ИНИСТ

АВТОМАТИЗАЦИЯ ФИНАНСОВЫХ И ФОНДОВЫХ ОПЕРАЦИЙ, ИНТЕРНЕТ-ТЕХНОЛОГИИ

Программа ИНИСТ Банк-Клиент

Техническое описание и система безопасности

МОСКВА, 2008

1. Архитектура системы

В этом разделе описываются основные понятия, используемые в системе Банк-Клиент, компоненты системы и пользователи системы. Данная информация необходима для понимания принципов функционирования системы.

1.1. Участники системы

Участниами системы Интернет Банк-Клиент являются юридические и физические лица, заключившие договор, определяющий их взаимоотношения в рамках Системы. Все участники системы делятся на два типа: *Центр* и *Клиент*.

Центр – основной участник системы, обеспечивающий весь документооборот между клиентами и банком.

Клиент – юридическое или физическое лицо, использующее возможности, предоставляемые системой для документооборота и управления счетами.

Система образует структуру с одним центром и произвольным числом клиентов. Клиенты связываются с центром, используя средства сети Интернет, через локальную сеть по прямому IP-соединению или через модем по коммутируемым либо по выделенным линиям.

Основным различием между *Центром* и *Клиентом* системы являются предоставляемые им возможности.

Клиент системы может:

- осуществлять управление своими счетами через *Центр*;
- получать информацию с Доски объявлений *Центра*;
- пользоваться справочной информацией, предоставляемой *Центром*.

Центр системы может:

- устанавливать и регистрировать новых *Клиентов* системы;
- осуществлять управление документооборотом;
- размещать информацию на Доске объявлений и редактировать ее;
- редактировать справочники, предоставляемые *Клиентам* системы.

1.2. Пользователи системы

Непосредственное управление документооборотом осуществляется персоналом, расположенным в *Центре*. В зависимости от предоставленных им прав доступа к информации, лица, осуществляющие управление Системой делятся на *администраторов* системы и *операторов*.

Права *администратора* системы

Администратор системы может регистрировать новых операторов и устанавливать уровень их привелегий в системе, изменять уровень привелегий зарегистрированного оператора и удалять операторов из системы. В обязанности администратора входит также обслуживание системы, периодическая архивация данных и обеспечение бесперебойной работы. Для осуществления этих задач администратор имеет доступ к *журналу действий* и *журналу ошибок*. Также администратор должен проводить необходимые действия для обеспечения работы базы данных ORACLE и ОС UNIX на серверной части комплекса. Администратор системы имеет доступ ко всем документам и может выполнять любые действия, доступные операторам системы.

Права *оператора* системы

Оператор системы может производить обработку полученных от клиента документов в соответствии с уровнем своих привелегий. Уровень привелегий оператора определяется администратором системы при регистрации.

1.3. Принципы работы системы Банк-Клиент

Система Банк-Клиент фирмы ИНИСТ реализована на основе архитектуры клиент-сервер. Это позволяет сочетать высокую эффективность работы программного комплекса с надежностью хранения данных и гарантированной защитой от несанкционированного доступа. Применение стандартных и хорошо зарекомендовавших себя средств разработки обеспечивает свободную переносимость комплекса на более мощную технику при росте поставленных перед комплексом задач.

Если клиент работает с банком через Web-интерфейс, единственным требованием является наличие на его компьютере программы Microsoft Internet Explorer версии 4.0 или выше. Клиенты системы используя Web-броузер подключаются к Web-серверу банка через сеть Internet либо через коммутируемую или выделенную линию, как это показано на рисунке.

Сформированные пользователем документы обрабатываются работающими на сервере Java-сервлетами и помещаются в базу данных на серверной части. Также Java-классы обеспечивают динамическую генерацию страниц, содержащих запрашиваемые пользователем данные. Безопасность данных при передаче обеспечивает многоуровневая цифровая подпись под документом, применение стандартных протоколов защиты информации и использование на клиентской машине специального элемента OCX, сертифицированного VeriSign.

В качестве Web-сервера используется являющийся наиболее распространенным на сегодняшний день сервер Apache, работающий под управлением ОС UNIX или Windows NT 4.0 / 2000. Защита Web-сервера осуществляется стандартными средствами Apache и установленной на сервере операционной системы.

Сервер базы данных системы реализован на базе СУБД ORACLE, работающей под управлением ОС UNIX либо Windows NT 4.0 с установленным Service Pack 6.

