Министерство образования и науки РФ
Автономная некоммерческая организация высшего образования
Самарский университет государственного управления
«Международный институт рынка»
Факультет заочного обучения
Кафедра банковского дела
Программа высшего образования
Направление подготовки 38.03.01 «Экономика»
Профиль «Финансы и кредит»

ДОПУСКАЕТСЯ К ЗАЩИТЕ
Заведующий кафедрой:
к.э.н. Ситнов В.В. _____

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

«Анализ рынка дистанционного банковского обслуживания клиентов»

Выполнил: Попов С.В.
Группа: ЗУф-25
Научный руководитель: старший преподаватель
Старикова Т.Е.

Самара
2017

Оглавление

Введение 3

1. Теоретические основы дистанционного банковского обслуживания 6

1.1 Понятие дистанционного банковского обслуживания, его преимущества и недостатки 6

1.2 Виды дистанционного банковского обслуживания 10

1.3 Технология продаж банковских продуктов в системе ДБО 15

2. Текущее состояние рынка дистанционного банковского обслуживания в России 21

2.1 Исследование потребительских предпочтений пользователей ДБО – физических лиц 21

2.2 Анализ современного состояния интернет-банкинга в России 26

2.2.1 Оценка эффективности интернет-банка для физических лиц 26

2.2.2 Оценка эффективности интернет-банка для малого бизнеса 29

2.3 Анализ современного состояния мобильного банкинга в России 33

2.3.1 Оценка эффективности мобильного банкинга для физических лиц 33

2.3.2 Оценка эффективности мобильного банкинга для малого бизнеса 38

3. Развитие систем дистанционного банковского обслуживания 42

3.1 Проблема электронного мошенничества в системах ДБО 42

3.2 Правовое решение проблемы электронного мошенничества в системах ДБО 50

3.3 Совершенствование дистанционного банковского обслуживания 56

Заключение 62

Список литературы 65

Введение

Востребованность и активность внедрения и использования электронных услуг и удаленных каналов обслуживания в России быстро растет, так как в настоящее время люди не представляет себе жизни без Интернета и компьютеров, а сотовый телефон стал предметом первой необходимости. Поэтому основным направлением развития современной банковской сферы является внедрение и развитие систем дистанционного банковского обслуживания. В последнее время количество банковских клиентов, интересующихся и переходящих к применению удаленных услуг, растет довольно быстрыми темпами. Обусловлен этот процесс, в первую очередь, теми преимуществами, которые предоставляют пользователям технологии дистанционного обслуживания. Данная система является выгодной и удобной формой взаимодействия, как для банка, так и для его клиента.

Современный деловой оборот предъявляет все более жесткие требования к участникам денежного рынка, а стремительный рост сферы финансовых услуг ведет к ужесточению конкуренции между банками. Новые условия деятельности требуют не только активного использования традиционных банковских решений, но и внедрения передовых достижений науки и техники, реализованных в различных способах дистанционного банковского обслуживания.

Развитие ДБО постепенно набирает обороты: за последние годы существования он превратился в полноценный продукт. Увеличивается число банков, внедряющих системы, которые позволяют им взаимодействовать с клиентами через Интернет. Перспективным направлением дистанционного банковского обслуживания стало предоставление клиентам механизмов, позволяющих быстро производить платежи и переводы независимо от места нахождения получателя и места нахождения кредитной организации.

Рынок систем ДБО в России продолжает расти, не уступая по функциональности системам западных банков. Данное направление банковских услуг очень перспективно, что подтверждает актуальность выбранной темы работы.

Предметом исследования выпускной квалификационной работы является дистанционное банковское обслуживание как базовый элемент сетевой финансовой технологии, используемый в системе расчетов и платежей субъектов экономики.

Объектом исследования выступает современный российский рынок ДБО клиентов в системах интернет-банкинга.

Цель выпускной квалификационной работы – анализ рынка интернет-банкинга в России и определение путей его развития.

Для достижения поставленной цели в данной работе поставлены следующие задачи:

- изучить сущность дистанционного банковского обслуживания, выделить его преимущества и недостатки;
- рассмотреть виды дистанционного банковского обслуживания;
- охарактеризовать технологии продаж банковских продуктов в системе интернет-банкинга;
- исследовать потребительские предпочтения пользователей ДБО – физических лиц;
- проанализировать современное состояние интернет-банкинга в России для физических лиц и малого бизнеса;
- проанализировать современное состояние мобильного банкинга в России для физических лиц и малого бизнеса;
- изучить проблему электронного мошенничества в системах ДБО;
- рассмотреть правовое решение проблемы электронного мошенничества в системах ДБО
- определить направления совершенствования дистанционного банковского обслуживания.

Структура работы включает в себя введение, три главы, заключение, список литературы.

Во введении обосновывается актуальность темы, определяются цели и задачи, отражена практическая значимость работы.

В первой главе определены теоретические основы дистанционного банковского обслуживания.

Во второй главе – проводится исследование потребительских предпочтений пользователей дистанционного банковского обслуживания и анализ текущего состояния рынка интернет- и мобильного банкинга в России для физических лиц и малого бизнеса.

В третьей главе рассмотрены проблемы электронного мошенничества в системах ДБО и направления совершенствования дистанционного банковского обслуживания.

В заключении обобщены результаты проделанной работы, сформулированы соответствующие выводы и рекомендации.

Работа написана на основе использования нормативно-правовых актов Российской Федерации, учебной литературы, статистических и аналитических данных Банка России, рейтинговых агентств, сведений, опубликованных в периодической печати, информационных ресурсов сети Интернет.

1. Теоретические основы дистанционного банковского обслуживания

1.1 Понятие дистанционного банковского обслуживания, его преимущества и недостатки

Дистанционное банковское обслуживание (ДБО) - это система, которая предоставляет клиентам возможность совершать банковские операции с использованием различных средств телекоммуникации, без непосредственного визита в офисы банка.

Первые системы ДБО в России появились в конце 1980-х гг., они применялись для удаленного обслуживания юридических лиц и получили название системы «клиент-банк». Функционирование системы осуществляется посредством программного обеспечения установленного как у клиента, так и у банка, связь между которыми осуществляется путем прямого модемного соединения с сервером банка либо через интернет [22].

Довольно часто используется также термин «home banking», определяющийся как совершение банковских операций на дому, самостоятельная форма предоставления банковских услуг населению, основанных на использовании электронной техники. Однако понятие «дистанционное банковское обслуживание» несколько шире и включает в себя обслуживание как физических, так и юридических лиц, причем не только «на дому», но и в любом удаленном от банковского офиса месте, где имеется соответствующий канал связи [14].

Под услугами дистанционного банковского обслуживания понимаются разные электронные услуги, разрешающие обслуживать клиентов с применением всех каналов доступа: Интернет (on-line и off-line доступ), телефон (обычный или мобильный), карманный компьютер, платежные терминалы и другие.

Дистанционное банковское обслуживание именуют также электронным банкингом. Для описания технологий ДБО применяют различные, иногда перекрещивающиеся по значению термины, например, интернет-банкинг,

домашний банкинг, телебанкинг, WAP-банкинг, PC-банкинг, мобильный банкинг, SMS-банкинг и другие.

Дистанционное банковское обслуживание (ДБО) представляет собой оказание банковских услуг посредством применения электронных каналов доставки.

Электронный канал доставки дистанционных банковских услуг – это найденное технологическое решение, созданное на базе современных средств связи, подобно, такому как Интернет, мобильная, стационарная связь, разные сетевые соединения и т.д.

Касательно этого, под ДБО можно подразумевать несколько дистанционных банковских услуг, предоставляемых клиенту с применением разных электронных каналов доставки и сосредоточенных в одной единой системе для каждого из каналов. Каждый отдельный канал при этом может дублировать и дополнять прочие.

Дистанционное банковское обслуживание представляет собой выгодную и удобную форму взаимодействия, как для банка, так и для его клиента. Именно благодаря своим главным преимуществам каналы ДБО нашли воплощение в современной жизни и постоянно развиваются.

К главным преимуществам удаленного банковского обслуживания для клиентов банков можно отнести:

1) удобное использование, то есть возможность воспользоваться банковскими услугами в любом месте и в любое время;
2) оперативная оплата, то есть оплата каких-либо банковских услуг происходит с достаточно высокой скоростью, иногда мгновенно;
3) доступность, так как стоимость применения услуг удаленного банковского обслуживания мала, часто банки предоставляют услуги ДБО бесплатно;
4) выгодность, то есть возможность выполнения удаленных банковских операций по более выгодным тарифам, чем при обслуживании клиентов в офисах банка;
5) разнообразие услуг, так как многие банки поддерживают и развивают различные виды и каналы дистанционного обслуживания [12].

Применение услуг удаленного банковского обслуживания дает возможность клиенту совершать необходимые банковские операции в удобном для него формате и месте, без каких-либо дополнительных денежных и временных затрат, так как для их использования не нужно приходить в офис банка, тратить время на дорогу и на длительные ожидания в очередях.

Внедряя систему дистанционного обслуживания, банк так же, как и его клиенты, получает важные преимущества.

1. Финансовая выгода благодаря уменьшению стоимости обслуживания клиентов, так как затраты на предоставление услуг клиенту в офисах банка гораздо выше, чем при удаленном обслуживании. Безусловно, банк тратит немало средств на внедрение данной системы, но эти затраты окупаются через некоторое время. Период окупаемости затрат уменьшается, если банк привлекает к использованию системы ДБО большое количество клиентов.

2. Удаленное обслуживание, к которому относится и такой вид, как обслуживание клиентов посредством терминалов и устройств самообслуживания, гораздо эффективнее, чем обслуживание в отделениях банка, так как банки не в силах обслужить в своих офисах огромное число клиентов. Пропускная способность обслуживания увеличивается, так как время на взаимодействие с клиентом уменьшается.

3. Банк имеет возможность привлекать клиентов, несмотря на их географическое местоположение. Банк получает возможность работать с новыми клиентами, которых банк не обслуживал до внедрения системы ДБО.

4. Повышается скорость и качество обслуживания клиентов банка.

5. Увеличивается точность совершаемых банковских операций и количество возможных ошибок становится меньше, снижаются операционные риски банка.

6. Для банка становится возможным решение важных дополнительных задач, например, предоставление клиенту информации о новых банковских услугах или сообщение клиенту о совершении необходимых действий.

7. Увеличивается конкурентоспособность банка [11].

Грамотно внедряя и развивая дистанционное обслуживание, банк повышает эффективность своей деятельности и расширяет свои возможности за счет продажи банковских продуктов и привлечения большого количества клиентов.

Но наряду с многочисленными преимуществами применение дистанционного банковского обслуживания не лишено и недостатков.

Недостатки системы удаленного обслуживания для коммерческих банков:

1) большие затраты на приобретение или создание системы удаленного обслуживания клиентов, её внедрение и обучение сотрудников;
2) затраты на обслуживание системы, в том числе и каналов связи с высокой пропускной способностью при обслуживании большого количества клиентов;
3) чтобы затраты на внедрение системы ДБО окупились, банку необходимо привлекать в удаленные каналы обслуживания большое число клиентов;
4) наличие высоких рисков хакерских и мошеннических атак на систему ДБО;
5) наличие рисков, связанных с ошибками в планировании расходов на внедрение и обслуживание системы удаленного банковского обслуживания.

Недостатки, имеющие место при использовании того или иного вида дистанционного банковского обслуживания, устранимы в той или иной степени разными организационными и техническими способами [11].

Динамика развития банковской отрасли показывает, что системы ДБО актуальны и востребованы бизнес-сообществом. При этом существующие формы удаленного обслуживания в большей степени являются взаимодополняющими, нежели конкурирующими, системами банковского обслуживания. Так как наличие разнообразных каналов передачи информации дает возможность выбрать не только одну форму удаленного банкинга, но и их комбинацию, позволяющую максимально удовлетворить потребности клиентов, исходя из функциональных возможностей нескольких систем дистанционного обслуживания и стоящих перед предприятиями задач.

Благодаря дифференциации способов передачи финансовой информации стало возможным разработать технические решения для использования

различных каналов связи в банковском деле, с целью повышения качества и уровня банковского обслуживания, а также минимизации финансовых и временных затрат.

1.2 Виды дистанционного банковского обслуживания

Систему дистанционного банковского обслуживания целесообразно классифицировать по типам информационных систем (программно-аппаратных средств), применяемых для реализации банковских операций [9].

1. ПК-банкинг (PC-banking) (к данному типу могут быть отнесены системы «клиент-банк») - это вид удаленного банковского обслуживания, который осуществляется с помощью персонального компьютера (ПК). Но сюда относятся не все дистанционные банковские услуги, которые применяютя с помощью компьютера, а только такие, при которых на персональный компьютер клиента устанавливается специальное программное обеспечение, благодаря которому и осуществляется взаимодействие клиента с банком. Системы «клиент-банк» существуют в двух формах:

- системы с «толстым» клиентом – подразумевает установку программного обеспечения на компьютере пользователя;
- системы с «тонким» клиентом – предполагает использование типового интернет-браузера для обеспечения доступа и взаимодействия с банковскими сетевыми ресурсами [16].

Первую форму принято считать классическим (традиционным) вариантом системы, позволяющей выполнять следующие операции:

- формирование и отправка платежных поручений, заверенных ЭЦП;
- получение банковских выписок по счетам;
- обмен информационными сообщениями с кредитной организацией;
- формирование заявки на получение наличных;
- формирование и отправка поручений на покупку и реализацию валюты и ценных бумаг;

- получение актуальной финансовой информации о курсах валют, котировках, обзорах финансовых рынков;
- получение консультаций;
- возможность информационного обмена сообщениями с другими клиентами банка, подключенными к системе.

Основным преимуществом использования систем «клиент-банк» является возможность экономить время и средства на посещении банка при осуществлении банковских операций. Кроме того, следует отметить ряд наиболее ярких функциональных возможностей данных систем, являющихся несомненным достоинством их использования:

- автоматизированная подготовка платежно-расчетных документов с использованием шаблонов и справочников системы;
- конвертация (экспорт и импорт) данных в бухгалтерские программы клиента;
- ведение архива документов с функциями их дальнейшего поиска, сортировки и печати;
- функция контроля принятия и исполнения банком платежного документа;
- электронное обновление баз данных;
- защита цифровой информации электронно-цифровой подписью и методами криптографического шифрования.

Традиционные системы ДБО типа «клиент-банк» получили наибольшее распространение в отечественном корпоративном секторе, прежде всего благодаря своей доступности: в той или иной комплектации данный вид обслуживания предлагают практически все банки. Кроме того они позволяют оперативно решать широкий круг стоящих перед бизнесом задач, получая удаленный доступ к банковским счетам (расчетным, депозитным, кредитным) и банковским услугам.

