



Fin
Mobility

Представляет спецвыпуск

SuperДайджест

статей по

МОБИЛЬНОМУ БАНКИНГУ

Форум «FinMobility-2013. Мобильный банкинг и маркетинг».
Практические кейсы лучших мобильных банков в России

Мобильный банк – дань хипстерской моде?
Или канал банковских продаж?

Вся информация о форуме на сайте finmobility.ru



www.reglament.net

FutureBanking™

www.futurebanking.ru

Статьи и материалы в Дайджесте защищены Законом РФ "Об авторском праве и смежных правах".
Перепечатка и распространение материалов запрещено без письменного согласия ООО «Регламент-Медиа»

Содержание

Форум профессионалов

Уступит ли интернет-банкинг свои позиции мобильному банкингу?

Сегодня в мире большинство крупных банков предлагают своим клиентам использовать для управления счетом мобильные приложения. Уже разработано мобильное приложение по снятию денежных средств в банкоматах без использования пластиковых карт. По итогам 2012 года оборот платежей через мобильный банкинг в России составил 8 млрд рублей, к 2017 году эта цифра, по мнению экспертов, может достичь 29 млрд рублей. Станут ли в ближайшее время услуги мобильного банкинга более востребованными, чем услуги интернет-банкинга?



А.А. БАБЕНКО, ЗАО НИП «Информ-защита» (РА-QSA),
руководитель направления

Мобильность без опасности

Масштабный рынок мобильных услуг стремительно растет за счет развития мобильных технологий. И одними из первых активно предлагать своим клиентам новейшие технологичные сервисы стали финансовые организации. С какими рисками сегодня сталкиваются банки, предлагающие мобильные услуги? Каковы превентивные меры обеспечения безопасности мобильного банкинга? В чем уязвимость систем аутентификации пользователя?



Ю.В. ДЕМЕНЮК, ВТБ24, вице-президент, заместитель директора
департамента розничного бизнеса

Мобильный или интернет-банкинг: что предлагать клиентам?

Мир поменялся — и в этом уже нет никаких сомнений. Мобильность сервисов достигла того уровня, когда ее уже никто не может игнорировать. С появлением телефонов мы оказались на связи 24 x 7, где бы ни находились, сейчас мы в ответ требуем, чтобы любой предлагаемый сервис был доступен 24 x 7 из любой точки мира с привычных портативных устройств — будь это лэптоп, мобильный телефон или планшет. Развитие интерактивных сервисов и постоянно растущие требования к удобству лишь сопровождают этот процесс. Что же вызвало эти процессы глобальной мобилизации сервисов и какую роль в них играют банковские институты?



П.В. РЕВЕНКОВ, Банк России, департамент банковского регулирования и надзора, заведующий сектором, к.э.н.

Мобильный банкинг: внутренний контроль источников рисков

Помимо множества преимуществ технологий дистанционного банковского обслуживания, существует ряд особенностей их функционирования, приводящих к возникновению дополнительных источников банковских рисков, включая риски отмывания денег. Автор рассматривает общую модель отмывания денег с использованием систем мобильного банкинга и порядок анализа источников сопутствующих рисков службой внутреннего контроля кредитной организации.



В.Ю. КОПЫТИН, Южный федеральный университет, кафедра бухгалтерского учета и аудита, доцент, к.э.н.

Мобильные платежные технологии: процедуры, стандарты, тенденции

В статье в систематизированном виде представлено описание платежно-расчетного взаимодействия участников платежных систем на основе мобильных телекоммуникационных стандартов и устройств. В контексте основных принципов разработки и функционирования платежных систем рассматриваются вопросы использования мобильных технологий, а также приводится обзор тенденций развития рынка мобильных платежных услуг за рубежом и в России.

Эволюция спроса и перспективы развития мобильного банкинга (фрагмент практического пособия «Электронные платежи: специфика, регулирование, технологии»)

Уступит ли интернет-банкинг свои позиции мобильному банкингу?

Сегодня в мире большинство крупных банков предлагают своим клиентам использовать для управления счетом мобильные приложения. Уже разработано мобильное приложение по снятию денежных средств в банкоматах без использования пластиковых карт. По итогам 2012 года оборот платежей через мобильный банкинг в России составил 8 млрд рублей, к 2017 году эта цифра, по мнению экспертов, может достичь 29 млрд рублей. Станут ли в ближайшее время услуги мобильного банкинга более востребованными, чем услуги интернет-банкинга?



А.Б. ДУДКА,
*ГУ Банка России
по Омской области,
к.э.н.*

В последние несколько лет наблюдается «бум» внедрения технологий дистанционного банковского обслуживания отечественными кредитными организациями, причем развитие их непосредственно следует за достижениями в области технологий компьютерной связи.

Например, обеспечиваемые системами интернет-банкинга удобства и гибкость получения банковских услуг привели к широкому распространению таких технологий первоначально среди юридических лиц — пользователей систем предыдущей эпохи «клиент–банк». Учитывая обострение борьбы за клиентуру и рынки сбыта финансовых продуктов, большинство кредитных организаций не ограничивается лишь одним каналом дистанционного банковского обслуживания, наращивая «технологические мышцы». Продолжая эволюцию систем интернет-банкинга, начинает свое развитие мобильный банкинг. С учетом количества мобильных телефонов и смартфонов в России данный вид дистанционного банкинга по праву может считаться наиболее перспективным среди населения на текущий момент. А общность используемых технологий и каналов связи во многом позволяет считать мобильный банкинг одной из разновидностей интернет-банкинга.



Вместе с тем не следует забывать, что внедрение систем электронного банкинга приводит к не всегда заметному смещению профилей рисков кредитных организаций, к чему многие из них на практике оказываются не готовы. Ситуация усугубляется еще и тем, что зачастую банки оказываются зависимыми от сторонних компаний — провайдеров, о телекоммуникационных системах которых специалисты кредитных организаций могут не иметь необходимых сведений. Следствием этого становятся крупные потери кредитных организаций и их клиентов из-за компьютерных мошенничеств и хищений, сетевых и вирусных атак, ошибок и инцидентов информационной безопасности. Все это как минимум повышает требования к уровню квалификации служб информационной безопасности и СВК банков.

На сегодняшний день мобильные устройства являются неотъемлемым атрибутом практически каждого из нас. Функциональные возможности мобильных устройств постоянно расширяются, при этом наряду с традиционными, характерными для пользователей мобильных устройств приложениям высоким спросом пользуются приложения коммерческих банков. На мой взгляд, динамика увеличения востребованности приложений мобильного банкинга на фоне увеличения проникновения мобильных устройств, а также повышения финансовой грамотности населения, наличия тарифных барьеров на совершение тех или иных операций в отделениях банков продолжится.

При этом указанная тенденция развития не окажет существенного влияния на снижение интереса населения к интернет-банкингу, так как традиционно мобильные приложения содержат популярный, но неполный перечень возможностей по расчетам и управлению средствами дистанционно. Стоит отметить, что имеющиеся ограничения способствуют более высокому уровню понятности функционала мобильных приложений и возможности их использования «на ходу». Это, в свою очередь, позволяет сделать вывод, что особенности каждого из направлений соответствуют определенной модели поведения клиента, его потребностям в конкретный момент времени. Как следствие, мобильный банкинг и интернет-банкинг не исключают друг друга и не конкурируют, а скорее дополняют друг друга, обеспечивая доступность банковских услуг для населения в соответствии с современными требованиями жизни.



Н.К. БОРИСОВА,
«Банк «Санкт-Петербург», Дирекция розничного бизнеса, заместитель директора — руководитель бизнеса электронной коммерции



А.В. АЛЕКСАХИН,
*Альфа-Банк, заме-
ститель директора
по развитию элект-
ронных услуг*

Я убежден, что мобильный банкинг превзойдет по популярности интернет-банкинг, причем случится это в обозримом будущем. Уже сейчас доля операций через мобильный банк «Альфа-Мобайл» среди операций клиентов, которые они осуществляют с помощью удаленных каналов, составляет около 30%. Более того, эта доля продолжает уверенно расти. Причем если раньше это были в основном операции по оплате мобильной связи, то сейчас растет доля операций, которые клиенты обычно совершали в интернет-банке, — например, платежей в другой банк. Это неудивительно, если учитывать все возрастающие возможности мобильных телефонов, распространение смартфонов, существенное развитие мобильного Интернета. Немаловажно и то, что ритм жизни современного человека все больше и больше ускоряется — ему все чаще требуются инструменты для совершения банковских операций «на бегу».



М.П. ЧУБАК,
*ОАО «Нордеа Банк»,
начальник отдела
инноваций и развития
работы с клиент-
скими сегментами*

Не совсем корректно рассматривать интернет- и мобильный банкинг как конкурирующие сервисы. Это скорее эволюция каналов предоставления банковских услуг.

Еще недавно клиенту для совершения банковского перевода со своих счетов требовалось лично посещать офис банка, чтобы отдать соответствующее поручение. В результате развития информационных технологий банки вышли за пределы стен офисов, сделав возможным дистанционное обслуживание своих клиентов. Более того, в условиях тотальной глобализации и постоянной нехватки времени подобные изменения стали жизненно необходимы. Результатом стал расцвет банковских интернет-сервисов, удобных как для клиентов (возможность получения банковских услуг, не выходя из дома), так и для банков (снижение операционных издержек, уменьшение живых очередей в отделениях). Развитие микроэлектроники и мобильных технологий связи сделало возможной следующую ступень этой эволюции. Сегодня компьютер, телефон, фотоаппарат, видеокамера и даже удаленное рабочее место умещаются в одном небольшом устройстве. Как следствие, появление мобильных банковских приложений было лишь вопросом времени. Мобильный банкинг является сервисом, делающим банковское обслуживание еще более доступным и удобным для потребителей. И, пожалуй, наиболее интересным с точки зрения перспектив развития. Но это ни в коем случае не означает, что традиционные каналы предоставления банковских услуг прекратят существование, ведь каждый клиент выбирает для себя то, что ему наиболее удобно.

дистанционный банкинг \ профиль рисков \ мобильные приложения

Развиваться будут оба рассматриваемых вида электронного банкинга. Причем интернет-банкинг будет иметь больше клиентов среди юридических лиц, а мобильный банкинг — среди физических.

Основная привлекательность последнего объясняется прежде всего желанием клиентов (особенно молодого поколения) не только быть всегда на связи, но и иметь возможность делать небольшие платежи или оплачивать покупки, не прибегая к каким-то другим устройствам, то есть действовать по принципу «мой офис там, где я».

Пожалуй, единственный вопрос, который остается открытым, — это обеспечение необходимого уровня безопасности, что является основным условием доверия клиентов к любому виду дистанционного банковского обслуживания. Если банки смогут добиться такой защиты (включая терпимость клиентов к использованию дополнительных средств защиты), чтобы кражи с «мобильных» счетов клиентов стали просто невыгодны для злоумышленников, то количество таких краж будет сведено к минимуму. В таких условиях можно с большой долей вероятности рассчитывать, что рост числа клиентов мобильного банка будет выше, чем у интернет-банкинга. 



П.В. РЕВЕНКОВ,
Банк России, Департамент банковского надзора, заведующий сектором, к.э.н.

Мобильность без опасности

Масштабный рынок мобильных услуг стремительно растет за счет развития мобильных технологий. И одними из первых активно предлагать своим клиентам новейшие технологичные сервисы стали финансовые организации. С какими рисками сегодня сталкиваются банки, предлагающие мобильные услуги? Каковы превентивные меры обеспечения безопасности мобильного банкинга? В чем уязвимость систем аутентификации пользователя?

Уже с начала 2000-х гг. российские банки стали предлагать своим клиентам услуги по удаленному управлению безналичными средствами и предоставлению информации. На сегодняшний день все большую популярность приобретают системы мобильного банкинга. Стоит отметить, что изначально данные системы могли предложить пользователям ограниченный функционал, который чаще всего сводился лишь к предоставлению информации без возможности осуществления каких-либо операций. Однако бум мобильных технологий позволил гаджетам сравняться по функционалу с ПК. А услуги мобильного банкинга стали востребованными среди обладателей мобильных устройств.

Основные риски мобильного банкинга

По результатам исследования MobileBankingRank 2012, проведенного в июне 2012 г. аналитическим агентством Marksw WebbRank&Report, среди 30 крупнейших российских розничных банков мобильный банкинг в том или ином виде предлагают 22 банка. Чаще всего банки предлагают такие услуги через интерфейс мобильных сайтов (реализовано у 12 банков из исследуемых), приложений для iOS (12 банков) и Android (11 банков).

Современный сервис мобильного банкинга включает большой спектр услуг, в том числе:



А.А. БАБЕНКО,
ЗАО НИП «Информ-
защита» (РА-QSA),
руководитель направ-
ления



По результатам исследования MobileBankingRank 2012, проведенного в июне 2012 г. аналитическим агентством Marksw WebbRank&Report, среди 30 крупнейших российских розничных банков мобильный банкинг в том или ином виде предлагают 22 банка.

- оплата услуг мобильного оператора, интернет-провайдера, услуг ЖКХ, коммерческого телевидения;
- переводы денежных средств между своими счетами, внутри-банковские переводы, переводы в другой банк;
- просмотр информации по счетам, доступного баланса, детальной информации по движениям средств, информации по кредитам и депозитам;
- информационные сервисы: курсы валют, справочная информация о ближайших отделениях, банкоматах и другая информация.