Персонал Центра системы использует стандартные персональные компьютеры с процессором фирмы Intel и установленной операционной системой Microsoft Windows. Для управления документооборотом и взаимодействия с внутрибанковским ПО используется Рабочее место оператора банка фирмы ИНИСТ.

Таким образом, при работе клиента через Web-интерфейс обработка документов в системе производится следующим образом: клиент, используя стандартный обозреватель Internet Explorer заполняет экранные формы требуемых банковских документов. Java-классы, работающие на Web-сервере, обрабатывают полученные данные и помещают их в базу данных. Операционист банка, использующий рабочее место фирмы ИНИСТ, получает информацию о новых документах и отправляет их на обработку внутрибанковскому ПО. Данное действие может производиться и автоматически, если система настроена требуемым образом. Ответы от внутрибанковского ПО также помещаются в базу данных. По запросу, поступающему от клиента Java-сервлет осуществляет извлечение требуемой информации из базы данных и формирует HTML-страницу с необходимой информацией, передаваемую клиенту.

Если клиент работает с банком через программу «Удаленное клиентское место», разработанную фирмой ИНИСТ, то в этом случае на клиентском компьютере должен быть установлен компонент DAO 3.5 (входящий в комплект поставки MS Office, либо поставляемый отдельным дистрибутивом), программа Microsoft Internet Explorer версии не ниже 4.0 и коммуникационный пакет «Удаленный доступ к сети» из дистрибутива Windows.

Клиент использует стандартные коммуникационные возможности системы Windows для подключения к серверу Банка. Связь может осуществляться непосредственно по коммутируемому каналу с использованием протоколов канального уровня таких, как PPP или X.25, протокола сетевого уровня IP, либо, как и в случае работы через Web-интерфейс клиент может использовать прямое IP-соединение с банком посредством Internet или локальной сети.

На стороне банка в зависимости от операционной системы компьютера (Windows, Linux, Unix и т.п.) должен быть установлен соответствующий системный сервис удаленного доступа (RAS, RRAS, PPPD и т.п.), обслуживающий модемный пул, и транспортная станция фирмы ИНИСТ, принимающая и обслуживающая запросы и команды Удаленного клиентского места, а так же осуществляющая взаимодействие с СУБД ORACLE.

Сформированные на стороне клиента документы, сообщения, получаемые из банка ответы на соответствующие команды, выписки, а так же различные справочники и прочие данные хранятся в локальной БД на компьютере клиента под управлением СУБД Access. В локальной БД фиксируется вся информация о текущей работе и протоколируются все действия пользователей. Администратор системы может получить разнообразные формы отчетов, представляющие протоколируемую информацию в систематизированном виде.

Для предотвращения несанкционированного доступа к базе данных клиента предусмотрена процедура идентификации пользователя по имени и паролю, выполняемая при запуске системы. Кроме того, для совершения операций, требующих аутентификации, необходимо обладать соответствующим уровнем полномочий, устанавливаемых Администратором системы Банк-Клиент, и знанием кодовой фразы, посредством которой шифруется секретная информация в БД клиента. Безопасность данных при передаче обеспечивается посредством алгоритма шифрования IDEA, а аутентификация подлинности документа обеспечивает система многоуровневых цифровых подписей под документом.

Цикл документооборота при использовании удаленного клиентского места происходит следующим образом: клиент, используя установленную на его компьютере программу, создает документы, которые сохраняются в локальной базе данных. В процессе создания документов пользователь может использовать различные справочники (справочник БИКов, корреспондентов, валют, назначений платежа, счетов, бенефициаров, SWIFT и др.), облегчающие и ускоряющие работу пользователя. Кроме того, в Системе Банк-Клиент реализован импорт из наиболее известных бухгалтерских систем (например: 1С), ускоряющий ввод большого количества документов. При сохранении документов в локальной БД система контролирует документы на правильность заполнения в соответствии с нормативными актами соответствующих государственных организаций. При установлении сеанса связи между клиентским компьютером и транспортной станцией банка, происходит обмен данными между локальной базой данных клиента и сервером БД банка. При этом от клиента передаются сформированные им новые документы, а из базы данных банка клиенту передаются ответы на присланные ранее документы, которые были обработаны АБС, а также обновления справочников и документов, формируемые персоналом банка. Следует так же отметить что во время сеанса связи одновременно с передачей документов система контролирует правильность заполнения соответствующих документов и проверяет их на достоверность.

