**ДИПЛОМНАЯ РАБОТА**

**на тему**

**"ОРГАНИЗАЦИЯ И ПЕРСПЕКТИВЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ЮРИДИЧЕСКИХ ЛИЦ (НА ПРИМЕРЕ РОССИЙСКОГО БАНКА"**

Содержание

Введение

[Глава 1. Современные информационные технологии в сфере дистанционного банковского обслуживания](#_Toc295058176)

1.1 Понятие, сущность и основные характеристики дистанционного банковского обслуживания

[1.2 Нормативная база и основные риски дистанционного банковского обслуживания](#_Toc295058178)

1.3 Анализ тенденций развития банковских услуг по дистанционному обслуживанию в России

[Глава 2. Современные системы дистанционного банковского обслуживания юридических лиц](#_Toc295058180)

2.1 Особенности использования системы "Банк-Клиент"

[2.2 Система "Интернет-Клиент" как наиболее оптимальная форма дистанционного банковского обслуживания юридических лиц](#_Toc295058182)

2.3 Преимущества и недостатки системы "Телефон-Банк"

[Глава 3. Направления совершенствования дистанционного банковского обслуживания на примере "Тусарбанк" ЗАО](#_Toc295058184)

3.1 Автоматизированная система "Интернет-Банк"

[3.2 Перспективы развития дистанционного банковского обслуживания на примере ТУСАРБАНК ЗАО](#_Toc295058186)

Заключение

[Библиографический список](#_Toc295058188)

# Введение

В начале 21 века российские банки показывают стабильный рост доходов, клиентуры, конкуренции и разнообразия оказываемых услуг. Это связано с ростом экономики России в целом - в основном по причине интенсивных экспортных операций.

Повышенная конкуренция и потенциально высокие доходы - это достаточные причины для дальнейшего распространения в регионы в виде создания множества филиалов и отделений. С развитием технических достижений и технологий конкуренция в банковской среде приобретает специфический оттенок: создаются новые рыночные ниши и новые способы воздействия на целевую аудиторию; те банки, которые смогут первыми занять эти ниши или создать новые, имеют большие шансы на успех.

Целью исследования в дипломной работе является выявление особенностей и перспектив дистанционного обслуживания юридических лиц, разработка предложений по развитию и совершенствованию каналов удаленного доступа к банковским услугам в российских условиях.

Достижению поставленных целей способствует решение следующих задач:

* исследовать современное понятие и сущность дистанционного банковского обслуживания юридических лиц;
* обобщить и систематизировать опыт оказания удаленных услуг организациям за рубежом и в России;
* раскрыть существующие каналы удаленного доступа к банковским услугам и их особенности;
* выявить особенности правового регулирования данного сегмента банковской деятельности;
* проанализировать преимущества, выявить тенденции и особенности, оценить перспективы развития дистанционного банковского обслуживания в современной России.

Предметом исследования дипломной работы являются различные формы дистанционного банковского обслуживания, предлагаемые банками клиентам - юридическим лицам.

Объектом исследования выступают российские и иные банковские кредитные организации, которые предоставляют организациям дистанционное управление их собственными счетами в режиме реального времени.

Дипломная работа выполнена при исследовании теоретических и практических разработок отечественных экономистов, изучении законодательных актов Российской Федерации и программ дистанционного обслуживания российских банков.

# Глава 1. Современные информационные технологии в сфере дистанционного банковского обслуживания

# 1.1 Понятие, сущность и основные характеристики дистанционного банковского обслуживания

В условиях обострения конкуренции между крупнейшими участниками рынка корпоративных финансовых услуг необходимо применять новые способы формирования конкурентных преимуществ и повышения эффективности деятельности банка.

Одним из важных факторов успеха российских банков в стратегическом периоде является их способность управлять издержками и возможность снижать их за счет внедрения новых технологий и методов обслуживания клиентов. Наиболее эффективными технологиями, которыми могут воспользоваться банки в конкурентной борьбе, являются внедрение различных форм дистанционного обслуживания юридических лиц (ДБО).

ДБО позволяет кредитным организациям, используя различные каналы взаимодействия с клиентами, предоставлять им не только традиционные банковские услуги, реализуемые в любом отделении банка, но и новые продукты, которые дают возможность на совершенно ином уровне качества удовлетворять потребности клиентов.

Понятие "дистанционное банковское обслуживание" несколько шире и включает в себя обслуживание как населения, так и юридических лиц, причем не только "на дому", но и в любом удаленном от банковского офиса месте, где имеется соответствующий канал связи.

В основе ДБО лежит принцип обмена информацией между банком и клиентом с обеспечением должного уровня безопасности и конфиденциальности. Клиентам предоставляется возможность получать информацию о состоянии своих счетов и управлять ими, не прибегая к традиционным визитам в банк, а используя имеющиеся у них под рукой средства телекоммуникации. В наш век бурного развития информационных технологий, глобализации рынков и повышенной тяги потребителей к комфорту предоставление банком своим клиентам таких услуг становится непременным условием сохранения конкурентоспособности банка.

С понятием "дистанционное банковское обслуживание" тесно связаны также термины "е-bank" (электронный банк) и "виртуальный банк". Под электронным, или виртуальным, банком обычно понимают банк, не имеющий традиционного офиса, а обслуживающий клиентов посредством телефона, Интернета и, при необходимости, почты. Если услуги по дистанционному совершению определенных банковских операций может предоставлять любой банк наряду с традиционным обслуживанием клиентов в своих офисах, то виртуальный банк, как правило, специализируется именно на обслуживании удаленных клиентов, не тратя деньги на строительство и содержание клиентских помещений.

При этом виртуальный банк предоставляет своим клиентам практически полный набор услуг, оказываемых обычными универсальными банками. Единственный вид услуг, которые не могут самостоятельно оказываться виртуальным банком - это кассовое обслуживание. Для выдачи наличных своим клиентам виртуальные банки используют сеть банкоматов и терминалов, принадлежащих другим банкам или, например, банковскому консорциуму, в который входит данный виртуальный банк. В услугах по сдаче наличных клиенты виртуальных банков обычно не нуждаются, а при необходимости используют для зачисления наличных на свои банковские счета другие банки, имеющие широкую сеть отделений.

Широкое внедрение систем ДБО началось за рубежом уже с начала 80-х годов, а в отдельных банках и еще ранее. Эволюция систем ДБО основывалась на развитии средств телекоммуникации и банковских компьютерных технологий. Вначале возникли системы предоставления банковских услуг по телефону и по модему, а в настоящее время наблюдается бум в развитии систем банковского обслуживания через Интернет. К модификациям ДБО можно отнести предоставление банковских услуг с использованием телефаксов, пейджеров, сотовых телефонов и видеотелефонов. За рубежом уже имеются системы банковского обслуживания посредством интерактивного телевидения. А корпорацией "Citi Corp" разработан домашний банковский терминал, оказывающий широкий спектр банковских услуг, в том числе выдачу кредитов. Он напоминает большой телефонный аппарат с экраном и клавиатурой и способен заменить персональный компьютер.

Первые дистанционные банки появились в Великобритании. В 1989 г. Midland Bank учредил First Direct, который начал осуществлять текущие банковские операции в режиме дистанционного банка. В настоящее время First Direct является бесспорным лидером на рынке дистанционных банковских услуг в Европе, обслуживая свыше 500 тыс. клиентов.

Во всех западных странах универсальные банки развивают дистанционные системы обслуживания. Так, во Франции первым дистанционным банком стал созданный в 1987 г. банк Cortal. В 1994 г. группа Paribas учредила дистанционный банк Banque Directe по образцу First Direct. Позднее появилось еще несколько дистанционных банков - Credit du Nord, Cetelem, UCB, Cardif и др. Но все же во Франции система дистанционных банков менее развита, чем в Великобритании. Так, ведущий французский дистанционный банк Cortal имеет всего 25 тыс. клиентов.

В США в настоящее время зарегистрировано около 100 Интернет-банков, занимающихся исключительно дистанционным обслуживанием. Большинство виртуальных банков довольно мелкие и уступают крупным банкам по масштабам как обычного, так и электронного банковского бизнеса. Основной движущей силой развития виртуальных банков является значительное снижение себестоимости банковских услуг. По оценкам экспертов, в США себестоимость операции по обработке одного чека снижается с 2 долл. при приеме через кассу банка до 0,7 долл. при передаче данных по закрытой сети, до 0,2 долл. при использовании телефона и до 0,05 долл. при осуществлении данной операции через Интернет.

В нашей стране настоящих виртуальных банков пока нет, хотя такие проекты существуют. Среди систем ДБО наибольшее распространение в России получили системы с использованием компьютера, модема и телефонной линии, известные как системы "клиент - банк". Подобный сервис предоставляют своим клиентам - юридическим лицам практически все российские коммерческие банки, за исключением ряда мелких провинциальных банков.

В последние годы ведущие столичные и наиболее крупные региональные банки внедряют также системы телефонного банкинга, Интернет-банкинга и пейджер-банкинга, начинают внедряться системы home banking для населения. Далее рассмотрим подробнее различные формы дистанционного банковского обслуживания, применяемые российскими банками.

Дистанционное банковское обслуживание (ДБО) - общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (то есть без его визита в банк), чаще всего с использованием [компьютерных](http://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 сетей. Для описания технологий ДБО используются различные в ряде случаев пересекающиеся по значению термины: Клиент-Банк, Банк-Клиент, Интернет-Банк, Система ДБО, Электронный банк, Интернет-Банкинг, on-line banking, remote banking, direct banking, home banking, internet banking, PC banking, phone banking, mobile-banking, WAP-banking, SMS-banking, GSM-banking, TV-banking.

Рассмотрим понятия Клиент-Банк, Банк-Клиент, Интернет-Банк, Система ДБО, Электронный банк, Интернет-Банкинг, on-line banking, remote banking, direct banking, home banking, internet banking, PC banking, phone banking, mobile-banking, WAP-banking, SMS-banking, GSM-banking, TV-banking с точки зрения общепринятого понимания:

"Банк-клиент" - общее название [программного обеспечения](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5), организующего удалённое банковское обслуживание и автоматизирующее документооборот между банками и их клиентами. Иначе говоря, банк-клиент обеспечивает клиенту удалённое управление (без личного визита в банк) своим расчётным счетом, например, включает в себя возможность отправления платежей и просмотр выписок по счету. К этому определению обычно относят также direct banking, home banking, Электронный банк. На самом деле это понятие несколько сложнее, далее оно будет изложено в более грамотной трактовке, которая используется специалистами, задействованными в процессе создания, установки и настройки систем дистанционного банковского обслуживания.

"Интернет-Клиент для юридических лиц" - это система, которая позволяет клиентам банка дистанционно осуществлять все виды платежных операций по своему счету, а также оперативно получать информацию, необходимую для взаимодействия с банком. Работать с системой можно из любой точки мира - достаточно иметь лишь доступ в Интернет. Очень часто понятия "Банк-Клиент", "Клиент-банк" и "Интернет-Клиент" воспринимаются населением как идентичные, содержащие одну и ту же смысловую нагрузку.

"Телефонный банкинг" - банковский сервис, основанный на использовании возможностей телефонов с тональным набором номера для получения интересующей информации и осуществления желаемых операций.

Далее рассмотрим эти понятия с точки зрения специалистов, занимающихся настройкой и сопровождением систем дистанционного банковского обслуживания.

Системы "Клиент-Банк" (PC-banking, remote banking, direct banking, home banking) - системы, доступ к которым осуществляется через персональный компьютер. Банк при этом предоставляет клиенту техническую и методическую поддержку при установке системы, начальное обучение персонала клиента, обновление программного обеспечения и сопровождение клиента в процессе дальнейшей работы. Системы "Клиент-Банк" обеспечивают полноценное расчетное и депозитарное обслуживание и ведение рублёвых и валютных счетов с удалённого рабочего места.

Системы "Клиент-Банк" позволяют создавать и отправлять в банк платёжные документы любых типов, а также получать из банка выписки по счетам (информацию о движениях на счёте). В целях безопасности в системах "Клиент-Банк" используются различные системы шифрования. Использование систем "Клиент-Банк" для обслуживания юридических лиц до сих пор является одной из наиболее популярных технологий ДБО в России. Системы "Клиент-Банк" принципиально подразделяются на 2 типа (толстый клиент и тонкий клиент):

Системы "Банк-клиент" ("толстый клиент",PC-banking, remote banking, direct banking, home banking) - классический тип системы Банк-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 Dial-Up соединение через модем или прямое соединение с Интернетом.

Интернет-Клиент (тонкий клиент) (On-line banking, Интернет-банкинг (Internet banking), WEB-banking) - пользователь входит в систему через Интернет браузер. Система Интернет-Клиент размещается на сайте банка. Все данные пользователя (платёжные документы и выписки по счетам) хранятся на сайте банка. По технологии Интернет-Клиент строятся также системы для мобильных устройств - [PDA](http://ru.wikipedia.org/wiki/PDA), смартфоны (Мобильный банкинг (mobile-banking). На основе Интернет-Клиент могут предоставляться информационные сервисы с ограниченным набором функций (Выписка On-Line).

На основе сравнения вышеизложенных определений можно сделать выводы о том, что техническая грамотность населения по вопросам дистанционного банковского обслуживания еще не достигла приемлемой величины и есть смысл её повысить. С другой стороны, для этого необходимо задействовать дополнительные ресурсы как со стороны банков (дополнительный персонал, время и деньги на обучение), так и со стороны клиентов (дополнительное время, которое в конечном итоге также отражается на финансовом благополучии), тогда как очевидной выгоды эти знания не принесут.

Руководствуясь этими соображениями, большинство решает не тратить на изучение этого вопроса лишнего времени и оперировать терминами, почерпнутыми из неспециализированных источников, увеличивая при этом риск возможного недопонимания и, как следствие, ошибок при использовании систем ДБО, что приводит к дополнительным затратам по времени на распознавание и выяснение причин неполадок как со стороны клиента, так и со стороны банка.

В этих случаях возможно также появление технических рисков (неправильно установленное программное обеспечение может стать источником ошибок при заполнении и передаче платежных документов и др.), а также рисков безопасности (при неполной/некорректной установке система ДБО может быть использована злоумышленниками).