Однако популярность и расширение функционала сервиса имеют и обратную сторону медали — пристальное внимание кибермошенников. Поэтому вместе с развитием мобильного банкинга растет число связанных с ним схем мошенничества. Пристальное внимание злоумышленников легко объяснимо. Как было сказано выше, мобильный банкинг наряду с информационными сервисами предоставляет возможность управления счетами клиента. Это означает, что компрометация системы мобильного банкинга может принести прямую финансовую выгоду мошенникам и, следовательно, эта система является одной из наиболее привлекательных мишеней.

Рассмотрим основные риски при использовании мобильного банкинга:

- раскрытие информации о счетах и совершенных операциях пользователя;
- подмена данных в реквизитах операций;
- совершение несанкционированных операций от лица пользователя;
- отказ в обслуживании.

Данные риски возникают из-за следующих основных недостатков систем/приложений мобильного банкинга:

- небезопасное хранение данных;
- слабый контроль операций, совершаемых клиентом, со стороны сервера приложений;
- недостаточная защита данных при передаче;
- уязвимость клиентского приложения;
- недостаточно надежная аутентификация и авторизация;
- некорректное использование сессионных механизмов;
- небезопасное взаимодействие со сторонними приложениями;
- некорректная настройка права доступа;
- неучтенные источники хранения данных;
- некорректное применение криптографии;
- раскрытие чувствительной информации;

- логические ошибки в предоставляемых операциях;
- использование ложного программного обеспечения;
- действия вредоносного программного обеспечения.

Кроме того, специфика мобильного устройства предполагает появление новых рисков, которых нет при использовании для удаленного банковского обслуживания персонального компьютера. Априори гаджеты больше подвержены утере/краже (или временному контролю со стороны злоумышленника). Возможность использования различных технологий связи (сотовая связь, wi-fi, bluetooth, NFC) также увеличивает количество потенциальных уязвимостей в системе.

Стратегия защиты

Несмотря на обширный перечень угроз, количество применяемых на данный момент средств защиты не так велико. Главной и основной превентивной мерой обеспечения безопасности сервиса мобильного банкинга является включение мер информационной безопасности при проектировании и разработке соответствующего программного обеспечения. Разработка программного обеспечения под мобильные платформы имеет свои специфические особенности. При этом накопленный опыт разработчиков зачастую не позволяет учитывать все нюансы использования практик безопасного программирования. Наконец, нередко случаи, когда проектирование программных средств для мобильных устройств осуществляется аналогично классическому программному обеспечению без учета специфики устройств и дополнительно возникающих рисков.

К основным недостаткам, допускаемым в процессе разработки мобильного программного обеспечения, относятся:

- хранение информации на устройстве в открытом виде, использование для хранения флэш-карт;
- шифрование информации с использованием криптографически слабых алгоритмов шифрования;
- хранение ключей шифрования вместе с зашифрованными данными, использование «захардкоженных» ключей (т.е. встроенных прямо в программный код);
- сохранение в кэше конфиденциальной информации;
- назначение общедоступных привилегий для хранимой информации;
- передача информации в открытом виде;
- отсутствие либо недостаточная фильтрация и типизация данных, обрабатываемых приложением;

Нередки случаи, когда проектирование программных средств для мобильных устройств осуществляется аналогично классическому программному обеспечению без учета специфики устройств и дополнительно возникающих рисков.

- использование идентификаторов устройства (IMEI, UUID) в качестве аутентифицирующих параметров либо идентификаторов сессии;
- использование в качестве идентификатора сессии легко предсказуемых значений;
- запись критичной информации в лог-файлы, «снимки» экрана, временные файлы;
- перенос конфиденциальной бизнес-логики сервиса в мобильное приложение;
- отсутствие контроля поступающих данных на стороне сервера приложений.

Нередко возникают проблемы с безопасностью, связанные с неучтенной спецификой мобильной платформы. Так, мобильные устройства одного из лидеров рынка смартфонов при возникновении более приоритетной операции (например, входящего звонка) делают «снимок» экрана и сохраняют его во временных файлах.

Отдельно стоит отметить класс логических ошибок. Данный вид ошибок практически не обнаруживается автоматизированными средствами и сложно вычисляется при тестировании. В качестве примера приведем известную уязвимость в дистанционном банкинге, обнаруженную специалистами ACROS Security. Исследователи обратили внимание, что округление чисел при проведении операций осуществляется до второго порядка. Таким образом, клиент банка мог осуществить обмен 1 цента на 1 евроцент, притом что реальная разница курса валюты составляла 25%, но 0,007 евро всегда округлялись до значения 0,01. В классическом банковском обслуживании данная ситуация не привлекла бы повышенного внимания. Но в дистанционном банкинге существует возможность выполнения множества операций за небольшие промежутки времени без участия человека. В описанном случае эта возможность приводит к многотысячным потерям в сутки при выполнении вполне легитимных действий.

Нередко возникают проблемы с безопасностью, связанные с неучтенной спецификой мобильной платформы. Так, мобильные устройства одного из лидеров рынка смартфонов при возникновении более приоритетной операции (например, входящего звонка) делают «снимок» экрана и сохраняют его во временных файлах для возможности быстрого возврата к используемому приложению. В данной ситуации при отсутствии маскирования значений «логин/пароль» во входной форме злоумышленник может спровоцировать сохранение в незащищенном виде критичной аутентифицирующей информации.

Следующий способ защиты от угроз безопасности информации — встроенные в приложение защитные механизмы. На сегодняшний день самым популярным и практически единственным из них является система аутентификации пользователя. Выражается она в большинстве случаев в запросе пары «логин/пароль», но может

быть усилена дополнительными факторами. Например, значением с PIN-калькулятора. Отметим, что использование классической для интернет-банкинга схемы двухфакторной аутентификации (помимо пары «логин/пароль» используется код, переданный через sms) в случае мобильного банкинга практически бесполезно. Исключением служат лишь случаи, когда для получения sms с кодом используется другое устройство.

Для мобильного банкинга неактуален еще один достаточно действенный способ быстрого реагирования на несанкционированные операции — sms-оповещение о списании средств со счета.

Как можно заметить, меры, действенные в других видах дистанционного банковского обслуживания, оказываются нежизнеспособными при обеспечении безопасности мобильного банкинга.

Особое внимание необходимо уделять обеспечению безопасности непосредственно устройства и операционной системы, с которой работает прикладное ПО. Все чаще появляется информация о новых типах вредоносного ПО для мобильных платформ. К сожалению, рост популярности мобильных устройств прямо пропорционален росту обнаруженных уязвимостей и брешей в их безопасности. Как следствие — появление множества автоматизированных средств, эксплуатирующих обнаруженные «дыры».

Как избежать проблем

Избежать заражения помогают достаточно простые правила безопасности — своевременная установка обновлений безопасности, выпущенных производителем, отсутствие «джейлбрейка» (повышения привилегий на устройстве), установка программ только из доверенных источников, установка средств антивирусной защиты и персонального межсетевого экранирования. Дополнительными мерами защиты будут:

- требование аутентификации при доступе к устройству;
- активирование беспроводных интерфейсов только при необходимости использования в доверенных сетях;
- контроль доступа приложений к личным данным, хранящимся на устройстве;
- посещение только доверенных внешних ресурсов.

Пользователю системы мобильного банкинга стоит помнить, что утерю мобильного устройства с системой мобильного банкинга в большинстве случаев необходимо рассматривать как получение злоумышленником доступа к управлению его счетами. Поэтому в первую очередь при возникновении прецедента необходимо осу-

Пользователю системы мобильного банкинга стоит помнить, что утерю мобильного устройства с системой мобильного банкинга в большинстве случаев необходимо рассматривать как получение злоумышленником доступа к управлению его счетами.

Программное обеспечение

существить блокировку доступа к системе мобильного банкинга и номера телефона.

Следующее, на чем стоит остановиться, — это программное обеспечение, используемое клиентом. При использовании надежных централизованных сервисов загрузки приложений проблема подмены не возникает. Но при использовании сервисов без должного входного контроля не исключена вероятность подмены используемого обеспечения и осуществления атаки типа «человек посередине», при которой злоумышленник получает возможность просмотра и изменения передаваемой информации.

Еще одним слабым местом мобильного банкинга становится доверие к номеру и SIM-карте абонента. На сегодняшний день есть прецеденты изготовления мошенниками дубликатов SIM-карт с использованием поддельных доверенностей от имени клиента и их дальнейшего использования для доступа к системе дистанционного банкинга. Возможность проведения данного типа мошенничества в большей степени зависит от изначальной архитектуры и реализации приложения. Но и для клиента отказ в работоспособности имеющейся SIM-карты должен служить тревожным сигналом.

Хорошей практикой является использование отдельно выделенного устройства только для осуществления доступа к системе мобильного банкинга. Такая мера будет способствовать резкому сокращению вероятности заражения через недоверенные источники и рисков компрометации злоумышленником. Но при этом неизбежны существенные затраты и уменьшение привлекательности использования сервиса.

Заключение

Производители ПО для мобильных платформ должны учитывать специфику работы устройств и требования информационной безопасности при проектировании и создании программного средства. Банк, предоставляющий услугу, должен обеспечить пользователей всей информацией о безопасном использовании сервиса, признаках мошеннических операций и правилах реагирования на произошедшие инциденты. Анализ различных характеристик и запросов от пользователя в реальном времени и выявление подозрительных операций позволяют банку повысить уровень безопасности своей системы мобильного банкинга.

При этом защита средств мобильного банкинга, как и многих других сервисов, всегда является задачей не только лиц, предоставляющих услугу, но и клиентов, ее использующих. Клиенты мобиль-

На сегодняшний день уже есть прецеденты изготовления мошенниками дубликатов SIM-карт с использованием поддельных доверенностей от имени клиента и их дальнейшего использования для доступа к системе дистанционного банкинга.

ного банкинга должны четко следовать рекомендациям банка в области обеспечения информационной безопасности при использовании сервиса, с осторожностью относиться к недоверенным источникам информации, особенно при установке программного обеспечения и посещении веб-сайтов, своевременно устанавливать обновления системного и прикладного ПО. К мобильному устройству с установленным сервисом рекомендуется относиться как к личному кошельку — станет ли человек оставлять личный кошелек с деньгами без присмотра, отдавать его на хранение людям, которым он не доверяет? Или отдавать в ремонт, не убедившись, что все ценное из него извлечено?

В настоящий момент средства мобильного банкинга не могут похвастаться высоким уровнем защищенности. Причина этого кроется в отсутствии наработанного опыта в данной области, не столь массовом распространении и специфичных особенностях платформ. Однако отчасти эти же причины являются дополнительными преимуществами в использовании: количество вредоносного программного обеспечения под мобильные платформы на порядок меньше, чем под «десктопные» операционные системы, малое распространение делает непривлекательным создание специализированного шпионского ПО для конкретных версий приложения интернет-банкинга. Технология мобильного банкинга, как и любая другая информационная технология, связанная с финансами, всегда будет под пристальным вниманием кибермошенников, а развитие мер защиты приведет к появлению новых методов атаки. Важно понимать лишь то, что для мошенника неважна цель компрометации, и под массовые «взломы» попадают наименее защищенные системы. Помня и соблюдая элементарные правила обеспечения информационной безопасности (это касается как банков-разработчиков, так и клиентов), можно существенно снизить риск того, что пользователи мобильного банкинга окажутся целью злоумышленников. 

Мобильный или интернет-банкинг: что предлагать клиентам?

Мир поменялся — и в этом уже нет никаких сомнений. Мобильность сервисов достигла того уровня, когда ее уже никто не может игнорировать. С появлением телефонов мы оказались на связи 24 × 7, где бы ни находились, сейчас мы в ответ требуем, чтобы любой предлагаемый сервис был доступен 24 × 7 из любой точки мира с привычных портативных устройств — будь это лэптоп, мобильный телефон или планшет. Развитие интерактивных сервисов и постоянно растущие требования к удобству лишь сопровождают этот процесс. Что же вызвало эти процессы глобальной мобилизации сервисов и какую роль в них играют банковские институты?

Глобальные процессы: драйверы развития ДБО и роль мобильного канала



Ю.В. ДЕМЕНЮК,
*ВТБ24, вице-президент,
заместитель дирек-
тора департамента
розничного бизнеса*

Парижское метро не отличается особенной комфортностью, но Парижу можно многое простить. Вагон полупустой, по сути, несколько человек. Пожилой мужчина листает iPad, компания молодых ребят в конце вагона смотрит на телефоне фотографии. Лишь молодая и с виду респектабельная дама сосредоточенно читает модный журнал. Однако и она вскоре его откладывает и начинает что-то также сосредоточенно проверять на своем iPhone четвертого поколения.

Конечно, очень большую роль в процессах глобальной мобилизации сервисов сыграло развитие инфраструктуры — совершенствование телекоммуникационных технологий, а также развертывание мобильными операторами поддерживающих их сетей — от EDGE к Wi-Fi и 3G к сетям четвертого поколения (LTE). На этом фоне активно шло проникновение мобильного Интернета, а постоянно снижающиеся издержки дали возможность мобильным операторам ввести безлимитные тарифы на передачу данных.