Серверная часть обоих комплексов практически не различается, причем при условии установки Web-сервера и транспортной станции одновременно банк может обслуживать как клиентов, использующих Web-интерфейс и программу Internet Explorer, так и клиентов, использующих удаленное клиентское место системы Банк-клиент. С точки зрения банка эти клиенты не будут отличаться друг от друга.

Рисунок 1. Структурная схема системы ИНИСТ Банк-Клиент

2. Документооборот в системе

Основной единицей, обрабатываемой системой Банк-Клиент является *документ*. Каждый документ характеризуется *типом документа* и *состоянием документа* в системе. Также с каждым документом связаны форма отображения на экране, печатная форма и набор операций, которые можно выполнить с этим документом.

Экранная и печатная форма документа разрабатываются банком и становятся доступными для клиентов при подключении к системе.

2.1. Типы документов

Тип документа определяет операции, которые может производить над ним система и тип получаемого клиентом ответа. Система Банк-Клиент может работать со следующими основными типами документов:

- рублевое платежное поручение;
- выписка по рублевым счетам;
- заявление на перевод валюты;
- заявление на покупку валюты;
- заявление на продажу валюты;
- поручение на продажу валютной выручки.

Данный список типов документов является базовым и может произвольно расширяться при соответствующем соглашении между банком-владельцем системы и фирмой-разработчиком.

Еще одной характеристикой типа документа является его происхождение относительно *Центра* системы.

Входящие документы поступают от клиентов и обрабатываются в системе.

Исходящие документы формируются пользователями системы в Центре и рассылаются клиентам.

Для клиентов данное разделение докуметнов действует по противоположному принципу:

Входящие документы поступают клиенту от Центра или от других клиентов.

Исходящие документы формируются клиентом системы и отсылаются в Центр.

2.2. Состояния документа

Состояние документа отражает его положение в системе и результаты его обработки. Переданный клиентом документ может находиться в одном из следующих состояний:

1. **Введен.** Это состояние присваивается документу, который введен клиентом, но еще не утвержден им и не имеет всех необходимых подписей. Это состояние используется при работе с клиентским местом системы Windows Банк-клиент.
2. **Утвержден.** Это состояние присваивается документу после того, как клиент полностью сформировал документ, проставил все необходимые подписи и поставил его в очередь на отправку. Как и предыдущее, это состояние используется при работе с клиентским местом системы Windows Банк-клиент. Документ, находящийся в этом состоянии будет отправлен в банк во время ближайщего активного сеанса связи.
3. **Обрабатывается.** Это состояние присваивается в центре входящему документу сразу после получения его от клиента. В этом состоянии документ находится до его передачи внутрибанковскому ПО.

4. **На исполнении.** Документ будет переведен в состояние «на исполнении» после его передачи на исполнение внутрибанковскому ПО. В этом состоянии документ будет находиться до его возвращения из опердня в систему.
5. **Отменен.** Если от клиента поступило сообщение об отмене обработки переданного ранее документа, то соответствующий документ будет переведен в состояние «отменен». Отменить можно только документы, находящиеся в состоянии «обрабатывается».
6. **Завершен без ошибки.** Если Система получила от опердня информацию об успешном исполнении документа, его состояние изменяется на «завершен без ошибок». Любой документ можно также исполнить в опердне вручную, не прибегая к встроенным средствам системы. В этом случае состояние документа изменяется при формировании оператором системы ответа клиенту.
7. **Завершен с ошибкой.** Документ переводится в это состояние, если программа обнаружила в нем какую-либо ошибку. Если ошибку обнаружил оператор системы, он может перевести документ в это состояние, сформировав соответствующий ответ клиенту.

При переходе документа из одного состояния в другое Центр системы формирует соответствующий ответ, который отправляется клиенту для информирования о процессе обработки его документа в системе. Возможны следующие варианты ответов:

1. **Дальнейшая обработка.** Оператор системы может сформировать данный ответ, чтобы отправить клиенту любую информацию, связанную с конкретным документом. После получения документа от клиента система автоматически посылает такой ответ с комментарием «***получен банком***». Данный ответ можно сформировать только для документов, находящихся в состоянии «обрабатывается», при этом состояние документа не изменяется.
2. **Отправлен на исполнение.** Система автоматически формирует ответ этого типа при передаче документа внутрибанковскому ПО для исполнения. Если оператор отправляет документ на исполнение вручную (не пользуясь встроенными средствами системы), ему необходимо сформировать ответ этого типа для изменения состояния документа.
3. **Успешное завершение.** Ответ данного типа автоматически формируется системой после получения информации об успешном исполнении документа в опердне банка. Если оператор проводил документ через внутрибанковское ПО, не используя средства системы, то он должен сформировать ответ данного типа для перевода документа в состояние «завершен без ошибки». При этом можно не формировать промежуточный ответ «отправлен на исполнение», а переводить документ в состояние «завершен без ошибки» из состояния «обрабатывается».
4. **Ошибка.** Данный ответ формируется при обнаружении какой-либо ошибки в документе клиента. В поле комментария оператор указывает причину возникновения ошибки, например «***Неверно заполнено назначение платежа***».
5. **Отмена.** Если клиент отменяет ранее переданный им в банк документ, то Система автоматически формирует ответ этого типа с комментарием «***Отменено оператором***».

