенные каналы связи и соответственно возможность осуществления таких денежных переводов. Такие отделения, как правило, расположены в населенных пунктах с населением менее 20 тыс. человек, что существенно повы-

шает доступность финансовых услуг для их жителей.

В 2007 г. через Почту России было погашено банковских потребительских кредитов почти на 200 млрд руб. Более 20 российских банков сотрудничают с ней в этой сфере.

Серьезную конкуренцию банковскому сектору и Почте России на рынке платежных услуг (микроплатежей) в последние годы начали составлять так называемые *электронные (агентские) платежные системы.* Возникшие около десяти лет назад для удовлетворения потребности операторов мобильной связи по массовому приему платежей абонентов, эти системы переросли в новое качество и де-факто начали формировать национальные стандарты индустрии микроплатежей. В настоящее время они обслуживают подавляющую часть платежей операторов мобильной связи, иных операторов связи и интернет-провайдеров, поставщиков медиаконтента, а также успешно осваивают новые сегменты – оплату жилищно-коммунальных услуг и услуг фиксированной электросвязи, возврат потребительских кредитов, продажу авиа-, железнодорожных и иных билетов и т. п. Объем операций, проходящих через такие системы, ежегодно увеличивался на 70–90 % и по итогам 2007 г. может быть оценен в 15 млрд дол. Новые технологии позволяют оказывать населению услуги по проведению платежей дистанционно, вне служебных помещений: с использованием платежных терминалов, предоплаченных платежных карт, применением технологий мобильной связи, использованием элек-

тронных платежных платформ, размещенных в сети Интернет, и квази-электронных денег. Более того, при внедрении предоплаченных финансовых продуктов и «мобильных кошельков» подобные услуги все более сближаются с операциями по приему депозитов (вкладов, сбережений).

В совокупности три электронные системы (CyberPlat, ОСМП – Kiwi, e-port) занимают около 90 % рынка микроплатежей.

Особая роль отводится вопросу о стоимости проведения операций в таких платежных системах. Для операторов мобильной связи затраты, связанные со сбором клиентских платежей, могут достигать 3–4 % от объема оказанных клиенту услуг связи. Несмотря на минимальные издержки, связанные с проведением отдельной электронной транзакции в таких платежных системах, повышение их эффективности будет возможно лишь при условии значительного расширения перечня товаров (работ, услуг), платежи за которые принимаются в этих системах, и соответствующего повышения оборотов «точек платежа» (терминалов, кассовых аппаратов и пр.). Для физических лиц – плательщиков, пользующихся услугами таких платежных систем, размер комиссии может достигать 10 % от размера платежа (в зависимости от вида торговой точки и региона). Наибольшая доля этой комиссии, как правило, причитается розничному агенту (субагенту), осуществляющему (возможно, через терминал) непосредственный прием наличных денежных средств,

а не направляется на развитие платежной системы.

4.1.2. Банковская и небанковская модель предоставления платежных услуг: опыт России

Фактическое разделение платежной индустрии на банковский и внебанковской сегмент не является исключительно российским феноменом. Видимо, наиболее интересной особенностью России является лишь быстрое распространение терминальных сетей (не предусматривающих использование банковских карт, а лишь прием наличных).

В настоящее время в мире получили развитие две модели вне-офисного банкинга с использованием розничных агентов: одна – осуществляемая банками, другая – коммерческими небанковскими (нефинансовыми) организациями. Внеофисный банкинг через розничных агентов позволяет снизить затраты на предоставление финансовых услуг (иногда очень значительно), сократить очереди в отделениях и выйти на новые рынки.

Модель с использованием банка предусматривает оказание кредитной организацией (банком) финансовых услуг через розничного агента. Банк лишь разрабатывает финансовые продукты и услуги и предлагает их через розничных агентов, которые отвечают за все контакты с клиентами или за большинство из них. Денежные средства клиентов хранят-

ся на счетах, открываемых в банке, а платежные операции опосредуют движение средств по этим счетам.