# 1.2 Нормативная база и основные риски дистанционного банковского обслуживания

Услуги по ДБО регулируются следующими положениями [Банка](http://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B1%D0%B0%D0%BD%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8) России:

* Положение от 26.03.2007 г. № 302-П "О правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории РФ"
* Положение от 03.10.2002 г. № 2-П "О безналичных расчетах в РФ".
* Положения от 24.04.2008 г. № 318-П "О порядке ведения кассовых операций в кредитных организациях на территории РФ" (п.2.8 "Организация работы с денежной наличностью при использовании банкоматов, электронных кассиров, автоматических сейфов и других программно-технических комплексов");
* Положения от 23.06.1998 г. № 36-П "О межрегиональных электронных расчетах, осуществляемых через расчетную сеть Банка России";
* Положения от 12.03.1998 г. № 20-П "О правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России".
* Временное положение от 10.02.1998 г. № 17-П "О порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении безналичных расчетов кредитными организациями"

Кроме того, необходимо учитывать требования:

* Федерального закона от 10.01.2002 г. № 1-ФЗ "Об электронной цифровой подписи";
* Стандарта Банка России СТО БР ИББС-1.0-2006 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации;
* Письма Банка России от 03.04.2004 № 16-Т "О рекомендациях по информационному содержанию и организации web-сайтов кредитных организаций в сети Интернет"
* Письма Банка России от 07.12.2007 № 197-Т "О рисках при дистанционном банковском обслуживании"
* Письма Банка России от 31.03.2008 № 36-Т "О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга"
* Письма Банка России от 30.01.2009 № 11-Т "О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга"

В законодательстве прописываются следующие понятия:

владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

сертификат средств электронной цифровой подписи - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

корпоративная информационная система - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Электронная цифровая подпись (ЭЦП) - вид аналога собственноручной подписи, являющийся средством защиты информации, обеспечивающим возможность контроля целостности и подтверждения подлинности электронных документов (далее - ЭД). ЭЦП позволяет подтвердить ее принадлежность зарегистрированному владельцу. ЭЦП является неотъемлемой частью ЭД (пакета ЭД).

Также ЭЦП можно определить как реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

Владелец ЭЦП - УБР, ВЦ, кредитная организация (филиал) или другой клиент Банка России, ЭЦП которого зарегистрирована в порядке, установленном договором между Банком России и его клиентом.

Электронный платежный документ (ЭПД) - документ, являющийся основанием для совершения операций по счетам кредитных организаций (филиалов) и других клиентов Банка России, открытым в учреждениях Банка России, подписанный (защищенный) ЭЦП и имеющий равную юридическую силу с расчетными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

Электронный служебно-информационный документ (ЭСИД) - документ, подписанный (защищенный) ЭЦП и обеспечивающий обмен информацией при совершении расчетов и проведении операций по счетам, открытым в учреждениях Банка России (запросы, отчеты, выписки из счетов, документы, связанные с предоставлением кредитов Банка России, и т.п.).

Пакет электронных документов - один или более ЭПД и / или ЭСИД, подписанных ЭЦП, при этом каждый ЭПД и / или ЭСИД в составе пакета не подписывается ЭЦП.

дистанционное банковское обслуживание россия

Подлинность ЭД (пакета ЭД) - положительный результат проверки ЭЦП зарегистрированного владельца, позволяющий установить факт неизменности содержания ЭД (пакета ЭД), включая все его реквизиты.

Центр сертификации или Удостоверяющий центр (англ. *Certification authority, CA*) - это организация или подразделение организации, которая выпускает сертификаты ключей [электронной цифровой подписи](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C), это компонент глобальной службы каталогов, отвечающий за управление [криптографическими](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде [цифровых сертификатов](http://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82).

Центр сертификации - это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей.

Открытые ключи и другая информация о пользователях хранится центрами сертификации в виде цифровых сертификатов, имеющих следующую структуру:

* серийный номер сертификата;
* объектный идентификатор алгоритма [электронной подписи](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C);
* имя удостоверяющего центра;
* срок годности;
* имя владельца сертификата (имя пользователя, которому принадлежит сертификат;
* [открытые ключи владельца](http://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%B9_%D0%BA%D0%BB%D1%8E%D1%87) сертификата (ключей может быть несколько);
* объектные идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
* электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Отличием аккредитованного центра является то, что он находится в договорных отношениях с вышестоящим удостоверяющим центром и не является первым владельцем самоподписанного сертификата в списке удостоверенных корневых сертификатов. Таким образом, корневой сертификат аккредитованного центра удостоверен вышестоящим удостоверяющим центром в иерархии системы удостоверения. Таким образом аккредитованный центр получает "техническое право" работы и наследует "доверие" от организации выполнившей аккредитацию.

Аккредитованный центр сертификации ключей обязан выполнять все обязательства и требования, установленные законодательством страны нахождения или организацией проводящей аккредитацию в своих интересах и в соответствии со своими правилами.

Порядок аккредитации и требования, которым должен отвечать аккредитованный центр сертификации ключей, устанавливаются соответствующим уполномоченным органом государства или организации выполняющей аккредитацию.

Центр сертификации ключей имеет право:

* предоставлять услуги по удостоверению сертификатов электронной цифровой подписи;
* обслуживать сертификаты открытых ключей;
* получать и проверять информацию, необходимую для создания соответствия информации указанной в сертификате ключа и предъявленными документами.

## В настоящее время существует большое количество российских удостоверяющих центров, вот некоторые из них:

* [Удостоверяющий Центр ФГУП НИИ "Восход"](http://www.uc.voskhod.ru/)
* Удостоверяющий Центр ЗАО "ПФ "СКБ Контур"
* [Удостоверяющий Центр ЗАО "Орбита" (Краснодар)](http://www.orbitacom.ru)
* Удостоверяющий Центр DIP
* [ООО Межрегиональный Удостоверяющий Центр](http://www.mruc.ru)
* НП "Национальный Удостоверяющий центр"
* [ЗАО "АНК"](http://www.ank-pki.ru)
* ООО ПНК
* [ЗАО Удостоверяющий Центр Ekey.ru (Москва)](http://www.ekey.ru)
* ЗАО Удостоверяющий Центр (Санкт-Петербург)
* [Удостоверяющий центр Информационно-аналитического центра Санкт-Петербурга (Санкт-Петербург)](http://www.ca.iac.spb.ru)

За рубежом также существует масса таких учреждений, ниже перечислены самые популярные и имеющие рейтинг "4 stars" и более

* DigiCert,
* SwissSign,
* StartCom,
* Entrust,
* Trustwave.

В соответствии с письмом от 30.08.2006 №115-Т "Об исполнении ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" в части идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая Интернет-банкинг)" Банк России обязал финансовые институты при оказании таких услуг идентифицировать не только владельца счета, но и других лиц, которые будут пользоваться этим счетом.

При этом ответственность банка по данным вопросам регламентирована крайне жестко. Нарушение требований закона может повлечь применение к Банку ответственности, предусмотренной ФЗ от 10.07.2002 года №86-ФЗ "О Центральном банке Российской Федерации (Банке России)" (рекомендуемые меры воздействия предусмотрены Письмом Банка России от 13.07.2005 года №98-Т "О методических рекомендациях по применению Инструкции Банка России от 31.03.1997 № 59 "О применении к кредитным организациям мер воздействия при нарушениях кредитными организациями нормативных правовых актов в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма").

В условиях кризиса обостряется битва за клиента в любой сфере бизнеса. И кредитно-финансовые организации здесь не исключение. Жесткая конкуренция приводит к необходимости улучшать обслуживание клиентов путём ввода новых видов услуг. Одним из направлений, способствующих предоставлению клиентам максимального удобства в их работе, является дистанционное банковское обслуживание, осуществляемое через сеть Интернет. Возможность полного управления своим личным счётом при условии простоты выполнения операций, комфорта и мобильности всегда привлекало и будет привлекать клиентов.

Однако наряду с удобствами, которые получает клиент, осуществление ДБО через Интернет становится причиной возникновения угроз нового типа. С одной стороны это связано с тем, что существенно возрастает доля рисков (угроз), контролировать которые силами финансовой организации практически невозможно, с другой стороны не меньшую долю рисков (угроз) приносят вопросы организации ДБО.

Основными направлениями распределения рисков в области безопасности для систем ДБО являются:

вопросы организации эксплуатации систем ДБО;

клиенты, обслуживаемые через Интернет;

каналы связи, используемые для транзакций;

глобальная сеть Интернет.

Внедрение систем ДБО подразумевает вовлечение в процесс специалистов различных областей знаний финансовых специалистов, специалистов информатизации, информационной безопасности, юристов и др. Отсутствие четко организованного и регламентированного взаимодействия между различными подразделениями кредитной организации может привести к возникновению уязвимостей, которыми не преминут воспользоваться нарушители. Практика показывает, что реализация угроз с использованием имеющихся "слабых мест" в системах ДБО приводит к весьма существенным финансовым потерям и (или) ослаблению конкурентных преимуществ со стороны кредитной организации.

Анализ инцидентов, происходящих в системах ДБО, позволяет разделить потенциальных нарушителей на внешних по отношению к системе ДБО - то есть клиентов (как авторизованных, так и нет, то есть хакеров или преступников) и внутренних - из числа сотрудников банка.

Важно понимать, что информация, циркулирующая внутри систем ДБО, фактически эквивалента реальным деньгам, а значит создать условия, при которых угроза несанкционированного использования этой информации будет полностью исключена невозможно. Иными словами, всегда найдётся тот, кто захочет завладеть этой информацией. А значит, её нужно защищать.

Правила работы в системах ДБО не являются конфиденциальной информацией и любой желающий может получить к ним доступ. Единственной защитой клиента от злонамеренных действий является его идентификационная информация (логин, пароли, криптоключи). Именно за этой информацией идёт охота. В большинстве случаев нарушителю достаточно украсть идентификационную информацию клиента системы, чтобы получить полный доступ к его счёту. Возможностей совершить такую кражу более чем достаточно. Например, с помощью "хакерских" инструментов, свободно распространяемых в Интернет.

На сегодняшний день, в сети предлагается широкий ассортимент всевозможных программ для перехвата пароля с помощью троянов, keylogger’ов (программ, считывающих вводимую с клавиатуры информацию) - "шпионов", которые незаметно для клиента "подсаживаются" на его компьютер и "ждут" указаний от своего создателя (или мастер - машины) для выполнения какой-либо "полезной нагрузки". Причем хозяин компьютера может в течение весьма длительного срока не подозревать о наличии вредоносного кода на своём ПК ведь даже "активация" такого "шпиона" не всегда приводит к его обнаружению. Это связано с тем, что вместе со "шпионом" "в комплекте" идёт также руткит-технология, позволяющая скрыть следы активности вредоносного кода на ПК жертвы.

Бороться с вредоносными программами и "шпионами" на их нынешнем уровне развития с помощью устаревших технологий сигнатурного анализа, используя для этого мощности компьютера конечного пользователя (что, естественно, связано с замедлением его работы), весьма неэффективно, да и уже практически невозможно. Объясняется это тем, что код "шпионов" и им подобных, как правило, вовсе не является вредоносным для операционной системы компьютера, а их быстрая мутация ставит под сомнение возможность сигнатурного анализа. Наиболее адекватным решением на сегодняшний день видится совместное использование технологий контентной фильтрации и сигнатурного анализа при помощи комплексного шлюзового решения, установленного "на входе" в корпоративную сеть или же, что еще более правильно, используемого в сети провайдера, предоставляющего доступ в Интернет. Такое решение позволяет блокировать любой неразрешенный трафик, генерируемый "шпионом" с персональных компьютеров сети организации, предоставляет средства антивирусной защиты, web-фильтрации и защиты от спама, предотвращает утечку конфиденциальных сведений, и, наконец, позволяет регулировать время пребывания пользователей в сети Интернет и блокировать их доступ к неразрешенным ресурсам.

Сегодня кража паролей и криптоключей с незащищённых носителей являются обыденным явлением. Но, к сожалению, столь же обыденным можно назвать стремление некоторых банков экономить на системах безопасности. А ведь такая экономия зачастую приводит к многомиллионным потерям и далеко не всегда это потери исключительно клиента. Применение устаревших технологий, таких как организация доступа по "логину" и паролю, использование ключевых носителей не способных защитить от кражи хранящуюся на них информацию, рост "фишинговых" атак в значительной степени повышают риск несанкционированного доступа к системам ДБО.

С другой стороны, часто используемые механизмы защиты не могут обеспечить юридическую значимость совершаемых клиентом действий в системе. А этот вопрос в последнее время приобретает всё более важное значение. Как показывает судебная практика, доказать факт кражи у клиента его идентификационной информации не всегда представляется возможным, а вот то, что пароль был известен сотрудникам банка, доказывается легко. Суды зачастую встают на сторону клиента, даже если в договорных обязательствах предъявляются очень высокие требования по обеспечению ими сохранности своей идентификационной информации. Объясняется это весьма просто, клиент мог не обладать необходимыми знаниями или условиями, указанными в договоре, а вот банк должен был предусмотреть адекватные меры защиты.

Этот факт уже взят на вооружение злоумышленниками. Маскируясь под добросовестных клиентов, они всё чаще начинают пользоваться недоработками кредитных организаций в технологических и юридических вопросах связанных с эксплуатацией систем ДБО для отстаивания своей "правоты" в судах. И надо отметить, что, при квалифицированном подходе, попытки эти бывают весьма успешны.

# 1.3 Анализ тенденций развития банковских услуг по дистанционному обслуживанию в России

Основными областями концентрации рисков, на которые кредитным организациям следует обращать внимание, являются следующие:

1) Нормативно распорядительная документация (договоры, регламенты, инструкции по использованию технологий ДБО и др.). Концентрация рисков в данной зоне связана с тем, что при внедрении и эксплуатации систем ДБО нормативно распорядительная документация должна обеспечить взаимодействие достаточно большого числа разносторонних сотрудников и внешних клиентов. Учитывая различные области производственной деятельности вовлечённых в процесс специалистов, вполне вероятно наличие нестыковок и недостаточная проработанность некоторых вопросов;

2) Отсутствие в кредитных организациях чёткой регламентации процессов, связанных с эксплуатацией систем ДБО, а также механизмов мониторинга адекватности действующей нормативной документации приводят к расширению состава негативных факторов, которые могут сказаться как на интересах клиентов, так и на финансовом состоянии организации;

3) Доступ пользователей к информационным ресурсам через не доверенную среду сети Интернет. Концентрация рисков в данной зоне связана, прежде всего, с ошибками или злоупотреблениями по предоставлению прав доступа и управлению идентификационными данными (паролями, криптоключами) клиентов. Кроме того, существенное влияние оказывают уязвимости программных, аппаратных средств и существующих технологий, а также рост попыток получения неправомерного доступа к информации, циркулирующей в системах ДБО;

4) Использование устаревших технологий создаёт дополнительные риски, вероятность реализации которых с течением времени увеличивается.