3. Схема документооборота в Центре

Ознакомившись с основными понятиями, связанными с прохождением документов в Системе, рассмотрим схему документооборота, приведенную на рисунке 2.

Клиент системы формирует необходимый документ, используя полученную от банка экранную форму, и передает его в банк, пользуясь средствами Интернет или линиями связи. Полученный банком документ помещается в таблицу входящих документов и ему присваивается состояние «обрабатывается». При этом клиенту автоматически передается ответ типа «дальнейшая обработка» с комментарием «***получен банком***».

Если для данного типа документов предусмотрена автоматическая обработка, то Система сразу же передает документ на исполнение опердню банка, переводя его в состояние «на исполнении».

Если автоматическая обработка для документа не предусмотрена, то Система оставляет документ в состоянии «обрабатывается», пока оператор не передаст документ

на исполнение внутрибанковскому ПО. При этом изменяется состояние документа и клиенту отсылается сообщение «передано на исполнение».

Пока документ находится в состоянии «обрабатывается», клиент может отменить его, послав соответствующее сообщение системе. В этом случае документ переводится в состояние «отменен», и клиенту передается сообщение типа «отмена» с комментарием «***отменено оператором***».

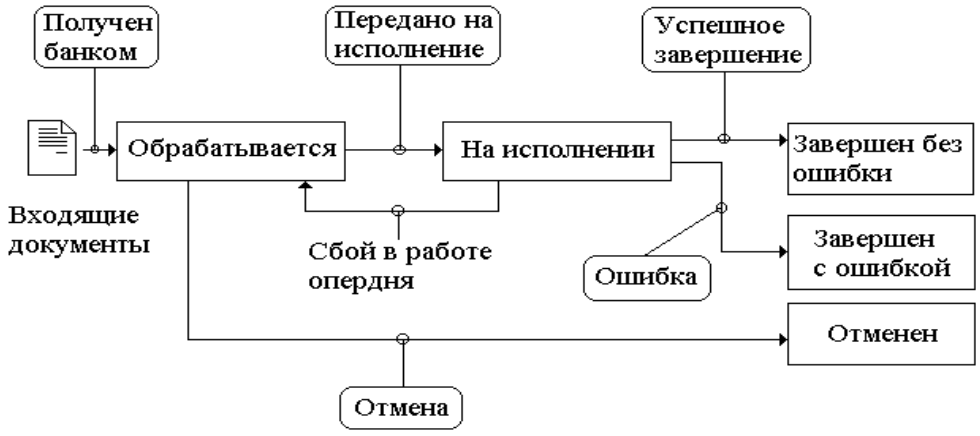

Рисунок 2. Схема документооборота в системе Банк-Клиент

Возможна ситуация, когда из-за программных или аппаратных сбоев в опердне банка выполнение переданного на исполнение документа становится невозможным. Такие документы возвращаются обратно в Систему и переводятся в состояние «обрабатывается».

Обработанные в опердне банка документы возвращаются в систему и, в зависимости от результата обработки внутрибанковским ПО, документ переводится либо в состояние «завершен без ошибки», либо в состояние «завершен с ошибкой».

Перевод документа в состояние «завершен без ошибки» сопровождается передачей клиенту сообщения с типом «успешное завершение». Получение этого сообщения свидетельствует о том, что документ был выполнен банком и не содержал ошибок.

При переводе документа в состояние «завершен с ошибкой» клиенту передается сообщение типа «ошибка» с кратким описанием возникшей проблемы. Для выполнения такого документа клиенту необходимо исправить ошибку и снова передать документ в систему.

Прохождение документов в системе может осуществляться как автоматически, так и вручную под управлением оператора. При автоматической обработке все сообщения формируются и отсылаются системой без вмешательства оператора. При ручной обработке оператор сам следит за состоянием документа и формирует ответы, передаваемые клиенту.