Наряду с явными преимуществами использование классических систем «клиент-банк» имеет и ряд недостатков:

- как правило, оффлайновый режим работы, т.е. изменения по счетам клиента в его базе не отражаются в режиме реального времени, а происходят лишь в период сеанса связи с банком;
- необходимость установки программного обеспечения на компьютер пользователя, установки обновлений системы;
- ограниченная мобильность системы, т.е. возможность использования с определенного компьютера;
- возможные трудности в установлении и поддержании соединения с банком (при использовании прямых коммутируемых соединений).

Однако динамичное развитие традиционных систем на основе интернета, привело к появлению сетевых программных комплексов дистанционного обслуживания клиентов (интернет-банкинг), использование которых минимизируют недостатки присущие работе с системами «клиент-банк» [17].

2. Интернет-банкинг (Internet-banking) - это вид удаленного обслуживания, который помогает осуществлять различные банковские операции через сеть Интернет. Важным достоинством данного вида системы ДБО является круглосуточный доступ к нему с любого устройства, имеющего доступ к сети Интернет. Банковское обслуживание клиентов, в ходе которого информационное и операционное взаимодействие с кредитно-финансовыми учреждениями осуществляется посредством интернет-браузера без установки специального программного обеспечения на компьютер клиента получило название интернет-банкинг. Для обозначения также используют термины интернет-клиент, онлайн-банкинг, «тонкий» клиент. За исключением сделок с наличностью системы интернет-банкинг дает своим клиентам доступ ко всему спектру банковских услуг. Варианты дополнительных опций онлайн-банкинга могут быть такие:

- формирование заявок на получение кредита;
- перевод средств во вклады;
- круглосуточный информационный и консалтинговый банковский сервис;
- обслуживание электронной коммерции (обмен электронных денег).

Интернет-системы банковского обслуживания могут функционировать посредством обращения клиента к web-сайту кредитной организации либо через приложение, установленное на ПК пользователя (системы «тонкий» клиент). Их главным отличием от традиционных систем «клиент-банк» является то, что пользователь работает с программным обеспечением и базами данных расположенными на удаленном веб-сервере банка. Системы ДБО, функционирующие в сети Интернет, обладают рядом преимуществ:

- отсутствие необходимости устанавливать объемное программное обеспечение на ПК пользователя;
- доступность (нет привязки к конкретному компьютеру, работать можно с любого устройства имеющего доступ к сети Интернет);
- возможность интеграции с бухгалтерскими программами.

3. Мобильный банкинг (mobile-banking) - это вид удаленного банковского обслуживания, благодаря которому управление банковскими счетами осуществляется с помощью планшетного ПК, смартфона или обычного телефона. Как правило, для этого на мобильное устройство нужно установить специальное приложение или программу, которое позволит использовать данный вид дистанционного банковского обслуживания.

4. Телефонный банкинг (phone-banking) (иногда применяется понятие «телебанкинг») - вид удаленного банковского обслуживания, при котором клиент получает банковские услуги посредством использования возможностей телефонов. Применяя систему телебанкинга, клиент может получать информационные услуги от банка и управлять средствами на своих собственных счетах. Данные системы имеют ограниченный функциональный набор (в сравнении с традиционными системами «клиент-банк» они в большей степени носят информационный характер) и дают возможность:

- получать информацию об остатках и поступлениях по счетам;
- вводить заявки на получение факсимильных документов (выписок, платежек), проведение платежей, заказ наличности;
- консультироваться со специалистами Call-центра.

Плюс телефонного банкинга состоит в возможности круглосуточного удаленного доступа к счету и справочной информации банка, минус – ограниченность функций системы.

5. Обслуживание с использованием банкоматов (ATM-banking) и устройств банковского самообслуживания. Данный вид системы ДБО отличается от других дистанционных услуг тем, что в этом случае клиент определенным образом зависит от местоположения конкретного терминала или банкомата и для осуществления банковских операций должен посетить то место, где расположено данное устройство. Безусловным преимуществом перед другими видами удаленного обслуживания является возможность для клиента работать с наличными деньгами. Долгое время обслуживание корпоративного сектора с использованием банкоматов и банковских терминалов было недоступно. Однако появление карточных счетов (корпоративных, таможенных, расчетных карт на взнос наличными) позволило запустить и этот процесс. Сегодня предприятия (как правило, малого и среднего бизнеса), открывшие специальные карточные счета (СКС), получают возможность с их помощью упростить банковское, в том числе кассовое обслуживание, а устройства банковского самообслуживания использовать в качестве альтернативы посещения отделений банка [18].

Карточные продукты дают удаленный доступ к счетам и позволяют осуществлять следующие операции:

- безналичные платежи;
- получение и взнос наличных в банкоматах;
- получение информации об остатках и оборотах по счетам.

Преимуществом данного вида ДБО является возможность обслуживания не только операций с безналичными денежными средствами (как в других системах), но и с наличными денежными средствами. Существенный недостаток – это территориальная привязка к стационарному банковскому оборудованию (банкоматам и терминалам) [12].

По субъектам обслуживания (клиентской базе) ДБО подразделяются на две группы:

- системы, обслуживающие корпоративный сектор, т.е. юридических лиц и индивидуальных предпринимателей;
- системы, используемые частными (физическими) лицами.

1.3 Технология продаж банковских продуктов в системе ДБО

Несмотря на трудные времена и сокращение ИТ-бюджетов, банки не планируют останавливать инвестиции в развитие систем дистанционного банковского обслуживания.

Экономические условия и конкуренция заставляют банки снижать тарифы. Чтобы удержать комиссионные сборы на прежнем уровне или обеспечить рост, кредитные учреждения должны увеличивать охват. Банки дружно рапортуют о росте популярности удаленных сервисов, при этом темпы прироста пользователей мобильных приложений обгоняют интернет-банкинг. Разные каналы дистанционного банковского обслуживания (ДБО), такие как интернет-банкинг, мобильные приложения, контакт-центры, банкоматы, должны быть интегрированы между собой и, по сути, стать дверьми в единую среду банка. Тогда у клиента появится возможность начать операцию в одном канале, а завершить – в другом. Спрос на омниканальность, то есть бесшовную интеграцию различных сервисов ДБО, определяет дальнейшее развитие удаленного взаимодействия клиентов и банков.

Если мультиканальное обслуживание предполагало обслуживание через совокупность каналов, то омниканальность предполагает построение единой среды обслуживания, когда каналы становятся лишь различными точками соприкосновения с централизованной платформой банка. Таким образом, происходит слияние традиционных и альтернативных каналов продаж, качество общения клиента с банком не зависит от выбранного канала [26].

При омниканальной архитектуре новый цифровой продукт, например, предварительно одобренные кредитные карты, сразу становится доступен во всех

каналах. Сокращается время вывода продуктов на рынок, и повышается интенсивность продаж.

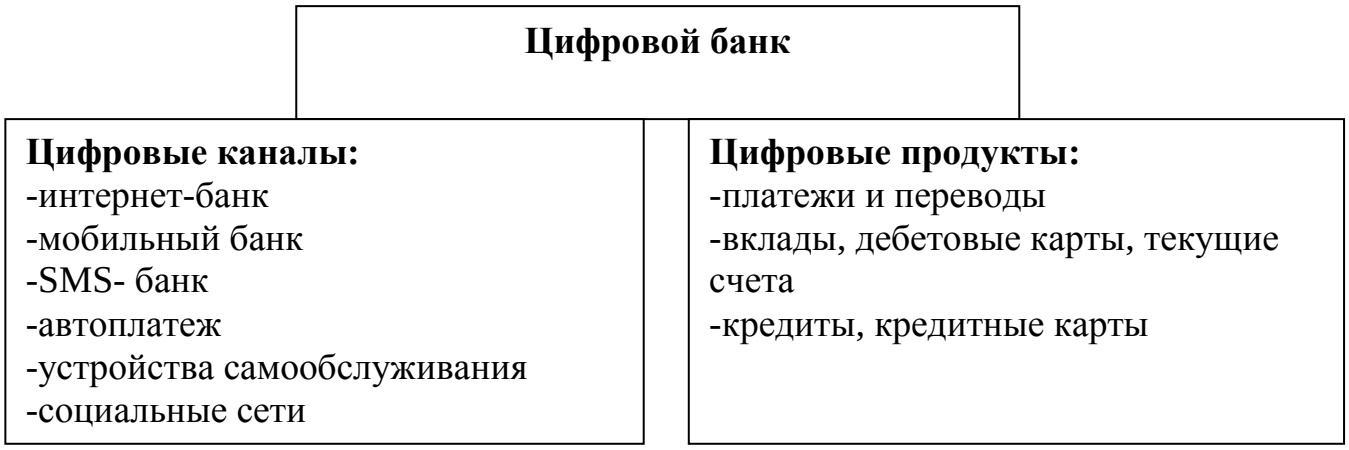

Рисунок 1.1 – Характеристика цифрового банка

Особенности интернет-продаж обуславливают основные условия к платежам, проводимым в платежной системе:

- авторизация, в процессе которой требование на проведение платежей одобряется или отклоняется;

- конфиденциальность, обеспечивающая неразглашение информации при проведении платежей;

- аутентификация;

- целостность информации;

- надежность;

- удобство;

- простота.

Необходимым фактором эффективности интернет-банкинга является наличие гибкой платформы дистанционного банковского обслуживания, которая обеспечивает выполнение стандартных функций и совершенствуется под новые клиентские требования.

Для банков важным условием эффективного функционирования интернет - банка является возможность с его помощью обеспечить продажу своих продуктов и услуг пользователям сервиса. Это становится возможным при

наличии системы формирования персонализированных предложений, интеграции с CRM-системами, интеграция гидов по продуктам и услугам и центра расчета их стоимости, внедрение e-commerce-витрин и PFM-систем услуг с учетом структуры расходов пользователя, внедрение алгоритмов сбора и анализа статистики и онлайн-магазин банковских карт [14].

Структура технологии продаж через систему интернет-банкинга представлена на рисунке 1.2.

Рисунок 1.2 – Этапы продажи продуктов через интернет-банкинг

Рассмотрим более подробно этапы осуществления банком продаж продуктов через систему интернет-банкинга (рис. 1.3).

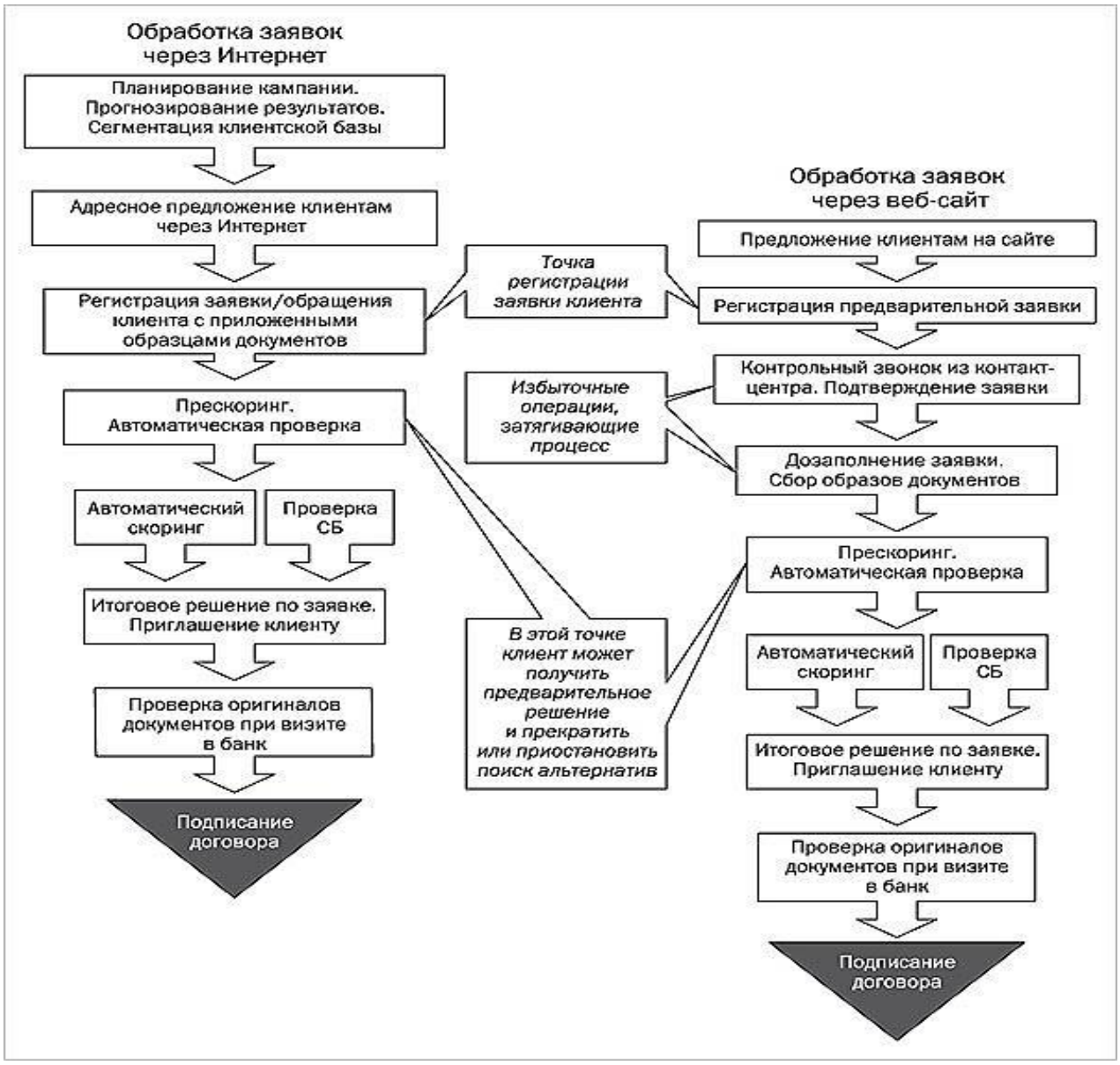

Рисунок 1.3 – Кредитный конвейер с использованием интернет-банкинга

1. Определение пользовательских сегментов на основании следующих критериев:

- статус клиента и наличие у него действующих банковских продуктов;
- история обслуживания пользователя и приобретения банковских продуктов, а также полученный клиентом результат;
- ранее поданные неудовлетворенные банком клиентские заявки на продукты;
- частота использования клиентом интернет-банкинга и спектр проводимых в системе операций.

2. Доставка персонализированных клиентских предложений.

3. Обработка ответов клиента, результатом чего может быть оформление заявки на интересующий продукт.

Так, например, заполнение анкеты на получение банковской карты или кредита в отличие от заполнения на сайте банка способствует сокращению издержек на проверку информации и минимизирует риск ошибок при вводе информации.

Схема операции при предложении клиенту депозита или инвестиционного продукта представлена на рисунке 1.4.