Основными направлениями в клиентской части системы, на которые следует обращать пристальное внимание, являются:

недостаточная проработанность документов, регламентирующих права и обязанности клиентов при получении услуг;

недостатки в обеспечении информационной безопасности;

недостатки, присущие конкретной банковской технологии ДБО;

недостатки и уязвимости, присущие операционным системам и другим прикладным программам, эксплуатируемым клиентами;

последствия, обусловленные ошибочными действиями персонала кредитной организации или безграмотностью клиентов.

Для кредитной организации направления, нуждающиеся в тщательной проработке, следующие:

недостаточная проработанность документов, призванных осуществить адаптацию довольно большого количества внутренних процессов и процедур к новым условиям деятельности;

недостатки в вопросах технического обеспечения информационной безопасности системы ДБО;

недостаточный анализ при внедрении новой банковской технологии, ориентированной на ДБО через Интернет, анализ тех "неприятностей" (организационных, юридических), которые клиент может доставить кредитной организации;

значительная зависимость кредитной организации от других вовлеченных в процесс сторон (провайдеров, поставщиков программно-аппаратных средств и др.).

Анализ существующих факторов риска поможет выявить процессы, влияющие на их уровень. Этот анализ должен включать:

разработку и поддержание в актуальном состоянии нормативно распорядительных документов;

поддержание требуемого уровня информационной безопасности, включая управление жизненным циклом автоматизированных систем (от разработки до окончания эксплуатации);

администрирование вычислительной сети и телекоммуникационного оборудования;

управление идентификацией и доступом пользователей к информационным ресурсам;

внедрение новых технологий повышающих безопасность эксплуатации систем ДБО;

мониторинг сетевого трафика с целью обнаружения вредоносного кода и вторжений.

Для своевременного реагирования на существующие риски кредитным организациям необходимо обеспечить выполнение комплекса организационных и технических мероприятий, направленных на обеспечение безопасного функционирования системы ДБО. Обеспечение удобства работы клиентов в системе, при выполнении такого комплекса, может явиться дополнительным конкурентным преимуществом.

Существует мнение, что усиление безопасности всегда негативно сказывается на удобстве работы клиента. Это не верно. Если безопасность не является "параноидальной", а используемые технологии современны и адекватны наличествующим угрозам, обеспечить одновременно удобную и безопасную работу для клиента вполне возможно.

Не менее распространённым является мнение о том, что необходимость дополнительных расходов за обеспечение безопасности всегда негативно воспринимается клиентами и ведёт к снижению их числа. Как показывает опыт передовых банков, если клиентам правильно и доходчиво объясняются существующие риски и возможные последствия, то, при наличии выбора механизма защиты, практически всегда выбор делается в пользу более высокого уровня безопасности. Поэтому внедрение новых безопасных аппаратных средств защиты идентификационной информации является насущной необходимостью.

Безусловно, стоимость и эффективность внедряемых технологий должна соответствовать тем объёмам финансовых операций, которые совершает клиент. Так, в случае небольших объёмов, для физических лиц чаще используются технологии одноразовых паролей, которые наряду с применением "запоминаемого" пароля, дают существенное увеличение безопасности совершаемых операций, при относительно небольшой стоимости. Использование инфраструктуры открытых ключей наряду с ключевыми носителями, способными надёжно сохранять идентификационную информацию о клиенте, по-прежнему остаётся практически безальтернативным вариантом для юридических лиц.

В последнее время появились довольно интересные решения в области повышения безопасности. Так, для технологии ЭЦП на рынке предлагаются смарт-карты на базе платформы Java, которые способны выполнить ЭЦП по алгоритму ГОСТ 34-10 2001 г., без использования криптопровайдера. При этом все криптографические операции с секретным ключом выполняются внутри смарт-карты, секретный ключ её никогда не покидает. Эта технология сводит к нулю вероятность кражи секретного ключа пользователя. Доступ к самой смарт-карте защищается PIN-кодом и, если она попадёт в посторонние руки, злоумышленнику не удастся ей воспользоваться. Кроме того, данная технология не требует установки, какого либо клиентского программного обеспечения на рабочем месте клиента. Совокупность всех этих факторов предоставляет клиентам высокую степень безопасности, удобство в работе и, главное, мобильность (клиент может получить доступ к системе практически с любого компьютера).

Ещё одной новинкой является технология, расширяющая возможности применения средств аутентификации для обеспечения защищенного удаленного доступа к информационным ресурсам. Она основана на жесткой фиксации адреса сервера ДБО внутри смарт-карты. При этом сама смарт-карта имеет "загрузчик" который позволяет в доверенном режиме скачать с сервера необходимое для работы в системе ДБО программное обеспечение. Клиент, использующий данную технологию, не может быть перенаправлен на какой либо другой сервер, при этом доступ к информационным ресурсам организуется с использованием SSL-протокола (Secure Sockets Layer - слой защищенных соединений), но без установки клиентского программного обеспечения. Эта технология делает практически невозможными "фишинг - атаки" и перехват критически важной информации.

Своевременный учёт и анализ реально существующих факторов риска позволяет разработать, а затем реализовать комплекс организационных и технических мероприятий, значительно снижающих вероятность реализации угроз информационной безопасности. Недооценка важности технических или организационных составляющих (равно, как и "перекос" в сторону одной из них) одинаково негативно отражается на безопасности систем ДБО.

Затраты на развитие и модернизацию технологий защиты систем ДБО, оправдывают себя, поскольку с одной стороны позволяют избежать значительных финансовых потерь, а с другой способствуют улучшению условий работы клиента. Кроме того, если смотреть на вопрос с позиции экономики: эти затраты, по сути, являются инвестициями в развитие конкурентных преимуществ банковских технологий.

Лидирующее место по разработке и поставке программного обеспечения ДБО на рынке на данный момент занимает компания BSS.

Основные системы, которые предлагает Компания своим Клиентам:

"ДБО BS-Client" - комплексное интегрированное решение, включающее в себя весь спектр банковских услуг, предоставляемых за пределами офиса банка юридическим лицам;

["ДБО BS-Client. Частный Клиент"](http://www.bssys.com/credit/sulfiz/private/) - полнофункциональное тиражируемое решение, обеспечивающее удобное и надежное электронное обслуживание розничных клиентов банка с помощью Интернет, КПК, киосков самообслуживания, сотовых и обычных телефонов;

"Расчетный Центр Корпорации" (РЦК) - полнофункциональное решение в сфере автоматизации централизованного управления в режиме реального времени корпоративными финансами предприятий с территориальной и организационной структурой любой сложности;

["CORREQTS"](http://www.bssys.com/credit/sulur/coreqts/)  - решение для автоматизации фронт-офиса банка (финансовой компании), всей сферы контакта с конечным потребителем банковских и финансовых услуг.

Спектр продуктов и услуг Компании постоянно расширяется. Сегодня Компания успешно развивает следующие бизнес-направления:

Системная интеграция - проектные работы по обеспечению комплексного взаимодействия различных автоматизированных систем - АБС, программного обеспечения процессингового центра, систем дистанционного банковского обслуживания, внешних платежных и других информационных систем;

[CRM-решения](http://www.bssys.com/clients/crm/) - проектные работы по выработке и реализации полноценной методологии управления взаимоотношениями с клиентами на базе продукта Terrasoft CRM Bank;

Учебный центр - профессиональная подготовка IT персонала в сфере ДБО и ИТ.

Более 50% крупнейших банков России используют системы, разработанные Компанией. В частности, по данным аналитических исследований CNews Analytics за 2009 год, 24 из 50 ведущих банков РФ используют подсистему "Интернет-Клиент" системы "ДБО BS-Client", а 28 из 50 - подсистему "Банк-Клиент". В целом, решения Компании эксплуатируются более чем в 1500 кредитных организациях России и стран СНГ.

В число клиентов Компании входят Банк ВТБ (ОАО), ГПБ (ОАО), ОАО "Россельхозбанк", ОАО "УРАЛСИБ", ЗАО ЮниКредит Банк, "НОМОС-БАНК" ОАО, ОАО Банк "Петрокоммерц", ОАО "АК БАРС" БАНК, ОАО АКБ "Связь-Банк", ОАО "ТрансКредитБанк", Банк "Возрождение" (ОАО), "ТУСАР банк" ЗАО и др.

По данным рейтингов РА "Эксперт" и Интернет-издания CNews.ru, BSS входит в сотню крупнейших и наиболее активно развивающихся IT-компаний России. Система менеджмента качества BSS [сертифицирована](http://www.bssys.com/_upload/editor_files/ISOcert_rus.jpg) по международному стандарту ISO 9001: 2000 (первой среди специализирующихся на решениях в сфере ДБО).

Система ДБО должна соответствовать основным направлениям развития бизнеса банка, тех услуг, которые банк планирует предлагать своим клиентам. Работа с матрицей клиентов в самых различных измерениях имеет высокий приоритет. Первым шагом в данном направлении является предоставление услуг ДБО в разрезе многофилиальной структуры банка.

По данным компании BSS, юридические лица пока остаются основными потребителями услуг дистанционного банковского обслуживания. Розница все еще только осваивает этот метод работы с банками. Практически во всех отечественных банках уже давно установлены системы ДБО, которые делают более удобными возможные аспекты взаимодействия с клиентами.

Например, дистанционные услуги юридическим лицам предоставляют почти 100% российских банков; банков, использующих системы для работы с физическими лицами, в России на порядок меньше, но эта тенденция постоянно меняется в сторону роста количества используемых систем. По данным компании, наибольшим спросом у банков пользуются системы типа "Банк-Клиент".

Можно заключить, что потенциал рынка по системам этого типа состоит в основном в продвижении этих систем среди других клиентских сегментов и в улучшении качества предоставляемых услуг. Следовательно, ожидается развитие специализированных решений по обслуживанию юридических лиц, где система "Банк-клиент" является составной частью, например, услуг private-банкинга. Сегмент Интернет-банкинга активно развивается, и российские банкиры отмечают постоянный рост клиентской базы - от 40% в год (по отдельным направлениям этот рост еще выше). Данный рост будет продолжаться и в будущем.

В области развития интеграционных решений необходимо отметить факт резко возросшей потребности в централизованных системах, позволяющих объединить распределенные филиалы и отделения банка, вызванный трендом объединения финансовых структур и развития региональных сетей.

Однако основной потенциал развития рынка систем ДБО составляют кредитные организации, планирующие внедрение и активное развитие Интернет-банкинга и систем дистанционного обслуживания физических лиц, а также мобильных решений для юридических лиц. Именно такие системы и решения будут наиболее динамично развиваться в ближайшие годы.

На сегодняшний день уже треть банков уровня ТОР-100 используют системы дистанционного банковского обслуживания физических лиц. Среди способов оказания услуг ДБО физическим лицам, наряду с распространением Интернет-банкинга, будет все более популярен мобильный банкинг. В Западной Европе средства мобильной связи выходят на первое место, обходя персональные компьютеры по популярности использования для совершения банковских операций.

В условиях отсутствия у значительной части населения России доступа к высокоскоростному проводному Интернету внедрение мобильных услуг является эффективным решением. Сегодня в подавляющем большинстве случаев банк, строящий инфраструктуру ДБО для физических лиц, планирует предоставление мобильных услуг на одном из этапов развертывания инфраструктуры.

По оценкам экспертов рынка, потенциал развития Интернет-банкинга огромен. Аудитория российской зоны Интернета уже сейчас насчитывает более 30 миллионов пользователей и, согласно данным опросов, каждый третий Интернет - пользователь готов управлять своим банковским счетом через Сеть. И если рынок Интернет - торговли увеличивается на 30-50% ежегодно, то число абонентов мобильной связи уже существенно превышает численность населения России. Можно утверждать с высокой степенью вероятности, что мобильные сервисы будут показывать максимальный прирост клиентской базы в ближайшие годы.

Все эти показатели формируют благоприятную почву для развития дистанционных платежных сервисов.

# Глава 2. Современные системы дистанционного банковского обслуживания юридических лиц

В настоящее время выделяют три основных способа взаимодействия, с помощью которых банки могут проводить обслуживание юридических лиц в соответствии с их потребностями: это система Банк-клиент, Интернет-клиент и обслуживание клиентов по телефону. Каждый из перечисленных способов имеет свои положительные и отрицательные стороны, выгоды и риски. Рассмотрим подробнее эти варианты обслуживания.

# 2.1 Особенности использования системы "Банк-Клиент"

Изначально система "банк-клиент" появилась для удаленного обслуживания юридических лиц, для которых мобильность сервиса не так важна, как для частных клиентов. Банк-клиент - это "толстая" система, которая требует установки дополнительного программного обеспечения на компьютер клиента, на котором и ведется база данных. Выход в Интернет нужен только для приема/передачи информации. Данная подсистема позиционируется и как самостоятельный продукт, и как часть комплексной системы и ориентирована, в первую очередь, на средних и крупных и/или консервативных клиентов банка - юридических лиц, а также на банки-корреспонденты и подразделения банка (филиалы, отделения, обменные пункты и т.п.).

### **Задачи, которые решает система Банк-клиент выглядят следующим образом:**

* Доставка и обработка различных типов платежных и иных формализованных документов в обе стороны;
* Обмен сообщениями произвольного формата (с возможностью включения файлов);
* Получение выписок в различных видах и форматах, а также иной информации из банка;
* Построение расчетных и клиринговых систем в режиме реального или квазиреального времени.

### **Существуют следующие отличительные особенности системы при её эксплуатации:**

* Поддержка любых систем коммуникации (в том числе по протоколу TCP/IP), наличие собственной транспортной подсистемы позволяет работать практически на любом оборудовании с минимальными требованиями, обычно перечисленными в руководстве по эксплуатации.
* Поддержка любых систем криптозащиты (в том числе КриптоПроCSP, Сигнал-Ком (продукты: криптобиблиотека Message Pro и сервер сертификации Notary PRO), Lan Crypto, Верба-OW, Крипто-Си) делает систему Банк-клиента наиболее защищенной (при условии строгого соблюдения полученных от банка инструкций установки и эксплуатации).
* Абсолютная гибкость системы: добавление/изменение форм ввода/редактирования и печатных форм документов, вида экранов, иконок, панелей инструментов, правил ввода и редактирования, пользователей, меню, подключения справочников, правил их репликации и т.д.;
* Настройка произвольного жизненного цикла любого документа и его статусов, адаптация системы статусов соответственно системам коммуникации и криптозащиты;
* Наличие внутрисистемного предметно-ориентированного языка программирования - гибкость задания правил контроля документов, привязок к бухгалтерским системам, АБС и другим учетным базам данных;
* Удаленное обновление клиентских частей - поддержка массовости внедрения системы;
* Привычный и удобный Windows-интерфейс.