В свою очередь, одной из причин запуска этих процессов стали постепенно формирующиеся потребности пользователей получать интерактивные, все более качественные решения взаимодействия



и потребления информации и контента. Для нас стало привычным делать покупки в Интернете, получать помощь и консультации в режиме реального времени, отдавать предпочтение электронным медиаизданиям. Следующим очевидным шагом должно было стать появление мобильных и **always-on мобильных платформ, позволяющих оптимизировать работу с контентом**. Как итог, на рынке появились платформы iPhone, Android, iPad. И именно в этот момент граница была окончательно преодолена — потребности, инструменты и инфраструктура сошлись вместе, чтобы поменять мир навсегда. Все эти процессы происходили одновременно, и сейчас уже сложно определить, что же оказалось основным драйвером. Одно неоспоримо — эти процессы подспудно были направлены на достижение одной цели — на удовлетворение «невыраженной», но в то же время очень мощной потребности клиентов в постоянном доступе к информации и контенту (рис. 1).

Теперь клиенты хотят получать любой сервис в режиме 24×7 , где бы они ни находились, и банки не могут и не должны оставаться в стороне. Клиентам теперь важно получать доступ к сервисам дистанционно, причем в наиболее комфортных условиях, через излюб-

Рисунок 1

Изменение моделей потребления финансовых услуг



Общество вступило в эру стремительного изменения пользовательских моделей поиска, распространения, потребления информации и интерактивных сервисов — одним из основных трендов является перевод традиционного опыта и сервисов из физического пространства в электронное (digitalization of the experience)

ленные устройства и с учетом той обстановки, в которой они находятся. Соответственно спектр каналов, через которые предоставляются банковские сервисы, должен расширяться. Если еще недавно интернет-канала обслуживания было вполне достаточно, то сейчас банк просто обязан предоставлять своим клиентам банковские приложения для всех наиболее популярных современных мобильных платформ. И, видимо, это только начало пути. Если для клиента такой подход означает дополнительную ценность, то от банков он требует концептуально иных архитектурных и организационных решений.

Если еще недавно интернет-канала обслуживания было вполне достаточно для удовлетворения большинства запросов клиентов, то сейчас банк обязан предоставлять своим клиентам банковские приложения для всех наиболее популярных современных мобильных платформ.

Так уж случилось, что потребность в изменениях оказалась на руку самим банкам: внедрение клиентоориентированных подходов и поиск банками эффективных каналов обслуживания и продаж вызвали необходимость развития и активного продвижения среди клиентов дистанционных каналов. Офис банка постепенно становится высокопрофессиональным консультационным центром, а все рутинные операции переводятся на дистанционные технологии: Интернет, мобильный банкинг, информационно-платежные терминалы.

Если говорить о той ценности, которую мобильные решения несут для банков, то в первую очередь это — удовлетворение спроса на мобильные услуги и сохранение конкурентных позиций, снижение издержек ввиду относительной дешевизны каналов дистанционного обслуживания, появление потенциально очень эффективного инструмента формирования лояльности клиентов, а также возможность предоставления дополнительных сервисов, основывающихся на специальных возможностях телефона.

Активное развитие рынка мобильного банкинга: быстрорастущий и многогранный рынок

В России активно происходит проникновение мобильных интернет-сервисов — 61 % клиентов интернет-банкинга регулярно просматривают при помощи мобильного телефона интернет-ресурсы, 24 % — закачивают мобильные приложения (по данным исследования ВТБ24, проведенного в конце 2010 г.). В свою очередь, активное развитие мобильных интернет-сервисов является драйвером для быстрого роста рынка мобильного банкинга: если рост числа активных пользователей интернет-банкинга в России до 2014 г. прогнозируется на уровне 35 %, аналогичный показатель для мобильного банкинга — 105 %. По нашим оценкам, к 2014 г. число пользователей мобильного банкинга финансовых институтов достигнет 4,3 млн человек.

В то же время стоит отметить наличие большого количества разнородных игроков (финансовые институты, платежные системы, мобильные операторы), присутствующих или заинтересованных в выходе на рынок с различным уровнем опыта в оказании финансовых услуг, продвижении продуктов и т.д., а также возможных технологий реализации мобильного банкинга, что создает пространство для внедрения кардинально отличающихся бизнес-моделей, включая модели, предполагающие сотрудничество между финансовыми институтами и мобильными операторами.

Стоит отметить, что всплеск активности использования интернет-сервисов во многом связан с появлением на рынке удобных мобильных инструментов управления и потребления контента: платформ iPhone, Android, iPad. Множество сравнительных исследований лишь подтверждают этот факт. Однако не стоит забывать, что на рынке до сих пор находится значительный парк устройств на других платформах, таких как Symbian и WM.

Выбор наиболее удобного канала мобильного банка лучше оставить за самим пользователем

Среди каналов мобильного банка можно выделить мобильный сайт интернет-банка, мобильные приложения мобильного банка и sms-банкинг.

1. Мобильный сайт (PDA) — это версия интернет-банка, адаптированная под мобильный браузер. Основными достоинствами мобильного сайта являются удобство ее использования на небольшом экране мобильного телефона по сравнению с интернет-версией, а также снижение интернет-трафика. В основном этот канал привлекателен для клиентов банка среднего класса и «консервативных» клиентов, так и не оценивших всех прелестей своих iPhone. Преимуществом канала является его доступность, так как практически все современные мобильные телефоны (за исключением самых дешевых моделей) позволяют выйти в Интернет через мобильный браузер. По функционалу канал может быть максимально приближен к функционалу интернет-банка.

2. Мобильные приложения позволяют предложить более богатый пользовательский интерфейс, а также могут задействовать аппаратные возможности телефона, такие как GPS, GSM-модуль, камера. По сравнению с браузерной версией подобные приложения позволяют сократить потребляемый трафик, так как на телефон загружаются только данные, а не интерфейс. Возможности современных платформ практически безграничны и постоянно развиваются,

Возможности современных платформ позволяют клиенту в удобном и безопасном режиме использовать максимальный перечень сервисов: управлять своими финансами, выполнять операции, получать в онлайн-режиме информацию банка (геолокация банкоматов, офисов, курсы валют...), в случае необходимости коммуницировать с банком.

что позволяет клиенту в удобном и безопасном режиме использовать максимальный перечень сервисов: управлять своими финансами, выполнять операции, получать в онлайн-режиме информацию банка (геолокация банкоматов, офисов, курсы валют...), в случае необходимости коммуницировать с банком.

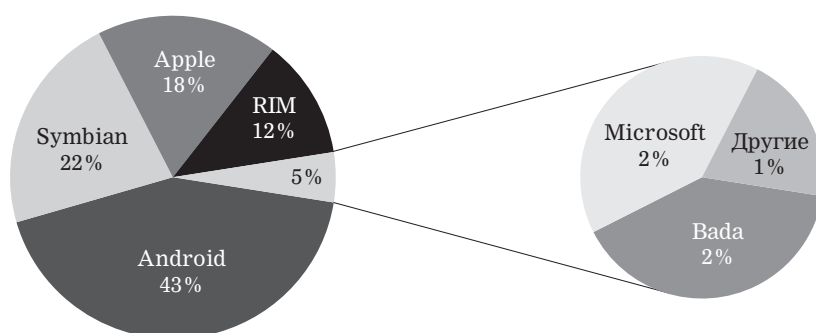
Устанавливаемые приложения можно развивать в двух направлениях: разрабатывать специально написанные под операционную систему смартфона нативные приложения мобильного банка или использовать универсальные J2ME-программы. Программы, написанные специально для операционной системы смартфона или коммуникатора, рациональней используют ресурсы процессора и потенциально могут обладать бóльшим функционалом, чем «универсальные» J2ME-программы. Создание нативных приложений сегодня неизбежно и в силу того, что некоторые производители из маркетинговых соображений искусственно урезают возможности операционной системы, не позволяя устанавливать на нее программы других разработчиков и ограничивая способы распространения приложений. Компания Apple, которая является законодателем мод среди бесклавиатурных телефонов, позволяет устанавливать исключительно приложения из магазина приложений App Store.

Определяя для себя путь развития, ВТБ24 ориентировался на высокоактивных пользователей мобильных устройств и ставил своей целью предложить безопасное, доступное, престижное, а главное — удобное и современное решение. Поэтому мы отдали предпочтение развитию нативных приложений.

При выборе платформ для разработки мобильных устройств мы исходили из текущего положения рынка и трендов его развития. Основными конкурентами на рынке сейчас являются платформа для смартфонов с открытым исходным кодом Android и iOS — операционная система телефонов iPhone. Разработка приложений для этих платформ стала первым этапом создания современного мобильного банка ВТБ24. Крупную долю среди инсталлированной базы также занимают компактная ОС компании Microsoft Windows Mobile и операционная система телефонов Nokia Symbian OS.

Среди остальных платформ можно выделить не очень распространенную на российском рынке BlackBerry OS (RIM) и новую разработку компании Microsoft Windows Phone 7 (рис. 2). Доля этих и прочих платформ пока еще слишком мала, но мы пристально наблюдаем за их развитием в частности и рынка в общем, чтобы предвосхитить потребности наших клиентов в поддержке банком различных операционных систем.

Рисунок 2

Доля продаж смартфонов в мире во II квартале 2011 г. в разбивке по операционным системам (по данным Gartner)

3. Sms-банкинг является основным каналом для пользователей, требующих в основном информирования об операциях и проведения наиболее простых и распространенных платежей при помощи sms-команд. Sms-банкинг также является незаменимым в отсутствие доступа к Интернету, так что мы отмечаем пик активности работы в этом канале, как правило, в периоды отпусков. Sms-канал отлично подходит для информирования клиентов (оповещения) и периодических информационных запросов (остаток по счету, последние операции). К недостаткам этого канала можно отнести ограниченность функционала, являющуюся следствием поиска компромисса между функциональностью, удобством и безопасностью.

Тем не менее выбор наиболее удобного для использования канала стоит оставить за пользователем, который сам сопоставит свои потребности и возможности выбранного им устройства. Развитие технологий, используемых в мобильных телефонах, и телекоммуникационного сектора уже превратило гаджеты в незаменимых помощников современного человека. Целью мобильного банка должно являться удовлетворение потребностей вечно занятых людей в простом, удобном, безопасном и сравнительно дешевом способе управления своими счетами и получения банковских сервисов. При этом никто, кроме самого пользователя, не может знать, как и с помощью какого канала ему будет удобнее пользоваться банковскими сервисами. Именно поэтому оптимальным решением будет внедрение всех мобильных устройств (как и поступили, например, в ВТБ24), чтобы каждый из клиентов банка мог воспользоваться

всеми мобильными услугами и выбрать наиболее комфортный и удобный для него способ.

От каналов мобильного банка к функциональному и сервисному наполнению

Услуги, предлагаемые каждым из каналов, должны отражать возможности канала, кроме того, следует учитывать их востребованность у потребителей в контексте мобильного характера обслуживания. Так, использование sms-банкинга в основном ограничено безопасными информационными задачами: проверкой состояния счетов/движения по счетам. Приложения и мобильный сайт имеют больше возможностей и могут быть не просто максимально приближены к интернет-банку, но даже иметь дополнительные функции, например сервис определения ближайшего банкомата или доступ к электронному почтовому ящику и записной книжке (при наличии мобильного приложения, имеющего доступ к ОС телефона). Однако особенности работы на небольшом экране мобильного устройства накладывают свои ограничения на подходы к созданию экранных форм. Банки постоянно находятся в непрерывном поиске разумного компромисса между удобством работы и функциональностью, и некоторым уже удалось добиться того, что в мобильном банке представлены практически все операции, доступные клиентам в интернет-банке.

Мобильный банкинг тесно связан с используемыми современными технологиями и, чтобы оставаться востребованным и привлекательным для клиентов, должен непрерывно развиваться. Банки должны внимательно относиться к замечаниям/пожеланиям своих клиентов и с момента создания непрерывно совершенствовать мобильные приложения на основе получаемого клиентского отклика. Например, в нашем банке приложения мобильного банка были запущены осенью 2011 г., но уже в декабре мы смогли выпустить большое обновление, расширившее не столько функциональные возможности (хотя при этом клиенты получили возможность быстро заблокировать банковскую карту (например, в случае ее утери), получить информацию о реквизитах своих продуктов в приложении и направить их по почте и др.), сколько возможности по настройкам (возможность включать/отключать сервисы, настраивать их параметры).

При создании мобильного банка всегда возникает необходимость поиска баланса между безопасностью системы и удобством для клиента. Как альтернативное решение можно рассматривать создание эффективных инструментов операционного контроля, например системы мониторинга транзакций, включая фрод-мониторинг,

лимитов, а также создание инструментов обучения клиентов и удобных и понятных интерфейсов. Отметим, что ВТБ24 уже избрал это направление как одно из основных в развитии своих дистанционных сервисов. При этом систему операционного контроля необходимо выстраивать как мультиканальную (операции отслеживаются в целом по банку, а не отдельно по каналам).

С развитием электронных сервисов меняются и представления о дистанционных банковских услугах: требования к финансовым интернет-сервисам начинают формироваться исходя из глобального пользовательского опыта клиентов в Интернете и мобильной среде (прежде всего это интерактивность, удобство интерфейсов (информационный и функциональный дизайн) и интеграция сторонних сервисов).