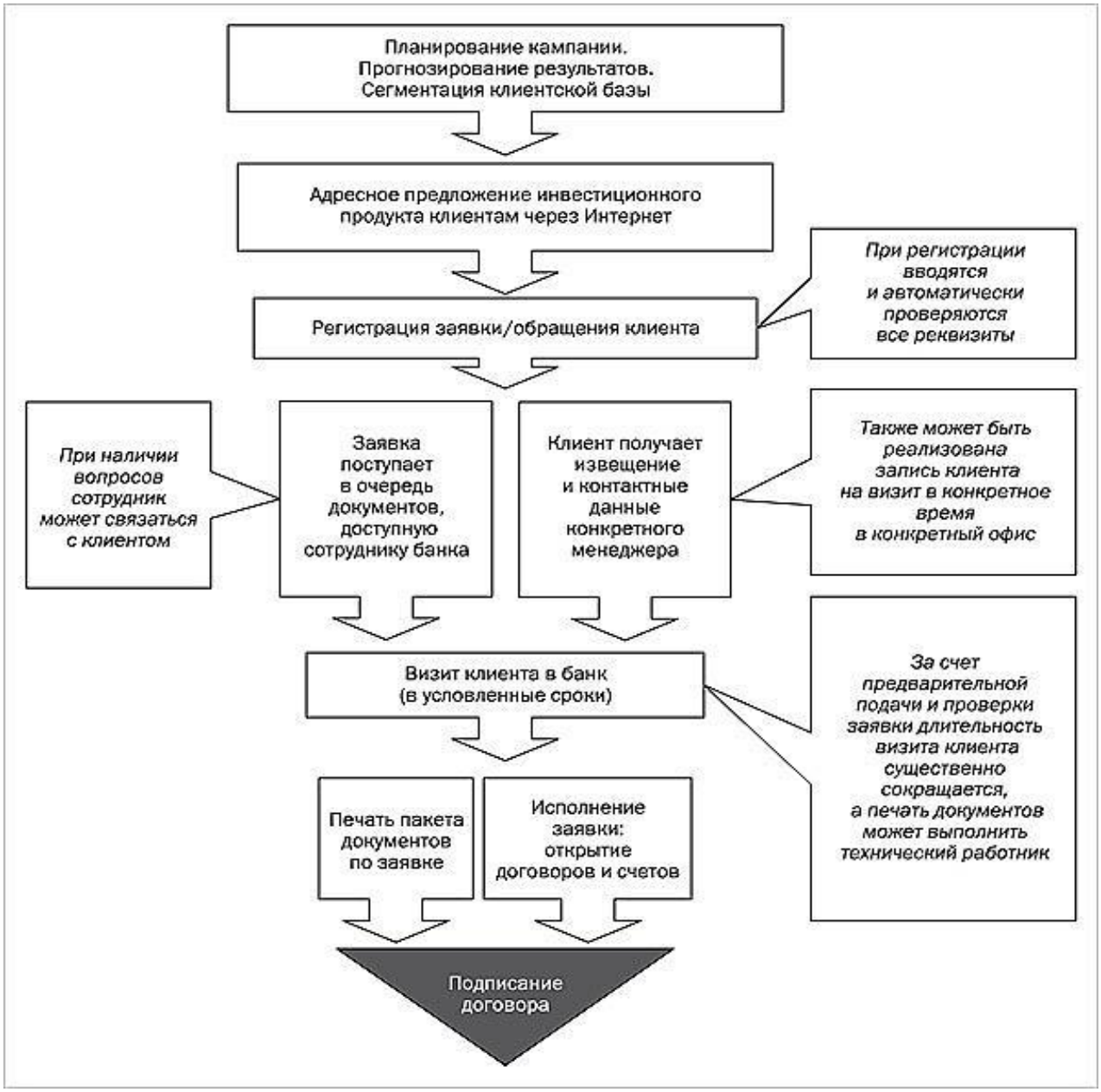

Рисунок 1.4 – Технология подачи предварительной заявки

2. Планирование и мониторинг показателей продаж.

Основой для плановых показателей продаж продуктов через интернет-банкинг могут выступать данные об объемах перекрестных и повторных продаж, реализуемых через контакт-центр.

Мониторинг показателей продаж проводится по следующим параметрам:

- отношение количества поданных запросов к числу разосланных обращений;

- отношение количества заключенных договоров к числу запросов;

- общий финансовый результат.

Оценка выполнения плановых показателей позволит модифицировать механизмы сегментации и обработки запросов клиентов [29].

3. Дополнительные инструменты, способствующие увеличению продаж:

1) платежный календарь может включать сведения об окончании сроков депозитов, карточек, страховок, периоды открытия интервальных фондов, график платежей по кредитам и т.д.).

2) калькулятор, позволяющий рассчитать стоимость предоставляемых банком продуктов и услуг и т.д.

В целях обеспечения персонального адресного подхода к клиенту для обеспечения возможности предложения новых продуктов и повышения продаж банкам целесообразно внедрять в систему дистанционного банковского обслуживания возможность управления личными финансами (PFM) [15].

Дистанционные каналы обслуживания банки рассматривают не только как источник дохода, но и способ привлечения и удержания клиентов. Сегодня банки выбираются не только по тарифам, но и по интерфейсам. При разработке клиентских систем и их интерфейсов в первую очередь надо учитывать потребности клиентов.

Банки и разработчики не останавливаются на достигнутом и продолжают пробовать новые технологии и форматы. Банки начинают с интересом смотреть в сторону новых форм-факторов: браслетов, часов и т.д.

2. Текущее состояние рынка дистанционного банковского обслуживания в России

2.1 Исследование потребительских предпочтений пользователей ДБО – физических лиц

Отношение к банковским мобильным приложениям крайне неоднозначное, и здесь аудитория четко делится на две группы.

1. Пользующиеся приложением:

− «Продвинутые» – активные пользователи (более выражено у молодой аудитории), которые пользуются всеми возможностями мобильных приложений, проводят все основные платежи через мобильный банк. В этой категории не выявлено случаев, когда какие-то платежи предпочитают проводить через другие каналы.

– «Осторожные» – пользуются только частью возможностей мобильного банка (телефон, интернет, транспортные карты, штрафы, переводы, реже коммунальные платежи). Не очень доверяют безопасности операций, проводимых через этот канал, из-за чего наиболее крупные и значимые платежи оставляют для интернет-банкинга, либо отделений. Есть потребность в бумажном подтверждении ряда платежей (коммунальные, оплата кредита), из-за чего проводят их через банкоматы/отделения.

– «Опасающиеся» - пользуются исключительно в качестве информационного канала – не проводят операции, а лишь отслеживают состояние своих счетов и поступающие от банка предложения.

1. Не пользующиеся приложением:

− «Отвергающие» – не пользуются активно мобильными приложениями в принципе (скорее аудитория 50+ в регионах), не разбираются и не хотят разбираться. Телефон используется для звонков, sms, интернета, навигации, другие приложения кажутся им слишком сложными, либо ненужными.

– «Консерваторы» – не пользуются именно мобильным банкингом при довольно активном пользовании другими мобильными приложениями, так как:

– нет доверия к уровню безопасности (считают, что через телефон к банковским счетам легко могут получить доступ третьи лица, что его можно потерять, подсмотреть коды доступа и пр.);

– считают важным иметь бумажное подтверждение проведенных платежей;

– не кажется удобным – на мобильном телефоне маленький экран, приложение кажется сложным для использования – предпочитают пользоваться интернет-банкингом, либо ходить в отделения/пользоваться банкоматами;

– нет потребности в пользовании – вполне хватает интернет-банкинга и банкоматов.

Первые пользуются как минимум обоими дистанционными каналами и делают это не реже 1 раза в неделю. Вторые, либо пользуются одним из исследуемых каналов, либо делают это реже 1 раза в месяц [32].

Возможности, которые наиболее актуальны для них в рамках приложений: оплата различных услуг, наличие подтверждения платежа, автоплатеж, страница с данными кредитора (единая страница, как с личными данными, так и с условиями кредита).

Преимущества мобильного банка становятся более заметны при осуществлении небольших денежных переводов. Этот дистанционный канал используется для мелких взаиморасчетов с друзьями, знакомыми, для небольших займов, оплаты «покупок по поручению», совместных обедов и т.п. Мобильный банк воспринимается как приемлемый по безопасности при условиях небольшой суммы и знакомого контрагента. При этом особую важность приобретает скорость платежа (и на уровне самого действия в смартфоне, и по срокам доставки денег). Если же сумма становится значительной или адресат знаком недостаточно, то требования к безопасности, к документальному подтверждению растут, и пользователь меняет канал на интернет-банк. Отметим, что

дополнительным фактором использования мобильного приложения является наличие у адресата карты того же банка, что и у отправителя, что позволяет использовать переводы по номеру телефона.

При необходимости проведения операции с большой суммой денег потребители отдают предпочтение визиту в банк, а преимущества комфорта и скорости, присущие дистанционным каналам, отступают на второй план. На первом плане – безопасность и контроль над ситуацией (табл. 2.1).

Таблица 2.1 - Модель выбора канала для проведения обязательных платежей и переводов физическим лицам и организациям

Вид платежа	Интернет			Платежный терминал / Банкомат	Банк/ЕРЦ
	Интернет-банк	Мобильный банк	Сайт поставщика		
Жилищно-коммунальные услуги	x		x		x
Связь: Интернет, мобильный телефон	x	x			
Оплата детских учреждений: детский сад, секции, школа	x			x	
Выплаты по кредитам (ипотека, кредитные карты и пр.)				x	x
Платежи в пользу государства: налоги, пошлины за госуслуги, штрафы	x			x	x
Финансовая помощь близким		x			
Взаиморасчеты с друзьями, знакомыми в рамках совместных покупок или мелких займов		x			
Переводы, связанные с трудовой деятельностью (часто для индивидуальных предпринимателей).	x	x			
Зарубежные переводы					
Переводы в пользу организаций, юридических лиц в основном для оплаты услуг (билеты, бронирование гостиниц, закупки товаров в рамках работы и пр.)	x				

Исследование показало, что и «продвинутые» пользователи, и «обыватели» подобрали для своих дистанционных платежных операций определенный канал оплаты, соответствующий требованиям жизненной ситуации (например, быстрый перевод знакомому через мобильный банк, оплата ЖКХ

через интернет-банк, оплата услуг детских дошкольных учреждений и т.п). Смена способа может происходить под давлением внешних обстоятельств, например, неработоспособности техники, внезапного изменения срочности платежа, отклонения от ежедневного маршрута (если по дороге есть отделение банка). Однако продвинутые пользователи в качестве исключения могут поменять канал оплаты из любопытства и стремления протестировать новый сервис [34].

Участники фокус-групп отметили, что обязательные платежи являются рутинной практикой, которая достаточно стабильна, редко меняется, тем более, что смена реквизитов требуется не часто. Для большинства предпочтительным способом проведения таких платежей стал интернет-банк. Большой экран стационарного компьютера или ноутбука позволяет работать с «длинными» реквизитами, а смс-подтверждения повышают доверие к безопасности этого канала. Барьерами для использования Интернет-банка чаще всего становятся отсутствие квитанции с «синей печатью», чека или других форм документарного подтверждения (особенно для больших сумм).

«TNS Россия» изучила, насколько электронные платежи популярны у жителей крупных городов, за что они чаще всего платят онлайн и какими способами. Исследование проводилось в феврале — марте этого года, в нем участвовали россияне в возрасте 18–55 лет из городов с населением более 700 тыс. человек в шести федеральных округах и городов Дальневосточного региона с населением от 600 тыс. человек. Участники опроса пользуются интернетом минимум раз в неделю.

Выяснилось, что в целом по стране платежи в интернете совершает подавляющее большинство пользователей из крупных городов: 92% опрошенных оплачивают онлайн минимум одну услугу за год.

Чаще всего люди платят онлайн за услуги, без которых сложно обойтись: сотовую связь оплачивают таким образом 77% пользователей, 66% опрошенных расплачиваются онлайн за покупки в интернет-магазинах, а 60% платят за ЖКУ. Больше половины интернет-пользователей (59%) отправляют онлайн денежные переводы, а 37% покупают билеты на концерты, в кино и театры. Следующие

по популярности категории интернет-платежей: штрафы ГИБДД и налоги - 34%, билеты на поезда и самолеты - 33%, кредиты - 31%, различный онлайн-контент - 23%, онлайн-игры - 19% [34].

Россияне используют разные способы онлайн-оплаты: банковские карты, интернет-банкинги, электронные кошельки и платежи через смс. Метод оплаты часто зависит от назначения платежа: через интернет-банкинг и смс чаще платят за сотовую связь, а с карт и из кошельков — за покупки в интернет-магазинах (табл. 2.2).

Таблица 2.2 - Способы онлайн-оплаты (доля пользователей,%)

Вид платежа	Электронные кошельки	Интернет-банкинг	Банковские карты	Оплата через смс
Заказы в интернет-магазинах	28	37	42	11
Сотовая связь	26	59	34	21
Денежные переводы	22	50	25	13
Коммунальные услуги	16	47	26	9
Онлайн-контент	11	13	13	7
Онлайн-игры	11	9	10	5
Билеты на концерты	10	19	24	5
Штрафы и налоги	9	28	13	5
Кредиты	7	25	12	5
Билеты на поезда и самолеты	6	18	22	-
Транспортные карты	5	10	6	-
Услуги учебных заведений	4	13	6	-

В среднем по России электронными кошельками минимум раз в год пользуются 62%. Больше всего пользователей кошельков среди жителей Юга (67%) и Дальнего Востока (69%).

В других регионах этот показатель совпадает со средним по стране или отличается совсем незначительно: в Москве - 63%, на Урале и в Санкт-Петербурге - 62%, в Сибири и Приволжье - 61% и 60% соответственно (табл. 2.3).

Таблица 2.3 - Онлайн-оплата со смартфонов (доля пользователей, %)

Регион	Электронные кошельки	Интернет-банкинг	Банковские карты	Оплата через смс
Россия в целом	38	61	55	49
Москва	39	66	58	49
Санкт-Петербург	35	55	54	47
Юг	41	61	52	48
Поволжье	38	59	57	47
Урал	36	59	52	47
Сибирь	35	61	49	53
Дальний Восток	44	63	53	54

С повсеместным распространением мобильного интернета заметно увеличилось число платежей со смартфонов. С их помощью в целом по России из электронных кошельков платят 38% пользователей, через смс - 49%, с банковских карт - 55%, а через приложения интернет-банкингов - 61%.

2.2 Анализ современного состояния интернет-банкинга в России

2.2.1 Оценка эффективности интернет-банка для физических лиц

Аналитическое агентство MarkswebbRank&Report по итогам 2016 года провело исследование эффективности российских сервисов интернет-банкинга.

Более эффективным для физических лиц считается интернет-банк, который наиболее полно удовлетворяет потребности пользователя и имеет удобный понятный интерфейс [38].

Исследование фиксирует следующие основные параметры эффективности.

