МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ

ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Защита удаленных банковских транзакций

Исполнитель Кин Илья Сергеевич

Руководитель Начальник НИО ПДТР и ТЗИ

Алейникова Оксана Вячеславовна

«К защите допускаю»

Заведущий кафедрой

профессор, доктор технических наук

Бурлов Вячеслав Георгиевич

«17» февраля 2017г.

Санкт-Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ

ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Защита удаленных банковских транзакций

Исполнитель Кин Илья Сергеевич

Руководитель Начальник НИО ПДТР и ТЗИ

Алейникова Оксана Вячеславовна

«К защите допускаю»

Заведущий кафедрой _____

профессор, доктор технических наук

Бурлов Вячеслав Георгиевич

«___»_____20__г.

Санкт-Петербург

2017

Содержание

ВВЕДЕНИЕ

История появления электронных денег начинается в 1993 году. Тогда Дэвид Чаум изобрел электронные деньги. Система называлась eCash, принцип действия которой лежит в большинстве существующих электронных платежных системах. Идея системы eCashсостояла в том, чтобы наличность хранилась на электронных носителях – жестких дисках, а для управления ею требовалось специальное программное обеспечение и подключение к интернету. В России первой системой электронных платежей является CyberPlat.

Не для кого не секрет, что в современном мире использование безналичных расчетов становится все более актуальным. Люди все чаще оплачивают покупки банковскими картами, используют мобильные банки и другие средства электронных платежей для оплаты покупок в интернет - магазинах, а также для перевода средств с одной карты на другую. Организации используют безналичные расчеты для перевода средств другим организациям, поставщикам, и при расчете с клиентами.

В связи с такой тенденцией появляется всё больше злоумышленников, которые постоянно находят различные пути несанкционированного доступа к чужим средствам. В 2013 - 2016 годах денежные потери банков России из – за деятельности интернет - мошенников составили порядка 100 млн. евро. В 2014 году мошенники незаконно списали с карт россиян 1,58 млрд рублей.[1,2,3,4]

Именно поэтому цель моей работы можно считать одной из самых актуальных в современном мире.

Целью данной работы является: выявление недостатков методов защиты информации для повышения уровня защищенности от несанкционированного доступа к средствам банка и клиентов на примере банк – клиентов таких банков, как: Газпромбанк, ВТБ, СберБанк, НовикомБанк, Федеральное казначейство РФ.

Задачи:

– Анализ информационной банковской системы;

– Выявление уязвимостей безопасности информации при использовании банковских транзакций;

– Разработка и выбор оптимальной системы защиты удаленных банковских транзакций.

1 АНАЛИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ, ОБЕСПЕЧИВАЮЩЕЙ ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ

1.1 Информационная банковская система

Информационная система – это программно – аппаратный комплекс, предназначенный для автоматизированного сбора, хранения, обработки и передачи информации.

Информационная система банка (ИБС) – программно – аппаратный комплекс, обеспечивающий с использованием специализированных банковских технологий автоматизацию обработки банковской информации, отражающей различные стороны деятельности банков.

Структурно ИБС состоит из множества различных элементов, разделенных по определенным признакам:

– объектным, определяется разветвленной структурой банка;

– функциональным, соответсвует назначению каждого из блоков ИБС;

– модульным, исходит из технологии разработки программного обеспечения ИБС;

– информационным, устанавливает правила использования информационных массивов ИБС.

Наиболее общие разделение подсистем ИБС - выделение функциональной и обеспечивающей частей. Функциональная часть фактически является моделью системы управления объектом. Применительно к системам управления признаком структуризации могут служить функции управления объектом, в соответствии с которыми ИБС состоит из функциональных подсистем. Обеспечивающая часть ИБС состоит из информационного, технического, программного, организационного, правового и других видов обеспечения.

Функциональная часть определяется совокупностью решаемых задач, выделенных по определенным видам деятельности различных хозяйствующих объектов.

Обеспечивающая часть - это комплекс взаимосвязанных средств определенного вида, которые обеспечивают функционирование системы в целом или ее отдельные элементы. Обеспечивающие подсистемы состоят из: информационного обеспечения, технического обеспечения, математического обеспечения, правового обеспечения, программного обеспечения, организационного обеспечения, технологического обеспечения.

Одним из самых популярных видов банковского обслуживания является удаленное обслуживание клиентов или Дистанционное банковское обслуживание.

Дистанционное банковское обслуживание – это технологии предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом, чаще всего используя компьютер и телефонные сети. Виды Дистанционного банковского обслуживания включают в себя следующие системы:

– доступ к счетам происходит через модем и общую телефонную сеть (Клиент – Банк);

– счета клиентов обслуживаются через интернет – это есть подсистема «Интернет – Клиент». Доступ к счету происходит через стандартные средства доступа к Интернет;

– система автоматического обслуживания клиентов по телефону.

Структурная схема информационной системы удаленного банковского обслуживания изображена на рисунке 1.