При этом сама природа мобильных приложений содержит в себе некую игровую составляющую, и клиент изначально ожидает получить не только функциональный инструмент, но и игрушку. Пользователи ожидают постоянного обновления и добавления новых функций, которые позволяют перейти им на «новый уровень владения» приложением, то есть задержавшиеся хоть на секунду сервисы быстро теряют актуальность, а пользователи — интерес к ним. В свою очередь, внедрение новых инновационных технологий создает дополнительную ценность для клиента, а банк обеспечивает себе лояльность клиентов, что можно рассматривать как дополнительные дивиденды. Необходимо учитывать особенности и потребности пользователей разных платформ: например, пользователи iPhone привыкли к стильным решениям интерфейса и более капризны — от них поступает наибольшее количество замечаний по юзабилити и дизайну приложения; пользователям Android важнее функциональное наполнение.

PDA-версия также не ограничится одной адаптируемой под все ведущие браузеры и модели телефонов версией: в самое ближайшее время мы планируем запустить как версию для любых устройств с доступом в Интернет, так и специальную сенсорную версию для клиентов, привыкших к удобству и богатым интерфейсным возможностям их телефонов.

На нашей волне: мобильный банк ВТБ24

Успех мобильного банка ВТБ24 уже оправдал затраченные на него усилия. Приложения «Мобильный банк ВТБ24» для мобильных устройств на платформах Android и iOS (iPhone) были запущены осенью 2011 г. Спустя всего три месяца с момента их появления на Android-маркете и App Store приложением воспользовались более

Альтернативным решением поиска баланса между безопасностью мобильного банка и удобством для клиента является создание эффективных инструментов операционного контроля (системы мониторинга транзакций, включая фрод-мониторинг, лимитов), а также инструментов обучения клиентов и удобных и понятных интерфейсов.

40 тыс. клиентов, что составляет уже более 3% от всех пользователей каналов дистанционного обслуживания ВТБ24. Через мобильный канал уже проводится более 1% операций от всех операций, осуществляемых через дистанционные каналы.

Запуск мобильных приложений был воспринят клиентами очень положительно, о чем мы можем судить по отзывам клиентов на различных интернет-площадках, созданных специально для общения. Развитие мобильных сервисов в банковском секторе в России находится сейчас на этапе активного становления, и самым важным для ВТБ24 было не пропустить эту волну развития рынка финансовых услуг. Мы не торопились с разработкой быстрого, но урезанного (как функционально, так и архитектурно) мобильного решения для наших клиентов, а постарались предоставить клиентам возможность работать с полнофункциональным мобильным банком, который позволяет не только просматривать информацию по своим счетам и картам и проводить элементарные операции оплаты услуг сотовой связи, но и осуществлять более сложные операции, например открывать и пополнять вклады, совершать переводы внутри банка и в другие банки, покупать и продавать валюту, оперативно блокировать карту без обращения в call-центр, а также найти ближайший банкомат, узнать время его работы и доступные функции, проложить маршрут к нему, узнать актуальные курсы валют и драгоценных металлов и многое другое. Еще до запуска приложение прошло целый цикл тестирований, одним из этапов которого стало тестирование юзабилити приложения в одной из ведущих российских юзабилити-лабораторий. Это тестирование позволило существенно оптимизировать приложение. В ближайшее время мы добавим больше информации о банковских продуктах и сервисах, новые операции, предоставим обновленный интерфейс, который разрабатывается на основании пожеланий клиентов и рекомендаций юзабилити-консультантов.

В планах развития канала мобильного банкинга — запуск в 2012 г. нативных приложений для платформ Symbian и Windows Mobile и мобильного сайта системы «Телебанк» (PDA-версии).

От совершенствования каналов к созданию единого пространства ДБО

С каждым днем ДБО становится все более мультиканальным — клиент выбирает наиболее удобный в данный момент канал коммуникации или обслуживания, при этом каждый из каналов равнозначен и равноправен, хотя они и могут выполнять разную роль

в концепции обслуживания клиентов банка: сиюминутный, on-demand характер взаимодействия в мобильном банке, где востребованы в основном «быстрые» операции; офис как канал продаж и профессиональных консультаций; Интернет как канал для осуществления более рискованных или «сложных» операций, требующих, например, принятия взвешенных решений или тщательного заполнения длинных форм. Все эти каналы играют свою особую роль, и каждый из них вносит свой вклад в восприятие банка как единого и монолитного института, способного обеспечить сохранность финансовых средств клиента. Соответственно возникает концептуально важная задача выстраивания единого пространства ДБО, когда каналы становятся «прозрачными» друг для друга, а роль и функциональность каждого из каналов оказываются четко сформулированными. И как финальная точка этого «путешествия» — когда каждый из каналов «знает» и «моментально узнает», что происходит в другом (всегда можно остановиться на одном этапе процесса в одном канале/возобновить на другом), а для контекстного отображения информации и применения интерактивных инструментов используется вся доступная информация о клиенте.

В это же самое время банки зачастую продолжают «общаться» с клиентом на языке банковских технологий и процессов, в этом случае сервисы и их пользовательские интерфейсы становятся «заложниками» внутренних ограничений банковской структуры и, как следствие, сервис становится неклиентоориентированным. Между тем для создания действительно удобных и востребованных банковских сервисов логика приложений и сервисов должна строиться исходя из моделей использования интерактивных сервисов типичными клиентами банка. Таким образом, банку необходимо постоянно и непрерывно отслеживать тенденции/требования/модели клиентов при использовании интерактивных сервисов.

И последнее. Клиенты, использующие дистанционные каналы, отличаются по моделям поведения и стереотипам в отношении интернет- и мобильной среды коммуникации, имеют различные требования к дистанционным банковским сервисам. Соответственно нельзя рассчитывать на массовое признание и лояльность клиентов к сервисам банка, пока он предоставляет их по принципу one-size fits all. Банкам необходимо формировать инструменты, позволяющие добиться идеального взаимодействия с банковскими сервисами за счет персонализации/прозрачности и интерактивности. То есть обеспечить клиенту максимальную свободу в кастомизации пользовательских интерфейсов и коммуницировать с ним, исходя из обстановки. 

Для создания удобных и востребованных банковских сервисов логика приложений и сервисов должна строиться исходя из моделей использования интерактивных сервисов типичными клиентами банка.

Мобильный банкинг: внутренний контроль источников рисков

Помимо множества преимуществ технологий дистанционного банковского обслуживания, существует ряд особенностей их функционирования, приводящих к возникновению дополнительных источников банковских рисков, включая риски отмывания денег. Автор рассматривает общую модель отмывания денег с использованием систем мобильного банкинга и порядок анализа источников сопутствующих рисков службой внутреннего контроля кредитной организации¹.



П.В. РЕВЕНКОВ,
Банк России, департамент банковского регулирования и надзора, заведующий сектором, к.э.н.

Горячая лошадь со всадником может сломать себе шею как раз на той тропинке, по которой осторожный осел идет, не спотыкаясь.

Готхольд Эфраим Лессинг

Распространение мобильного банкинга

За последние 10–15 лет в банковском бизнесе произошли такие изменения, которые не только предоставили клиентам возможность совершать свои операции, не посещая офиса банка, но и потребовали пересмотра всей методологии учета типичных банковских рисков².

Одними из самых распространенных способов дистанционного банковского обслуживания являются интернет-банкинг и мобильный банкинг. Интернет-банкинг — способ ДБО клиентов, осуществляемого кредитными организациями в сети Интернет (в т.ч. через веб-сайты) и включающего информационное и операционное взаимодействие

¹ Настоящая статья выражает исключительно мнение автора и не отражает позицию Банка России.

² Речь идет о типичных банковских рисках, перечисленных в Письме ЦБ РФ от 23.06.2004 № 70-Т «О типичных банковских рисках».



с ними¹. Мобильный банкинг — способ ДБО клиентов, при котором им предоставляется возможность управлять своими банковскими счетами и картами с помощью карманных персональных компьютеров, коммуникаторов, смартфонов и других подобных устройств.

Президент Ассоциации региональных банков России А. Аксаков в своем недавнем интервью отметил, что ключевым направлением в области банковской автоматизации в 2012 г. останется внедрение новых дешевых каналов обслуживания клиентов. Бизнес банковских карт, мобильный и интернет-банкинг будут приоритетными направлениями².

Согласно данным Ассоциации GSM³ количество мобильных телефонов, подключенных к сетям во всем мире, превысило отметку в 4 млрд. Число соединений, по прогнозам ассоциации, к 2013 г. может достигнуть 6 млрд, что фактически вплотную приближается к численности населения Земли⁴.

Можно утверждать с высокой степенью вероятности, что мобильные сервисы будут показывать максимальный прирост клиентской базы в ближайшие годы.

Так, по данным World Bank, только в Индии в 2009 г. было осуществлено мобильных транзакций почти на \$45 млрд, а в Китае за тот же период — на \$40,5 млрд⁵. Многие банкиры признают, что у сферы беспроводных денежных транзакций отличные перспективы, поскольку потенциал такой связи велик, а появление смартфонов и соответствующих финансовых приложений к ним дает возможность создавать «мобильный кошелек/электронный банк в кармане»⁶.

Представляется, что интенсивное развитие бизнеса, связанного с мобильным банкингом, обусловлено стремительным распространением смартфонов, а также потребностью в новых нетрадиционных каналах отправки денег.

¹ Данное определение приведено в Письме ЦБ РФ от 31.03.2008 № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга».

² См. интервью с А. Аксаковым «Правовое поле стимулирует банки к внедрению новых технологий» // Банковские технологии. 2011. № 9.

³ Ассоциация GSM — международная организация операторов сотовой связи стандарта GSM (от названия группы Groupe Special Mobile), которая объединяет более 700 операторов GSM из 217 стран. Операторы — члены Ассоциации GSM обслуживают более двух миллиардов абонентов во всем мире — более 82% всех пользователей мобильной связи.

⁴ <http://www.theglobeandmail.com/news/technology/article971335.ece>

⁵ Зайцев О. Мировая финансовая сеть // Банковская практика за рубежом. 2012. № 1.

⁶ Данная услуга может быть весьма привлекательна для иммигрантов и тех, кто выезжает на работу в зарубежье, где они зачастую не имеют собственных банковских счетов. Подобная технология существенно упрощает отправку денег на родину своим семьям и родственникам.

Платежи с использованием мобильного банкинга все чаще используются в сложных схемах, предназначенных для легализации преступных доходов. Возможность открытия счетов и проведения финансовых транзакций без необходимости личного посещения банка создает для этого максимально благоприятные условия.

Главными преимуществами мобильного банкинга являются низкая стоимость, высокая скорость передачи данных и простой доступ к передовым технологиям.

Сотовые телефоны распространены на всех континентах, благодаря чему финансовые институты могут теперь осваивать самые отдаленные уголки планеты, которые ранее были для них недоступны из-за проблем с инфраструктурой.

Стремительное распространение денежных переводов с использованием систем мобильного банкинга по всему миру обусловлено, по меньшей мере, двумя ключевыми факторами:

1) в ряде развивающихся стран (на разных континентах) большой процент населения не имеют доступа к традиционным банковским инструментам (например, к банкоматам, провайдером денежных переводов, а зачастую и непосредственно к самим кредитным учреждениям). По некоторым оценкам, во всем мире до 2 млрд человек не охвачены финансовыми услугами¹;

2) мобильный телефон становится основным инструментом коммуникаций по всему миру и главным элементом глобальной телекоммуникационной инфраструктуры².

В силу своих особенностей платежи с использованием мобильного банкинга все чаще используются в сложных схемах, предназначенных для легализации преступных доходов. Возможность открытия счетов и проведения финансовых транзакций без необходимости личного посещения банка создает для этого максимально благоприятные условия. Банковские работники по различным причинам не всегда обращают внимание на возможный криминальный характер совершаемых транзакций. Таким образом, риски, связанные с возможным использованием систем мобильного банкинга для отмывания денег, постепенно приобретают глобальный характер.

На глобальный характер рисков, возникающих при использовании систем электронного банкинга (включая мобильный), было обращено особое внимание ФАТФ³. Напомним, что ФАТФ разработала стандарты противодействия отмыванию доходов, полученных преступ-

¹ По мнению менеджера проектов для развивающихся рынков Всемирной ассоциации операторов мобильной связи (GSM Association) Бена Сопита, счет в банке имеют менее 1 млрд жителей планеты, и единственный способ сделать процедуру перевода денег безболезненной для остальных — это использовать мобильную связь (<http://www.procontent.ru/news/3917.html>).

² Наиболее высокие темпы роста услуг мобильной связи сегодня наблюдаются в Африке, Латинской Америке, на Ближнем Востоке и в Азии. В этих регионах существуют реальные предпосылки для дальнейшего развития сектора банковских услуг (из-за большой численности населения, не охваченного ими), в том числе благодаря внедрению мобильного банкинга.

³ Международная организация Financial Action Task Force (FATF), созданная в 1989 г. странами «Большой семерки». Сейчас в ФАТФ входят 33 государства. Российская Федерация является членом ФАТФ с июня 2003 г.

ным путем, которые получили название «Сорок рекомендаций». В дополнение к ним 31 октября 2001 г. ФАТФ были утверждены специальные рекомендации по предотвращению финансирования терроризма¹.

Основная обязанность кредитных организаций (возложенная на них Рекомендациями ФАТФ) состоит в надлежащей проверке клиентов и информировании компетентных органов обо всех сомнительных операциях, совершаемых клиентами банка.