1. Функциональность — возможности управления собственными финансами клиента:

–получение информации по карте;

–платежи и переводы;

–изменение настроек карты;

–заказ и получение новых продуктов банка онлайн (открытие счетов и вкладов, заказ карт, заявки на кредиты и т.д.);

–получение справочной информации (табл. 2.4).

Таблица 2.4 - Критерии оценки функциональных возможностей для физических лиц

Группы критериев функциональных возможностей	Вес группы критериев
Средства связи с банком	5%
Новые продукты: открытие счетов и вкладов, заказ карт, заявки на кредиты и другие продукты	20%
Настройки карты: PIN-код, блокировка, уведомления, управление лимитами по карте	5%
Платежи, переводы, проверка начислений и задолженностей, лимиты на переводы	50%
Информация по карте клиента: остатки, параметры, тарифы, выписки, квитанции, аналитика	20%

2. Удобство пользования — простота и понятность совершения операций в интернет-банке:

–удобство входа в интернет-банк;

–возможность дистанционной регистрации и восстановления потерянного доступа;

–удобство навигации;

–упрощение повторных операций

–удобство экспорта данных;

–удобство платежных форм;

–упрощение повторных операций;

–дружелюбность интерфейса (табл. 2.5).

Таблица 2.5 - Критерии оценки удобства пользования для физических лиц

Группы критериев удобства пользования	Вес группы критериев
Регистрация и восстановление доступа	10%
Вход в интернет-банк	15%
Удобство навигации	10%
Удобство экспорта данных	10%
Удобство платежных форм	10%
Упрощение повторных платежных операций	15%
Дружелюбность интерфейса	5%
Оценка привлекательности дизайна	5%
Общая оценка предпочтительности	5%
Средняя оценка удобства выполнения задач	15%

Общие оценки функциональных возможностей и удобства пользования рассчитывались как сумма выполненных критериев, умноженных на их веса. Итоговая оценка эффективности измеряется по шкале от 0 до 100 баллов.

За прошедший год из первой десятки рейтинга интернет-банков выбыли Московский Кредитный Банк, Запсибкомбанк, Банк Траст, Банк Русский Стандарт и Банк Санкт-Петербург. Пополнили топ-10 Сбербанк России, Банк Уралсиб, Почта Банк, Райффайзенбанк и Совкомбанк (табл. 2.6).

Таблица 2.6 - Рейтинг эффективности интернет-банков для физических лиц

Место	Интернет-банк	Оценка
1	Бинбанк	77,8
2	Тинькофф Банк	77,4
3	Промсвязьбанк	73,5
4	Альфа-Банк	66,3
5	ВТБ24	65,5
6	Сбербанк России	64,3
7	Банк Уралсиб	64
8	Почта Банк	63
9	Райффайзенбанк	62,5
10	Совкомбанк	61,8

Наиболее эффективными интернет-банками с точки зрения удобства интерфейсов и функциональности были признаны интернет-банки Бинбанка (ранее интернет-банк МДМ Банка), Тинькофф Банка, Промсвязьбанка, Альфа-Банка и ВТБ.

Интернет-банку Бинбанка удалось подняться на первое место за счет улучшения удобства и реализации большого количества важных функций, в том числе:

−форма перевода между произвольными картами с картами с автоматическим определением платежной системы и банка-эмитента по введенному номеру карты;

−форма поиска задолженностей по штрафам ГИБДД и налогам по персональным данным пользователя;

−продвинутые возможности блокировки карты и установки пользовательских лимитов на операции по карте;

−возможность открытия текущих счетов и выпуска карт без посещения банка и звонка в контактный центр.

Must-have функции интернет-банка:

−переводы между собственными счетами и картами, в том числе в разных валютах;

−возможности упрощенных переводов другим клиентам банка;

−наличие истории операций по карте;

−переводы в другие банки по номерам счетов и карт;

−формы переводов на счета в электронных деньгах;

−оплата коммунальных услуг, мобильной и стационарной телефонной связи, интернет-провайдеров, телевидения;

−упрощенная оплата штрафов ГИБДД (по УИН, по номеру транспортного средства, номеру прав и свидетельству о регистрации транспортного средства);

−возможность заблокировать карту;

−форма открытия вклада;

−создание и редактирование шаблонов платежей.

2.2.2 Оценка эффективности интернет-банка для малого бизнеса

Интернет-банки для малого бизнеса интегрируются с партнерскими сервисами, в частности, с сервисами проверки благонадежности контрагента, онлайн-бухгалтериями, 1С.

В некоторых интернет-банках появляется функционал для ведения бухгалтерской отчетности. Например, налоговый календарь в Точка Банке, где отображается расписание необходимых платежей и отчислений в бюджет, причем платежное поручение формируется автоматически при выборе конкретного платежа.

Под малым бизнесом в исследовании понимается широкий круг лиц, занимающихся предпринимательской деятельностью: начиная от частных лиц со статусом ИП и пассивным доходом (например, от сдачи недвижимости в аренду) и заканчивая коммерческими организациями со штатом до 100 человек, занимающимися сложной внешнеэкономической деятельностью.

Под эффективностью интернет-банка понимается полнота возможностей управления расчетными счетами и другими продуктами, доступными клиентам сегмента малого бизнеса, и удобство реализации этих возможностей [38].

Исследование оценивает эффективность интернет-банка сточки зрения двух моделей малого бизнеса:

1) начинающий бизнес – предприниматели, только начинающие свою деятельность, не имеющие сложившихся бизнес-процессов и опыта финансовых операций;

2) профессиональный бизнес – предприниматели, давно ведущие деятельность в рамках одного или нескольких юридических лиц, имеющие сложившиеся бизнес-процессы, в том числе, в финансовых операциях.

Начинающий малый бизнес использует небольшой набор продуктов и услуг — преимущественно расчетный счет. Профессиональному малому бизнесу может потребоваться расширенный набор продуктов и услуг, например, зарплатный проект, эквайринг, кредиты, депозиты, дополнительные счета, корпоративные карты, валютный счет и его производные: обмен валют, валютные платежи и, соответственно, валютный контроль.

Оценка эффективности интернет-банка для начинающих предпринимателей, учитывает самые базовые потребности клиентов: быстро и легко открыть расчетный счет, удобный вход в интернет-банк с любого устройства, возможность быстро в удобном виде просматривать информацию по счету и совершать платежи.

Критерии оценки эффективности интернет-банка для начинающих предпринимателей представлены в таблице 2.7.

Таблица 2.7 - Критерии оценки эффективности интернет-банка для начинающих предпринимателей

Группа критериев	Вес группы критериев
Подключение интернет-банка	15%
Вход в интернет-банк	15%
Проверка состояния счета	15%
Получение выписки	20%
Проведение платежа	20%
Выдача доступа к интернет-банку другому сотруднику	5%
Настройка уведомлений	5%
Онлайн-чат	5%

Оценка эффективности интернет-банка для профессионального малого бизнеса, учитывает полный спектр финансовых задач малого бизнеса, включая выпуск и обслуживание корпоративных карт, управление начислением зарплат сотрудникам через функционал зарплатного проекта, открытие депозитов и управление кредитами, валютные операции и валютный контроль (табл. 2.8).

Таблица 2.8 - Критерии оценки эффективности интернет-банка для профессионального малого бизнеса

Группа критериев	Вес группы критериев
Подключение интернет-банка	5%
Вход в интернет-банк	10%
Проверка состояния счета	5%
Получение выписки	10%
Проведение платежа	15%
Выдача доступа к интернет-банку другому сотруднику	5%
Настройка уведомлений	5%
Онлайн-чат	5%
Обмен валют	5%
Валютный контроль	5%
Валютный платеж	5%
Зарплатный проект	5%
Эквайринг	5%
Кредиты, депозиты, дополнительные счета и корпоративные карты	15%

Лучшие интернет-банки для малого бизнеса сделали Точка Банк, Тинькофф Банк, Альфа-Банк, Промсвязьбанк и ВТБ24. Причем, если первые два специализируются на дистанционном обслуживании, то Альфа-Банк, Промсвязьбанк и ВТБ24 —примеры того, как хорошо банк, который специализируется на обслуживании крупного бизнеса, может соответствовать ожиданиям малого бизнеса.

Как и годом ранее, первое место в рейтинге эффективности интернет-банков для малого бизнеса (начинающего и профессионального) занял Точка Банк. После редизайна он стал еще удобнее и функциональнее: как и раньше, на главной странице интернет-банка выводится остаток по счету, есть поиск по операциям и возможность написать в чат, однако теперь основные пользовательские задачи выполнять еще проще и удобнее (табл. 2.9).

Таблица 2.9 - Рейтинг эффективности интернет-банков для малого бизнеса

Место	для начинающего малого бизнеса		для профессионального малого бизнеса	
	банк	оценка	банк	оценка
1	Точка Банк	91,3	Точка Банк	79,1
2	Тинькофф Банк	78,9	Промсвязьбанк	60,6
3	Альфа-Банк	74,4	ВТБ24	59,7
4	ВТБ24	70,5	Альфа-Банк	55,6
5	УБРиР	66,3	Тинькофф Банк	53,8
6	Запсибкомбанк	58,3	Авангард	53,2
7	Райффайзенбанк	57,4	УБРиР	50,3
8	Азиатско-Тихоокеанский Банк	57,1	Азиатско-Тихоокеанский Банк	49,3
9	Промсвязьбанк	56,9	Сбербанк России	47,9
10	Авангард	56,6	Райффайзенбанк	43,6

Еще один редизайн—интернет-банк Сбербанка для малого бизнеса. Однако в нем, в отличие от Точка Банка, изменения интерфейса не повлекли за собой значимых функциональных изменений.

Что касается технических решений, лучшие интернет-банки (Точка Банк, Тинькофф Банк, Альфа-Банк, Промсвязьбанк) — это собственные разработки банков, сделанные с прицелом на потребности банка и его клиентов.

В интернет-банках появляются инструменты аналитики для малого бизнеса: диаграммы, графики по движению средств (поступления, списания), контрагентам, статистика по эквайрингу вплоть до диаграмм по конверсии. При этом можно выделить 3 уровня аналитики: макроуровень – все движения по счету, средний уровень — доли контрагентов в общем объеме операций и микроуровень – динамика операций по конкретному контрагенту.

Упрощаются формы платежных поручений. Например, поля для бюджетных платежей скрываются во вкладки, появляются подсказки по заполнению форм и возможность настроить уведомления для получателя платежа на почту и телефон. Также интернет-банки учатся распознавать квитанции и платежные поручения, переводя изображение в текст, и сами подставляют полученные данные в поля форм.

2.3 Анализ современного состояния мобильного банкинга в России

2.3.1 Оценка эффективности мобильного банкинга для физических лиц

Аналитическое агентство MarkswebbRank&Report по итогам 2016 года провело исследование эффективности российских сервисов мобильного банкинга для физических лиц. Под эффективностью мобильного банка понимается степень удовлетворения потребностей конечных пользователей.

Общие оценки функциональных возможностей и удобства пользования рассчитывались как сумма выполненных критериев, умноженных на их веса. Итоговая оценка эффективности измеряется по шкале от 0 до 100 баллов [38].

Исследование фиксирует следующие основные параметры эффективности.

1.Функциональность — возможности управления собственными финансами клиента:

–получение информации по карте;

–платежи и переводы;

–изменение настроек карты;

–заказ и получение новых продуктов банка онлайн (открытие счетов и вкладов, заказ карт, заявки на кредиты и т.д.);

–поиск банкоматов и офисов банка (табл. 2.10).

Таблица 2.10 - Критерии оценки функциональных возможностей мобильного банка для физических лиц

Группы критериев функциональных возможностей	Вес группы критериев
Средства связи с банком	5%
Информация по банкоматам и офисам	10%
Новые продукты: открытие счетов и вкладов, заказ карт, заявки на кредиты и другие продукты	10%
Настройки карты: PIN-код, блокировка, уведомления, управление лимитами по карте	5%
Платежи, переводы, проверка начислений и задолженностей, лимиты на переводы	50%
Информация по карте клиента: остатки, параметры, тарифы, выписки, квитанции, аналитика	20%

2.Удобство пользования — простота и понятность совершения операций в мобильном банке:

–возможность дистанционной регистрации и восстановления потерянного доступа;

–удобство входа, навигации, совершения платежей;

–возможность упрощения повторных операций (табл. 2.11).

Таблица 2.11 - Критерии оценки удобства пользования мобильного банка для физических лиц

Группы критериев удобства пользования	Вес группы критериев
Регистрация и восстановление доступа	10%
Вход в мобильный банк	15%
Удобство навигации	15%
Открытость (экспортируемость) данных	5%
Удобство платежных форм	10%
Упрощение повторных платежных операций	15%
Дружелюбность интерфейса	5%
Оценка привлекательности дизайна	5%
Общая оценка предпочтительности	5%
Средняя оценка удобства выполнения задач	15%

По результатам исследования - лучший мобильный банк для iPhone и Android—у Тинькофф Банка. В мобильном приложении есть авторизация по отпечатку пальца (в том числе, для Android), онлайн-чат с консультантами банка, реализована технология бесконтактных платежей смартфоном (только для Android), а также возможность подключить автоплатежи и платежи по расписанию, удаленно заказать продукты банка, привязать к аккаунту в приложении карту любого банка и пополнять карту Тинькофф с карты другого банка. История операций и выписка объединены в единую ленту событий (табл. 2.12).

Таблица 2.12 - Рейтинг эффективности мобильных банков для физических лиц

Место	для iPhone		для Android	
	Мобильный банк	Оценка	Мобильный банк	Оценка
1	Тинькофф Банк	67,3	Тинькофф Банк	67,3
2	Сбербанк России	62,3	Альфа-Банк	60,2
3	Почта Банк	60,5	Сбербанк России	59,2
4	Альфа-Банк	59,8	МДМ Банк	58,9
5	МИнБанк	58,8	Почта Банк	58,3

Лучший мобильный банк для смартфонов на базе Windows Phone—у Сбербанка. Тинькофф потерял лидирующие позиции из-за сокращения функционала (нет фильтров в истории операций, формы оплаты штрафов ГИБДД, возможности проложить маршрут до банкомата и т.д.). В целом большинство исследованных мобильных банков для смартфонов на базе Windows Phone имеют более «урезанный» функционал по сравнению с iPhone и Android.

Лучшим мобильным банком для iPad стало приложение Альфа-Банка за счет расширения функционала выписки по карте и экспорта данных, реализации автоматического определения провайдера по номеру телефона, а также за счет увеличения суммы переводов за разовую операцию. Банки Авангард и Уралсиб потеряли лидирующие позиции, так как в их приложениях существенных изменений за год не произошло.

Для планшетов Android лучшим мобильным банком стало приложение Райффайзенбанка. В нем появился PFM-сервис, возможность пополнения карты с

карты другого банка и возможность входа по короткому цифровому коду (табл. 2.13).