Форма и вид рабочего места клиента (включая экранное "меню") создаются в банке. Клиент получает готовое рабочее место, которое он может изменять в пределах заданных банком полномочий. Работа клиента ограничивается только вводом документов и, при необходимости, импортом\экспортом данных с бухгалтерскими программами, а также просмотром поступивших из банка сообщений.

Импорт/экспорт данных может осуществляться встроенными или внешними процедурами в любые форматы. Импорт осуществляется с одновременным контролем импортируемых данных (например, на реквизиты банка и ключ счета). У разных клиентов могут быть как различные меню, так и различные справочники, шаблоны и базы, которые автоматически реплицируются системой. Количество, взаимосвязь и вид справочников настраиваются в банке тем же "Построителем форм", что и визуальные формы, причём каждый клиент может иметь любое количество индивидуальных справочников.

Инсталляция системы реализована в виде трех частей - инсталлятор банковской части, генератор клиентской части в банке и инсталлятор клиентской части у клиента, разворачивающий клиентское место, подготовленное в банке. Удобство и надежность инсталляции гарантируются и тем, что в одном цикле происходит настройка "ДБО BS-Client", системы коммуникации и криптозащиты.

В системе организована собственная транспортная подсистема, представленная ядром подсистемы и произвольным набором настраиваемых шлюзов, реализующих тот или иной способ коммуникации. В стандартной поставке представлены шлюзы TCP/IP, файловый, E-Mail (POP3, SMTP). Шлюз представлен как внешний модуль \*. dll, который импортирует и экспортирует пакеты информации. Таким образом, любая внешняя система коммуникации описывается своим шлюзом и легко интегрируется в систему Банк-клиент.

Основными положениями, на базе которых разработана транспортная система, являются:

1. Многопоточность - как ядро транспорта, так и шлюз поддерживают работу с произвольным настраиваемым количеством потоков информации. Например, шлюз TCP/IP позволяет одновременно обслуживать любое количество клиентов, ограничиваемое только пропускной способностью канала связи и аппаратными ресурсами;
2. Поддержка ядром транспорта общих правил работы для каждого подключенного шлюза, например, автоматическое разбиение большого пакета для некоторых типов электронной почты;
3. Одновременное использование произвольного количества шлюзов. Таким образом поддерживается работа клиентов по различным каналам связи, существование резервных каналов и т.д.;
4. Архивация всех входящих и исходящих пакетов по каждому шлюзу, обеспечивающая глубокое протоколирование и аудит всех событий в системе внешнего документооборота, для достижения абсолютной юридической значимости;
5. Признак "он-лайности" шлюзов. В случае TCP/IP этот признак максимален (клиент получает квитанцию о корректном приеме или даже обработке документа банком в том же сеансе связи), в случае off-line системы коммуникации (например, электронной почты), этот признак минимален. Возможны любые промежуточные варианты этого признака. Статусы документа настраиваются под признак "онлайности", что позволяет построить наиболее полную и ясную для клиента систему статусов при произвольной системе коммуникации.

Существует определенная группа данных, используемых всеми участниками системы ДБО. Эти данные необходимо поддерживать в одинаковом состоянии у каждого участника в целях исключения возможных конфликтов из-за несовпадения данных. При большом количестве участников и данных эта задача становится трудноразрешимой без специального механизма, обеспечивающего поддержание копий данных у всех участников в одинаковом состоянии. В "ДБО BS-Client" для этих целей встроена подсистема репликации.

При создании построителем какого-либо справочника система задает вопрос - реплицировать ли справочник и на каких клиентов - у разных клиентов возможны разные справочники, разные шаблоны и базы запросов, разные системы коммуникации и криптозащиты. В базе каждого реплицируемого справочника автоматически создаются три служебных поля - уникальный номер записи, признак записи - изменена, удалена или добавлена и дата последнего обновления.

Рассмотрим справочник банков как частный случай общего подхода. Мы можем менять его вручную в банке, а также, по мере необходимости, сверять стандартной процедурой со справочником, поставляемым ЦБ или существующим в АБС. При этом процедура проставит записям в служебное поле соответствующие статусы. В определяемое настройками "Сервера ДБО" время запускается системная процедура, которая готовит и высылает указанным клиентам запросы на изменение отдельных записей справочников согласно служебных полей. Почтовые статусы этих запросов видны так же, как и для других документов, что позволяет банку визуально контролировать процесс репликации (хотя, в штатных случаях, процесс происходит полностью автоматически и в мониторинге не нуждается).

При соединении с банком клиент автоматически получает команды - задания на изменение справочников, которые отрабатываются абсолютно незаметно для клиента. История этих репликаций хранится у клиента и может быть "поднята" в случае необходимости.

Этот механизм может быть применен для автоматического сообщения клиентам о курсах валют, котировках ценных бумаг и т.д. и не требует никаких усилий не только от клиентов (они видят только результат процедур - измененный справочник), но и от банка (изменив корпоративный справочник как внутрибанковский - вручную или внешней процедурой - получаем автоматическую и наглядную репликацию на необходимых клиентов).

Важным механизмом ДБО является удаленное обновление рабочего места клиента. Этот механизм позволяет вносить изменения в технологию "на лету" вне зависимости от количества и территориальной удаленности клиентов. Система Банк-клиент позволяет производить корпоративное обновление системы (любой сложности, включая изменение экранных форм, структуры баз, конвертацию, добавление нового справочника или документа) полностью автоматически и незаметно для клиентов (у клиентов обновления производятся непосредственно после приема почты из банка) с помощью дополнительной подсистемы "Корпоративная база". Таким образом, осуществляются:

1. Автоматическое изменение структур базы данных, настроек просмотра, фильтров и сортировок, а также импорта и экспорта. При изменении состава или наименования структур база данных клиента автоматически конвертируется;
2. Автоматическое изменение экранных и печатных форм;
3. Автоматическое изменение параметров клиентского места в соответствии с заданными условиями (удаленное администрирование);
4. Автоматическое изменение исполняемых модулей и динамических библиотек системы "ДБО BS-Client".

Все данные, пересылаемые клиентам для репликации и обновления, подписываются и зашифровываются банком. Их также возможно (персонально для каждого клиента) разбить на пакеты любой величины, при этом система сама контролирует целостность прихода всей информации к клиенту. Следует отметить, что подсистема репликации справочников встроена в ядро системы, подсистема же "Корпоративная база" служит только для автоматического удаленного обновления и администрирования клиентских мест по заданиям из банка и поставляется отдельно.

Стандартная схема работы системы "Клиент - Банк" представлена на рисунке 1.

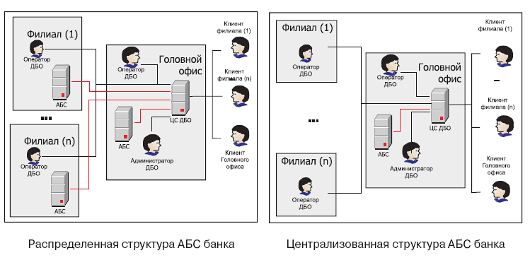


Рис.1. Схема работы системы "Клиент - Банк".

Для того чтобы получить доступ к системе "Клиент - Банк" необходимо иметь компьютер, принтер и модем с телефонной линией (без выделения отдельного номера) или компьютер, подключенный к сети Интернет, как правило, для установки программы не нужно закупать сверхмощные рабочие станции, подойдет обычный офисный компьютер.

В любом банке для заключения договора на ДБО через систему "Клиент - Банк" и получения дистрибутива по ней необходимо будет прийти в клиентский отдел банка и подать заявку на установку системы "Клиент - Банк" и заключить договор на ее обслуживание. В договоре сообщается данные о специалисте, имеющем право на ведение финансовых документов и право наложения электронной подписи, это может быть как бухгалтер, так и директор, либо просто сотрудник бухгалтерии, наделенный правом распоряжаться денежными средствами на расчетном счете.

В зависимости от условий договора, время работы банка с организацией может не ограничиваться часом окончания рабочего дня в банке - 16-30 - 18.00, но такие условия, как правило, редкость и относятся к крупным клиентам категории VIP. Но даже если организация не является VIP клиентом, отправка платежей все равно происходит 24 часа в сутки, и если по каким то причинам платеж пришел после окончания рабочего дня, он будет исполнен утром следующего операционного дня.

Если все условия договора удовлетворили клиента, то после его подписания в течение 7-14 рабочих дней специалист банка устанавливает в офисе клиента требуемое программное обеспечение и обучит пользованию им. Как правило, эта услуга оказывается на платной основе. Стоимость услуги по установке системы варьируется в пределах от 100 рублей до 4000 рублей - в зависимости от объемов и сроков исполнения заказа, а также от особенностей индивидуального подхода. Либо клиент сам получает программное обеспечение в банке и самостоятельно устанавливает его на своем рабочем месте - если он уверен, что справится.

Чаще всего установка не вызывает проблем у клиентов банка, особенно если в штате организации есть IT-специалист, и не стоит также забывать о том что у банка всегда есть служба технической поддержки, где клиенту всегда могут оказать квалифицированную помощь. Стоимость самой услуги без учета установки специалистом банка колеблется в пределах от 1500 до 5000 рублей. Средняя цена ежемесячного обслуживания - 700 рублей.

К стоимости услуги, зафиксированной в условиях договора, прибавляется процент от стоимости проведения каждого платежа, либо это фиксированная сумма, которая берется с каждого платежа после окончания операционного дня. Чтобы ежемесячно оплачивать услугу, платежное поручение не потребуется: оплата производится в порядке безакцептного списания с расчетного счета.

Современные системы "Клиент - Банк" предлагают пользователям следующие возможности в работе с программой:

Простой, понятный интерфейс. Экранные формы максимально приближены к привычным печатным формам. Создание нового документа занимает менее 1 минуты;

Мощный механизм проверки документов. Проверка правильности заполнения документов осуществляется уже при вводе документа. Если при заполнении платежных документов были допущены ошибки, клиент получит об этом сообщение в течение нескольких минут. При этом проверяется широкий спектр реквизитов.

Справочники корреспондентов, бенефициаров, БИКов, кодов SWIFT, курсов валют, кодов бюджетной классификации и других реквизитов бюджетных платежей, кодов видов валютных операций, мотивов отказа от акцепта. Данные этих справочников всегда актуальны, их обновления автоматически рассылаются всем Клиентам.

Широкий спектр типов документов. Система "Клиент - Банк" реализована с учетом всех требований Банка России и позволяет корпоративным клиентам отправлять в банк следующие финансовые документы:

платежное поручение;

платежное требование;

инкассовое поручение;

аккредитив;

заявление об отказе от акцепта;

кассовая заявка;

реестр переданных на инкассо расчетных документов;

заявление на перевод валюты;

поручение на покупку валюты;

поручение на продажу валюты;

поручение на обязательную продажу валюты;

поручение на конвертацию валюты;

заявление на открытие импортного аккредитива;

заявка на выдачу наличной валюты;

справка о валютных операциях;

выписка по счету за произвольный период;

оборотно-сальдовая ведомость за произвольный период;

платежное требование, выставленное клиенту;

В большинстве систем "Клиент - Банк" встроен механизм автоматического обновления клиентского программного обеспечения. Версии дорабатываются с учетом нормативных актов Банка России, требований банка и пожеланий клиентов.

Оказание консультаций. По системе "Клиент - Банк" имеется подробная документация, а специалисты банка всегда готовы предоставить необходимую консультацию.

Для полной автоматизации деятельности организации в большинстве "Банк - Клиентов" есть возможность импорта и экспорта документов с внешними бухгалтерскими программами. Такое решение, несомненно, облегчает жизнь бухгалтеру организации, так как все записи, операции и прочие бухгалтерские материалы уже давно ведутся в электронном виде с помощью специализированных программ. Но в большинстве случаев обмен данными настроен у "Клиент - Банков" только с программой "1С: Бухгалтерия", если же клиент использует какую-либо другую программу для ведения бухгалтерского учета, предполагается что обмен данными будет настроен сотрудниками организации самостоятельно. Это связано с тем, что зачастую организации разрабатывают самостоятельно, либо покупают бухгалтерские программы с учетом специфики своей деятельности, и они несколько отличаются от стандартных.

# 2.2 Система "Интернет-Клиент" как наиболее оптимальная форма дистанционного банковского обслуживания юридических лиц

Как уже было сказано, Интернет-Клиент для юридических лиц - это система, которая позволяет клиентам банка дистанционно осуществлять все виды платежных операций по своему счету, а также оперативно получать информацию, необходимую для взаимодействия с банком. Работать с системой можно из любой точки мира - достаточно иметь лишь доступ в Интернет. Очень часто понятия "Банк-Клиент", "Клиент-банк" и "Интернет-Клиент" воспринимаются населением как идентичные, содержащие одну и ту же смысловую нагрузку.

Интернет-Клиент - основная подсистема комплексного решения "ДБО BS-Client. Частный Клиент", обеспечивающая розничным клиентам банка проведение полного комплекса удаленных операций через Интернет в защищенном режиме. "Интернет-Клиент" может использоваться банком совместно с другими подсистемами комплексного решения "ДБО BS-Client. Частный Клиент", обеспечивая единое пространство электронного обслуживания клиентов по всем сервисам системы "ДБО BS-Client. Частный Клиент".

Подсистема "Интернет-Клиент" в полном объеме обеспечивает использование всех банковских продуктов, входящих в состав "ДБО BS-Client. Частный Клиент". В качестве Аналога Собственноручной Подписи клиента могут использоваться как сеансовые ключи (в т. ч. и сформированные с помощью MobiPass), так и Электронно-Цифровая Подпись, сформированная сертифицированными ФСБ Средствами КриптоЗащиты Информации.

При работе клиентов с подсистемой "Интернет-Клиент" управление счетом и проведение банковских операций происходит через web-сайт банка, доступ к которому осуществляется через сеть Интернет. Клиент банка из дома, с работы или любого другого места через браузер (Internet Explorer) обращается по стандартному протоколу HTTP к веб-серверу банка. При успешной аутентификации пользователь начинает защищенный сеанс работы с системой "Интернет-Клиент" - производится обмен информацией в доступных форматах HTML и XML.