Надлежащая проверка клиентов заключается в идентификации и подтверждении личности не только самого клиента, но и бенефициара, а также в постоянном отслеживании деловых отношений (в т.ч. сделок) клиента. С целью идентификации бенефициара банку необходимо установить, в чью собственность перейдут денежные средства или имущество. Если бенефициаром является юридическое лицо, следует выяснить, кто его учредитель и не являются ли стороны такой сделки взаимозависимыми лицами.

Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», целью которого является защита прав и законных интересов граждан, общества и государства путем создания правового механизма ПОД/ФТ, предлагает ряд превентивных мер, таких как:

- обязательные процедуры внутреннего контроля;
- запрет на информирование клиентов и иных лиц о принимаемых мерах по ПОД/ФТ;
- иные меры, принимаемые в соответствии с федеральными законами.

Надлежащая организация внутреннего контроля в рамках выполнения мероприятий по ПОД/ФТ в совокупности с должной работой подразделения по финансовому мониторингу может заметно минимизировать риски вовлечения кредитной организации в операции, направленные на отмывание денег.

Модели отмывания денег

Перед тем как перейти к особенностям внутреннего контроля в условиях мобильного банкинга, рассмотрим обобщенную модель, которая используется при отмывании «грязных» денежных средств. Она включает три фазы:

Надлежащая проверка клиентов заключается в идентификации и подтверждении личности не только самого клиента, но и бенефициара, а также в постоянном отслеживании деловых отношений (в т.ч. сделок) клиента.

¹ С перечнем рекомендаций можно познакомиться на сайте Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (http://www.eurasiangroup.org/ru/FATF_40.php).

- размещение (placement);
- расслоение (layering);
- интеграцию (integration).

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

Размещение «грязных» наличных денежных средств необходимо для их отделения от места происхождения. Для этого применяются различные финансовые инструменты, используются различные финансовые учреждения, предприятия розничной торговли. Чаще всего такие операции проводятся за пределами страны.

Этап размещения крупных сумм наличности является самым слабым звеном в процессе отмыwania денег. Незаконно полученные деньги наиболее легко могут быть выявлены на этом этапе.

Расслоение — отрыв незаконных доходов от их источников при помощи сложной цепи финансовых операций, направленных на маскировку проверяемого следа происхождения денег. Если размещение больших сумм денег прошло успешно, то есть не было обнаружено, то вскрыть дальнейшие действия «отмывателей» денег становится намного труднее. Различные финансовые операции наслаиваются одна на другую с целью усложнить работу правоохранительных органов по отысканию незаконных фондов, подлежащих конфискации. На данном этапе часто используются технологии ДБО.

Интеграция — стадия процесса легализации, непосредственно направленная на придание видимости законности преступно нажитому состоянию.

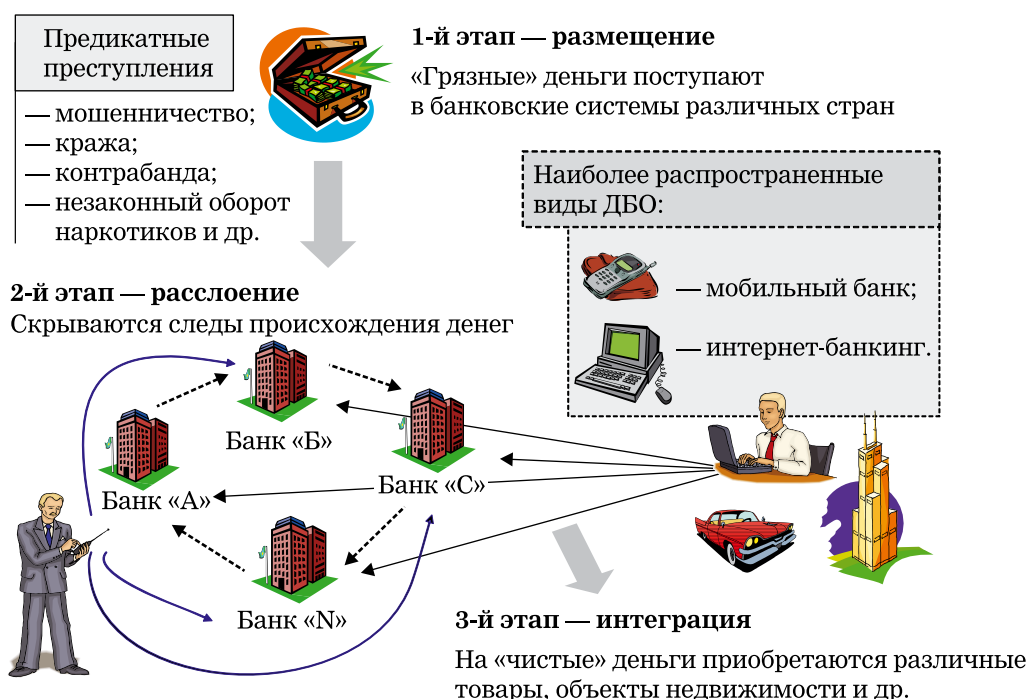
Существует и четырехфазовая модель структурирования процесса отмыwania (используется, например, в исследованиях экспертами ООН): первая фаза — освобождение от наличных денег и перечисление их в банки на собственные счета подставных лиц; вторая — распределение денежных средств путем банковских операций и операций с ценными бумагами; третья — маскировка следов совершенного преступления путем использования для открытия счетов банков, удаленных от места совершения преступления и проживания преступников, и перевода денег со счетов иностранных фирм на счета преступников в рамках фиктивных хозяйственных договоров; четвертая — инвестирование отмытых капиталов в легальную экономику¹.

Если размещение больших сумм денег прошло успешно, то вскрыть дальнейшие действия «отмывателей» становится намного труднее. Различные финансовые операции наслаиваются одна на другую с целью усложнить работу правоохранительных органов по отысканию незаконных фондов, подлежащих конфискации.

¹ См. Каратаев М.В. Современные тенденции легализации преступных доходов и российская специфика // Банковское дело. 2011. № 4.

Рисунок 1

Обобщенная схема отмыwania денег с использованием технологии ДБО



Внутренний контроль и методология оценки рисков отмыwania денег

Как уже было отмечено выше, одним из основных инструментов контроля за противоправным использованием систем мобильного банкинга в кредитном учреждении является организация внутреннего контроля, ответственность за которую возлагается на службу внутреннего контроля (далее — СВК).

Основополагающим нормативным актом, устанавливающим порядок осуществления внутреннего контроля в кредитных организациях и банковских группах на территории Российской Федерации, а также порядок осуществления Банком России надзора за соблюдением указанных правил, является разработанное Банком России в соответствии с Федеральным законом от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» и Законом РФ от 02.12.1990 № 395-1 «О банках и банковской деятельности» Положе-

Зачастую использование новейших электронных технологий в банковском бизнесе оставляет открытыми вопросы их безопасного применения, так как не сопровождается совершенствованием методологии процедур внутреннего контроля.

ние ЦБ РФ от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» (далее — Положение № 242-П).

В соответствии с Положением № 242-П в части управления банковскими рисками система внутреннего контроля¹ кредитной организации должна обеспечивать контроль:

- за функционированием системы управления банковскими рисками;
- оценкой банковских рисков;
- управлением информационными потоками (получением и передачей информации);
- обеспечением информационной безопасности.

СВК кредитной организации действует под непосредственным контролем совета директоров (наблюдательного совета) и по собственной инициативе докладывает совету директоров (наблюдательному совету) о вопросах, возникающих в ходе осуществления своих функций, и предложениях по их решению, а также раскрывает эту информацию единоличному и коллегиальному исполнительному органу кредитной организации.

Новая реальность и вопросы безопасности, с которыми приходится сталкиваться кредитным организациям и их клиентам при использовании технологий ДБО, требуют модернизации, а в ряде случаев и значительного пересмотра процедур мониторинга и парирования рисков, соответствующей организации процедур внутреннего контроля и повышения квалификации специалистов СВК.

Изучение сложившейся практики показывает, что зачастую использование новейших электронных технологий в банковском бизнесе оставляет открытыми вопросы их безопасного применения, так как не сопровождается совершенствованием методологии процедур внутреннего контроля, а если и сопровождается, то это касается лишь незначительных изменений внутренней нормативной базы кредитной организации (как правило, добавляются новые полномочия и функции специалистов СВК).

В подавляющем большинстве случаев отсутствуют не только специализированные подразделения (в рамках СВК или иной форме), но и целенаправленно подготовленные специалисты (несмотря на формальное наличие соответствующих обязанностей в должностных

¹ В соответствии с Положением № 242-П под системой органов внутреннего контроля понимается определенная учредительными и внутренними документами кредитной организации совокупность органов управления, а также подразделений и служащих (ответственных сотрудников), выполняющих функции в рамках системы внутреннего контроля.

инструкциях). В результате качество проверок участков, задействованных в системе мобильного банкинга, попадает в зависимость от практического навыка специалистов СВК и других субъективных факторов, что в свою очередь порождает новые источники рисков. В связи с этим по результатам проверок выявляются лишь отдельные малозначительные дефекты, недостаточные для получения полноценной объективной картины. При этом нельзя забывать, что в случае организации ДБО остается зависимость банков от компаний-провайдеров и других поставщиков оборудования и услуг, задействованных в информационном контуре системы мобильного банкинга.

Немаловажным является и такой факт, как наличие в руководстве кредитной организации менеджеров, которые могли бы обеспечить правильность принимаемых решений по результатам проверок функционирования систем мобильного банкинга, проведенных СВК¹.

Аналогичные требования предъявляются и к специалистам СВК, которые непосредственно участвуют в проверках технологии ДБО. Такие специалисты в идеале должны иметь не только экономическое или юридическое, но и техническое образование, которое позволяло бы им разбираться в распределенных компьютерных системах, иметь четкое представление о построении информационных контуров банковской деятельности при организации банковского обслуживания через Интернет и посредством сотовой связи, а также связанных с данными областями рисков².

Подобный подход рекомендован также Базельским комитетом по банковскому надзору (подробно раскрыт в документе «Принципы управления рисками для предоставления банковских услуг в электронной форме»). В противном случае затраты на устранение последствий рискованных ситуаций могут значительно превысить расходы на соответствующую подготовку специалистов.

В отношении общего понимания организации внутреннего контроля в кредитных организациях, применяющих технологии электронного банкинга, следует отметить, что цели, на которых базируется внутренний контроль, остаются прежними (обнаружение источников рисков, предупреждение появления рисков, парирование выявленных рисков), но при этом расширяются функции СВК.

¹ Данные менеджеры должны иметь достаточно хорошую техническую подготовку и представлять все возможные последствия проявления рисков, связанных с использованием кредитной организацией ДБО.

² Например, вопросы подготовки специалистов СВК по вопросам информационной безопасности в условиях электронного банкинга были освещены в статье П.В. Ревенкова и А.Б. Дудки «Электронный банкинг: особенности обучения информационной безопасности специалистов СВК» // Регламентация банковских операций. Документы и комментарии. 2008. № 5. С. 62–68.

Основой формирования общего подхода может стать так называемый «жизненный цикл» системы. Состав жизненного цикла любой системы (в т.ч. систем мобильного банкинга) не уникален и содержит ряд стандартных процедур.

Помимо традиционных, появляются дополнительные функции контроля, связанные в первую очередь с технической составляющей в организации удаленного доступа для клиентов.

Что касается непосредственно организации, содержания и методологии внутреннего контроля в части системы мобильного банкинга, они во многом зависят от специфических факторов, связанных с конкретными кредитными организациями. Большинству из них свойственны индивидуальная архитектура внутрибанковских распределенных компьютерных систем и индивидуальный набор требований к обеспечению целостности и безопасности информационных ресурсов, а также оригинальный набор методов и средств внутреннего контроля.

Специфика деятельности кредитной организации, безусловно, должна учитываться в организации системы внутреннего контроля, но общие рамочные подходы все же могут быть выработаны. Основой формирования общего подхода может стать так называемый «жизненный цикл» системы. Состав жизненного цикла любой системы (в т.ч. систем мобильного банкинга) не уникален и содержит ряд стандартных процедур. Примером тому может служить так называемая модель непрерывного циклического процесса менеджмента (модель Деминга), состоящая из нескольких стадий: планирования, реализации, проверки, совершенствования¹.

Логично предположить, что ошибки или источники рисков, заложенные на начальных стадиях (на стадии планирования), последовательно приведут к проявлению рисков событий на последующих этапах, а значит, и к снижению уровня безопасности системы мобильного банкинга. Следовательно, необходимо осуществлять соответствующие процедуры внутреннего контроля на каждом этапе жизненного цикла, которые могут быть выделены путем детализации стадий модели Деминга².

Специалисты СВК должны участвовать во всех этапах жизненного цикла системы мобильного банкинга и при этом контролировать выполнение мер, направленных на минимизацию банковских рисков.

¹ Данная модель используется в межотраслевом стандарте Банка России по информационной безопасности «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0.-2010).