3. Требования к аппаратному и программному обеспечению

Система Банк-Клиент, как видно из рисунка 1, делится на несколько функционально законченых модулей:

1. Сервер базы данных ORACLE
2. Web-сервер
3. Транспортная станция
4. Рабочее место оператора системы
5. Рабочее место клиента, использующего Web-интерфейс
6. Рабочее место клиеннта, использующего Удаленное клиентское место

Ниже рассмотрены требования к программному и аппаратному обеспечению, необходимому для стабильной работы системы.

3.1. Сервер базы данных

Для работы системы Банк-Клиент необходим сервер базы данных, отвечающий следующим требованиям:

Требования к аппаратному обеспечению

- **Процессор**: Pentium II 600МГц и выше.
- **ОЗУ**: 256M
- **Свободно на HDD**: не менее 10 Гбайт.

Требования к программному обеспечению

- ОС Unix, Linux, Windows NT4 с установленным Service Pack 6 или Windows 2000
- СУБД Oracle версии 8.x.x.

4.2. Web-сервер

Чтобы клиенты системы могли работать через Web-интерфейс необходим Web-сервер, отвечающий следующим требованиям:

Требования к аппаратному обеспечению

- **Процессор**: Pentium II 600МГц и выше.
- **ОЗУ**: 256M
- **Свободно на HDD**: не менее 200 Мбайт.

Требования к программному обеспечению

- ОС Unix, Linux, Windows NT4 с установленным Service Pack 6 или Windows 2000
- Apache версии не ниже 1.3.14.
- Apache JServ версии не ниже 1.1.2.
- JDK версии не ниже 1.1.8. (рекомендуется 1.3.1)
- JSDK версии 2.0.

4.3. Транспортная станция

Чтобы клиенты системы могли использовать Удаленное клиентское место в банке необходимо установить транспортную станцию на компьютере отвечающем следующим требованиям:

Требования к аппаратному обеспечению

- Процессор: Pentium II 600МГц и выше.
- ОЗУ: 256М
- HDD: не менее 200 Мбайт

Требования к программному обеспечению

- ОС Unix, Linux, Windows 2000 или Windows NT4 с установленным Service Pack 6
- JDK версии 1.1.8.
- Стандартные программы для работы с модемом и TCP/IP протоколом.

Сервер базы данных, Web-сервер и транспортная станция могут работать совместно на одной машине. В этом случае рекомендуется использовать компьютер, отвечающий следующим требованиям:

- Процессор: Pentium II 800МГц и выше.
- ОЗУ: 512М
- HDD: не менее 12 Гбайт.

4.4. Рабочее место оператора

Для работы оператора системы используются одно или несколько рабочих мест оператора. Рабочие места соединяются с сервером посредством сети. Компьютер, на который будет установлено рабочее место оператора должен отвечать следующим требованиям:

Требования к аппаратному обеспечению

- **Процессор**: Pentium 233МГц и выше.
- **ОЗУ**: 32М
- **Свободно на HDD**: не менее 100 Мбайт.

Требования к программному обеспечению

- ОС Windows 95/98/Me, Windows 2000 или Windows NT4 с установленным Service Pack 6
- Internet Explorer версии 5.0 и выше.
- Клиентская часть СУБД Oracle версии 8.x.x и выше.
- BDE версии не ниже 4.0.

4.5. Рабочее место клиента, использующего Web-интерфейс

Компьютер, используемый клиентом для работы с системой через Web-интерфейс, должен удовлетворять следующим требованиям:

Требования к аппаратному обеспечению

- **Процессор**: Pentium 133 и выше.
- **ОЗУ**: 16М

Требования к программному обеспечению

- ОС Windows 95/98/Me, Windows 2000 или Windows NT4 с установленным Service Pack 6
- Internet Explorer версии не ниже 5.0.

4.6. Рабочее место клиента, использующего Удаленное клиентское место

Компьютер, используемый клиентом для работы с системой с использованием удаленного клиентского места, должен удовлетворять следующим требованиям:

Требования к аппаратному обеспечению

- **Процессор:** Pentium 200 и выше
- **Память:** не менее 64 Мбайт
- **HDD:** не менее 2 Гбайт.

Требования к программному обеспечению

- Операционная система Windows 95/98/Me, NT4/2000
- DAO версии не ниже 3.5. DAO 3.5. входит в стандартную поставку пакета Microsoft Office.