Все документы (база данных платежных поручений, выписок, справочников корреспондентов (получателей), справочник банков России и т.д.) и иные ресурсы, необходимые клиенту для работы с банком, находятся на стороне банка. Это позволяет пользователям не зависеть от конкретного компьютера и получать доступ к управлению счетом из любого удобного места, используя компьютер, подключенный к интернету.

Клиент может создавать, редактировать и отправлять в обработку платежные (рублевые и валютные) документы, просматривать архив документов, просматривать и распечатывать сообщения из банка и выписки за любой период, пользоваться справочниками, физически находящимися на стороне кредитной организации, и т.д. Все операции между банком и организацией проводятся в режиме реального времени. Возможности подсистемы позволяют отслеживать все этапы обработки платежных документов на банковском сервере.

Благодаря онлайн-обмену информацией в подсистеме "Интернет-Клиент" реализован контроль корректности вводимых данных, обеспечивающий банку получение от клиентов только верно заполненных документов. Опция онлайн-контроля облегчает и ускоряет для кредитной организации обработку поступивших документов и предоставляет удобство их оформления клиентам.

Внедрив у себя "Интернет-Клиент для юридических лиц", банк получает целый ряд преимуществ:

1. Безопасная и стабильная работа клиентов. Безопасность достигается за счет использования сертифицированных ФСБ средств криптографической защиты информации, современных протоколов защиты данных, передаваемых через Интернет (SSL/TLS), и специфических внутренних механизмов защиты подсистемы, а стабильность - за счет промышленных веб-серверных приложений (Apache, IIS). Все действия по созданию новых ключей СКЗИ и изменению старых клиент производит самостоятельно - для этого служит простой и удобный пользовательский интерфейс.
2. Быстрое и простое подключение любого количества клиентов. Для того чтобы подключится к подсистеме, клиенту не требуется приезжать в банк. Ему достаточно зайти на веб-сайт кредитной организации и зарегистрироваться в системе - далее он может сразу начинать работу. Нет нужды устанавливать на стороне клиента дополнительное ПО - вполне хватит и системы криптозащиты информации. Все это достигается благодаря механизму удаленного подключения, с помощью которого возможно быстрое подсоединение большого количества пользователей.
3. Простота установки системы. Инсталляция "Интернет-Клиента для юридических лиц" не требует особых усилий и может быть произведена в кратчайший срок специалистами самого банка. Благодаря внутренним механизмам автоматической настройки подсистемы весь комплекс работ по ее установке и настройке на месте занимает в среднем 30 минут.
4. Легкость и оперативность обновления ПО системы. Поскольку необходимость обновлять клиентскую компоненту отсутствует (так как на стороне клиента нет никакого специального программного обеспечения), срок обновления подсистемы сокращается в десятки, а иногда и в сотни раз. Это позволяет своевременно и оперативно добавлять в нее новый функционал, а также изменения, отражающие актуальное законодательство.

Подсистема "Интернет-Клиент для юридических лиц" заключает в себе совокупность платежного, информационного и служебного сервисов для обеспечения производительной и удобной работы клиента с банком. Главным достоинством системы является то, что она сочетает полноту функционала, характерного для приложения классического типа "клиент-банк", с новыми возможностями, которые открываются благодаря использованию интернет-технологий.

Высокий интерес к интернет-банкингу со стороны клиентов обусловлен, прежде всего, более привлекательными условиями по сравнению с тем, что предлагают традиционные банки. Отечественные банковские организации не уступают сегодня своим западным коллегам в освоении современных финансовых технологий. В качестве примера можно привести WАР-банкинг - удаленное управление счетами посредством мобильного телефона, оснащенного специальным программным обеспечение на базе протокола беспроводной передачи данных.

К сожалению, компании мобильной связи, предлагая клиентам телефоны стандарта GSM с возможностью выхода в Интернет, далеко не всегда могут поддерживать необходимую степень защиты передаваемых или получаемых сведений на том уровне, как это организовано в Интернете. Поэтому банки не могут взять на себя ответственность за конфиденциальность платежей клиентов и предлагают им при помощи мобильного телефона лишь просматривать остаток на счете и список последних операций. Однако уже разрабатывается программное обеспечение, способное довести услугу WАР-банкинга до совершенства. Пока же для того, чтобы обеспечить безопасность платежей, некоторые банки оговаривают с клиентом список операций и присваивают каждой из них соответствующий код. При проведении какой-либо из операций пользователю WАР-банкинга достаточно ввести код, который при подтверждении банком активизирует необходимую транзакцию. За операции по счету банк комиссию не берет.

Сам факт того, что многие услуги могут быть осуществлены дистанционно через глобальную Сеть, привел к тому, что сам банк как физический объект (здание и пр.), в принципе, может не существовать. В свою очередь, теоретически это приводит к снижению операционных издержек, уменьшению стоимости услуг и повышению прибыли самого банка. Именно по этим причинам с 1995 по 2000 год в США и в Европе стали открываться так называемые "виртуальные банки", у которых не существовало ни одного офиса. Открытие счета и управление им, получение кредита - все это осуществлялось только через интернет.

В США к 2000 году насчитывалось 26 подобных кредитных организаций. Самым первым виртуальным банком считается американский [Security First Network Bank](http://www.sfnb.com), открывшийся 18 октября 1995 года. За первые полтора года существования средний прирост капитала банка составлял 20% в месяц, активы выросли до 40 млн. долларов, было открыто более 10 тыс. клиентских счетов. В Европе первым виртуальным банком был Advance Bank, дочерняя структура Дрезденской банковской группы (Германия). Подразделение появилось в 1996 году.

В 2000 году, когда стереотипы новой экономики развеялись и стало понятно, что не любая компания, действующая через интернет, может использовать сетевой эффект, а для клиентов банков главное - надежность и безопасность, а не доступ к счету 24 часа в сутки, многие виртуальные банки прекратили свое существование. Тем не менее, большинство из них было приобретено традиционными банками для использования их как одного из каналов предоставления собственных услуг.

В России, как и на Западе, интернет-банкинг вырос из систем класса "Клиент-Банк". И многие системы для юридических лиц сегодня являются "переходными". Появление российского интернет-банкинга принято отождествлять с системой "Интернет Сервис Банк", разработанной специалистами Автобанка в 1998 году, которая была предназначена исключительно для физических лиц. Клиенту для управления счетом требовался только стандартный браузер, а для хранения идентификационной информации служило специальное аппаратное средство, подключаемое к компьютеру. Сейчас же для обеспечения безопасности почти во всех российских системах используется специальное программное обеспечение, хранимое на дискете.

Сама клиентская часть и интерфейс, как правило, реализуются при помощи либо языка HTML и Java-апплетов, либо специальных плагинов для веб-браузеров, т.е. на стороне клиента специальное программное обеспечение в традиционном понимании не устанавливается. Большинство российских банков для предоставления своих услуг через интернет используют системы, разработанные сторонними производителями, и только 12 банков используют собственные разработки.

Так сложилось, что на российском рынке интернет-банкинга, помимо самих банков и их клиентов, принято выделять еще один институт - IT-компании, которые непосредственно разрабатывают и внедряют решения интернет-банкинга. Поэтому, говоря о системах интернет-банкинга российских банков, обычно упоминают и компанию-разработчика самого решения. Конечно, на Западе банки для построения своих интернет-услуг прибегают к помощи сторонних софтверных компаний, но их решения носят индивидуальный и кастомизированный характер для каждого банка. Наши же разработчики предлагают банкам стандартный программный пакет, на базе которого и развертывается система интернет-банкинга. Некоторые разработчики подобных систем устанавливают конкретную цену на свои продукты, которая может изменяться в зависимости от количества клиентских мест. Таким образом, многие российские банки имеют абсолютно идентичные системы, которые обладают одинаковыми функциями, интерфейсом, уровнем безопасности и пр.

# 2.3 Преимущества и недостатки системы "Телефон-Банк"

Телефонный банкинг - это банковский сервис по управлению расчетным счетом посредством использования возможностей телефонов с тональным набором номера. В классическом понимании телефонный банкинг это система интерактивного речевого взаимодействия (IVR).

Как правило, системы Телефон-Банк имеют ограниченный набор функций по сравнению с системами "Клиент-Банк":

* информация об остатках на счетах;
* информация о суммах поступлений в пользу клиента;
* ввод заявок на предоставление факсимильной копии выписки по счету;
* ввод заявок о проведении платежей, заказ наличности;
* ввод заявок на передачу факсимильной копии платежного поручения;
* ввод заявки на исполнение подготовленного по шаблону поручения на перевод средств;

Передача информации от клиента в банк может производиться различными способами в зависимости от реализации системы:

* Общение клиента с оператором телефонного обслуживания (Call Center).
* С использованием кнопочного телефона (Touch Tone Telephone) и голосового меню (средств компьютеризованной телефонной связи (технологии IVR (Interactive Voice Response)), Speech to Text, Text to Speech).
* Посредством передачи SMS сообщений (SMS-banking)

Наибольшее распространение, из всех услуг дистанционного банковского обслуживания, в нашей стране получил телефонный банкинг, который осуществляется благодаря технологии звуковой передачи данных, применяемый операторами телефонной связи. Также для телефонного банкинга применяются компьютерные возможности телефонной связи и технологии, доступные для телефонов кнопочного типа. Перечень услуг, предоставляемых клиентам банков при использовании телефонного банкинга достаточно широк. Так, можно узнавать о финансовых поступлениях на индивидуальный счет пользователя, получать информацию о текущем состоянии счета, а также осуществлять подачу заявок на осуществление платежей и получение квитанций

Телебанкинг включает выбираемые по усмотрению банка виды обслуживания:

* информационно-справочную службу (курсы валют, изменения котировок ценных бумаг, условия размещения депозитов, операции банка);
* проведение платежей (коммунальные услуги, телефонные счета и другие услуги связи, покупка и продажа валюты);
* управление счетом (переводы средств со счета на счет, баланс счета, пополнение или блокировка карточки при ее утере).

Когда банк выходит на рынок телебанкинга, т.е. включает функцию удаленного дистанционного осуществления финансовых операций, то это значит, что используется информационная справочная система, позволяющая обслуживать клиента по телефону. Создание такой системы позволяет банку значительно увеличить число обслуживаемых клиентов, не развертывая необходимой в таких случаях сети дополнительных филиалов и отделений. По некоторым оценкам объем услуг, предоставляемый по телефону первопроходцами этого бизнеса, то есть банками Великобритании, в течение ближайших 5 лет десятикратно увеличится, т.е. с 2 млн. в настоящее время до 20 млн.

Существуют следующие преимущества телебанкинга:

* Количество обслуживаемых клиентов ограничивается не количеством филиалов и отделений банка, а факторами, которыми легче управлять: мощностью компьютерной системы и количеством подключенных к ней телефонных линий.
* Автоматический факсимильный сервис с успехом заменяет бумажный документооборот между клиентом и банком.
* Клиент не привязан к банку территориально. Банк может обслуживать иногородних и даже иностранных клиентов, не открывая дополнительных отдаленных филиалов.
* Поскольку все операции производятся на центральном компьютере, можно быстро и без существенных организационных издержек добавлять дополнительные услуги.
* Существенно сокращается количество сотрудников банка.
* Клиенту не нужно посещать банк, чтобы узнать состояние своего счета или произвести какие-либо операции.
* Хорошо сочетается с карточными платежными системами.
* Обеспечивает круглосуточный сервис.

Для клиента телебанкинг - это еще одна возможность получить банковскую услугу в выходные дни или в нерабочие часы. По статистике пик платежей по телебанкингу приходится на время между 1 и 2 часами ночи. Для банка телебанкинг - возможность привлечь клиента и сэкономить на штате операционистов.

Телефонный банкинг работает с Разговорным компьютером, который каждую сказанную команду понимает и отвечает хорошо понятной речью.

Он принимает звонки и обрабатывает их или соединит по желанию с диспетчером. Разговорный компьютер может управляться через набор команды клавиатурой (телефон с импульсным тоном) При этом существуют три различных возможности:

***1) Разговорный способ***

У клиента есть возможность получить интересующую информацию посредством голосовых команд, называющих ту или иную цифру выбора меню (от 1 до 9). Также клиент может назвать ключевое слово для упрощения диалога и авторизации пользователя.

***2) Ввод команды через клавиатуру телефона***

Клиент имеет возможность выбрать напрямую имеющиеся цифры через импульсный телефон. При специальных комбинациях кнопок возможно переключение телефона назад в предыдущее меню.

***3) Ввод через прибор "сигналвводчик"***

Клиент имеет возможность вводить цифры чрез специальный прибор - сигналвводчик, который используется для дистанционного опроса автоответчика. Для использования такого диалога необходимо дополнительно установить устройство сигналвводчика, приспособив его для телефона

### **Как банк принимает необходимые меры для защиты данных:**

***1) Защита через телефонное кодовое число***

Для первоначального использования телефонного банкинга, клиент часто получает от банка собственное кодовое число, которое нужно для входа в систему. Это число меняется сразу же после первого звонка в число, которое известно только клиенту (5-и значное, только цифры) При этом нужно выбрать предложенный разговорным компьютером пункт меню 'Управление счётом и карточкой' и далее функцию 'Изменение кодового числа'. Это кодовое число будет запомнено в системе защиты.

***2) Надёжность через блокирование***

Если клиент определил или предполагает, что постороннее лицо знает кодовое число, необходимо сразу это число изменить или заблокировать. Для этого клиенту необходимо позвонить в центр телефонного банкинга и выбрать пункт меню диалога "Управление счётом и карточкой" Другой возможностью осуществить блокирование кодового числа, является письменная форма, через ближайшее почтовое отделение.

Если кодовое число будет три раза ошибочно введено, это повлечёт за собой блокирование компьютером входа в систему телефонного банкинга.

***3) Надёжность через контроль***

Через выбор пункта диалога "Управление счётом и карточкой" клиент может быть информирован, сколько и как часто в течении месяца было произведено банковских операций перевода, для которых клиент вводил своё кодовое число. Если клиент эту информацию сверил, то он сразу может определить, использовал ли кто-то его кодовое число для входа в систему телефонного банкинга.