При этом уполномоченные розничные агенты несут ответственность за сохранность денежных средств, которыми они распоряжаются: банк может также нести субсидиарную ответственность перед клиентом в случае мошенничества или небрежности со стороны розничных агентов. В отдельных случаях агент может наделяться правом осуществлять транзакции между банками.

Отдельно следует рассмотреть риски и преимущества использования субагентской модели, когда банк заключает договор с уполномоченной организацией (агентом), которая подбирает розничных агентов (субагентов). Потенциально розничные агенты могут проводить все транзакции по открытию счета и в некоторых случаях даже идентификацию клиентов и обслуживание займов.

Независимо от рода своей деятельности каждый розничный агент должен обладать оборудованием для связи с банком, от имени которого он работает. В качестве такого оборудования может служить мобильный телефон или электронный кассовый терминал (КТ) с устройством считывания карт.

После открытия счета и (или) одобрения банком кредитной заявки клиент может получить у розничного агента полный перечень услуг. Как только счет открыт или заявка на получение займа одобрена, клиент может осуществить непо-

средственно в офисе розничного агента желаемые финансовые операции. Розничный агент проверяет документы клиента и обрабатывает операцию, дебетуя счет клиента и кредитуя счет банка-получателя, если это покупка или перевод средств со счета на счет. Электронная запись об операции непосредственно передается от розничного агента банку либо обрабатывается агентом по проведению платежей, который осуществляет перевод средств со счета клиента на счет получателя.

В ***модели с использованием небанковской (нефинансовой) организации*** клиент не имеет отношений с банком и может вообще не иметь банковского счета. При этом кредитная организация может вообще не принимать участия в процессе взаимодействия сторон. Вместо этого клиенты имеют дело с небанковскими (нефинансовыми) организациями: (1) оператором мобильной связи, (2) эмитентом предоплаченных финансовых продуктов (карт). Розничные агенты играют роль пунктов контактов с клиентами. В этой модели клиенты производят обмен наличных денежных средств на электронные деньги (или их аналоги), которые хранятся на виртуальном индивидуальном электронном счете в компьютерной системе небанковской (нефинансовой) организации, которая никак не связана с банковскими счетами. Клиенты могут пересылать электронные деньги другим лицам, делать покупки или использовать электронный счет для сбережения средств. Они могут также обменять их на наличные

деньги у любого из розничных агентов.

Если небанковская организация является эмитентом предоплаченных финансовых продуктов (карт), она использует устройства считывания карт и другое оборудование розничных агентов. Операторы мобильной связи располагают сложившейся сетью розничных агентов и широкой группой клиентов, которые приобретают мобильные телефоны или получают услуги мобильной связи. В отличие от клиентов, использующих платежные карты, клиенты банкинга на основе мобильной связи могут проводить операции в любом месте, где существует покрытие мобильной сети. Для них потребность в обращении к розничным агентам возникает только тогда, когда операции предусматривают внесение или снятие наличных денежных средств. Розничные агенты в модели с использованием небанковской (нефинансовой) организации выполняют такие же основные функции, как и в модели с привлечением банков. Они принимают и выдают наличные денежные средства, используя для этого мобильные телефоны или устройства считывания с карт для регистрации операций.

В ***комбинированных*** *моделях* коммерческие банки могут прибегать к услугам небанковской (нефинансовой) организации, либо выступать местом хранения денежной выручки (поступлений) небанковской организации при выпуске электронных денег. При этом инвестирование вырученных сумм позволяет небанковской организации получать доход и обес-

печивает ее ликвидность.

4.1.3. От противостояния банковской и небанковской модели – к их синергии

Формирование национальной розничной платежной системы требует целенаправленной технологической, организационной и правовой интеграции нескольких, до настоящего времени слабо взаимосвязанных, сегментов, которые формируют современный национальный рынок розничных платежно-расчетных услуг. Наряду с традиционными банковскими переводами денежных средств населения, включая операции по банковским картам, здесь присутствуют значимая доля почтовых переводов, бурно растущий рынок микроплатежей (в основном за услуги связи), представленный электронными (агентскими) платежными системами, а также нарождающиеся системы (квази-)электронных денег и мобильных платежей[25].