Таблица 2.13 - Рейтинг эффективности мобильных банков для Windows Phone, iPad и планшетов на базе Android

Место	для Windows Phone		для iPad		Для планшетов Android	
	Мобильный банк	Оценка	Мобильный банк	Оценка	Мобильный банк	Оценка
1	Сбербанк России	56,7	Альфа-Банк	62,5	Райффайзен-банк	55,8
2	МДМ Банк	55,8	Сбербанк России	60,4	ВТБ24	52,6
3	МИнБанк	55,7	МИнБанк	60,0	Авангард	51,4
4	Банк Санкт-Петербург	52,6	ВТБ24	58,0	Росбанк	47,2
5	ВТБ24	51,3	Райффай-зенбанк	55,3	Открытие	43,2

Must-havefункционал мобильного банковского приложения: перевод между собственными счетами/картами и на карты других клиентов, оплата коммунальных услуг, мобильной и стационарной телефонной связи, интернет-провайдеров, ТВ, создание и редактирование шаблонов платежей, обмен валют, вход по короткому цифровому коду или графическому ключу, открытие вкладов и счетов. Расширяется функционал card2card переводов и производных от них, в том числе, пополнение счета/карты с карты другого банка, оплата штрафов, налогов и коммунальных услуг с поиском задолженности, пополнение с карт других банков. Сами card2card переводы становятся удобнее за счет создания шаблонов, платежей по расписанию и автоплатежей.

На смену колл-центрам приходят онлайн-чаты с консультантами банка в интерфейсе мобильного приложения для оперативно поддержки пользователей мобильного банкинга.

Интерфейсы приложений становятся проще и понятнее: сложные коды операций заменяются понятными формулировками, обмен валют выносится в список операций, как отдельная функция. Ввод номера карты заменяется

сканированием, и постепенно этот функционал распространяется на сканирование штрих-кодов квитанций.

Банки добавляют возможность привязать к аккаунту в мобильном приложении карты других банков. Пока эта функция реализована у 5 банков.

В России мобильными банками пользуются 18 млн. человек в возрасте от 18 до 64 лет (рис. 2.1).

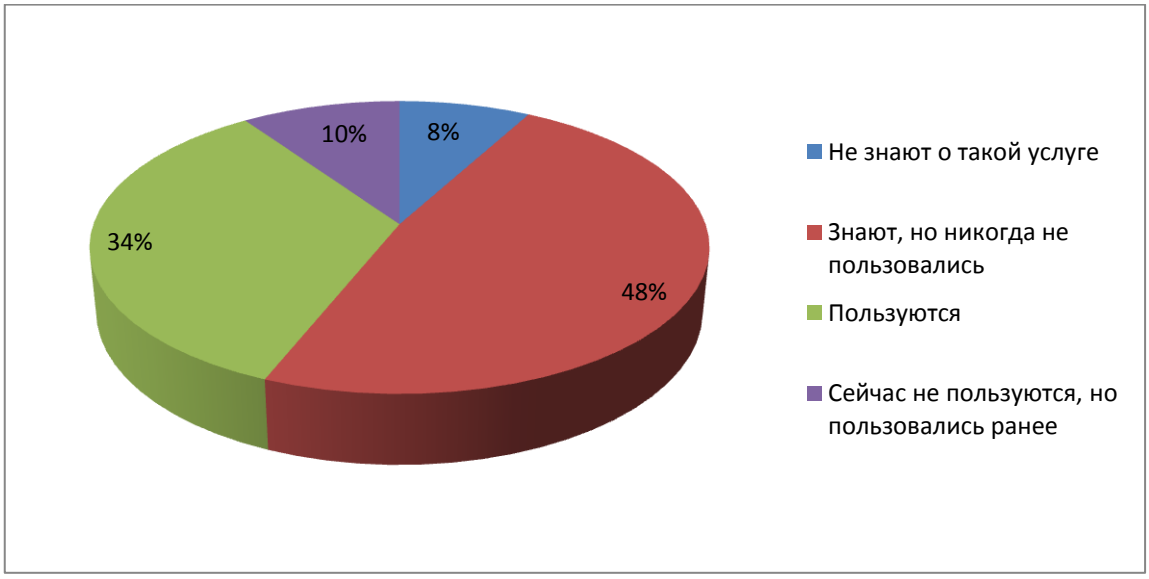

Рисунок 2.1– Структура пользователей мобильным банкингом

75% пользователей мобильного банкинга пользуются только одним банковским мобильным приложением, 18% –мобильными приложениями двух банков (рис. 2.2).

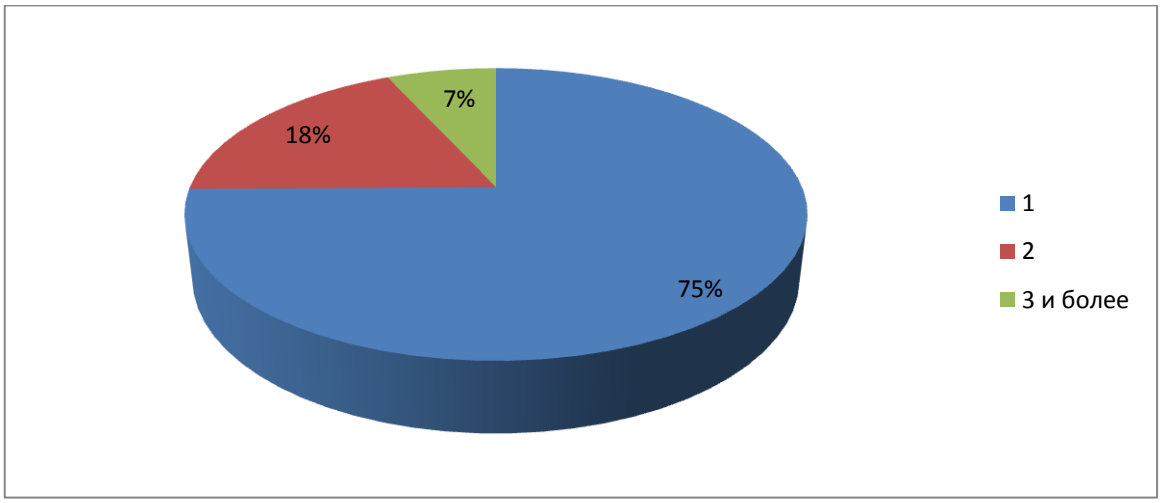

Рисунок 2.2 – Распределение пользователей мобильного банкинга по количеству используемых приложений

89% пользователей мобильного банка пользуются и интернет-банком тоже, причем 17% из них пользуются мобильным банком чаще, чем интернет-банком.

За прошедший год аудитория мобильного банкинга для частных лиц выросла на 2%, или 1 млн. пользователей - 33%, или 18 млн. российских интернет-пользователей в возрасте от 18 до 64 лет пользуются мобильными банками для частных лиц.

2.3.2 Оценка эффективности мобильного банкинга для малого бизнеса

Способы входа в мобильный банк для бизнеса используются те же, что и в приложениях для частных лиц. Самые распространенные на iOS и Android— комбинация логин/пароль и короткий код. Популярный для iPhone вход по отпечатку пальца в приложениях для Android есть только у Тинькофф Банка, а графический ключ используется только в приложении Промсвязьбанка для iPhone.

Проникновение онлайн-чатов в мобильных банках для малого бизнеса выше, чем в приложениях для частных лиц. Чаты есть в 8 приложениях из 10 на iOSи в 7 приложениях из 9 на Android, но работают они по-разному: где-то можно узнать только общую информацию о банке или услугах, а где-то даже отправлять распоряжения. В отличие от мобильных банков для частных лиц, которые обычно выходят одновременно на разных платформах и имеют одинаковый функционал, развитие мобильных банков для бизнеса на разных платформах происходит по-разному. Одни банки запускают или перезапускают обе платформы сразу (Модульбанк, МДМ Банк, Тинькофф Банк), другие отдают предпочтение какой-то одной, обычно это iOS(Точка Банк, Промсвязьбанк, ВТБ24).

На текущий момент только 3 банка соблюдают гайдлайны Apple и Google —это МДМ Банк, Тинькофф Банк и Сбербанк. Другие банки соблюдают их частично (Промсвязьбанк, Модульбанкдля iOS, Точка, Альфа-Банк для Android) или не соблюдают (Райффайзенбанк, УБРиР).

Первые 3 места в рейтингах для iPhone и смартфонов Android заняли Тинькофф Банк, Точка и Альфа-Банк. В приложениях этих банков наиболее полно реализован платежный функционал (можно отправлять платежи любым контрагентам), есть шаблоны платежей, сервис проверки контрагента, графическая аналитика и распознавание платежного поручения по фото. В банках, занявших последние места (ВТБ24, УБРиР, МДМ Банк), нет возможности отправлять платежи, можно только посмотреть выписку и остаток по счетам. Тем не менее, в некоторых банках (например, МДМ Банк) очень хорошо реализованы другие базовые пользовательские задачи (вход, просмотр остатка, получение выписки), и поэтому их оценка значительно выше: 55,4 балла у МДМ Банка против 32,6 у УБРиР и 21,9 у ВТБ24 (для iPhone) [38].

Банки в середине рейтинга (Сбербанк, Райффайзенбанк, Промсвязьбанк для iOS) имеют платежный функционал, но он ограничен: можно отправлять платежи только доверенным контрагентам или повторять уже совершенные через интернет-банк платежи (табл. 2.14).

Таблица 2.14 - Рейтинг эффективности мобильных банков для малого бизнеса

Место	для iPhone		для Android	
	банк	оценка	банк	оценка
1	Точка Банк	73,4	Тинькофф Банк	72,8
2	Тинькофф Банк	72,8	Точка Банк	65,4
3	Альфа-Банк	66,6	Альфа-Банк	65
4	Модульбанк	64,3	Модульбанк	62,9
5	Сбербанк России	57	Сбербанк России	57,1
6	Промсвязьбанк	56,7	МДМ Банк	52,7
7	МДМ Банк	55,4	Райффайзенбанк	49,4
8	Райффайзенбанк	52,9	УБРиР	32,6
9	УБРиР	32,6	Промсвязьбанк	31,9
10	ВТБ24	21,9	ВТБ24	-

В отношении платежного функционала ситуация за прошедший год не изменилась — по-прежнему можно выделить 3 группы мобильных банков:

–можно отправлять платежи любым контрагентам (лидеры рейтинга — Тинькофф Банк, Точка, Альфа-Банк, Модульбанк);

–можно отправлять платежи только доверенным контрагентам (середина рейтинга: Райффайзенбанк, Сбербанк, Промсвязьбанк для iOS);

–нельзя отправлять платежи (последние места рейтингов: ВТБ24, УБРиР, МДМ Банк, Промсвязьбанк для Android).

Мобильные банки для планшетов — сервис не очень функциональный и достаточно редкий. У некоторых банков их нет: например, лидеры рейтингов для iPhoneи смартфонов Android, Тинькофф Банк и Точка, вместо приложений для планшетов предлагают удобный ифункциональный интернет-банк, который хорошо адаптирован для работы с планшета. Некоторые банки делают приложения для планшетов с тем же функционалом, что и для смартфонов (Сбербанк, ВТБ24, Промсвязьбанк, УБРиР), другие - с урезанным (Альфа-Банк, Райффайзенбанк).

Под приложением для планшета в исследовании подразумевается мобильный банк, разработанный специально для устройств этого типа. В частности, в них есть дополнительные интерфейсные элементы, которые используют пространство большого экрана с пользой (например, меню слева, фильтр на часть экрана).

Не считается приложением для планшета мобильный банк для смартфона, который просто растягивается на большой экран.

Разброс оценок эффективности мобильных приложений для бизнеса на платформе Android меньше, чем на iPhone. Отчасти это связано с тем, что многие банки уделяют больше внимания iPhone: перезапускают их в первую очередь и добавляют больше функциональных возможностей (табл. 2.15).

Таблица 2.15 - Рейтинг эффективности мобильных банков для планшетов

Место	для iPad		для Android	
	банк	оценка	банк	оценка
1	Альфа-Банк	57,7	Альфа-Банк	57,7
2	Сбербанк России	56,5	Сбербанк России	56,8
3	Райффайзенбанк	43,6	Промсвязьбанк	32,6
4	УБРиР	32,6	УБРиР	32,6
5	ВТБ24	21,6	ВТБ24	-

Выделяется группа банков, которые ориентированы на дистанционное обслуживание клиентов, причем это не только Тинькофф Банк и Точка, которые работают в формате безофисного обслуживания, но и крупные федеральные банки — Альфа-Банк и Промсвязьбанк.

Эти банки одинаково активно развивают и интернет- и мобильные банки для бизнеса. Однако большинство банков отдает предпочтение какому-то одному каналу ДБО (например, ВТБ24 интернет-банку, МДМ-Банк мобильному банку)

3. Развитие систем дистанционного банковского обслуживания

3.1 Проблема электронного мошенничества в системах ДБО

Электронное мошенничество в банковской сфере превратилось в теневую отрасль экономики. Это криминальный рынок, на котором определены роли – организация хищений, взлом компьютеров, вывод и обналичивание денег. Службы безопасности банковской сферы и правоохранительные органы порой не в силах справится с этим явлением, а государство ещё не осознало в должной мере важности этой проблемы.

Сегодня у злоумышленников очень популярен взлом персональных компьютеров – рабочих мест клиентов различных банков. Эти компьютеры являются доверенными участниками систем дистанционного банковского обслуживания, электронных кошельков, денежных переводов, в том числе банков-корреспондентов платёжных систем (Contact, WesternUnion, Moneygram, Unistream, Migom и других) [33].

Компьютерные преступления в системах ДБО квалифицируются как мошенничество, расследованием их (далее киберпреступлений) занимаются подразделения «К» Бюро специальных технических мероприятий (БСТМ) МВД России. Одним из последних документов, который описывает практику расследования этих преступлений, стало Постановление Пленума Верховного Суда РФ от 27 декабря 2007 года № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Согласно п. 1 этого постановления, «мошенничество совершается путём обмана или злоупотребления доверием, под воздействием которых владелец имущества или иное лицо либо уполномоченный орган власти передают имущество или право на него другим лицам, либо не препятствуют изъятию этого имущества или приобретению права на него другими лицами». Соответственно, обман и злоупотребление доверием – это способы совершения мошенничества. В банковской сфере речь идет о завладении обманным путем секретными

реквизитами пострадавшего (логином, паролем и закрытым ключом) и о совершении от его имени электронных платежей в системе ДБО.

В постановлении определяется момент окончания мошенничества и отличие его от других преступлений. Мошенничество считается оконченным, когда у мошенника возникает юридически закрепленная возможность вступить во владение или распорядиться чужим имуществом как своим собственным. Таким образом, сложилась практика: расследование киберпреступлений должно проводиться по месту окончания мошенничества, где было проведено обналичивание денежных средств. Поэтому материалы доследственной проверки, проведённой по обращению пострадавшего в правоохранительные органы, передаются в территориальные подразделения «К» по месту снятия похищенных средств в банкомате.