² В предыдущих номерах журнала достаточно подробно рассматривался жизненный цикл системы электронного банкинга. Отдельные рекомендации для каждого из этапов жизненного цикла можно использовать для системы мобильного банкинга. См.: Дудка А.Б. и Ревенков П.В. Электронный банкинг: этап планирования и проектирования системы // Внутренний контроль в кредитной организации. 2009. № 4. С. 48–54; Электронный банкинг: внутренний контроль на этапе разработки системы // Внутренний контроль в кредитной организации. 2010. № 3. С. 43–57; Электронный банкинг: внутренний контроль на этапе испытаний и приема в эксплуатацию // Внутренний контроль в кредитной организации. 2010. № 4. С. 53–65.

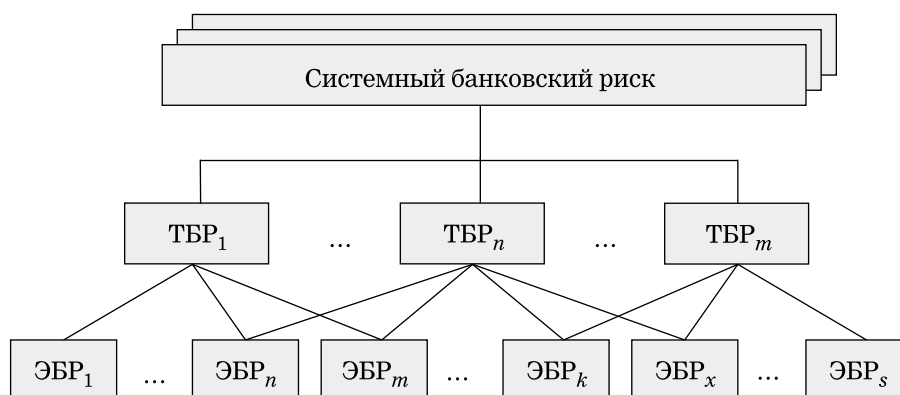
Выявление источников банковских рисков является только частью процесса управления рисками в кредитной организации, в который также входят оценка и анализ рисков.

В основу анализа последствий проявления источников рисков, связанных с отмыванием денег, должны быть заложены четко установленные причинно-следственные связи, то есть каждый недостаток (другими словами, элементарный банковский риск (далее — ЭБР)) должен восприниматься как причина повышения уровня одного из типичных банковских рисков (далее — ТБР) (рис. 2).

В целом методология анализа рисков, связанных с использованием систем мобильного банкинга, должна строиться по следующей схеме: источники рисков → возможные последствия → сложившаяся ситуация. Такого подхода следует придерживаться при разработке конкретных методик и процедур внутреннего контроля. В совокупности с непрерывной подготовкой специалистов СВК он будет очень полезен при проведении анализа источников банковских рисков, связанных с использованием технологий ДБО и систем мобильного банкинга в частности.

Рисунок 2

Иерархическая структура банковских рисков в условиях мобильного банкинга



Примеры элементарных банковских рисков:

- при оформлении договоров с клиентами недостаточно подробно изучаются документы, характеризующие их основную деятельность;
- в кредитной организации не принимаются дополнительные меры по идентификации клиентов, использующих для выполнения своих операций технологии ДБО (включая системы мобильного банкинга);
- сотрудники банка фиксируют не все сомнительные операции клиентов;
- специалисты, ответственные за проведение мероприятий по ПОД/ФТ, не проходят регулярную переподготовку и т.д.

Методики проведения проверок технологий ДБО, используемых в кредитной организации специалистами СВК, должны быть адаптированы под условия нового информационного контура банковской деятельности (основу которого составляют аппаратно-программные средства, используемые как банком, так и клиентом, а также надежность провайдеров и других участников контура).

Топ-менеджеры кредитных организаций должны хорошо понимать, что клиенты коммерческих банков, использующие для выполнения своих операций системы мобильного банкинга и занимающиеся противоправной деятельностью, могут не только нанести удар по репутации банка, но и стать причиной серьезных осложнений во взаимоотношениях с регулирующими органами вплоть до отзыва лицензии на осуществление банковских операций. Достаточно вспомнить, что в 2009 г., например, Банк России отозвал лицензии у 46 кредитных организаций, почти у трети из них в качестве причины в пресс-релизе Банка России указано неисполнение Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»¹. По информации, размещенной на официальном сайте Федеральной службы по финансовому мониторингу (<http://www.kfm.ru>), в 2008 г. в связи с нарушением вышеупомянутого закона Банк России отозвал лицензии у семи банков. Аналогичных случаев в 2007 г. было гораздо больше — тогда лицензий лишились 44 банка.

Заключение

В заключение хотелось бы сделать несколько выводов:

- 1) только налаженная система ПОД/ФТ может обезопасить кредитные организации от различных рисков, а также обеспечить стабильную и долгосрочную бесперебойную работу;
- 2) сотрудники, в чьи функции входят анализ источников рисков и их оценка, должны иметь соответствующую подготовку, позволяющую разбираться в информационном контуре банковской деятельности при организации обслуживания клиентов посредством систем мобильного банкинга и хорошо представлять, какие недостатки могут стать причинами возникновения банковских рисков;
- 3) методики проведения проверок технологий ДБО, используемых в кредитной организации специалистами СВК, должны быть адаптированы под условия нового информационного контура банковской деятельности (основу которого составляют аппаратно-программные средства, используемые как банком, так и клиентом, а также надежность провайдеров и других участников контура);
- 4) требования к сотрудникам СВК постоянно возрастают. В связи с этим специалисты СВК должны проходить постоянное обучение по тематике, связанной с особенностями функционирования различных видов технологии ДБО.

¹ Источник информации: Lenta.ru от 29.12.2009.

Мобильные платежные технологии: процедуры, стандарты, тенденции

В статье в систематизированном виде представлено описание платежно-расчетного взаимодействия участников платежных систем на основе мобильных телекоммуникационных стандартов и устройств. В контексте основных принципов разработки и функционирования платежных систем рассматриваются вопросы использования мобильных технологий, а также приводится обзор тенденций развития рынка мобильных платежных услуг за рубежом и в России.



В.Ю. КОПЫТИН,
Южный федеральный университет, кафедра бухгалтерского учета и аудита, доцент, к.э.н.

Развитие электронной торговли, использование Интернета и мобильных коммуникаций привело к появлению новых платежных технологий. Широкое использование мобильных устройств для совершения финансовых и платежно-расчетных операций способствовало становлению такого вида деятельности, как мобильная коммерция. Под этим понятием подразумеваются различные коммерческие сервисы (кроме услуг связи), использующие мобильный телефон в качестве основного интерфейса пользователя при работе с платежными, финансовыми и банковскими системами.

Следует обратить внимание на то, что технические инновации не изменяют основных процедурных характеристик платежно-расчетных взаимоотношений. В основе безналичного перевода денежных средств при использовании мобильных технологий лежат такие же операции и процедуры, как и при переводах с использованием традиционных платежных инструментов. Однако иногда из-за технических различий процедурной реализации осуществления платежей общность концептуальных подходов не распознается. Поэтому представляется полезным рассмотреть мобильные способы перевода денежных средств в контексте общих процедур — составляющих процесса перевода денежных средств от плательщика к получателю.

Платежные процедуры и услуги

Мобильные переводы денежных средств являются разновидностью розничных платежей, совершаемых между различными физическими



лицами, предприятиями, государственными учреждениями и организациями. Обычно эти платежи сравнительно небольшой стоимости и невысокой срочности, которые обрабатываются в системах массового перевода денежных средств.

В рамках платежной системы на основе мобильных технологий взаимодействия также осуществляется перевод денежных средств от плательщика к получателю в соответствии с установленными процедурами. Однако при совершении расчетов платежные процедуры могут выполняться без участия банковских организаций.

Процесс осуществления платежей включает три основные процедуры: инициирование платежа, обмен платежными инструкциями и процедуру расчета.

Инициирование платежа — процедура, при помощи которой один из участников расчетной операции (клиент) поручает обслуживающему его расчетному институту произвести платежи между участниками платежной операции. Инициирование мобильного платежа осуществляется при помощи платежных инструментов¹ посредством мобильных средств связи. Основанием для процедуры инициирования являются электронные платежные инструкции, которые порождаются платежным инструментом и передаются между участниками расчетов с использованием мобильных стандартов информационного взаимодействия.

Процедура обмена платежными инструкциями между участниками платежной системы состоит в передаче инструкций, которые являются основаниями для зачисления или списания средств. Обычно эта процедура определяется системой платежных и информационных сообщений, а также других средств коммуникационного взаимодействия, составляющих мобильную платежную инфраструктуру, которые необходимы для осуществления платежей.

Процедура расчета между участниками представляет собой установленные операции, которые определяют порядок списания и зачисления денежных средств (расчетных активов) на счета плательщика, получателя и обслуживающих их расчетных институтов.

Платежная система на базе мобильных стандартов и технологий, как и другие разновидности платежных систем, является конфигурацией различных видов институционального взаимодействия и инфраструктуры, способствующей переводу денежной стоимости между сторонами.

В основе безналичного перевода денежных средств при использовании мобильных технологий лежат такие же операции и процедуры, как и при переводах с использованием традиционных платежных инструментов, общность которых иногда трудно распознать из-за технических различий.

¹ Платежный инструмент — любой инструмент, предоставляющий держателю или пользователю возможность для перевода денежных средств.

Институциональное взаимодействие — это практика и организационные формы взаимодействия по предоставлению различных видов платежных услуг специализированными организациями пользователям этих услуг. Эти формы включают рыночные соглашения, правовую и нормативную базу и механизмы для консультаций и координации действий между заинтересованными сторонами в платежной системе.

Платежная инфраструктура — совокупность сетевого оборудования, технологий и процедур для осуществления доступа и операций с платежными инструментами, а также для обработки, клиринга и расчета по соответствующим платежам.

Услуги платежной инфраструктуры — платежные услуги, предоставляемые через платежную инфраструктуру, по осуществлению доступа и операций с платежными инструментами, а также для обработки, клиринга и расчета по соответствующим платежам.

Платежная инфраструктура включает в себя:

- операционные системы;
- клиринговые системы;
- расчетные системы.

В рамках вышеназванных систем предоставляются соответствующие им услуги. Основными инфраструктурными сервисами являются следующие услуги и связанные с ними операции.

Операционные услуги по созданию, подтверждению и передаче платежных инструкций посредством:

- аутентификации сторон, участвующих в операции, иногда с использованием технологий шифрования;
- подтверждения соответствия платежного инструмента системным стандартам;
- проверки платежеспособности плательщика;
- авторизации перевода денежных средств между расчетными институтами получателя и плательщика;
- учета и обработки платежной информации;
- распространения информации между участниками расчетов.

Клиринговые услуги по передаче, согласованию и в некоторых случаях подтверждению платежных инструкций между участниками расчетов и вычислению расчетных позиций посредством:

- сортировки и сверки платежных инструкций между участниками;
 - сбора, обработки и группировки платежных данных по каждому участнику;
-

— хранения отчетности по платежам и передачи ее каждому участнику;

— вычисления позиций по валовому или нетто-расчету (подлежащих уплате или получению) по каждому участнику расчетных операций.

Расчетные услуги по переводу денежных средств посредством:

— сбора расчетных требований и проверки их полноты;

— проверки наличия денежных средств для расчета на счетах учреждений — участников в расчетном банке;

— осуществления расчета по требованиям через переводы денежных средств по этим счетам в расчетном банке;

— осуществления учетных записей по расчету и доведения их до сведения лиц, участвующих в платежных операциях.

Завершая краткий обзор платежных процедур и услуг, обратим внимание на то, что платежные системы на основе мобильных средств информационного взаимодействия являются одним из видов систем розничных платежей, использующих стандарты и сервисы, разработанные в рамках создания мобильных технологий.

Расчетные активы и методы расчетов

Расчетный актив — актив, используемый для прекращения расчетных обязательств в соответствии с правилами, инструкциями или обычной практикой платежной системы.

В платежных системах на базе мобильных технологий расчетные активы могут быть представлены обязательствами кредитных организаций, небанковских эмитентов платежных инструментов и мобильных операторов.

Расчетный актив в виде обязательства кредитной организации обычно выражен остатком на банковском счете клиента.

Денежные средства, предварительно предоставленные клиентом в обмен на обязательства кредитной или небанковской организации предоставить в будущем определенные услуги или для исполнения денежных обязательств клиента перед третьими лицами, являются расчетными активами в виде электронных денег (далее — ЭД). Под электронными деньгами понимается хранимая стоимость или предоплаченный продукт, в котором данные о средствах или стоимости, доступных держателю для многоцелевого использования, хранятся на электронном устройстве, принадлежащем держателю. Учет информации о размере предоставленных денежных средств осуществляется без открытия банковского счета.

Платежные системы на основе мобильных средств информационного взаимодействия являются одним из видов систем розничных платежей, использующих стандарты и сервисы, разработанные в рамках создания мобильных технологий.

Для проведения расчетов в платежных системах на базе мобильных технологий используются расчетные активы, представленные обязательствами различных эмитентов, окончательный расчет между участниками платежных операций может осуществляться на валовой или нетто-основе.

При совершении расчетов с использованием денежных средств на счете абонента у операторов мобильной связи задействуются денежные средства, внесенные клиентами в качестве предоплаты за услуги мобильной связи.

В платежных системах на основе мобильных стандартов взаимодействия расчеты могут совершаться путем переуступки различных типов обязательств, выраженных расчетными активами в виде остатков на банковских и мобильных счетах, а также другими электронными средствами платежа. Пополнение и изъятие расчетных активов могут осуществляться в наличной и безналичной формах.