Приведем пример меню, которым располагает клиент в процессе диалога с банком по телефону:

*1) Информация счёта:*

1. Состояние счёта 'Счёт'
2. Актуальные расходы 'Расход'
3. Таблица переводов 'Таблица'
4. Смена счёта
5. Переводы 'Перевод'
6. назад в главное меню 'Меню'

*2) Фонды и курсы:*

1. Цены инвестиционных фондов
2. Передовые курсы
3. Сорты курсов
4. назад в главное меню 'Меню'

*3) Информация о продуктах:*

1. Продукты экономии
2. Продукты кредитования
3. Электронный банкинг
4. Кредитные карты
5. Советы 'Консультация'
6. назад в главное меню 'Меню'

*4) Счёт/ управление счётом:*

1. Смена персонального кода
2. Блокирование персонального кода
3. Блокирование карточки
4. Логическая книга
5. назад в главное меню 'Меню'

*5) Соединение с 'Прямым сервисом':*

1. Опрос состояния счёта 'Перевод'
2. Совет
3. назад в главное меню 'Меню'

*6) Заказ бланков 'Бланк':*

1. Счётные конверты
2. Распечатка для 'Переводов'
3. Распечатка для счётов
4. EC-Scheks
   1. *назад в главное меню 'Меню'*

Схемы работы систем телефонного банкинга у всех разработчиков примерно одинаковы. Они представлены на рисунках 2 и 3.

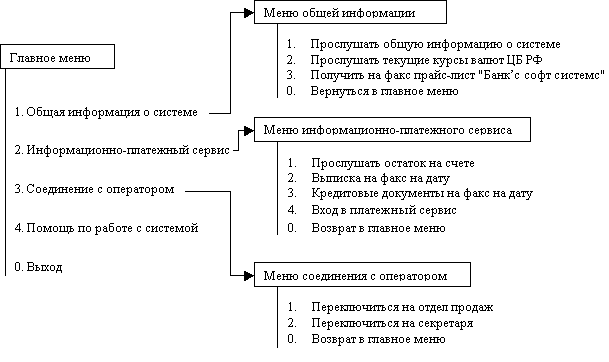


Рис.2. Схема работы системы "Телефон-Клиент" от разработчика банковского программного обеспечения ООО "Банк'с софт системс".



Рис.3. Схема модуля "Phone-Банкинг" системы "iBank 2" от производителя систем дистанционного банковского обслуживания ООО "БИФИТ".

Модуль "Phone-Банкинг" системы "iBank 2" взаимодействует с оборудованием Intel Dialogic, полностью реализован на Java 2 и работает под операционными системами Windows, Linux и Solaris. Все голосовые примитивы хранятся в Сервере БД системы "iBank 2" и могут быть легко модифицированы банком

Для описания сценариев взаимодействия клиентов с банком в модуле используется язык CallXML. При необходимости банки могут самостоятельно модернизировать и расширять типовые сценарии, голосовые меню, отчеты на факс.

Таким образом, несмотря на рекламу на сайтах банков об удобстве телефонного банкинга, о том, что есть возможность получать информацию о состоянии счета 24 часа в сутки 7 дней неделю, имея под рукой один лишь телефонный аппарат, можно сделать вывод, что телефонный банкинг - устаревшая услуга с ограниченным набором функций. Услуга была разработана еще в 1997 году в Гута - банке под названием "Телебанк" и с тех пор не слишком изменила свои функциональные возможности.

Все меньше корпоративных клиентов продолжают ею пользоваться из-за низких стандартов безопасности, отсутствия наглядности в отображении информации, и новые корпоративные клиенты практически ее не покупают, отдавая предпочтение современным системам дистанционного банковского обслуживания "Клиент-Банк" и Интернет-банкингу. Ведь в современных условиях тяжело себе представить клиента, у которого не было бы в офисе компьютера, подключенного к глобальной сети Интернет.

# Глава 3. Направления совершенствования дистанционного банковского обслуживания на примере "Тусарбанк" ЗАО

# 3.1 Автоматизированная система "Интернет-Банк"

При дистанционном обслуживании ЗАО "Тусарбанк" использует систему Интернет-Банк проекта "ДБО BS-Client" компании ООО "Банк`с Софт Системс".

Компания BSS основана в 1994 году и на сегодняшний день является лидером в области разработки автоматизированных систем дистанционного банковского обслуживания и управления финансами.

Компания предоставляет полный комплекс услуг по организации электронного обслуживания всех типов респондентов банка (клиентов - юридических и физических лиц, отделений, филиалов, банков-корреспондентов, обменных пунктов).

Более 50% крупнейших банков России используют системы разработанные этой компанией. В частности, по данным аналитических исследований CNews Analytics за 2009 год, 24 из 50 ведущих банков РФ используют подсистему "Интернет-Клиент" системы "ДБО BS-Client", а 28 из 50 - подсистему "Банк-Клиент". В целом, решения Компании эксплуатируются более чем в 1500 кредитных организациях России и стран СНГ.

В число клиентов Компании входят Банк ВТБ (ОАО), ГПБ (ОАО), ОАО "Россельхозбанк", ОАО "УРАЛСИБ", ЗАО ЮниКредит Банк, "НОМОС-БАНК" ОАО, ОАО Банк "Петрокоммерц", ОАО "АК БАРС" БАНК, ОАО АКБ "Связь-Банк", ОАО "ТрансКредитБанк", Банк "Возрождение" (ОАО).

По данным рейтингов РА "Эксперт" и Интернет - издания CNews.ru, BSS входит в сотню крупнейших и наиболее активно развивающихся IT-компаний России. Система менеджмента качества BSS сертифицирована по международному стандарту ISO 9001: 2000.

На текущий момент штат Компании составляет более 300 сотрудников.

"Интернет-Клиент" ("тонкий" браузерный "банк - клиент") реализует в рамках "ДБО BS-Client" канал предоставления полного спектра банковских услуг исключительно с помощью интернет-технологий. Данная подсистема позиционируется и как самостоятельный продукт, и как часть комплексной системы "ДБО BS-Client" и ориентирована, ввиду особенностей своей реализации, на "продвинутых" клиентов банка, как физических, так и юридических лиц.

### **Система решает следующие задачи:**

* Ввод и обработка различных типов платежных и иных формализованных документов клиентов банка, как юридических, так и физических лиц;
* Обмен сообщениями произвольного формата;
* Получение выписок в различных видах и форматах, а также иной информации из банка;
* Организация интернет-коммерции как самому банку, так и любому его клиенту;
* Построение расчетных и клиринговых систем в режиме реального времени.

### **Выделим отличительные особенности системы:**

* Гибкость системы и возможность внесения любых настроек;
* Высокая производительность - трафик по одному документу составляет ~ 20Кб;
* Использование стандартных СКЗИ (КриптоПроCSP, Сигнал-Ком (продукты: криптобиблиотека Message Pro и сервер сертификации Notary PRO), Lan Crypto, Верба-OW, Крипто-Си), в т. ч. сертифицированных ФАПСИ (ФСБ);
* Простота использования и массовость внедрения за счет использования только web-технологий;
* Абсолютная юридическая значимость, шифрование и ЭЦП всего трафика в обе стороны;
* Использование только стандартного HTML;
* Отсутствие возможности вскрытия - наряду с внутренней системой защиты HTTP-трафика BS-Defender "ДБО BS-Client" включает в себя два дополнительных механизма обеспечения безопасности соединения с банком - протоколы SSL и TLS, позволяющие повысить надежность связи и защитить передаваемую информацию от несанкционированного доступа;
* Элегантный, удобный и интуитивно понятный документо-ориентированный интерфейс.

Массовость внедрения "Интернет-Клиента" обеспечивается "легкостью" самой системы и простотой начала работы с ней, что обуславливается использованием только стандартных интернет-технологий, а также ее стоимостью.

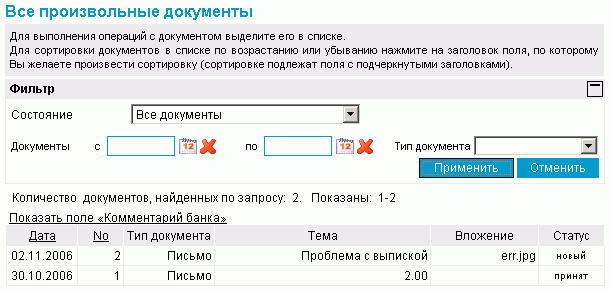
При использовании "Интернет-Клиента" управление счетом и проведение различных банковских операций происходит при работе с обычным Web-сайтом банка, доступ клиентов к которому осуществляется через сеть Интернет. Безусловно, банк может организовать резервный канал доступа к системе - создав с помощью модемного пула сеть Интранет для дозвонившихся в банк клиентов - на случай как сбоев у провайдеров, так и для клиентов, не имеющих (или не желающих иметь) доступ во всемирную сеть.

Клиент, из любой точки мира, при помощи встроенного в операционную систему Windows браузера (Internet Explorer), обращается по протоколу HTTP к Web-серверу банка. Взаимная аутентификация клиента и банка осуществляется при помощи системы BS-Defender. При успешной аутентификации клиент начинает защищенный сеанс работы с системой "Интернет-Клиент" - производится обмен информацией в формате HTML. Обеспечению безопасности и защищенности сеанса работы с системой ниже посвящен отдельный раздел.

На клиентской стороне не содержится никакой информации - все документы, справочники и иные ресурсы находятся в банке. Клиент может создавать и редактировать платежные (рублевые и валютные) и иные документы, просматривать архив документов, сообщения из банка и выписки за любой период, пользоваться стандартными справочниками (как общими - банков, курсов валют и др., так и персональными - корреспондентов, оснований платежа и т.д.) физически находящимися на стороне банка.

При подготовке любого документа осуществляется его контроль на корректность введенных данных, после чего осуществляется операция электронно-цифровой подписи. Далее документ пересылается на сервер банка и после процедур проверки подписи и правильности заполнения попадает в общую базу данных единой банковской части "ДБО BS-Client", где и производится его дальнейшая обработка (распечатка, посылка уведомлений, выгрузка в АБС, исполнение или отказ). При выполнении общих для всех подсистем ДБО автопроцедур обработки документа, клиент получает результат об исполнении документа или его отказе с указанием причины такового.

Документо-ориентированный интерфейс прост, элегантен и интуитивно понятен любому пользователю - окно браузера разделено на три части: вверху находится панель управления с рядом стандартных кнопок ("Новый документ", "Просмотр документа" и т.д.), слева содержится дерево документов по типам, (аналогично файловой структуре), справа находится рабочее окно, служащее для отображения собственно документов, форм и списков документов выбранного типа. Данная модель в наиболее простой и наглядной форме позволяет пользователю работать с документами. Типовой клиентский интерфейс системы "Интернет-Клиент"приведен на [рисунке](http://www.bssys.com/_upload/editor_img/web_client.gif) 4.



### Рис.4 Типовой клиентский интерфейс системы

Помимо простоты повседневной работы с системой, крайне важно обеспечение безболезненного начала работы с ней даже самого неподготовленного клиента. В подсистеме "Интернет-Клиент" системы "ДБО BS-Client" для начала работы клиенту необходимо лишь:

* Получить (или зарегистрировать уже имеющиеся) ключи (или электронный сертификат) ЭЦП и шифрования в банке согласно акта ввода в действие ключей (при этом, в случае получения ключей в банке, клиент имеет возможность самостоятельной перегенерации ключей непосредственно на своем АРМ);
* Получить дистрибутив системы (программное обеспечение защиты HTTP-трафика - BS-Defender - объемом менее 1 Mb) либо при визите в банк, либо непосредственно с сайта банка;
* Запустить программу DefStart. exe из дистрибутива системы, которая автоматически осуществит установку системы защиты HTTP-трафика BS-Defender, настроит браузер и параметры работы с ключами ЭЦП и шифрования, запустит браузер, установит защищенное соединение с банком и осуществит вход в систему "Интернет-Клиент".

Для работы на любом другом компьютере в любой точке мира клиенту необходима лишь дискета или флеш-карта с дистрибутивом системы и ключами ЭЦП. Технология работы с системой отражена на рис.5

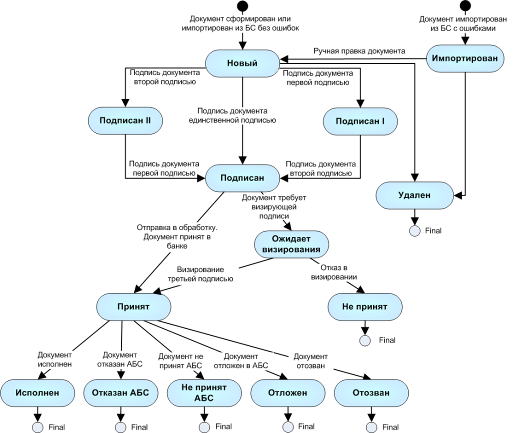


Рис.5 Технология обработки документооборота

При заключении соглашения об использовании электронных документов и электронной подписи в рассчетно-кассовом обслуживании закрепляются следующие понятия:

1. Информационная система Клиент-Банк (далее - Система) - комплекс программно-технических средств и организационных мероприятий для создания и передачи электронных документов Сторонами по телекоммуникационным каналам, в том числе и сети "Интернет". Система состоит их двух частей: подсистемы "Клиент" и подсистемы "Банк", установленных у соответствующих Сторон.

2. Электронный документ (ЭД) - документ, в котором информация: представлена в электронно-цифровой форме (в виде последовательности двоичных символов), защищена от искажений с помощью одной или более электронных цифровых подписей, с помощью средств Системы преобразуется в форму, пригодную для однозначного восприятия человеком, хранится в базе данных, либо в файле.

3. Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, защищающий ЭД от подделки (определяющий подлинность ЭД).

ЭЦП представляет собой уникальную последовательность символов, полученную в результате определенного математического преобразования содержания ЭД с использованием Закрытого ключа.

4. Определение подлинности ЭД, производимое с помощью Сертификата ключа предполагает:

установление факта отсутствия (наличия) искажений ЭД с момента подписания ЭЦП;

идентификацию владельца соответствующего Закрытого ключа, как лица, подписавшего ЭД.

5. Сертификат ключа - автоматически создаваемый, средствами Системы при генерации Открытого и Закрытого ключей, документ на бумажном носителе установленной формы, подписываемый Сторонами, удостоверяющий принадлежность приведенного в нем Открытого ключа и соответствующего ему Закрытого ключа физическому лицу (Пользователю Системы, Администратору Системы). Подписанный Сторонами Сертификат ключа подтверждает факт наделения данного физического лица правами на использование Системы в соответствии с условиями настоящего Дополнительного о Соглашения к Договору банковского счета.

Сертификат ключа создается в двух экземплярах, для Клиента и для Банка, оформляется Актом регистрации электронной подписи. Сертификат ключа Администратора Системы подписывается только уполномоченным представителем Банка.