5. Вопросы безопасности

При работе с банковской информацией встают вопросы безопасности при передаче информации по линиям связи и защиты от возможных подделок со стороны клиентов или других лиц.

Безопасность системы Банк – Клиент основывается на следующих основных положениях:

- Использование стандартных средств безопасности, встроенных в используемую на серверной части комплекса ОС и СУБД Oracle.
- Использование стандартного протокола SSL для защиты передаваемой информации по открытым каналам связи.
- Использование "Аналога Собственной Подписи" для предотвращения подделки документов как со стороны клиента, так и со стороны других лиц.
- Поддержка системного журнала, в котором регистрируются все существенные действия операторов и клиентов, а также их ошибки и попытки запрещенных действий.

5.1. Протокол SSL

Протокол SSL является, фактически, стандартом при решении задачи защиты данных, передаваемых по Интернету. Большинство современных WEB-серверов и WEB-броузеров обладают встроенной поддержкой данного протокола. Использование данного протокола позволяет решить следующие задачи:

- Аутентификация WEB-сервера. Данная процедура гарантирует, что клиент системы связывается с конкретным сервером системы, имеющим определенный международный сертификат.
- Генерация уникального сессионного ключа. Наличие сессионного ключа позволяет обеспечить защиту данных, даже если в одной конкретной сессии (в одном сеансе связи) она была нарушена.
- Передачу данных по интернету в защищенном виде, гарантирующем безопасность данных.

5.2. Аналог собственной подписи клиента

Для защиты банковских документов от подделок каждый клиент системы использует электронный Аналог Собственной Подписи. Кратко рассмотрим основные моменты использования этого механизма защиты:

- Каждый клиент системы, обладает одним или несколькими ключами для создания Аналога Собственной Подписи под произвольным электронным документом. Аналог Собственной Подписи может быть создан с использованием одного из двух алгоритмов: *надежного* и *упрощенного*. Выбор конкретного алгоритма производится заблаговременно при совместном участии клиента и ответственного сотрудника банка.
- Надежный алгоритм основан на реализации алгоритма RSA. Минимальная длина ключа – 512 байт. Ключевая информация хранится на компьютере пользователя в виде файла, закрытого кодовой фразой. Таким образом реализована двойная защита: постороннее лицо, каким-либо образом получившее ключевой файл, все равно не сможет использовать его не зная кодовой фразы. При использовании этого метода защиты банк, получающий Ваши документы также не сможет создать под документом Ваш аналог собственной подписи.
- Упрощенный алгоритм основывается на знании секретной информации: *кода пользователя* и его *пароля*. Аналог Собственной Подписи формируется на основе алгоритма IDEA. Применение данного алгоритма не приводит ни в каком виде к передаче по открытому каналу пароля пользователя. Для работы упрощенного

алгоритма по созданию Аналога Собственной Подписи не требуется хранение секретной информации на диске, но данный алгоритм предполагает, что проверяющая сторона (банк) может не только проверить подпись, но и создать ее.

- Банк, как одна из сторон системы, также обладает своими ключами для создания подписи на основе надежного алгоритма.
- Клиенты банка производят генерацию своей ключевой информации непосредственно в офисе банка. Открытая сторона ключей сохраняется в базе данных банка. Ключи надежного алгоритма хранятся в подписанном виде, упрощенного алгоритма – в закрытом виде.
- Создание Аналога Собственной Подписи производится на рабочем месте клиента непосредственно при работе с системой. Для этого разработаны специализированные активные элементы (ActiveX), передаваемые клиенту по Интернету при обращении к первой WEB-страницы системы Интернет Банк-Клиент. Аналог Собственной Подписи формируется клиентом под каждым значимым документом системы.
- Проверка Аналога Собственной Подписи производится на стороне банка сразу при получении документа (команды). Только при прохождении проверки по аутентичности принятых данных производится исполнение принятой команды. Ни одна команда клиента банка не будет исполнена, если не пройдет контроль правильности Аналога Собственной Подписи под принятым документом.

Система хранит все полученные по Интернету документы и все ключи клиентов. Тем самым, в любой момент можно осуществить повторную проверку подписи под любым из хранимых документов.

Контакты

ЗАО «ИНИСТ»

Адрес: 119991, Москва, 5-й Донской проезд, д. 15, стр. 2

Телефон: +7 (495) 956 36 26

Факс: +7 (495) 956 75 04

E-mail: info@inist.ru

Сайт: http://inist.ru

Генеральный директор: Ревенок Дмитрий Андреевич