По принципам осуществления расчетов между участниками платежных систем различают системы валовых расчетов и системы нетто-расчетов. Синтезом характеристик валовых и нетто-расчетов являются системы смешанных расчетов¹.

Структура платежной системы на основе модели мобильной коммерции

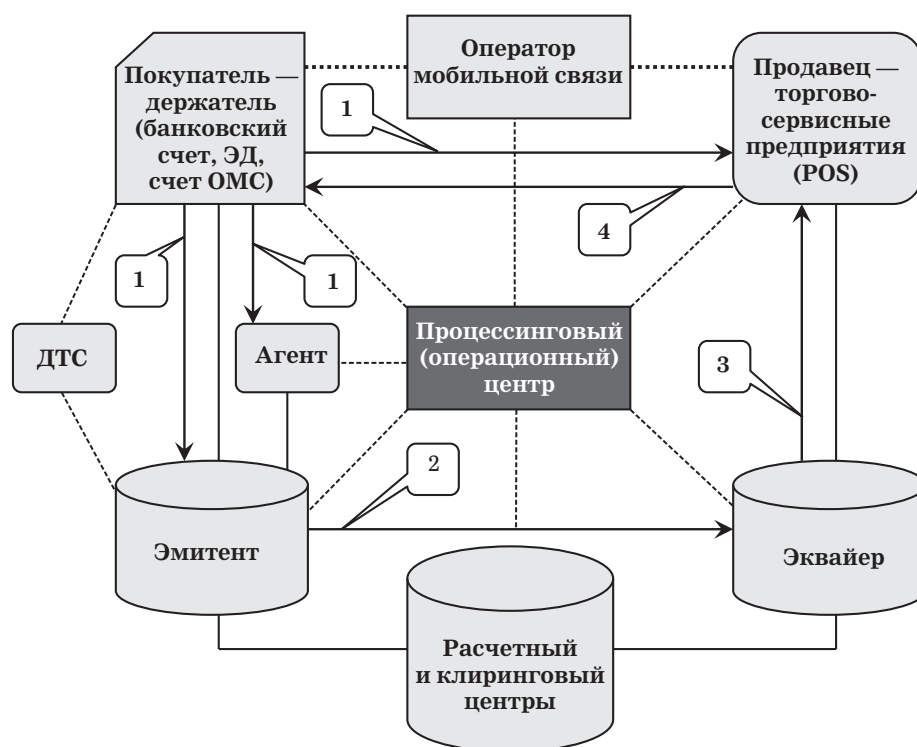
В основе распространенных представлений о мобильных платежных технологиях лежит эталонная модель мобильной коммерции, разработанная Open Mobile Alliance (OMA)². Далее при объяснении порядка взаимодействия участников платежно-расчетных отношений будет использоваться модифицированная схема мобильной коммерции, которая в большей мере соответствует традиционной структуре платежных систем.

В модели мобильной коммерции определены четыре ключевые роли в любой транзакции: покупатель, продавец, эмитент (организация, которая обеспечивает покупателя средствами для оплаты товаров и услуг — осуществляет выпуск электронных средств оплаты) и эквайер (организация, с которой взаимодействует продавец, чтобы получить денежные средства за товары и услуги). Другими участниками мобильных платежных систем являются платежные агенты, оператор мобильной связи (далее — ОМС), оператор платежной системы, процессинговый (операционный), клиринговый и расчетный центры. Все они участвуют в платежно-расчетных процедурах, выполняя конкретные функции. Расчетный и клиринговый центры обычно совмещаются в рамках одной кредитной организации. Однако

¹ Практический пример моделирования методов расчетов см.: Копытин В.Ю. О платежных системах и моделировании расчетных систем // Расчеты и операционная работа в коммерческом банке. 2006. № 3.

² Информация об эталонной модели мобильной коммерции представлена на информационном портале Инфокоммуникационного союза (<http://www.mobilepaymentsrussia.ru>).

Рисунок

Схема взаимодействия участников мобильной коммерции

Примечание: На схеме пунктирными линиями обозначаются информационные взаимодействия между участниками, сплошными линиями определяются расчетно-кассовые отношения, а стрелки с цифрами показывают схему выполнения платежно-расчетных операций:

1 — инициирование покупателем перевода продавцу;

2 — перевод безналичных денежных средств от эмитента к эквайеру через расчетный и (или) клиринговый центр;

3 — зачисление денежных средств эквайером продавцу;

4 — поставка товаров, проведение работ или предоставление услуг.

функции расчетного и клирингового центров также могут выполняться одним из эмитентов или эквайеров. Участником платежной системы, отвечающим за идентификацию клиента в соответствии с требованиями законодательства РФ, является служба доверенной третьей стороны (далее — ДТС). Схема взаимодействия участников мобильной коммерции приводится на рисунке.

Процедура инициирования платежа с использованием мобильного телефона может выполняться тремя альтернативными способами (см. стрелки с цифрой 1):

- в точке продажи торгово-сервисного предприятия;
- через платежного агента;
- путем мобильного взаимодействия с эмитентом платежного инструмента.

Процедура обмена платежной информацией для осуществления расчетов между покупателем (плательщиком) и продавцом (получателем) проводится с использованием электронных сообщений, которые передаются между участниками платежей посредством программно-технических средств мобильного оператора и процессингового центра. Форматы сообщений и порядок взаимодействия участников определяются правилами и стандартами электронного обмена.

Процедура расчета может выполняться как в режиме реального времени, так и методами периодической (отложенной) валовой обработки, а также двухстороннего или многостороннего неттинга. В случае отложенного валового или нетто-расчета на расчетный центр возлагаются функции клирингового центра, который формирует расчетные позиции между эмитентами и эквайерами. При этом окончательный расчет между всеми участниками расчетов осуществляется по результатам клиринговой обработки платежных инструкций (стрелки с цифрами 2 и 3), а поставка товаров, проведение работ или предоставление услуг (стрелка с цифрой 4) могут выполняться после получения информации от эмитента о платежеспособности покупателя и блокировки средств, необходимых для совершения платежа.

В рамках совершения мобильных платежных операций все функциональные обязанности по платежно-расчетному посредничеству между плательщиком и получателем средств могут выполняться в рамках одной платежной системы, организованной оператором мобильной связи. Однако, как правило, функции эмитента, эквайера и расчетного центра выполняют банковские организации, а функции процессингового центра возлагаются на организации, специализирующиеся в области платежного и информационно-телекоммуникационного взаимодействия.

Основные разновидности мобильных платежных технологий

Мобильные средства связи при совершении финансовых и торговых операций могут использоваться различными способами¹.

¹ Более подробно о функционировании международных платежно-расчетных технологий с использованием мобильных средств см.: Mas I., Kumar K. (2008). Banking on Mobiles: Why, How, for Whom? // Focus Note 48. Washington, D.C.: CGAP, June (http://www.cgap.org/gm/document-1.9.48929/FN48_RU.pdf); Mas I., Rotman S. (2008). Going Cashless at the Point of Sale: Hits and Misses in Developed Countries // Focus Note 51. Washington, D.C.: CGAP, December (http://www.cgap.org/gm/document-1.9.48930/FN51_RU.pdf).

Во-первых, мобильный телефон может использоваться как банковская карта. Банковская карта — это, по сути, принадлежащее клиенту запоминающее устройство, которое выполняет две функции: идентификацию пользователя и идентификацию счета, где находятся финансовые средства пользователя. Мобильный телефон используется для надежного хранения этой информации, позволяя избежать больших затрат на обеспечение картами всех клиентов банка. Фактически модуль идентификации абонента — SIM-карта (Subscriber Identification Module) — в мобильных телефонах представляет собой смарт-карту (т.е. карту со встроенным чипом, аналогичную наиболее современным банковским картам), хотя и не в привычной пластиковой форме. Идентификационный номер клиента банка и номер счета могут быть записаны на этой SIM-карте или в памяти телефона, действующих как виртуальная карта.

Во-вторых, устройства на базе мобильных аппаратов могут выполнять функции терминала в торгово-сервисном предприятии (point of sale, POS), а также использоваться для направления запросов на осуществление платежей и установления связи с соответствующим банком для получения разрешения на совершение расчетных операций.

В-третьих, мобильный телефон может выполнять функции элементов банкомата. Если использовать денежные средства, доступ к которым обеспечивает мобильный телефон, для оплаты в магазине, тогда он и кассовый аппарат магазина выполняют функции банкомата по внесению и выдаче наличных.

В-четвертых, мобильный телефон может использоваться как терминал для обслуживания клиентов через Интернет. Банковское обслуживание через Интернет (интернет-банкинг) удовлетворяет двум основным условиям, представляющим ценность для клиента: возможность контроля (моментальный доступ к любым понадобившимся реквизитам счета) и удобство (возможность дистанционного совершения платежей и денежных переводов). Мобильный телефон и беспроводная связь могут обеспечить клиентам интернет-терминал.

Кроме того, устройства на базе мобильного телефона могут предоставлять и другие возможности в части совмещения технических средств: связи, электронной торговли и оплаты.

Разновидности мобильных платежных технологий определяются признаками использования телекоммуникационных стандартов в рамках выполнения операций, составляющих мобильную коммерцию. Процедуры совершения платежа (инициирование, обмен информацией и расчет) осуществляются на основе разнообразных мобиль-

Как правило, функции эмитента, эквайера и расчетного центра выполняют банковские организации, а функции процессингового центра возлагаются на организации, специализирующиеся в области платежного и информационно-телекоммуникационного взаимодействия.



Выступая продолжением электронной коммерции, мобильная коммерция является результатом объединения передовых технологий мобильной связи, Интернета, финансовых услуг и электронной торговли.

ных стандартов и сервисов, которые являются компонентами процесса перевода расчетных активов от плательщика к получателю.

Мобильная коммерция является одним из ключевых направлений развития рынка телекоммуникаций и финансовых услуг. Выступая продолжением электронной коммерции, мобильная коммерция является результатом объединения передовых технологий мобильной связи, Интернета, финансовых услуг и электронной торговли.

Мобильная коммерция подразделяется на два направления — мобильный банкинг и мобильные платежи.

Мобильный банкинг

Мобильный банкинг предполагает управление банковским счетом с использованием мобильного телефона в качестве средства идентификации владельца банковского счета. При осуществлении платежных операций используются денежные средства, находящиеся на банковском счете.

Широкое распространение получил тип мобильного банкинга на базе услуги SMS. С помощью сообщений этого сервиса клиент может постоянно контролировать состояние своего лицевого счета. При организации взаимодействия между банками и клиентами в платежных системах на базе мобильных технологий могут также использоваться:

- IVR (Interactive Voice Response) — система интерактивного голосового ответа, так называемое голосовое меню, при использовании которого человек общается с автоматизированным звуковым интерфейсом, выполняющим навигацию действий пользователя посредством выбора пунктов меню;

- WAP (Wireless Application Protocol) — это технический стандарт, который описывает методы передачи информации из сети Интернет в мобильные устройства;

- MMS (Multimedia Messaging Service) — услуга обмена мультимедийными сообщениями (изображения, мелодии, видео) в сетях сотовой связи, которая является объединением служб SMS и WAP;

- USSD (Unstructured Supplementary Service Data) — сервис в сетях GSM (Groupe Special Mobile), позволяющий организовать интерактивный информационный обмен между абонентом сети и приложением в режиме передачи коротких сообщений;

- Bluetooth — спецификация обмена данными между устройствами (персональными компьютерами, мобильными телефонами, ноутбуками, принтерами и т.д.) в беспроводных персональных сетях (Wireless Personal Area Network) ближнего радиуса действия (от 1 до 10 м).

Мобильные платежи

Мобильные платежи подразумевают совершение платежа при помощи мобильного телефона, который используется в качестве платежного терминала. Денежные средства владельцев мобильных телефонов, используемые для совершения платежей, размещаются на prepaid-носителях или счетах у мобильных операторов связи. Мобильные платежи осуществляются без использования банковских счетов пользователя и доступны абонентам, не имеющим собственного банковского счета.

Широко распространенным методом совершения мобильных платежей является Premium SMS — отправка сообщения на «короткий номер» с последующим перечислением денежных средств от покупателя к продавцу и комиссии оператору мобильной связи.

Разновидностью мобильных платежей является мобильный контент, который позволяет использовать мобильный телефон не только в качестве удаленного средства идентификации плательщика, но и устройства для приема заказанной услуги. Он применяется при продаже наиболее популярных видов электронного контента — мелодий, изображений, Java-игр, видеофайлов, текстовых файлов, интерактивных медиапроектов и т.д.

При осуществлении мобильных платежей используются такие же технологические решения, как и в мобильном банкинге. Однако стандартные сервисы мобильной связи могут быть расширены за счет специфических возможностей операторов мобильной связи, если оператор заинтересован в функционировании платежной системы.

Стандарт NFC

В настоящее время наиболее распространенной и перспективной технической основой реализации услуг мобильной коммерции является технология беспроводной связи малого радиуса действия NFC (Near Field Communication), обеспечивающая обмен данными между устройствами на расстоянии около 10 см. Технология NFC была стандартизована международной ассоциацией по стандартизации информационных и коммуникационных технологий (Ecma International, ECMA). Эта технология является конкурентом решения широкополосного доступа короткого радиуса действия Bluetooth, превосходя ее в скорости установки соединения, механизме безопасности, аппаратной совместимости и возможности работы, когда одно из устройств не снабжено источником электричества. В стандартизацию NFC включены следующие спецификации:

Денежные средства владельцев мобильных телефонов, используемые для совершения платежей, размещаются на prepaid-носителях или счетах у мобильных операторов связи.

