1. Банковский бизнес – будущее за дистанционным банковским обслуживанием (ДБО) и мобильным банкингом.

Шабалина Арина Александровна

9 класс

МБОУ Лицей №60

Республика Башкортостан, г.Уфа

Выбранная мной тема актуальна и важна из-за популярности дистанционного банковского обслуживания, и его известность со временем только растет. Одна из причин - это удобство для клиентов и выгода для банков. Интерес к этому вопросу в настоящее время велик, поэтому нельзя не рассмотреть и наличие рисков, возникающих при работе с ним. Попробую рассмотреть все плюсы и минусы ДБО и объяснить, почему оно будет только набирать обороты. Для начала разберусь, что это такое.

Дистанционное банковское обслуживание (ДБО) — общий термин для технологий предоставления [банковских услуг](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2%D1%81%D0%BA%D0%B8%D0%B5_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8) на основании распоряжений, передаваемых клиентом удаленным образом, чаще всего с использованием [компьютерных](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) и [телефонных](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) сетей.

Мобильный банкинг - управление банковским счетом с помощью планшетного компьютера, смартфона или обычного телефона. Это один из видов ДБО.

Можно выделить несколько видов ДБО по типу используемых информационных систем:

**Системы «Клиент-Банк»**

Это системы, доступ к которым осуществляется через персональный компьютер. Системы «Клиент-Банк» позволяют отправлять платежи в банк и получать выписки по счетам из банка. Банк при этом предоставляет клиенту: техническую и методическую поддержку при установке системы, начальное обучение персонала клиента, обновление программного обеспечения и сопровождение в процессе дальнейшей работы. Системы «Клиент-Банк» обеспечивают ведение рублёвых и валютных счетов с удалённого рабочего места. Но не все банки обеспечивают клиентам полное ведение своих счетов, [отклоняясь от мировых стандартов](https://ru.wikipedia.org/wiki/%D0%A1%D0%B1%D0%B5%D1%80%D0%B1%D0%B0%D0%BD%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8). В целях безопасности в системах «Клиент-Банк» используются различные системы криптографической защиты информации (СКЗИ), обеспечивающие шифрование и контроль целостности передаваемой в Банк информации. Системы «Клиент-Банк» принципиально подразделяются на 2 типа: [толстый клиент](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D0%BB%D1%81%D1%82%D1%8B%D0%B9_%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82) и [тонкий клиент](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D0%BD%D0%BA%D0%B8%D0%B9_%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82).

**Банк-Клиент (толстый клиент)**

На рабочей станции пользователя устанавливается отдельная программа-клиент. Программа-клиент хранит на компьютере все свои данные, как правило, это платёжные документы и выписки по счетам. Программа-клиент может соединяться с банком по различным каналам связи. Наиболее часто для соединения с банком используется прямое соединение через модем или через интернет. Преимущество систем «Банк-клиент» заключается в том, что клиенту для непосредственной работы с клиентской частью системы не требуется постоянное подключение к банковской части системы ДБО. Также преимуществом некоторого вида систем «толстых клиентов» является их богатый внутренний функционал по разделению ролей пользователей и разбору инцидентов. В частности это актуально для юридических лиц. Базы данных толстого клиента, как правило, могут устанавливаться на полноценную [систему управления базами данных (СУБД)](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B1%D0%B0%D0%B7%D0%B0%D0%BC%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85), что для организаций с большим документооборотом даёт возможность обеспечить удобное резервирование базы данных, а также полноценную работу с сетевой версией без потери скорости обработки документов.

Для толстого клиента необходима электронная цифровая подпись (ЭЦП), применяемая для подписи электронных документов.

Электронную цифровую подпись можно разделить на три составляющие: открытый ключ, закрытый ключ и сертификат.

Сертификат содержит сведения о владельце ЭЦП и может включать в себя не только персональные данные, но и реквизиты компании, то есть служить аналогом печати.

С помощью закрытого ключа осуществляется формирование подписи электронного документа. Открытый ключ служит для верификации подписи. Он виден всем участникам системы электронного документооборота.

Закрытый ключ используется для генерации самой подписи и хранится, как правило, на смарт-карте (карте со встроенным чипом) или флешке – брелке [eToken](http://www.banki.ru/wikibank/eToken/).

Для генерации ЭЦП необходимо установить на компьютер специальную сертифицированную программу-криптопровайдер (CryptoPro, Lissi и т. п.).