Такая практика приводит к децентрализации проведения расследования и передаче материалов доследственной проверки в территориальные подразделения БСТМ или ГУЭБиПК, которые не обладают необходимым потенциалом для расследования подобных дел. В результате много времени уходит на передачу документов между подразделениями МВД России, теряется драгоценное время, необходимое для оперативных действий – проведения расследования, поиска злоумышленников.

Местом совершения киберпреступления, в отличие от привычного подхода, следует считать место расположения взломанного компьютера, который является доверенным клиентом платёжного инструмента – системы ДБО, платежной системы, провайдера услуг/товаров.

В данном случае несущественно, что преступление совершается последовательно в нескольких ключевых пунктах (рис. 3.1):

- источник заражения взломанного компьютера;
- организатор;
- источник удалённого управления заражённым компьютером для вывода денежных средств;
- взломанный компьютер;

- ПИ – платёжный инструментарий;
- банк;
- транзит;
- точка обналичивания.

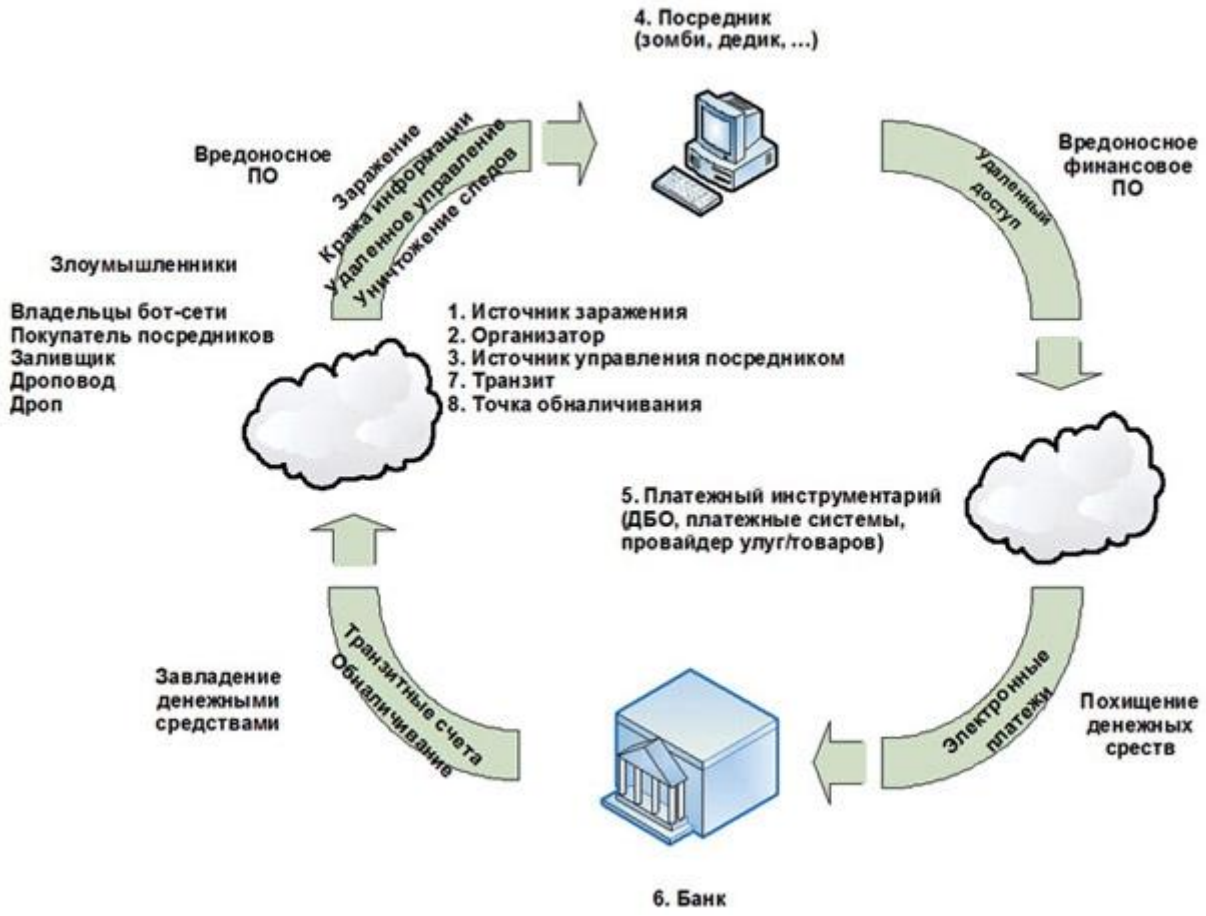

Рисунок 3.1 - Место совершения киберпреступления

В большинстве случаев предпосылкой кражи является заражение компьютера вредоносным программным обеспечением. В результате компьютер может стать звеном бот-сети, которая иногда объединяет сотни тысяч заражённых компьютеров (так называемых «зомби»). Код вредоносного программного обеспечения постоянно модифицируется и не всегда отслеживается антивирусами. Заражённый компьютер способен использоваться для спам-рассылки, DDoS-атак (массового одновременного обращения к одному источнику с целью вывода его из строя), а также при краже электронных денежных средств.

«Вредонос» выявляет подключение заражённого компьютера к системе ДБО и загружает на него специальный код для системы ДБО конкретного разработчика. Код, копируя логин/пароль и электронные ключи пользователя, пересылает их злоумышленникам. Кроме того, часто встречаются случаи, когда перевод денежных средств осуществляется непосредственно с компьютера жертвы посредством специально загружаемого кода для удалённого управления клиентским местом системы ДБО [27].

Рассмотрим обобщённую схему хищения. Заказчик намечает жертвы и выходит на организатора хищения. На криминальном рынке в наличии готовые «решения» – продукты от хакеров (взломщиков). Предлагаются списки взломанных компьютеров («дедиков», «дедов», «зомби» – звеньев бот-сети) под удалённым управлением хакеров, вредоносные коды троянов для работы с платёжным инструментарием (включая системы дистанционного обслуживания, банк-клиент, платёжных переводов или электронных денег).

Схемы краж отработаны и проверены. Организатор под заказчика подбирает инструменты и исполнителей. Подбирается «заливщик» – специалист по выводу денег, который организует списание денег со взломанных счетов для получения в итоге наличных или товарного эквивалента. Следующим в схеме будет «дроповод», который предоставляет «дропов» – получателей наличных.

На этом этапе мошенничества неважно, «разведённый» это дроп, который не догадывается о своём участии в мошенничестве и искренне считает себя посредником в легальных сделках, или же «неразведенный», участвующий в криминальной схеме сознательно. Важно, что цепочка замкнулась, организатор получает деньги и передает их заказчику.

Действия службы информационной безопасности банка.

В случае хищения необходимо зарегистрировать инцидент и описать все обстоятельства кражи денег. Для начала можно просто зафиксировать время обращения в службу информационной безопасности банка о данном инциденте и, начиная с этого времени, протоколировать все действия. Нужно подготовить

материалы для дальнейших мероприятий: копии платёжек мошеннических переводов, логи системы ДБО, контактные телефоны пострадавшего клиента.

Необходимо предложить клиенту письменно объяснить обстоятельства произошедшего, предложить ему сформулировать свои требования. Клиент может запросить полную информацию об инциденте, содействия в предотвращении обналичивания украденных средств, в поиске злоумышленников и т.п.

В первую очередь следует попытаться остановить движение похищенных сумм и узнать получателя денежных средств. Нужно связаться с банком-корреспондентом, через который осуществлён вывод денежных средств, похищенных со счёта клиента. Надлежит отправить сообщение по системе SWIFT, написать письмо на имя председателя правления банка-корреспондента. Не стоит обольщаться, надеясь на быстрый результат: у банка-корреспондента, на счета которого выводятся похищенные средства, нет оснований для блокирования этих средств.

Информацию о получателе платежа можно найти в открытых источниках и передать в правоохранительные органы. Банк – получатель денег может пойти навстречу, задержав перевод этих денег на другие счета или снятие наличных. Формальной причиной приостановки операции может служить необходимость идентификации клиента и получения подтверждения перевода денег плательщика. Основания могут быть следующие.

Кредитная организация обязана идентифицировать лицо, находящееся у нее на обслуживании, при совершении банковских операций и иных сделок в соответствии с федеральным законом «О банках и банковской деятельности» на основании программы идентификации клиентов, установления и идентификации выгодоприобретателей» (п.1 ст. 7 Федерального закона № 115-ФЗ от 07 августа 2001 года и п. 1.1. Положения Банка России № 262-П от 19 августа 2004 года).

Что касается самостоятельных действий – участия в расследовании компьютерных преступлений, то хотелось бы отметить, что банк не имеет полномочий этого делать. Не являясь специалистом-криминалистом, можно, не желая того, уничтожить улики. Законодательство пока не определяет порядок

самостоятельного сбора доказательной базы компьютерных преступлений, а у уполномоченного органа – БСТМ нет дежурных частей для неотложного выезда на место преступления. Поэтому до контакта с правоохранительными органами лучше всего заблокировать учётную запись клиента, предотвращая смену секретных логина, пароля и закрытого ключа.

Теперь об обращении в правоохранительные органы. Клиент должен написать заявление в территориальные органы МВД России. После регистрации это заявление, как правило, направляется в территориальные подразделения УЭБ или подразделения «К» БСТМ. При проведении доследственной проверки сотруднику банка необходимо подъехать к следователю и написать объяснения.

Следует провести согласительную комиссию с клиентом, как это обычно предусматривает договор ДБО. Особенно если этого требует сам клиент в тексте заявления в банк. В договоре оказания банковских услуг может быть предусмотрено создание экспертной или согласительной комиссии для проверки подлинности подписи под электронным платёжным поручением. В таком случае письменно приглашается на разбор инцидента пострадавший клиент и представители разработчика платёжного инструментария. Действия сотрудников банка, имеющих доступ к взломанному компьютеру клиента, должны быть хорошо продуманными. Каждый шаг должен регистрироваться и быть под контролем руководства.

Сотрудникам банка на рабочем месте клиента, чьи средства были похищены, рекомендуется проводить следующие мероприятия. Необходимо ограничить доступ к объектам, задействованным в инциденте. Постараться локализовать инцидент, предотвратить его продолжение, развитие, а также угрозу уничтожения доказательств совершенного преступления. Следует зафиксировать сам факт инцидента – пусть клиент напишет о нём письмо в банк, в котором изложит следующие требования:

- получить информацию о похищенных средствах;
- блокировать учётную запись клиента и его ключи системы ДБО;
- предотвратить вывод и обналичивание похищенных средств.

Клиент обязательно должен написать заявление в правоохранительные органы. Оно подаётся в местные органы полиции, регистрируется в КУСП (книге учёта сообщений о происшествиях), взамен клиент получает талон регистрации заявления.

1. Организационные мероприятия.

1.1. Выявить, кто имел доступ к компьютеру, к программному обеспечению системы ДБО и её секретным реквизитам, таким как логин/пароль и секретные ключи.

1.2. Опросить всех имевших доступ для выяснения полной картины инцидента. Для дальнейшего расследования желательно получить письменные объяснения.

1.3. Получить дополнительную информацию об инциденте: имели ли место подобные случаи хищений денежных средств в это же время, использовались ли для вывода похищенных средств такие же организации или физические лица. Для поиска дополнительной информации можно использовать сеть интернет.

1.4. Принять решение, станет ли информация об инциденте публичной, можно ли сообщать об инциденте в разные источники, включая интернет и прессу. В любом случае нужно избегать репутационных рисков и разглашения конфиденциальной информации.

2. Технические мероприятия.

2.1. Надо определить, кто будет проводить расследование инцидента. Лучше всего, при возможности, если это расследование будет проводить сторонняя специализированная организация, имеющая оборудование и сотрудников соответствующей квалификации.

2.2. Если есть возможность, привлечь специализированную стороннюю организацию. Если нет, собственными силами проводить расследование и сбор материалов для предоставления в правоохранительные органы.

2.3. Надлежит, по возможности, не использовать взломанный компьютер, а обесточить и опечатать до приезда компетентных лиц. До отключения компьютера нужно проверить и зафиксировать следующее:

- пользователей, подключенных к системе (при помощи утилиты NTLast);
- открытые соединения (командой netstat-ano);
- приложения с открытыми соединениями (утилитой fport);
- текущие процессы (утилитой PSList);
- недавние соединения NetBIOS (командой nbtstat-c).

2.4. Если таких возможностей нет, надо сделать копию жёсткого диска пострадавшего компьютера при помощи специальных утилит побитового копирования диска. Копирование диска оформляется документально, а копии обеспечивается безопасное хранение.

2.5. Провести анализ сетевых служб (межсетевого экрана, прокси-сервера, при наличии – системы обнаружения вторжений); журналы/логи сохраняются на носитель без возможности перезаписи (на болванку CD или DVD);

2.6. Провести анализ компьютера, для чего, с сохранением результатов проверки (также на носитель без возможности перезаписи), изучаются:

- события в журналах операционной системы Windows (системном, приложений и безопасности; или же эти журналы сохраняются в окне проводника, выбрав в контекстном меню для значка «Мой компьютер» опцию «Управление и Просмотр событий»);
- журналы приложений (самой системы ДБО, запуска приложений в операционной системе Windows, антивируса, брандмауэра, если он включен);
- список загруженных процессов (запускаемых при загрузке msconfig);
- скрытые административные ресурсы (общие ресурсы со значком $);
- реестр операционной системы (проверяются установленные приложения, разорванные связи в системе, недавно использованные файлы);
- список локальных пользователей и все попытки доступа к компьютеру;
- службы удаленного управления;
- планировщик заданий и созданные задания.

2.7. Провести анализ жесткого диска, который может включать в себя:

- поиск подозрительных и скрытых файлов (созданные и измененные в неурочное время или во время инцидента файлы);
- просмотр корзины.

Основная цель расследования – не допустить повторения инцидентов и обеспечить защиту компьютерного оборудования [27].

3.2 Правовое решение проблемы электронного мошенничества в системах ДБО

Появление новой «отрасли» теневой экономики диктует необходимость объединения усилий бизнеса и государства – законодательных, регулирующих банковский рынок и правоохранительных органов. Особенно остро стоит вопрос времени, оперативности реагирования на инциденты.

Пока недоработки нормативно-правовой базы облегчают киберпреступникам взлом компьютеров, кражи и обналичивание денежных средств. Не хватает юридически определённых процедур расследования, сбора доказательств на всех этапах киберпреступлений. Более всего актуальны юридически значимые определения места и времени совершения киберпреступления, мошеннического или несанкционированного платежа, алгоритма блокировки движения похищенных средств и их обналичивания.