— стандарты Европейского института стандартов электросвязи относительно платформы смарт-карт по интеграции SIM-карт и микросхем NFC;

— GlobalPlatform — технология инфраструктуры (разрабатываемая одноименной организацией), в рамках которой объединяются стандарты карт, устройств, взаимодействующих с картами, и систем, обеспечивающих их согласованное функционирование;

— EMV (Europay, MasterCard and Visa) — стандарт совместимости для кредитных и дебетовых платежных карт на основе микросхем, а также устройств, обеспечивающих прием их к оплате.

Крупнейшие операторы, контролирующие половину мирового рынка сотовой связи, объединились, чтобы создать единый формат использования технологии NFC в сотовых телефонах.

Для использования сервиса NFC необходимо установить в телефон абонента специальный модуль или микросхему. Благодаря встроенному таким образом в телефон чипу может осуществляться беспроводное соединение между телефоном и считывателем информации, установленным в POS-терминале или банкомате. В результате соединения со счета владельца мобильного телефона возможно списание денежных средств, соответствующих платежной операции.

В России работа по развитию бесконтактных платежей (NFC) и мобильных интерактивных сервисов, предоставляющих финансовые, государственные и муниципальные услуги, в основном ведется в рамках специальных проектов Инфокоммуникационного союза, направленных на создание универсальной платежной платформы.

Международные перспективы

Прогнозируется, что в ближайшее время начнется сокращение количества держателей пластиковых карт, поскольку для оплаты небольших покупок все чаще будут использоваться такие мобильные устройства, как iPhone, Droid и BlackBerry. Системы бесконтактных мобильных платежей будут развиваться быстрыми темпами.

В этом году ожидается выход на рынок большого количества моделей мобильных телефонов, поддерживающих технологию бесконтактной оплаты, соответственно увеличится и число пользователей указанной услуги. Эксперты полагают, что со временем пластиковая карта выйдет из употребления. Большие международные компании Visa, MasterCard, Google, Bank of America, Citi и U.S. Bank проводят тестирование системы бесконтактных мобильных плате-

жей и планируют сделать для своих клиентов доступной услугу мобильного кошелька.

В ноябре 2010 г. появилась новая мобильная платежная система Isis, составившая конкуренцию Visa и MasterCard. Преимущество мобильного кошелька названной системы состоит в том, что с его помощью можно не только осуществлять платежи, но и хранить информацию нескольких пластиковых карт (страховой карты, водительских прав и иных документов), проверять баланс и т.д. Рассматриваются варианты создания бесконтактного банкомата.

Рынок мобильных платежных решений, по оценкам экспертов, исчисляется миллиардами долларов, поэтому за влияние на этом рынке конкурируют не только банки, операторы сотовых и платежных систем, но и другие организации, которые ранее не занимались мобильными платежными технологиями. Свою платежную платформу продвигает компания одного из основателей Twitter Джека Дорси — Square, предлагаемое техническое решение позволяет рассчитываться платежной картой через специальное устройство, подключаемое прямо в аудиоразъем смартфона или планшетного компьютера. Предполагается, что в одной из следующих моделей iPhone будет встроен NFC-чип, а Apple разрабатывает собственную платформу для бесконтактных платежей. Значительную долю рынка в ближайшее время может занять сегодняшний лидер смежного рынка интернет-платежей — компания eBay, владеющая популярной платежной системой PayPal. Недавно была представлена мобильная платежная услуга от Google — Google Wallet, разработанная в сотрудничестве с Citi, MasterCard, First Data и американским оператором Sprint.

Компания Google, анонсируя свое платежное решение, сообщает, что новый сервис позволит превратить мобильное устройство в электронный кошелек. Google Wallet будет работать на смартфонах под управлением операционной системы Android, доступ к нему можно будет осуществлять с помощью бесплатного приложения. Сервис основывается на использовании беспроводной технологии NFC. Компания Google предполагает, что она будет сотрудничать со всеми, от кого поступят предложения, включая Apple с его iPhone, RIM с BlackBerry и Microsoft Windows Phone. В предлагаемом Google решении необязательна аппаратная реализация NFC — возможно использование для смартфонов без встроенного NFC специальных NFC-модулей «платежных стикеров», само приложение Google Wallet сможет работать на таких аппаратах. Google Wallet будет хранить виртуальные копии пластиковых карт (Citi MasterCard), купонов на скидки, подарочных карт и т.д., то есть функционально платеж-

С помощью мобильного кошелька системы Isis можно не только осуществлять платежи, но и хранить информацию нескольких пластиковых карт (страховой карты, водительских прав и иных документов), проверять баланс и т.д.

ное приложение будет максимально приближено к обычному кошельку. Кроме того, будет заведена виртуальная карта Google Prepaid Card, которую можно пополнить с любой другой платежной карты. «Расплатиться смартфоном» можно будет везде, где имеются терминалы MasterCard PayPass, возможно, затем присоединятся и другие системы.

Национальные тенденции

На российском рынке также осуществляется работа по внедрению мобильных платежных решений, которую проводят организации банковского сектора, операторы связи и специализированные компании.

Мобильная платежная услуга Google Wallet будет работать на смартфонах под управлением операционной системы Android, хранить виртуальные копии пластиковых карт (Citi MasterCard), купонов на скидки, подарочных карт и т.д., то есть платежное приложение будет максимально приближено к обычному кошельку.

Пилотные решения бесконтактной оплаты проезда в метро запустили операторы связи «МТС» и «МегаФон». Компания «Технологии процессинга» реализовала проект для аэроэкспрессов: теперь проезд в них можно оплатить при помощи сотового телефона с поддержкой NFC. Компания i-Free проводит опытную эксплуатацию платежной системы, базирующейся на NFC-технологиях.

Платежная система «Яндекс.Деньги» выпустила мобильное приложение для смартфонов на платформе Android. Приложение позволяет непосредственно с мобильного устройства оплачивать покупки или услуги, проверять баланс и просматривать историю платежей. Кроме этого, с его помощью можно найти ближайшие точки пополнения счета в системе «Яндекс.Деньги». Приложение определяет местонахождение пользователя и показывает список банкоматов, терминалов или розничных точек, находящихся поблизости. Система «Яндекс.Деньги» поддерживает мобильный сайт со всеми основными платежными функциями, который доступен на любых телефонах с браузером.

Существенное влияние на развитие в области мобильных платежных систем оказывает процесс взаимовыгодной кооперации между банковским и телекоммуникационным сообществами, что позволяет оказывать клиентам современные мобильные платежные услуги. Планируется создавать технические решения на основе сотрудничества между кредитными, телекоммуникационными и технологическими организациями. В рамках общих проектов организаций с различной специализацией разрабатываются новые платежные технологии, сочетающие характеристики мобильного банкинга и мобильных платежей.

Например, в рамках совместного проекта Visa, Альфа-Банка и ОАО «ВымпелКом» («Билайн») создан платежный продукт, который позво-

ляет абонентам «Билайн» выпускать к номеру своего мобильного телефона предоплаченную карту — виртуальную или пластиковую. Виртуальная карта позволяет использовать средства на балансе мобильного телефона для оплаты покупок в Интернете и снятия наличных в банкоматах Альфа-Банка. Пластиковую карту, выпущенную к номеру телефона, можно будет использовать для оплаты покупок за счет средств на мобильном телефоне в торговых точках, Интернете и для снятия наличных в банкоматах любых банков. Проект стартовал в феврале 2011 г. и в течение года должен распространиться на все филиалы банка. Кроме этого, «ВымпелКом» и Альфа-Банк создали платежную систему RURU, которая позиционируется как универсальная. Альфа-Банк будет выполнять процессинговые и эквайринговые операции, а также функции расчетного центра системы. Система RURU позволяет осуществлять платежи из различных источников средств: лицевой счет абонента «Билайн» (а со временем, возможно, и других сотовых операторов), денежные средства на банковских картах Visa и MasterCard, денежные средства на электронных кошельках WebMoney (в будущем — и других эмитентов электронных денег).

Проект, связанный с мобильными платежами, намерен запустить в конце 2011 г. Сбербанк.

В Федеральном законе от 27.06.2011 № 161-ФЗ «О национальной платежной системе» заложены основы регулирования мобильных платежей. В соответствии с этим законом оператор электронных денежных средств может заключить с оператором связи, который имеет право оказывать услуги радиотелефонной подвижной связи, договор, по условиям которого оператор электронных денежных средств будет вправе увеличивать остаток электронных денежных средств физического лица — абонента такого оператора связи — за счет его денежных средств, которые уплачиваются авансом оператору связи.

В связи с принятием федеральных законов от 27.06.2011 № 161-ФЗ «О национальной платежной системе» и от 27.06.2011 № 162-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона “О национальной платежной системе”» в России создаются правовые условия для использования мобильного телефона как устройства для осуществления самых разных платежей. Поэтому, вероятнее всего, в ближайшее время в России рынок платежных технологий выйдет на уровень, соответствующий передовой международной практике. 

Эволюция спроса и перспективы развития мобильного банкинга

Спрос на мобильные сервисы банков динамично растет. Возможности мобильного банкинга с использованием моделей телефонов более раннего поколения были ограничены функционалом самих телефонных аппаратов. Однако даже при этих ограничениях возможность оперативно получить информацию об остатке на счете либо совершить простую платежную операцию посредством направления кодов операций на специальный номер была востребована клиентами как безопасный и оперативный способ информирования и (или) оплаты без посредников.

Важно, что наиболее часто встречающееся возражение клиента при использовании мобильных сервисов — это безопасность совершения операций онлайн, то есть отсутствие риска мошенничества. При этом, согласно данным опроса НАФИ «Потенциальный спрос на банковские услуги. Точки роста» (март 2012 г.), банковские учреждения имеют наивысшую степень доверия клиентов.

Что потребитель вкладывает в понятие доверия финансовым организациям (по результатам качественных исследований):

- выполнение своих обязательств, честность перед клиентами;
- отсутствие мошенничества;
- прозрачность информации;
- стабильность, устойчивость, отсутствие вероятности банкротства;
- государственная поддержка, гарантия;
- известность, хорошая репутация.

Это позволяет определять потенциал банков в развитии мобильных сервисов на фоне конкурентов на данном рынке.

Современные и перспективные возможности телефонных аппаратов, а также тенденции развития IT-решений банков, обеспечивающих реализацию простых и эффективных мобильных банковских сервисов, позволяют прогнозировать продолжающийся рост спроса на мобильный банкинг, расширение функциональных возможностей систем, повышение уровня простоты использования интерфейсов и т.д.

Так, основными трендами мобильного банкинга на ближайшую перспективу, по нашему мнению, являются следующие.



Во-первых, расширение инфраструктуры рынка мобильного банкинга — все больше участников банковского сообщества и их клиентов будут осуществлять взаимодействие посредством мобильных сервисов. Как следствие, логично предположить увеличение количества и сумм операций, совершаемых с использованием систем мобильного банкинга.

Во-вторых, развитие функционала систем мобильного банкинга в соответствии с особенностями устройств — активное использование реализованных в интерфейсах телефонных аппаратов функций, например напоминаний, уведомлений, возможностей геолокации, наличия сенсорных экранов, камер, считывателей QR-кодов и др.

В-третьих, повышение юзабилити интерфейсов: стремление к простоте и удобству использования систем — важная задача, над которой банки должны работать постоянно. При этом необходимо учитывать как функциональность оборудования (размеры экранов и виртуальных клавиатур, особенности той или иной модели телефонного аппарата (тип ориентации)), так и модель поведения клиента, использующего дистанционный способ банковского обслуживания посредством мобильного телефона в конкретной ситуации. Важен постоянный анализ востребованности и ценности сервиса для клиента в его стремлении к мобильности.

В-четвертых, актуальной тенденцией в обозримом будущем может стать повышение социальности и персонализации систем мобильного банкинга. Так, интеграция мобильных приложений банков и социальных ресурсов, очевидно, будет способствовать не только расширению клиентской базы и повышению лояльности клиентов, но и удобству пользования (например, при реализации эффективного дизайн-решения такая операция, как, например, перевод другу, станет не скучным созданием платежного перевода, а интерактивной игрой). А возможность визуально персонифицировать получателей переводов и (или) платежей, а также банковские продукты (карты, счета и другие сервисы) позволит существенным образом облегчить клиенту использование системы.

В-пятых, важной составляющей развития мобильного банкинга, на наш взгляд, будет повышение безопасности систем мобильных сервисов. Высокий уровень защиты информации — обязательное условие функционирования и востребованности сервиса ДБО на мобильном устройстве.

Таким образом, перспективы развития мобильного банкинга более чем впечатляющие. Можно с уверенностью говорить о том, что в ближайшем будущем, привлекая на обслуживание клиентов, банки будут оперировать уже не только наличием в линейке выгодного овердрафта, кредитной карты либо депозита, а в том числе и преимуществами мобильного сервиса, который становится базовым требованием при обслуживании клиента в банке.