Каждый из разрозненных сегментов, составляющих национальную систему розничных платежей и денежных переводов, имеет собственные историю возникновения, назначение и порядок регулирования, основанный на различных право-

[25] Под мобильными платежными системами здесь понимаются системы платежей и перевода стоимости, построенные на основе нефинансовых организаций, движение расчетных единиц (передача поручений, инструкций) в которых осуществляется посредством использования мобильных устройств (телефонов) и не опосредует операций по личным банковским счетам абонентов.

вых принципах и законодательных (подзаконных) правовых актах. Технологические и правовые ограничения в совокупности определяют потенциальный уровень доступности соответствующих платежно-расчетных услуг.

Различается также потенциал развития рассматриваемых сегментов. Если объем традиционных банковских платежных операций ежегодно увеличивается на 20–25 %, не обнаруживая столь же заметного роста по количеству транзакций, то инновационный рынок микроплатежей, (квази-)электронных денег и мобильных финансов демонстрирует уверенный рост на 80—100 % в год при сопоставимом увеличении количества транзакций и постоянном расширении перечня оплачиваемых услуг. Наиболее бурное развитие наблюдается в областях, где собственно финансовые услуги (платежи, переводы) оказываются практически неотличимы с точки зрения нормативного регулирования и технического исполнения от услуг связи и коммуникации.

Действующее законодательство не содержит общих положений о платежах, расчетах и переводах. Это затрудняет систематическое регулирование и унификацию платежной сферы.

До настоящего времени розничная система безналичных банковских расчетов (платежей) была нацелена не на интеграцию, а на конкуренцию с широчайшей сетью сбора и обработки платежей за услуги связи, созданной мобильными операторами, а также с системами (квази-) электронных де-

нег, автономно развивающимися на платформе Интернета. Наметившееся сближение двух последних инновационных сегментов платежно-расчетной системы лишь обостряло задачи и вызовы, стоящие перед российскими банками. Достижение максимальной доступности банковских услуг станет возможным лишь в случае продуманного соединения технологических и операционных достоинств инновационных систем с классическими надзорными риск-ориентированными подходами, доминирующими в банковской сфере.

Развитая розничная платежно-расчетная система формирует базис для самого широкого предложения населению прочих финансовых услуг – кредитных, сберегательных, инвестиционных, страховых и пенсионных. Необходимо гарантировать, чтобы развитие инновационных (небанковских) сегментов этой системы не затрудняло предложение (обслуживание) через нее традиционных банковских продуктов.

Сложность универсального подхода к регулированию платежной системы объясняется специфическими чертами банковского права. Его известной особенностью является неразделенность (неразрывная связь) понятий «кредитная организация» (банк) и «банковская операция», которая в последующем перекочевала и закрепилась в гражданском праве. Этому во многом способствовала жесткая позиция банковского регулятора (ЦБ РФ), отстаивавшего исключительное право кредитных организаций на осуществление большей части банковских операций (оказание финансовых услуг).

Именно это обстоятельство серьезно усложняет подготовку и принятие законодательства о небанковских финансовых институтах (кооперативах, МФО), оказывающих населению отдельные виды финансово-банковских услуг.