Для примера приведу работу в системе Банк-Клиент общества с ограниченной ответственностью «Бизнес Системы». Чтобы отправить платежи поставщикам услуг, бухгалтер, прямо в свой компьютер, на котором установлена программа Банк-Клиент, вставляет флешку eToken (закрытый электронный ключ) и с помощью паролей заходит в систему Банк-Клиент. Формирует в электронном банке платежные поручения, подписывает их ЭЦП и отправляет в банк. В качестве дополнительной защиты бухгалтер получает пароль через СМС и вводит его для подтверждения платежа. После этого денежные средства списываются со счета ООО «Бизнес системы» на счет поставщика указанного в платежном поручении. Спустя некоторое время через систему Банк-Клиент приходит подтвержденное платежное поручение. Все действия: приход и расход денежных средств, выписка со счета, заявка на получение наличности, справки и т.д. отражаются в системе.

Оплатой за использование системы Банк-Клиент будут банковские расходы по договору банковского обслуживания, то есть все возможные тарифы банка. Например, комиссия за проведение платежного поручения, за ведение счета, за прием и снятие наличности и т.д.

**Интернет-Клиент (тонкий клиент)**

Пользователь входит в систему через Интернет браузер. Система Интернет-Клиент размещается на веб-сервере банка. Все данные доступны на [веб-сайте](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B0%D0%B9%D1%82) банка. По технологии Интернет-Клиент строится также мобильный сайт банка. На основе Интернет-Клиента могут предоставляться информационные сервисы с ограниченным набором функций.

Чтобы работать в системе Интернет-Клиента необходимо обязательно зайти на сайт банка в Интернет Банкинг. Установка специальной программы не требуется.

**Системы «Телефон-Банк»**

Как правило, системы Телефон-Банк имеют ограниченный набор функций по сравнению с системами «Клиент-Банк». Все функции становятся доступными только после персональной идентификации клиента банком на основе системы персональной идентификации. Работа осуществляется с помощью логина и пароля, который выдается при регистрации или приходит по СМС. Эта система является разновидностью мобильного банка.

В качестве примера могу привести систему Сбербанк Онлайн, которая успешно зарекомендовала себя. Для работы необходимо физическому лицу открыть карту и зарегистрироваться в системе, получить постоянные пароли для подтверждения операций. С помощью Системы Сбербанк Онлайн можно оплачивать платежи, в том числе коммунальные, штрафы, переводить денежные средства на лицевые счета других клиентов этой же системы и других систем, между своими лицевыми счетами, погашать кредиты и т.д. Подтверждение платежей происходит паролем, присланным банком по СМС. Переводы другим клиентам системы Сбербанк Онлайн осуществляются даже по номеру мобильного телефона, на который зарегистрирована карта Сбербанка клиента. Денежные средства списываются в режиме реального времени. И мгновенно попадают на карту клиента, указанного в платеже. Все платежи, совершаемые в регионе, в котором была открыта карта, совершаются без комиссии, за остальные списывается 1% от перечисляемой суммы.

Но у этой системы существует и один большой недостаток – вирусы, с помощью которых считывается информация о счетах и паролях. Если компьютеры защищены наиболее надежными антивирусами, то мобильные системы отстают от этого.

**Обслуживание с использованием банкоматов и**

**устройств банковского самообслуживания**

Технологии дистанционного банковского обслуживания с использованием устройств банковского самообслуживания являются одними из наиболее популярных в мире и в России. Банкоматы и терминалы попадают в категорию ДБО, так как почти полностью предоставляют банковские услуги дистанционно. Примером использования таких технологий может служить установка вышеуказанных устройств в любом крупном торговом центре или в маленьком салоне на остановочном пункте.

**Мобильный банк будущего**

Думаю, что роль пластиковых банковских карт со временем будет снижаться*.* Их заменит [технология беспроводного обмена](http://mobilebanking-sberbank.ru/blog/nfc_ili_near_field_communication_koshelek_v_mobilnom/2012-05-29-34) между устройствами, находящимися на небольшом расстоянии друг от друга, – **Near Field Communication** (NFC), в переводе с английского – «коммуникация с близкого расстояния».

Функционирует она благодаря микрочипу, который встраивается в мобильный телефон. Устройство взаимодействует с банкоматом, торговым терминалом, мобильным телефоном, в которых тоже используется NFC.

Такое мобильное устройство – это **платежная карта с расширенными возможностями**. В нем есть интерфейс пользователя, где владелец мобильного аппарата может подтвердить или отклонить оплату, ввести необходимые банковские данные для осуществления транзакции, проконтролировать историю платежей.

Например, выяснится, что женщина постоянно покупает корм для питомца одной марки. Телефонный оператор узнает ее местоположение благодаря мобильному телефону. И когда пользовательница проходит мимо зоомагазина, то ее сразу оповещают по SMS, что корм привычной марки есть в продаже со скидкой 30%. Женщина заходит в магазин, прикладывает телефон к считывающему устройству, получает скидку и платит за товар.