6. Закрытый ключ - уникальная последовательность символов, полученная в результате работы программы генерации Комплекта ключей. Закрытый ключ предназначен для выработки Системой ЭЦП в ЭД.

7. Открытый ключ - связанная с Закрытым ключом особым математическим соотношением уникальная последовательность символов, полученная в результате работы программы генерации Комплекта ключей. Открытый ключ предназначен для проверки подлинности ЭЦП.

8. Комплект ключей - комплект из Закрытого и соответствующего ему Открытого ключей.

9. Компрометация ключей - утрата, хищение, несанкционированное копирование или подозрение на копирование Закрытого ключа или Сертификата ключа, а также другие ситуации, при которых достоверно неизвестно, что произошло с Закрытым ключом или Сертификатом ключа.

10. Пользователь Системы - физическое лицо, уполномоченное Клиентом с помощью своего Закрытого ключа подписывать ЭЦП от имени Клиента ЭД, отправляемые в Банк, а также получать из Банка ЭД, предназначенные Клиенту.

Банк предоставляет Клиенту право использования Системы (программного продукта) исключительно в порядке и объеме, установленных в соответствии с Лицензионным договором между Банком и ООО "Банк`с Софт Системс" № BSS-TUSAR/S от 31.12.2008г. Предметом соглашения Банка и Клиента являются следующие положения:

Стороны осуществляют прием-передачу ЭД, подписанных ЭЦП, в соответствии с установленным орядком расчетов, являющимся неотъемлемой частью соглашения.

Стороны признают используемую в банке систему защиты информации достаточной для защиты от несанкционированного доступа, а также для подтверждения авторства и подлинности электронных документов.

Стороны имеют право в электронной форме передавать или получать от другой стороны при помощи Системы любой из ЭД, используемой банком.

Банк и клиент договариваются признавать действие Комплекта ключей каждой Стороны на основании Сертификата ключа без обращения за удостоверением Сертификата ключа к какой-либо третьей стороне.

Стороны признают, что Закрытый ключ Пользователя Системы создается средствами Системы в единственном экземпляре, соответствует Открытому ключу, приведенному в Сертификате ключа, и известен только Пользователю Системы. Стороны признают, что доступ (регистрация) Пользователя Системы в Систему, а также создание корректной ЭЦП в ЭД невозможны без наличия Закрытого ключа.

ЭД, созданные средствами Системы, соответствующие определенным требованиям системы защиты информации, и подписанные ЭЦП Пользователя Системы или Банка, признаются Сторонами документом, имеющим равную юридическую силу с банковским бумажным документом, с надлежащим образом оформленными, документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенных печатью Стороны - отправителя документа и порождают аналогичные им права и обязанности Сторон по настоящему Соглашению и Договору банковского счета.

# 3.2 Перспективы развития дистанционного банковского обслуживания на примере ТУСАРБАНК ЗАО

Использование Тусарбанком системы Интернет-Клиент компании BSS говорит о стремлении банка следовать в ногу со временем. Отличительной особенностью этого банка является полное соответствие его стандартов по дистанционному обслуживанию стандартам ЦБ.

Интернет-Клиент является очень перспективным проектом из-за недорогого обслуживания, круглосуточного доступа через Интернет к управлению своими счетами, высокой безопасности и удобства.

Одним из проектов, предлагаемых банком, является "Выписка он-лайн"

Подсистема "Выписка Он-Лайн" комплексного решения для обслуживания юридических лиц "ДБО BS-Client" предназначена для информационного обслуживания клиентов кредитных организаций в сегментах малого и среднего бизнеса.

Подсистема "Выписка Он-Лайн" позволяет клиентам банка получать информацию об остатках и выписки по счетам через сеть Интернет в режиме 24х7х365. Данное решение может использоваться банком совместно с другими подсистемами комплексного решения "ДБО BS-Client", обеспечивая единое пространство электронного обслуживания клиентов по всем сервисам системы "ДБО BS-Client".

Работа в системе начинается с ввода логина и пароля: (рисунок 6)

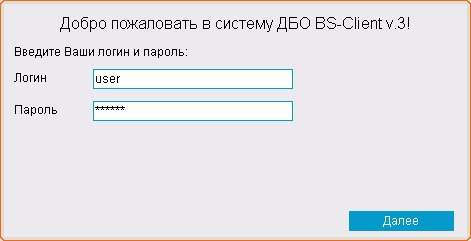


Рис.6 Страница Вход в систему при авторизации по учетной записи пользователя

* вход для просмотра данных о проведенных операциях осуществляется по логину/паролю. Защита соединения в подсистеме "Выписка Он-Лайн" осуществляется с помощью протокола SSL;
* пользователь видит только те операции, которые доступны для работы с выписками по счетам;
* пользователь может формировать отчеты за выбранный промежуток времени, устанавливать параметры отбора, распечатывать необходимые выписки необходимые документы в полном формате и пр.

Система Тусарбанка имеет следующие преимущества:

* не требуется установка дополнительного программного обеспечения (компонентов ActiveX, СКЗИ и пр.);
* пользователю не требуется скачивание каких-либо компонент, что позволяет работать на компьютерах без прав администратора (интернет-кафе и т.п.);
* система поддерживает работу с наиболее популярными браузерами - Internet Explorer, Opera, Mozilla, Firefox.

При ориентации на массовое использование системы "Интернет-Клиент" для банка крайне важно иметь возможность проводить обновления системы, не затрагивая клиентов. Примененная в системе "Интернет-Клиент" Тусарбанка технология, подразумевающая присутствие на клиентском месте только минимального, не зависящего от логики системы, "защитного" программного обеспечения, обеспечивает безболезненное внесение любых изменений и модернизаций, поскольку вне зависимости от количества клиентов они касаются только банковского сервера.

Причем изменение содержания банковского Web-сайта (применительно к подсистеме "Интернет-Клиент" системы "ДБО BS-Client"), его дизайна и наполнения возможно силами самого банка - необходимы лишь стандартные средства для работы с языком HTML, а также поставляемые в составе системы "ДБО BS-Client" средства работы с базами данных и "Редактор задач RTS".

Остановимся подробнее на технических аспектах реализации подсистемы "Интернет-Клиент" в рамках "ДБО BS-Client":

В основу подсистемы "Интернет-клиент" положены широко распространенные технологии:

* CGI - интерфейс;
* HTML-шаблоны.

Как известно, технология HTML-шаблонов базируется на наборе заготовок HTML-документов, в которых, следуя определенному синтаксису, внедрены места подстановки значений. Исполняемый модуль на WEB-сервере банка, исходя из данных полученного HTTP-запроса, определяет, какой шаблон ему нужно взять и затем заменяет места подстановки в шаблоне на текстовые фрагменты. Готовый HTML-документ отправляется клиенту.

Для обеспечения описанной функциональности, в подсистеме "Интернет-Клиент" используются задачи для серверной части. Задача содержит набор указаний, представляющих собой выражения на простом внутреннем языке и описывающих:

* какой шаблон использовать для формирования ответного HTML;
* какие данные из запроса клиента нужно использовать для того или иного взаимодействия с БД;
* какие взаимодействия осуществить с БД;
* куда в HTML-шаблоне и каким образом подставить ответные данные для последующей отправки клиенту.

В запросе, наряду с остальными данными, фигурирует ссылка на ту или иную задачу. К каждому HTML-шаблону, как правило, "привязано" несколько задач (количество задач равно количеству различных возможных переходов из HTML-документа, сформированного на основе этого шаблона). Подстановка ссылки на ту или иную задачу может осуществляться, например, с помощью простых функций на JavaScript или VBScript. Существует несколько возможных переходов из HTML-документа при работе системы "Интернет-Клиент". Например, из формы-диалога платежного поручения можно перейти в список платежек с сохранением введенных данных; либо перейти к справочнику корреспондентов; и т.д. Причем каждый переход в общем случае сопровождается не только формированием HTML-документа, но и определенными действиями с базой данных в банковской части системы.

Очевидно, что время от времени потребуется вносить какие-либо изменения в систему, и от того, каким образом реализована клиентская часть будет зависеть простота и скорость их внесения. Получившие признание среди разработчиков объемные (порядка 300 - 600 Кб), JAVA-приложения являются целостной программой, и требуют для внесения любых, даже мелких, изменений заказа доработок у фирмы-разработчика, либо покупки исходных текстов и разбор чужого программного кода большого объема, не говоря уже о необходимости знания языка программирования JAVA специалистами банка.

Обычные же HTML-страницы (как это и реализовано в подсистеме "Интернет - Клиент") не требуют значительного времени на обновление, имеют небольшой объем, просты для восприятия и могут быть изменены специалистами банка.

Для быстрого и наглядного написания задач и "привязки" их к HTML-шаблонам создан специальный инструмент - " Редактор задач RTS", дающий возможность описывать произвольные функции на собственном встроенном языке BS-Script.

Зная основы HTML, JavaScript (VBScript) и освоив язык задачи для серверной части BS-Script, можно создавать законченные системы оборота различных типов документов.

"Тонкий" браузерный "банк-клиент", равно как и любая другая полноценная система электронных расчетов, должен иметь под собой четкую юридическую базу. Именно в силу отсутствия таковой, интернет-решения многих разработчиков не нашли своего применения в реальной жизни. Юридическая значимость подсистемы "Интернет-Клиент" в рамках комплекса "ДБО BS-Client" обеспечивается следующими основными принципами:

* Существованием между клиентом и банком договора на обслуживание по системе "Интернет-Клиент", определяющего их взаимоотношения, а также механизм решения конфликтных ситуаций со ссылками на основные функции системы, скрепленный физическими подписями и оттисками печатей сторон. Ключевым моментом такого договора является понятие электронно-цифровой подписи банка и клиента;
* Использованием для обеспечения юридической значимости договора "стандартных", хорошо отработанных систем ЭЦП и шифрования, в том числе сертифицированных ФАПСИ;
* Оформлением акта ввода в действие ключей ЭЦП и шифрования;
* Электронно-цифровой подписью не только каждого документа со стороны клиента, но и всех сообщений, проходящих по системе в обе стороны, от клиента в банк и из банка клиенту. Причем ЭЦП всего трафика из банка обязательна, поскольку в противном случае сохраняется вероятность подделок документов со стороны злоумышленников;
* Сохранением в журналах работы (обязательно на стороне банка и опционально у клиента) всего прошедшего по системе траффика в исходном зашифрованном и снабженном электронно-цифровыми подписями сторон виде для разрешения возможных конфликтных ситуаций.

Безопасность и защита от несанкционированного доступа в подсистеме "Интернет-Клиент" обеспечивается применением в комплексе:

* Произвольных внешних криптографических средств защиты (СКЗИ - КриптоПроCSP, Сигнал-Ком, Верба-OW, КриптоЭкс);
* Протоколов безопасности SSL и TLS, позволяющих повысить надежность связи и защитить передаваемую информацию от несанкционированного доступа;
* Собственной системы защиты траффика BS-Defender;
* Аутентификации, авторизации, протоколирования;
* Организационно-административных мероприятий;
* Штатных средств защиты ОС и СУБД;
* Контролирования;
* Межсетевого экранирования.

Центральной системой для обеспечения безопасности является поставляемая как в составе "Интернет-Клиента", так и отдельно собственная система защиты HTTP-трафика BS-Defender, реализованная в виде симметричных прокси-серверов, в функции которой входят:

* Фильтрация трафика, относящегося к системе "Интернет-Клиент" и его маршрутизация;
* Вызов внешних систем криптозащиты для шифрования/дешифрования траффика;
* Протоколирование всего трафика, прошедшего по системе;
* Сжатие/распаковка сообщений, проходящих по системе.

Приведенная схема на рис.7 демонстрирует построение всего комплекса защиты в системе "Интернет-Клиент", включая общие средства обеспечения безопасности информационных ресурсов банка.

В настоящее время вопросам безопасности данных в распределенных компьютерных системах уделяется очень большое внимание. Разработано множество средств для обеспечения информационной безопасности, предназначенных для использования на различных компьютерах с разными ОС. В качестве одного из направлений можно выделить межсетевые экраны (Firewalls), призванные контролировать доступ со стороны пользователей одного множества систем к информации, хранящейся на серверах в другом множестве. В нашем применении это доступ клиентов из сети Интернет к ресурсам, находящимся в сети банка.

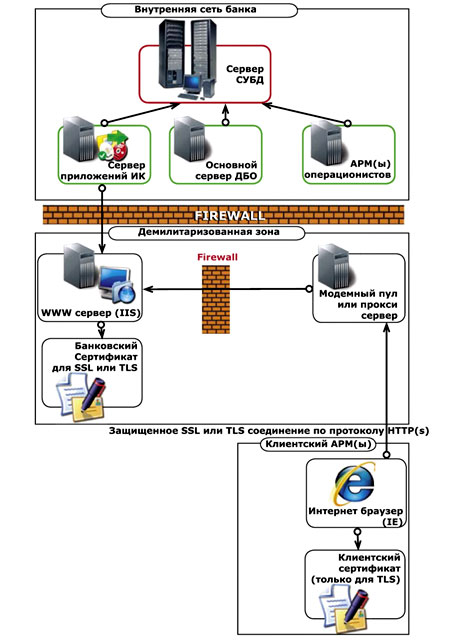


Рис.7. Построение комплекса защиты в системе "Интернет-Клиент"

Экран выполняет свои функции, контролируя все информационные потоки между этими двумя множествами информационных систем, работая как некая "информационная мембрана". В этом смысле экран можно представить как набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа. В частности, фиксировать все "незаконные" попытки доступа к информации и сигнализировать о ситуациях, требующих немедленной реакции, т.е. поднимать тревогу.

Обычно экранирующие системы делают несимметричными. Для экранов определяются понятия "внутри" и "снаружи", и задача экрана состоит в защите внутренней сети от "потенциально враждебного" окружения. Важнейшим примером потенциально враждебной внешней сети является Интернет.

Firewall может строиться разными путями, используя различные механизмы:

* Фильтры, установленные на маршрутизаторах (router-based filters);
* Межсетевые шлюзы на хостах, или крепости-бастионы (host computer gateways);
* Разделение изоляционными сетями (a separate, isolation network).

Наиболее типичным решением проблемы обеспечения защиты от НСД со стороны внешней сети является устанавка Proxy-сервера и межсетевого экрана (Firewall). Помещение межсетевого экрана после прокси-сервера обеспечивает необходимый уровень защиты с сохранением возможности доступа клиента к web-серверу банка с любого компьютера из любой точки мира. Данное решение является одним из возможных и может базироваться на использовании специализированных продуктов Check Point Firewall-1 компании Check Point Software Technologies, TIS Firewall Toolkit компании Trusted Information Systems и т.п.