По прогнозам экспертов, в 2017 году ожидается дальнейших рост числа атак на счета клиентов, в том числе через платежные системы, платформы для оплаты государственных услуг, посредством средств мобильной связи и систем дистанционного банковского обслуживания.

Противодействие киберпреступности является многосторонней системной задачей. Такая работа в настоящее время ведётся по нескольким направлениям. Кроме формирования необходимой инфраструктуры, использования технических и организационных мер, необходимо, конечно, совершенствование законодательной базы. Ощутимого результата добиться не получится, внеся

изменения в какой-то отдельный закон. Предстоит актуализировать, усовершенствовать целый комплекс нормативных актов, принадлежащих к разным отраслям права: уголовному, процессуальному, административному и финансовому.

В настоящее время проходят согласования поправки в Уголовный кодекс РФ об изменении статей, касающихся компьютерных преступлений, разработанные с участием ведущих банков. Эти поправки разрабатывались, исходя из насущных требований современной практики. В частности, в статье 1596 Уголовного Кодекса РФ предполагается изменить квалификацию ряда киберпреступлений в финансовой сфере с мошенничества на кражу.

Отличительной чертой мошенничества является способ завладения чужим имуществом – обман или злоупотребление доверием. В киберпреступлениях хищение или приобретение права на чужое имущество сопряжено с преодолением компьютерной защиты и осуществляется путем манипуляции с компьютерной информацией. Обмана или злоупотребления доверием, в том смысле, в каком он был определен Пленумом Верховного Суда еще в 2007 году, по сути, нет. Предстоит устранить это несоответствие.

Учитывая общественную опасность компьютерных преступлений в кредитно-финансовой сфере, можно ожидать дальнейшего ужесточения ответственности за их подготовку и совершение. Подготовлен законопроект изменений в Уголовный кодекс РФ, касающихся усиления уголовной ответственности за хищение денежных средств с банковского счета, включая электронные платежи. До сих пор такие деяния квалифицировались согласно части 1 статьи 158, по общему состав преступления, - как обычная кража. Виновные проговаривались к наказанию в виде лишения свободы на срок всего до 2 лет. После принятия предлагаемых изменений такие кражи смогут квалифицироваться как специальный состав преступления. Подобные преступления начнут подпадать под действие части 3 статьи 158-й Уголовного Кодекса РФ, перейдут из категории небольшой степени тяжести в тяжкие. Наказание за их совершение лишением свободы увеличится на срок до 6 лет.

Одновременно законопроект расширяет объективную сторону состава преступления, связанного с мошенничеством с использованием электронных средств платежа – не только платёжных карт, но и интернет-банкинга и других подобных современных способов. Ранее состав подобных преступлений предусматривал действия только с платёжными картами и вообще не наказывался лишением свободы, только штрафом. Теперь такие преступления предлагается наказывать лишением свободы на срок до 3 лет.

Кроме того, в законопроекте ужесточается наказание за мошенничество в сфере компьютерной информации согласно уже упомянутой статья 1596 Уголовного Кодекса РФ. Срок лишения свободы за подобные преступления увеличивается до 5 лет. Этот законопроект находится на согласовании в Правительстве России и Верховном Суде РФ. Конечно, этот процесс не будет быстрым и простым, но предлагаемые нововведения должны пройти всестороннюю проверку на соответствие системному характеру законодательства, принципам соразмерности и справедливости. В этом видится залог эффективности работы по совершенствованию законодательства.

Ещё одна тенденция, как показывает зарубежный опыт, в частности, США и Великобритании, - усиление детализации в уголовном законодательстве различных видов компьютерных преступлений. Таких, как кража паролей, DDoS-атаки и многие другие незаконные действия злоумышленников. Превалирующая пока в российском уголовном законодательстве квалификация подобных деяний как неправомерного доступа к информации перестала соответствовать их серьезности и опасности.

Однако следует помнить, что в США и Великобритании действует прецедентная система права, при которой велика роль судейского усмотрения, способного компенсировать коллизии между специальными нормами уголовного закона. Этот правовой механизм имел свои предпосылки, формировался веками, и нельзя просто так скопировать его на наши реалии. В Российской Федерации - свой путь правотворчества, адаптации норм к судебной практике[33].

Ещё одним узким местом остаются пробелы в законодательстве, не позволяющие сформулировать официальные критерии неправомерных электронных платежей. Такие критерии необходимы, чтобы приостанавливать сомнительные транзакции до результатов разбирательства. По мнению экспертов, это мешает выстраивать безопасное информационное пространство в кредитно-финансовой сфере.

Законопроект получил положительную оценку Банка России. Сейчас идет процесс согласования с Правительством Российской Федерации. Он направлен на решение проблемы несанкционированных снятий денежных средств со счетов физических лиц, которые осуществляются в первую очередь с использованием платёжных карт, посредством сети интернет и устройств мобильной связи. Законопроект закрепляет право, а в ряде случаев и обязанность банка приостанавливать транзакцию, если выявлены признаки совершения перевода денежных средств без согласия плательщика. Обязательные признаки несанкционированных снятий будут вырабатываться Банком России. Так же банки могут самостоятельно вырабатывать факультативные признаки неправомерных транзакций, которые они смогут использовать в работе с клиентами.

Кроме того, для случаев, когда выявлены признаки совершения перевода денежных средств без согласия плательщика, устанавливается порядок действий банков для возврата денег законному владельцу. Законопроект определяет порядок возврата денежных средств при доказанности факта, что перевод был осуществлен без согласия клиента. Нужно подчеркнуть: при этом законопроект не удлиняет срок проведения платежей клиентов кредитных организаций.

С практической точки зрения данный правовой механизм выглядит так. Дело не безнадежно, даже если деньги по поддельному электронному платёжному поручению списаны со счёта владельца без его согласия. Банк-плательщик на основании имеющихся признаков несанкционированного списания может направить банку-получателю уведомление о приостановлении зачисления денежный средств. Далее в течение 14 рабочих дней банк-плательщик должен

представить решение арбитражного суда, принятое по особой ускоренной процедуре, в котором устанавливается факт несанкционированного снятия денежных средств. Тогда несанкционированно переведённые денежные средства могут быть возвращены их владельцу. Если же такого судебного решения своевременно не поступит, то деньги зачисляются на счет банка-получателя. В этом случае ответственность за ущерб, причинённый владельцу денежных средств, возлагается на него самого. Банк может сам выявить подозрительный платёж и дополнительно проверить его правомерность.

Но и клиент банка, владелец денежных средств на счету, должен заботиться о том, чтобы добросовестно незамедлительно уведомлять банка об инцидентах - списании денежных средств без его согласия. Чтобы, в отведённое на это время, несанкционированный платёж был приостановлен, и проведены процедуры возврата денег.

Для противодействия киберпреступности в финансовой сфере нуждаются в развитии нормы федеральных законов Ф3-152 от 27 июля 2006 года «О персональных данных» и 395-1-ФЗ «О банках и банковской деятельности» в части, касающейся банковской тайны. Ряд норм нуждаются в дополнении и конкретизации, поскольку препятствуют обмену информацией банками друг с другом и с правоохранительными органами о дропперах. То есть о лицах, напрямую занимающихся выводом и снятием наличными денежных средств, похищенных в результате киберпреступлений.

Подготовленный законопроект создаст правовую возможность формирования базы данных покушений совершения переводов денежных средств без согласия клиента, включая удачные случаи. Главным оператором этой базы, согласно федеральному законодательству, будет ведущий государственный регулятор финансового сектора - Банк России. Кредитные организации обязаны будут направлять регулятору информацию обо всех подобных инцидентах. Объем и порядок предоставления такой информации будет устанавливаться ведомственными нормативными документами Банка России.

Банк России проведет масштабную проверку дистанционного банкинга. Регулятор должен будет оценить уровень безопасности платежных онлайн-сервисов. Кроме того, в перспективе будет введен определенный стандарт и сертификация интернет-банкинга на соответствие требованиям информационной безопасности [36].

До настоящего времени регулирование дистанционного банковского обслуживания госорганами не проводилось, каждый банк самостоятельно обеспечивал безопасность перевода. Однако участившиеся кибератаки вынуждают регулятор взять эту сферу под контроль, оказалось, что эффективность борьбы банков с растущим числом таких мошенничеств очень низка.

За 2016 год хакеры пытались похитить только со счетов физических лиц 1,25 млрд. рублей. Согласно статистике Банка России, удалось предотвратить хищение не более 3% средств. Чуть лучше ситуация складывается с защитой денег корпоративных клиентов банков. С начала года было зафиксировано 365 попыток несанкционированного списания средств компаний через дистанционные банковские сервисы, объем хищений составил около 1,1 млрд. рублей, банкам удалось спасти почти треть этих денег. Что касается корреспондентских счетов ЦБ, из 2,87 млрд. рублей уберечь от злоумышленников удалось чуть более половины.

Тем временем, в Центральном банке не намерены ограничиваться только проверкой дистанционного банкинга. Специальная межведомственная рабочая группа, в состав которой помимо сотрудников ЦБ входят представители Минфина, МВД России, Минкомсвязи и ФСТЭК, разрабатывает требования информационной безопасности. По итогам проверки регулятор на основе этих стандартов введет сертификацию банковских сервисов.

Более того, от степени соответствия онлайн-банкинга стандартам безопасности будут зависеть требования к достаточности капитала кредитных организаций. То есть чем больше риски в системах платежных сервисов, тем выше требования к достаточности капитала соответствующего банка, тем меньше

у него возможностей наращивать кредитование и вкладывать средства в прочие активы.

3.3 Совершенствование дистанционного банковского обслуживания

Согласно данным поступающей в Банк России отчетности по форме 0409070 «Сведения об использовании кредитной организацией интернет-технологий» около 98% всех кредитных организаций, действующих на территории Российской Федерации, предоставляют услуги ДБО. При этом активность со стороны клиентов значительно ниже, чем в Европе или США. Этому есть несколько причин:

- отсутствие доверия клиентов к технологиям ДБО в связи с ростом активности киберпреступников и недостаточной надежностью аппаратно-программного обеспечения систем ДБО (включая надежность провайдеров услуг, задействованных в информационном контуре банковской деятельности в условиях ДБО клиентов);
- недостаточное качество дистанционных банковских услуг.

Остановимся подробнее на каждой причине.

Отсутствие доверия к технологиям ДБО.

Доверие к технологиям ДБО начинается с уверенности клиентов в том, что деньги, находящиеся на их счетах, надежно защищены. Но рост числа компьютерных преступлений и высокий уровень их латентности подрывают доверие к данному виду банковского обслуживания.
При внедрении технологий ДБО риски возникают чаще всего на стороне клиента. Чтобы их минимизировать, нужны усилия как кредитных организаций, так и клиентов. Банки должны предоставить клиенту возможность применять наиболее современные и адекватные средства защиты, объяснить разницу между предлагаемыми средствами защиты и особенности их эксплуатации. Далее уровень обеспечения безопасности будет зависеть от выбора клиента.

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее — Закон № 161-ФЗ) создает реальные предпосылки для повышения доверия клиентов к технологиям ДБО. На основании п. 15 ст. 9 Закона № 161-ФЗ, если деньги клиента исчезнут со счета в банке, тот должен сначала вернуть деньги, а уже потом разбираться, куда они исчезли и кто в этом виноват. Это довольно радикальное средство вернуть доверие клиентов к услугам банка.

Заметим, что подобные меры защиты клиентов ДБО соответствуют мировой практике. При этом у банка появляется возможность в случае подозрений на мошенничество блокировать электронное средство платежа, которым пользуется клиент.

Для ухода от крайностей целесообразно правильно определить цель: не защищать клиентов от банков или, наоборот, банки от клиентов, а сделать информационное взаимодействие клиента и банка безопасным, удобным и при этом недорогим. Заметим, что, приняв Закон № 161-ФЗ, законодатель много сделал для блокирования рисков клиентов, и теперь самое время подумать о том, как уменьшить риски банков.

Суть информационного взаимодействия клиента и банка заключается в том, что клиент, используя электронное платежное поручение, поручает банку выполнить ту или иную операцию с его деньгами, находящимися на его счете. Волеизъявление клиента должно быть соответствующим образом оформлено. При использовании услуги ДБО это означает, что поручение клиента должно быть подписано электронной подписью. Электронная подпись как инструмент для обеспечения целостности электронного сообщения и подтверждения авторства может эффективно выполнять свою функцию при условии, что она вырабатывается и устанавливается в доверенной среде, в доверенном сеансе связи клиента и банка. Средство, с помощью которого ведется работа с электронной подписью, называется средством электронной подписи. Главная особенность средства электронной подписи — оно должно быть ненастраиваемым, работать «в одно касание» (one touch).

Одним из примеров «хорошей практики» решения данного вопроса можно назвать организацию обучения на сайтах кредитных организаций основам работы с различными системами ДБО, включая просмотр обучающих видеороликов и консультации специалистов.

Недостаточное качество дистанционных банковских услуг.

Качество дистанционных банковских услуг во многом зависит от удобства программного продукта. Очевидно, что восприятие розничными клиентами каналов ДБО базируется на ключевом пользовательском опыте:

- удобство и понятность интерфейса;
- наличие необходимого функционала;
- уникальные инструменты и сервисы, отличающие банк от конкурентов.

Банкам и разработчикам программных продуктов для систем ДБО необходимо уделять повышенное внимание удобству и клиентоориентированности своих разработок. Например, разрабатывать меню с изменяющимся содержанием, которое регулируется как самим банком, так и пользователем — розничным клиентом.

В основе такого меню сразу несколько идей:

- объединить наиболее востребованные конкретным пользователем функции (как избранные, так и последние использованные функции);
- мотивировать клиента к совершению дополнительных операций;
- повысить персонализированность решения для каждого клиента.

Немаловажны для клиентов «встроенное» обучение и дополнительные пояснения в пользовательском интерфейсе. Также можно расширить функционал мобильного и интернет-банка и собирать данные по востребованности функций и популярности интерфейса. Например, некоторые разработчики современных систем ДБО к мобильному банкингу добавляют программы финансового анализа (анализ финансовых операций и выдача рекомендаций), а к интернет-банкингу — интеграцию с интернет-бухгалтерией.

Согласно исследованию в 90% банков ежеквартально проводится сбор информации о качестве обслуживания и удовлетворенности клиентов. Получение

таких данных с помощью мобильного и интернет-банкинга снижает издержки на сбор информации и повышает ее качество.

Следующее поколение ДБО — это системы, которые будут способны анализировать свою популярность и помогать менеджерам банка создавать эффективные каналы дистанционного обслуживания. Это позволит каждому банку оценить востребованность собственных функций и повысить популярность в области комиссий, маркетинга и обучения клиентов финансовой грамотности, а также внедрить подход к индивидуальному ценообразованию продуктов.

Вероятнее всего, мобильный банкинг будет развиваться в части платежных возможностей, а интерфейсы сервисов будут дорабатываться, чтобы основные пользовательские задачи выполнялись проще и быстрее.