**Преимущества и недостатки дистанционного банковского обслуживания через интернет**

К преимуществам можно отнести невысокую стоимость эксплуатации интернет-системы, возможность интеграции с бухгалтерскими системами клиента, доступность интернет-услуг для конечного пользователя, поддержание лояльности клиентов, активно использующих данные услуги. ДБО выгодно для банков из-за сокращения затрат на содержание помещений, на наем работников, их обучение. Но оно требует затрат на внедрение систем, которые могут себе позволить только банки, рассчитывающие на будущую прибыль. Также только крупные банки могут обеспечить безопасность в сети интернет при использовании систем Интернет-клиент. Для удобства пользователей постоянно улучшается и упрощается интерфейс системы удаленного обслуживания, добавляются шаблоны для каждого вида платежа.

К недостаткам относится слабая защищённость интернета от несанкционированного доступа. Несмотря на стремление разработчиков создавать и совершенствовать систему защиты, многочисленные опасности продолжают появляться. Поддержание уровня защиты требует значительных материальных затрат, которые могут себе позволить в основном крупные банки, рассчитывающие на значительные доходы от предоставления подобных услуг. Использование ДБО всегда сопровождается рисками. Увеличивается количество преступлений, направленных на то, чтобы получить доступ к деньгам удаленно, оставив меньше следов. Информация о пользователях, операциях и счетах, которая идет через отдельные процессинговые центры, становится более доступной. Законодательно она не попадает под термин банковская тайна, а относится к коммерческой тайне, и ответственность за ее разглашение уже менее строгая.

Конечно, банки в качестве мотивации клиентов для обслуживания с помощью ДБО предлагают всевозможные виды страхования, которые являются не только дополнительными расходами, но и защитой для клиента.

При использовании ДБО нужно быть крайне внимательными и аккуратными, следить за безопасностью устройств, с помощью которых осуществляется вход в сеть интернет. В том числе устанавливать надежные программы, защищающие от вирусов.

Все технологии, применяемые в новейших системах мобильного банка, обязательно должны обладать высокой стабильностью, уровнем [безопасности](http://mobilebanking-sberbank.ru/blog/obespechit_bezopasnost_platezhej/2015-02-16-272), доступностью, удобством в применении. Все зависит от задач, которые необходимо решать. Зависимо от этого, должен избираться банковский продукт, партнер, осуществляющий внедрение либо же поставщик. Наиболее оптимальным подходом задач по безопасности будет выбор зарекомендовавших себя методов, проверенных временем. В задачах, касающихся коммуникаций, приоритетами должны выступать стабильность и надежность самой связи.

**Вывод**

Условия дистанционного обслуживания для клиента удобны тем, что экономят его время, так как для совершения операций не нужно тратить время на дорогу и очереди. Клиент может воспользоваться многими из банковских услуг в любом месте, без лишних финансовых и временных затрат. В связи с этим, банки активно развивают свои мобильные приложения. Внедрение дистанционного обслуживания помогает банку работать эффективнее и расширять свою деятельность за счет продажи банковских продуктов и привлечения новых клиентов.

Я соглашусь с мнением специалистов, что в борьбе за клиента банкам придется персонализировать систему ДБО. Современный человек ставит во главу удовлетворение своих потребностей и учится беречь свое время. Банкам нужно это учитывать.

Для совершения дистанционных банковских операций лично я выбрала бы самый простой и удобный интерфейс, и предпочтение бы отдала надежности и стабильности банка, предоставляющего такие услуги.

Участившиеся случаи мошенничества с использованием ДБО позволяют предполагать, что одним из направлений развития этих систем будет совершенствования средств их же безопасности.

В ближайшее время будет активно развиваться технология биометрической идентификации клиента — это считывание радужки глаз, рисунок вен, геометрия лица, голосовая идентификация. Сейчас все банки интересуются этим направлением. Мне бы хотелось, чтобы биометрия стала доступной во всех каналах банковского обслуживания, где требуется идентификация клиента.

Кроме того, есть надежда, что в скором времени все дисконтные и бонусные карты можно будет оцифровать и, расплачиваясь в магазинах, использовать только смартфон. Я уверена, что в будущем технология NFC обретет немалую популярность.

В своей работе я не рассмотрела важный аспект дистанционного банковского обслуживания - его стоимость. Это очень интересная и обширная тема, требующая тщательного анализа, и которую я не смогу уместить в рамках этого эссе.

Я думаю, наше представление о том, какими должны быть платежные технологии, изменится в самое ближайшее время. Будущее – это эксперименты, разработки и новые технологии.

**Список литературы:**

* https://ru.wikipedia.org
* http://www.banki.ru
* <http://www.bankdbo.ru>
* <http://www.mobilebanking-sberbank.ru>
* <http://www.ttfinance.ru>
* <http://euroasia-science.ru>
* Рекламные буклеты ПАО «Сбербанк»
* Рекламные буклеты АО «АБ «РОССИЯ»
* Рекламные буклеты АО «Газпромбанк»