При использовании системы "ДБО BS-Client" возможно как задействовать уже существующую в банке систему защиты от несанкционированного доступа извне, так и получить консультации и помощь специалистов Компании в разработке системы безопасности "с нуля". При этом возможен как выбор одного из предлагаемых Компанией "типовых" решений для организации защиты сети банка от НСД со стороны Интернет, так разработка специалистами Компании индивидуального решения.

В систему "Интернет-Клиент" введен ряд технологических решений, обеспечивающих корректную работу в случае сбоев и\или обрывов связи:

* Механизм сессий - каждое окно браузера, запущенное определенным клиентом, получает уникальный номер сессии, и вся работа происходит в рамках этой сессии (вплоть до закрытия сессии по окончании работы или после того, как истечет таймаут, устанавливаемый в настройках серверной части системы);
* Сквозная нумерация запросов в рамках сессии - каждый запрос в рамках определенной сессии имеет уникальный идентификатор. Обрабатываются запросы с номером больше или равным предыдущему;
* Хранение на сервере данных, необходимых для формирования текущего запроса только до момента поступления запроса со следующим номером.

Последние два технических момента позволяют корректно обрабатывать повторные запросы.

В случае обрыва связи во время работы клиента (например, при заполнении формы документа), в течение некоторого установленного настройками времени он может соединиться с сервером и продолжить работу. Его форма находится в открытом браузере. Следует отметить, что заполняемая на стороне клиента форма до отправки запроса на банковский сервер нигде, кроме как в браузере, не существует и исчезает только после его закрытия.

Если обрыв связи произошел в момент отправки запроса, но до получения ответа, то при возобновлении соединения и повторной отправке запроса (в течение таймаута) клиент получит как раз тот ответ, который он недополучил. При этом дублирование исключено и повторной модификации данных не произойдет.

Если же обрыв связи произошел в момент получения ответа сервера, когда запрос уже обработан, то после возобновления соединения клиент найдет свой документ, отправленный до обрыва связи, активизируя ссылку на панели навигации.

Подсистема позволяет юридическому лицу поддерживать актуальность собственных финансовых данных. Любой сотрудник компании с соответствующим уровнем доступа, может в любой момент получить необходимую информацию из любого удобного места с доступом в Интернет.

Данное решение может служить кредитным организациям эффективным инструментом привлечения новых клиентов. Предоставление услуг с помощью подсистемы "Выписка Он-Лайн" - хорошая возможность для повышения востребованности банковских услуг и эффективное решение для увеличения доли пользователей подсистемы "Интернет-Клиент" среди клиентов банка.

В целом можно сказать, что этот проект весьма актуален и, что самое главное, успешен. В целях привлечения большего количества клиентов и сохранения уже существующих предлагаем рассмотреть несколько вариантов улучшения взаимодействия банка и клиента:

1. Разработка двух типов интерфейса: обычного (для опытных пользователей) и упрощенного (для начинающих: с пояснением каждого действия). Это позволит снять лишнюю нагрузку со специалистов технической поддержки, которым в основном приходится отвечать на одни и те же вопросы.

2. Осуществление технической поддержки по почте в оперативном режиме позволило бы разгрузить телефонные линии, дать специалисту время разобраться в вопросе и выслать адресату полный и исчерпывающий ответ на интересующий вопрос, также появилась бы возможность сохранять историю переписки с клиентом, что немаловажно.

3. Создание и поддержание в актуальном виде подробной инструкции по использованию системы Клиент-Банк с возможными ошибками и их решением для минимизации затрат по многократному разъяснению клиентам необходимых действий.

4. В целях безопасности создание только одного оригинального носителя секретных ключей с невозможностью его копирования.

5. В целях привлечения новых клиентов рекомендуется увеличение масштабов рекламы и ее упрощение для потенциальных начинающих пользователей. Использование рекламы представляется возможным в основном в Интернете (на сайтах банков, банковских форумах и прочих ресурсах, на которых бывают потенциальные клиенты).

Для кредитной организации направления, нуждающиеся в тщательной проработке, следующие:

недостаточная проработанность документов, призванных осуществить адаптацию довольно большого количества внутренних процессов и процедур к новым условиям деятельности;

недостатки в вопросах технического обеспечения информационной безопасности системы ДБО;

недостаточный анализ при внедрении новой банковской технологии, ориентированной на ДБО через Интернет, анализ тех "неприятностей" (организационных, юридических), которые клиент может доставить кредитной организации;

значительная зависимость кредитной организации от других вовлеченных в процесс сторон (провайдеров, поставщиков программно-аппаратных средств и др.).

# Заключение

Проведенный анализ позволяет сделать выводы о том, что дистанционное обслуживание юридических лиц - это наиболее перспективное направление банковского бизнеса в сфере предоставления услуг корпоративным клиентам.

На данный момент точно определить объем оказываемых банками удаленных услуг невозможно, существуют только косвенные оценки, по которым электронные формы обслуживания предоставляют около 70% банков, а рост клиентов, дистанционно управляющих собственными счетами, составляет 20-30% в год.

Исследуя различные понятия дистанционного банковского обслуживания организаций, были сделаны следующие выводы.

Системы удаленного доступа к банковским услугам реализуются через предоставление этих услуг по запросу клиента без непосредственного взаимодействия с сотрудником кредитной организации по различным каналам: с помощью компьютера с выходом в глобальную сеть Интернет ("Клиент - Банк", Интернет-банкинг) и стационарного (Телефонный банкинг).

Определенный слой клиентов банков, для которых удаленные коммуникации становятся все более привычными средствами общения с кредитными организациями, уже появился. Как правило, это организации, имеющие понятие о новых услугах банков, руководство которых разбирается в современных технологиях, сформировавшее положительное мнение об удобстве и безопасности мобильной и Интернет - связи для операций с финансами.

Клиенты ценят в ДБО прежде всего удобство, доступность и работу в режиме реального времени, а банки - экономию издержек, максимальную близость к клиенту, независимо от региона страны, и наличие дополнительных конкурентных преимуществ.

Проанализировав рынок дистанционных банковских услуг коммерческих банков в России, можно выделить следующие тенденции:

расширение спектра предоставляемых возможностей через Интернет;

внедрение систем ДБО для юридических лиц через мобильные устройства;

желание банков отказаться от телефонного банкинга в связи с его крайне ограниченным кругом возможностей.

Наиболее динамично развивающимся современным каналом дистанционного банковского обслуживания, действующим в режиме он-лайн, является дистрибуция продуктов и услуг через глобальную сеть Интернет. Основное преимущество Интернет-банкинга состоит в удобстве, ведь дистанционно управлять своими счетами клиент может с обычного компьютера или ноутбука с выходом во всемирную сеть, не ограничивая себя ни территориально, ни во времени, экономя при этом деньги и нервы.

Основные сервисы, которые сейчас доступны клиентам в режиме он-лайн, следующие:

* информационный сервис - предоставление информации и выписок по расчетным счетам, рассылка оповещений о произведенных транзакциях, лента новостей;
* оформление платежных документов - осуществление регулярных и произвольных платежей;
* сервис по работе с рублевыми, валютными и бизнес счетами;

Скорее всего, в будущем "корзину дополнительных сервисов" ожидает такой же подход, который демонстрируют западные банки, сделавшие в этом направлении большой шаг вперед, - это более тесная интеграция различных каналов ДБО между собой и с электронными платежными системами - создание так называемых контакт - центров. Будет происходить трансформация классических отдельных каналов онлайн - банкинга в сторону центров, способных работать с клиентом через использование самых разных средств и методов связи - телефон, SMS, MMS, Интернет, е-mail, чат и т.д.

Российскому банковскому бизнесу сделать это пока что не представляется возможным. Ведь широкому предоставлению кредитными организациями интерактивных услуг в режиме реального времени препятствуют многие факторы, среди которых:

невысокий уровень доверия и популярности банковских услуг у организаций;

низкий уровень финансовой культуры и технической грамотности (например, в некоторых организациях платежные поручения до сих пор делают на печатной машинке);

отсутствие качественного продвижения дистанционных услуг со стороны банка;

неразвитость коммуникационной инфраструктуры в регионах;

законодательные ограничения.

Тем не менее, положительные тенденции присутствуют: это и повсеместное распространение Интернета и мобильной связи, и рост активности разработчиков автоматизированных банковских систем для кредитных организаций, и совершенствование законодательной базы, и расширение спектра предоставляемых банками онлайновых услуг.

Поэтому вполне возможно, что в будущем традиционное здание банка как место встречи банкиров со своими клиентами, в конце концов, отойдет в прошлое и будет вытеснено электронными средствами коммуникаций.

# Библиографический список

1. Гражданский кодекс РФ, Части первая, вторая, третья и четвертая. - М.: Проспект, 2007. - 560 с.;
2. Федеральный закон от 10.07.2002 № 86-ФЗ (ред. от 25.11.2009)"О Центральном банке Российской Федерации (Банке России)" (принят ГД ФС РФ 27.06.2002);
3. Федеральный закон от 02.12.1990 № 395-1 (ред. от 27.12.2009)"О банках и банковской деятельности" (с изм. и доп. от 01.01.2010);
4. Федеральный закон от 10.01.2002 № 1-ФЗ (ред. от 08.11.2007)"Об электронной цифровой подписи (принят ГД ФС РФ 13.12.2001);
5. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (принят ГД ФС РФ 08.07.2006);
6. Федеральный закон от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" (принят ГД ФС РФ 13.07.2001) (с изм. и доп., вступившими в силу с 06.12.2009);
7. Письмо ЦБ РФ от от 3 февраля 2004 г. N 16-Т "Рекомендации по информационному содержанию и организации WEB-сайтов кредитных организаций в сети интернет" // Российская газета. - 2004. - № 198. - С.18.
8. Письмо ЦБ РФ от 7 декабря 2007 г. N 197-Т "О рисках при дистанционном банковском обслуживании" // Вестник Банка России. - 2007. - №68. - С.56.
9. Порядок организации работы по предоставлению услуг с использованием системы "Клиент - Сбербанк" №1331-2-р. // Акционерный коммерческий Сберегательный банк Российской Федерации. - 2008.
10. Арт Я., Паперная И. Банкиры на дистанции // BusinessWeek Россия. - 2007. - № 68. - С.48.
11. Букин М. Портативный банк // PC Week Mobile. - 2007. - №3. - С.14.
12. Буркова А.Ю. Дистанционное банковское обслуживание: преимущества и риски // Юридический справочник руководителя - 2009. - №6. С.63.
13. Веретенников Д. Виртуальное самообслуживание // ЭКСПЕРТ. - 2008. - № 9. - С.24.
14. Веретенников Д. Бесплатная виртуальность // ЭКСПЕРТ. - 2009. - №14. - С. 19.
15. Гамза В.А. Безопасность банковской деятельности.2-е изд., перераб. и доп: Учебник для ВУЗов / под ред. Гамза В.А. - Маркет ДС, 2008 - 408 с.
16. Городецкий П. Обзор рынка ИБ в России // Connect - 2009. - №7-8. - С.31.
17. Додонова И.В. Автоматизированная обработка банковской информации: учебное пособие для студентов ВУЗов / Додонова И.В., Кабанова О. В.: под ред. Додоновой И.В. - КНОРУС, 2008. - 176 с.
18. Ермолаев Е. Интернет-банкинг в мире и в России: история, текущее положение дел и перспективы развития // ITСпец - 2009 - №2. С.62.
19. Изофенко Р.Н. Дистанционные каналы работы с клиентами // Банковское дело - 2009. - №8. - С.17.
20. Калемберг Д., Комарова Н. Какие угрозы в электронном банкинге? // Банковские технологии - 2009. - №6. - С.58.
21. Климов Е. Практические аспекты борьбы с инсайдерами // Информационная безопасность - 2009. - №3. - С.21.
22. Козулькова К. Счета выходят на связь // Газета "КоммерсантЪ". - 2008. - 21.09.08 № 176. - С.23.
23. Коробова Г.Г. Банковское дело: учебник // Коробова Г.Г. - Экономистъ, 2008.
24. Лаврушин О.И. Банковское дело: учебник / О.И. Лаврушин, И.Н. Мамонова, Н.И. Валенева; под ред. засл. деят. науки, проф.О.И. Лаврушина. - М.: КНОРУС, 2009.
25. Логвинова Н. "Толстый" против "тонкого" // Финанс. - 2008. №6. - С.57.
26. Мартынова Т. Аргументы в пользу дистанционного банкинга // Банковское обозрение. - 2009. - № 4. - С.36.
27. Мишакова А. ДБО стремится к системности // CIO: руководитель информационной службы. - 2009. - №2. С.41.
28. Насакин Р. Сервисы интернет-банкинга с расширенным набором функций // Компьютерра - 2008. - №4. - С.65.
29. Поляк Г.Б. Финансовый менеджмент: учебник для вузов / под ред. акад.Г.Б. Поляка. - М.: ЮНИТИ-ДАНА, 2008.
30. Рудычева Н. Кризис не поменял лидеров на рынке ДБО // CNEWS - 2009 - №8. С.22.
31. Серегин А.Ю. Рынок ДБО в России и в мире. Перспективы развития электронного банкинга в России // Банковские технологии. - 2008. - №10 - С.52.
32. Скиннер К. Будущее банкинга. Мировые тенденции и новые технологии в отрасли: учебник / К. Скиннер - Гревцов Паблишер, 2009.
33. Соколова А. Интернет-банкинг: отражение реальности // Расчет - 2008. - №8. - С.74.
34. Теренин А. Современные технологии для банка // Банковские технологии - 2008. - №7. - С.23.
35. Титюнник А.В. Информационные технологии в банке. ИТ-менеджмент, операционное управление, управление проектами, практические решения / А.В. Титюнник, А.С. Шевелев. - М.: ИД "БДЦ-пресс", 2008. - 368 с.
36. Шестопалова Н. iFin-2007: в поисках мобильности // PC Week Mobile. - 2008. - №3. - С.16.
37. 1. Модин Е. ДБО в зоне риска // (электронный ресурс) - www.alladin.ru 17.02.2009.
38. [www.bankir.ru](http://www.bankir.ru) (электронный ресурс).
39. Интернет-портал www.bifit.com (электронный ресурс).
40. Интернет-портал [www.rbc.ru](http://www.rbc.ru) (электронный ресурс).