Взгляд на банки (кредитные организации) как на эксклюзивных поставщиков банковских услуг прочно закрепился в доктрине гражданского и финансового права. В частности, только они вправе предоставлять кредиты (заключая кредитные договоры) и принимать депозиты (заключая договоры вклада). Субъектный состав признается одним из квалифицирующих признаков соответствующих гражданско-правовых договоров. Прочие финансовые институты (например, кредитные кооперативы) вынуждены использовать гражданско-правовые договоры «второго» сорта – договор займа (реальный договор) вместо кредитного договора (консенсуальный договор), договор передачи личных сбережений в пользование кредитному кооперативу вместо договора вклада. Наделение нового вида финансовых институтов правом осуществлять деятельность, схожую по содержанию с одной из банковских операций, до сих пор реализовывалось одним из двух возможных способов – (1) отнесением таких институтов к кредитным организациям либо (2) искусственным конструированием нового типа договоров. По второму пути законодатель, в частности, пошел при написании Федерального закона от 7 августа 2001 г. № 117-ФЗ «О кредитных потребительских кооперативах граждан».

Аналогичным образом Гражданский кодекс Российской Федерации наделяет кредитные организации исключительным право осуществлять безналичные расчеты на территории Российской Федерации, а банковское законодательство вводит для этих целей специальные виды банковских операций. С учетом того что понятие «безналичные расчеты», «платежи» и вообще «расчеты» нигде в законе не раскрывается, сохраняются самые широкие возможности для толкования этих понятий. Оказывается просто невозможным провести точное юридическое разграничение между банковской операцией (услугой) или (услугой) операцией по передаче информации, агентской услугой по приему денежных средств и т. д. Ситуация еще более запутывается, когда содержанием информационного сообщения становятся сведения о размере денежного обязательства, или когда агент, принимающий платежи от клиентов, предлагает свои услуги самому широкому числу продавцов.

4.1.4. От небанковского платежного агента к электронным деньгам

Платежный агент, оказывающий услуги по сбору платежей десяткам или даже сотням продавцом (в режиме билинга), по экономической сути ничем не отличается от расчетной кредитной организации. Другое дело, что на практике движение средств в его частной платежной системе осу-

ществляется не по текущим (банковским) счетам клиентов, а по виртуальным счетам (записи в компьютерной базе). При этом сам агент превращается в оператора платежной системы и обрастает широкой сетью субагентов. При возникновении временного разрыва между моментом внесения денежных средств в такую систему и моментом передачи распоряжения на их перечисление конкретному продавцу автоматически возникает система (квази-) электронных денег. Как уже было сказано, особенностью России является то, что такая система возникла «снизу», в результате технических и организационных инноваций участников телекоммуникационного рынка, в отсутствие какого-либо специального регулирования и за пределами банковского сектора. Более того, все существующее до сегодняшнего дня регулирование Банка России вообще никак не затрагивает существующих небанковских эмитентов (квази-)электронных денег.

Эффективное регулирование электронных денег и других предоплаченных инструментов является важной предпосылкой развития розничных (микро-)платежных систем. Все больше организаций выходят за рамки обычных платежных услуг и предлагают виртуальный текущий счет, на котором клиент может разместить средства в электронной форме на неограниченный период времени и осуществлять платежные и другие денежные переводы в любой момент. Эти модели в силу того, что они облегчают платежи благодаря использованию мобильных телефонов и терминалов, таят в се-

бе огромный потенциал для развития внеофисного банкинга, поскольку они эффективно формируют сеть розничных платежей, которая значительно превосходит существующую банковскую сеть и сеть POS-терминалов.

Однако если речь идет о модели с использованием небанковской организации, в которой оператор мобильной сети, эмитент предоплаченных карт или оператор электронной платежной системы создает виртуальный счет для клиента, а клиент не имеет договорных отношений с банком, который подлежит пруденциальному регулированию и надзору, уровень контроля является минимальным или вообще отсутствует.

Даже если средства, полученные лицом, оказывающим услугу, хранятся в банке и накапливаются на его счете, клиент может заявлять требования только в отношении такого лица, но не его банка. Более того, если не существует норм, направленных на разрешение таких проблем, то отсутствуют гарантии того, что у эмитента хватит ликвидности, чтобы удовлетворить требования потребителя, а также что такие требования потребителей будут иметь приоритет по отношению к требованиям других кредиторов эмитента.

Конец ознакомительного фрагмента.