В мобильных банках для малого бизнеса будут появляться решения, которые уже используются в приложениях для частных лиц (вход по отпечатку, распознавание платежек по фото, 3D Touch). Однако существенного ускорения развития мобильного банкинга скорее всего не произойдет в силу консервативности пользователей, которые пока предпочитают интернет-банки.

Мобильные банки становятся полноценным инструментом для управления финансами, картами и банковскими продуктами. Подключить его можно будет напрямую в приложении, не используя логин и пароль интернет-банка.

Мобильный банкинг и банкинг в целом будет пытаться переместиться в более привычные для клиентов среды — чаты и мессенджеры (Telegram, Facebook, Viber и т.д.).

Традиционные платежи будут заменяться автоплатежами, когда операция на оплату или перевод средств инициируется получателем платежа, а владельцу карты остается только увидеть уведомление и одобрить операцию.

Будут развиваться приложения для умных часов, которые реализуются как дополнение к мобильному банку для смартфона или планшета.

Ключевые тенденции развития интернет-банкинга

1.Расширяются возможности перевода другому клиенту банка, наибольший прирост – у перевода по номеру мобильного телефона.

2.Расширяются возможности card2card-переводов: появляется возможность пополнения счета или карты с карты другого банка и перевод между двумя произвольными картами сторонних банков. Кроме этого, в формах card2card-переводов все чаще встречается функция автоматического определения банка по введенному номеру карты.

3.Увеличиваются возможности упрощенных платежей в бюджет: штрафы ГИБДД по УИН, задолженности судебным приставам по номеру исполнительного производства и по персональным данным, оплата налогов с запросом задолженности по ИНН.

4.Расширяются возможности упрощения оплаты коммунальных услуг с помощью форм с запросом задолженности.

5.Расширяются возможности настроек карт: подключение и отключение SMS-уведомлений о совершенных операциях по карте, настройки различных лимитов на расходные операции по карте.

6.Расширяются возможности приобретения банковских продуктов в режиме онлайн: значительно увеличилось количество интернет-банков с формой открытия накопительных счетов.

7.Упрощается оплата мобильной связи – автоматическое определение мобильного оператора по номеру телефона, наличие маски ввода номера телефона, автоплатежи для оплаты мобильной связи.

В целом все идет к тому, что для конечного клиента будет проще мигрировать из одного банка в другой — например, из неудобного в тот, где управлять счетами можно будет полностью дистанционно. Банки будут предлагать упрощенные пути перехода: в Точка Банке уже есть возможность сформировать список шаблонов платежей по выписке из старого банка.

В отличие от ДБО частных лиц, для малого бизнеса выделяется устойчивая группа банков, которые на хорошем уровне обслуживают своих клиентов полностью онлайн. Соответственно, для клиентов выбор банка для обслуживания малого бизнеса будет очевидным.

Сегодня кредитные организации привлекают клиентов на дистанционное обслуживание не только функциональностью, так как основной набор функций предлагается в своих системах большинством банков и по этому критерию сложно обойти конкурентов.

Системы ДБО нового поколения стремятся к уходу от жесткой привязки к остальным IT-компонентам, что позволяет подключать новый сервис в течение короткого периода времени (в среднем два дня) и ускоряет процесс вывода новых банковских продуктов на рынок. Еще одним очень важным направлением совершенствования дистанционного банковского обслуживания является обеспечение интеграции интернет-банка со сторонними поставщиками и операторами услуг.

Заключение

Усиление конкурентной борьбы на финансовом рынке формируют предпосылки для постановки перед банками стратегической задачи по активному наращиванию темпов роста объема бизнеса и диверсификации направлений деятельности в системах дистанционного обслуживания клиентов.

Значительный потенциал для роста функционала ДБО заключен не только в формировании персонифицированных предложений для клиентов, но и в онлайн-одобрении и оформлении кредитов, дистанционном открытии и закрытии вкладов, расчетных счетов и проведении операций по ним.

Большинство российских банков сейчас предлагает клиентам классический набор дистанционных банковских услуг: систему «Банк — Клиент», интернет - и мобильный банкинг, смс-информирование, операции через колл-центр и т. д.

Выделяется группа банков, которые ориентированы на дистанционное обслуживание клиентов, причем это не только Тинькофф Банк и Точка, которые работают в формате безофисного обслуживания, но и крупные федеральные банки — Альфа-Банк и Промсвязьбанк.

Эти банки одинаково активно развивают и интернет- и мобильные банки для бизнеса. Однако большинство банков отдает предпочтение какому-то одному каналу ДБО (например, ВТБ24 интернет-банку, МДМ-Банк мобильному банку)

Согласно исследованию в 90% банков ежеквартально проводится сбор информации о качестве обслуживания и удовлетворенности клиентов. Получение таких данных с помощью мобильного и интернет-банкинга снижает издержки на сбор информации и повышает ее качество.

За прошедший год аудитория мобильного банкинга для частных лиц выросла на 2% или 1 млн. пользователей; 33% или 18 млн. российских интернет-пользователей в возрасте от 18 до 64 лет пользуются мобильными банками для частных лиц. 89% пользователей мобильного банка пользуются и интернет-банком тоже, причем 17% из них пользуются мобильным банком чаще, чем интернет-банком.

В интернет-банках появляются инструменты аналитики для малого бизнеса: диаграммы, графики по движению средств (поступления, списания), контрагентам, статистика по эквайрингу вплоть до диаграмм по конверсии. При этом можно выделить 3 уровня аналитики: макроуровень – все движения по счету, средний уровень — доли контрагентов в общем объеме операций и микроуровень – динамика операций по конкретному контрагенту.

Упрощаются формы платежных поручений. Например, поля для бюджетных платежей скрываются во вкладки, появляются подсказки по заполнению форм и возможность настроить уведомления для получателя платежа на почту и телефон. Также интернет-банки учатся распознавать квитанции и платежные поручения, переводя изображение в текст, и сами подставляют полученные данные в поля форм.

Следующее поколение ДБО — это системы, которые будут способны анализировать свою популярность и помогать менеджерам банка создавать эффективные каналы дистанционного обслуживания. Это позволит каждому банку оценить востребованность собственных функций и повысить популярность в области комиссий, маркетинга и обучения клиентов финансовой грамотности, а также внедрить подход к индивидуальному ценообразованию продуктов.

Вероятнее всего, мобильный банкинг будет развиваться в части платежных возможностей, а интерфейсы сервисов будут дорабатываться, чтобы основные пользовательские задачи выполнялись проще и быстрее.

В мобильных банках для малого бизнеса будут появляться решения, которые уже используются в приложениях для частных лиц (вход по отпечатку, распознавание платежек по фото, 3D Touch). Однако существенного ускорения развития мобильного банкинга скорее всего не произойдет в силу консервативности пользователей, которые пока предпочитают интернет-банки.

Мобильные банки становятся полноценным инструментом для управления финансами, картами и банковскими продуктами. Подключить его можно будет напрямую в приложении, не используя логин и пароль интернет-банка.

Мобильный банкинг и банкинг в целом будет пытаться переместиться в более привычные для клиентов среды — чаты и мессенджеры (Telegram, Facebook, Viber и т.д.).

Традиционные платежи будут заменяться автоплатежами, когда операция на оплату или перевод средств инициируется получателем платежа, а владельцу карты остается только увидеть уведомление и одобрить операцию.

Будут развиваться приложения для умных часов, которые реализуются как дополнение к мобильному банку для смартфона или планшета.

В целом все идет к тому, что для конечного клиента будет проще мигрировать из одного банка в другой — например, из неудобного в тот, где управлять счетами можно будет полностью дистанционно. Банки будут предлагать упрощенные пути перехода: в Точка Банке уже есть возможность сформировать список шаблонов платежей по выписке из старого банка.

В отличие от ДБО частных лиц, для малого бизнеса выделяется устойчивая группа банков, которые на хорошем уровне обслуживают своих клиентов полностью онлайн. Соответственно, для клиентов выбор банка для обслуживания малого бизнеса будет очевидным.

Сегодня кредитные организации привлекают клиентов на дистанционное обслуживание не только функциональностью, так как основной набор функций предлагается в своих системах большинством банков и по этому критерию сложно обойти конкурентов.

Системы ДБО нового поколения стремятся к уходу от жесткой привязки к остальным IT-компонентам, что позволяет подключать новый сервис в течение короткого периода времени (в среднем два дня) и ускоряет процесс вывода новых банковских продуктов на рынок. Еще одним очень важным направлением совершенствования дистанционного банковского обслуживания является обеспечение интеграции интернет-банка со сторонними поставщиками и операторами услуг.

Список литературы

1. Гражданский Кодекс РФ, 1 и 2 часть, от 26.01.1996 №14-ФЗ (с изменениями и дополнениями)
2. Федеральный закон от 2 декабря 1990 г. N 395-I «О банках и банковской деятельности» (с изменениями и дополнениями)
3. Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (с изменениями и дополнениями)
4. Федеральный закон от 27.06.2011 N 161-ФЗ "О национальной платежной системе" (с изменениями и дополнениями)
5. Федеральный закон от 20 февраля 1995г. №24-ФЗ «Об информации, информатизации и защите информации» (с изменениями и дополнениями)
6. Федеральный закон от10 января 2002г. №1-ФЗ «Об электронной цифровой подписи» (с изменениями и дополнениями)
7. Указание ЦБ РФ от 01.03.2004 «О порядке информирования кредитными организациями ЦБ РФ об использовании в своей деятельности Интернет-технологий»
8. Письмо ЦБ России от 31.03.2008 №36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга»
9. Амельчиц, А. Г. Виды дистанционного банковского обслуживания клиентов посредством интернета / А. Г. Амельчиц, Е. А. Мурзо, Е. С. Харитончик // Информационные системы и технологии: управление и безопасность. - 2013
10. Банковское дело: учебник / О.И. Лаврушин, Н.И. Валенцева; под ред. О.И. Лаврушина. – 10-е изд., перераб. и доп. – М: КНОРУС, 2013
11. Баранов, А. М. Недостатки и преимущества систем дистанционного банковского обслуживания / А. М. Баранов, Н. В. Коротаева // Социально-экономические явления и процессы. – 2013

12. Баранов А.В. Дистанционное банковское обслуживание коммерческих банков как основное направление развития России на современном этапе // Экономика и управление в XXI веке: тенденции развития. 2016
13. Дворецкая, А. Е. Деньги, кредит, банки: учебник для академического бакалавриата. – УМО. – М.: Юрайт, 2014
14. Евдокимова, С. С. Системы удаленного банковского обслуживания как инструмент многоформатного взаимодействия с клиентом / С. С. Евдокимова // Финансы и кредит. – 2013
15. Инструментарий и методы анализа систем дистанционного банковского обслуживания / Д. Г. Ловянников, Н. С. Ловянникова. – Ставрополь: Фабула, 2014
16. Интернет-технологии в банковском бизнесе: перспективы и риски: учеб.-практ. пособие / Ю. Н. Юденков [и др.]. – 2-е изд. стереотип. – М.: КНОРУС, 2015
17. Ишкова, С. В. Тенденции развития дистанционного банковского обслуживания в России / С. В. Ишкова, В. А. Якушина // Наука и современность. – 2013
18. Кабакова, Е. В. Дистанционное банковское обслуживание: проблемы и перспективы развития / Е. В. Кабакова // Формирование общекультурных и профессиональных компетенций финансиста: сборник научных трудов студентов, аспирантов и преподавателей Финансового университета при Правительстве Российской Федерации / Редакционная коллегия: А.Н. Лебедев, Н.В. Анненкова ,Е.В. Камнева, Ю.Е. Мужичкова. Москва, 2014
19. Каджаева М.Р. Банковские операции. - М.: Издательский центр «Академия», 2014
20. Киреев В.Л. Банковское дело. – М.: МИИТ, 2014
21. Костерина Т.М. Банковское дело: Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2014

22. Направления модернизации услуги интернет-банкинга в системе розничного дистанционного банковского обслуживания в России / А. Н. Хоминок. – Смоленск: Маджента, 2013
23. Ольхова, Р.Г. Банковское дело: управление в современном банке: учебное пособие / Р. Г. Ольхова. – УМО. – М.: КНОРУС, 2015
24. Организация выявления, раскрытия и расследования хищений денежных средств в системе дистанционного банковского обслуживания: учебно-практическое пособие / А. В. Шмонин, В. В. Баранов. – Москва: Академия управления МВД России, 2014
25. Павлович А.А., Достов В.Л. Электронные платежи: специфика, регулирование, технологии. – М.: Москва, 2013
26. Самочетова Н.В., Мартыненко Н.Н. Дистанционное банковское обслуживание в России и риски на пути его развития // Современная наука: актуальные проблемы теории и практики. Серия: Познание. 2016. № 5-6
27. Сиротский А.А. Анализ типовых угроз информационной безопасности автомати- зированных систем применительно к дистанционному банковскому обслуживанию. В сборнике: Информационная безопасность бизнеса и общества. Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности. Российский государственный социальный университет. М., 2016.
28. Тосунян Г.А., Викулин А.Ю., Экмалян А.М. Банковское право Российской Федерации. Общая часть: учебник/под общ. ред. Б.Н. Топорнина. М.: Юристъ, 2014
29. Финансовый мониторинг в условиях интернет-платежей / П. В. Ревенков. – Москва: ЦИПСИР: КноРус, 2016
30. Электронные платежи: специфика, регулирование, технологии: практическое пособие / А. П. Александрович, Н. К. Борисова, Д. В. Громов – Москва: Регламент-Медиа, 2013

31. Электронные деньги в коммерческом банке: практическое пособие / А. В. Пухов, А. Ю. Мацкевич, А. В. Рего, П. В. Ушанов. - Москва : КноРус: ЦИПСИР, 2015
32. Косарев В.Е. Виртуальный банк в соцсетях и реальные риски//Банковское дело. – 2014. – № 3
33. Центр исследований платежных систем и расчетов. Мошенничество в платежной сфере: Бизнес-энциклопедия. — М.: Интеллектуальная Литература, 2016
34. Тенденции развития Интернет-аудитории в России // Исследовательская компания «GFK» // URL: http://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-tendenciirazvitija-internet-auditorii-v-rossii/(дата обращения 25.04.2017)
35. «Статистический бюллетень Банка России» №1,2017, http://cbr.ru/
36. Официальный сайт Центрального Банка России – http://www.cbr.ru. (дата обращения: 12.04.2017)
37. Официальный сайт Ассоциации российских банков – http://arb.ru. (дата обращения: 10.05.2017)
38. Аналитическое агентство Markswebb rank report – http://markswebb.ru/e-finance/internet-banking-rank-2016/, Internet Banking Rank 2016
39. Справочно - правовая система КонсультантПлюс. – http://www.consultant.ru
40. Справочно - правовая система Гарант. – http://www.garant.ru