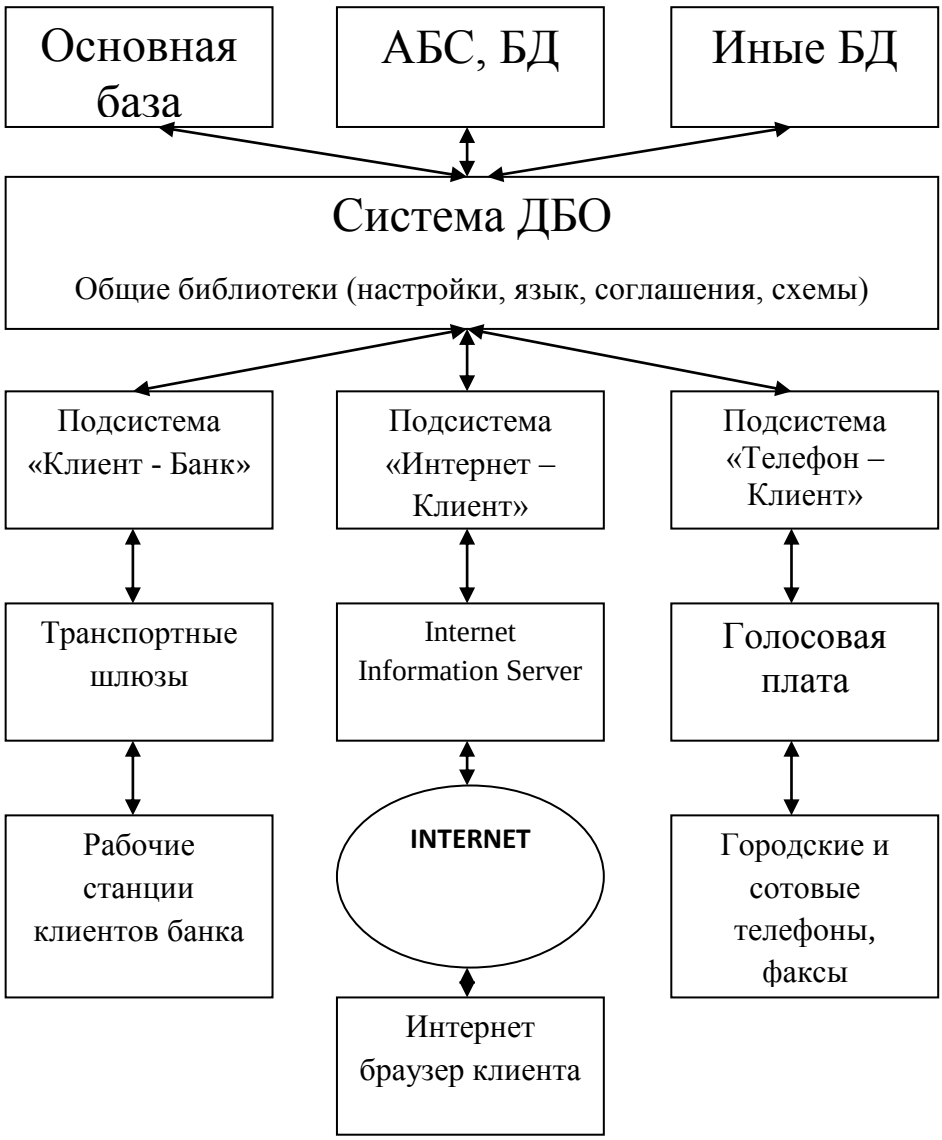

Рисунок 1 – Структурная схема информационной системы удаленного банковского обслуживания

1.2 Банковская транзакция

Операция перевода, ввода, вывода денежных средств со счета, в том числе и с помощью систем Дистанционного банковского обслуживания, называются банковскими транзакциями.

Типичная схема проведения банковской транзакции изображена на рисунке 2.

Этапы прохождения банковской транзакции:

1 - Передача данных счета от ОРГ1 к ОРГ2 в момент оплаты товара или услуги;

2 и 2А - Проверка наличия средств на счете (запрос – ответ);

3 – Изготовление слипа у ОРГ2;

4 – Продажа продукции или оказание услуг;

5 – Предоставление в банк – эквайрер слипов;

6 – Предъявление слипов в банк – эмитент для оплаты;

7 – Списание средств со счета ОРГ1 в банке – эмитенте, перечисление их на счет в банк эквайрер;

8 – Зачисление средств на счет ОРГ2;

9 – Уведомление ОРГ2 о зачислении денежных средств;

10 – Уведомление ОРГ1 о списании денежных средств.

Банк – эквайер – это что то вроде посредника между организацией и банком, в котором открыт счет.

Банк – эмитент – это банк, в котором был открыт счет.

Расчетный банк - уполномоченный платежной организацией соответствующей платежной системы банк, открывает счета членам платежной системы и принимает участие в проведении взаиморасчетов между ними.

Процессинговая компания обеспечивает информационное и технологическое взаимодействие между участниками расчетов.

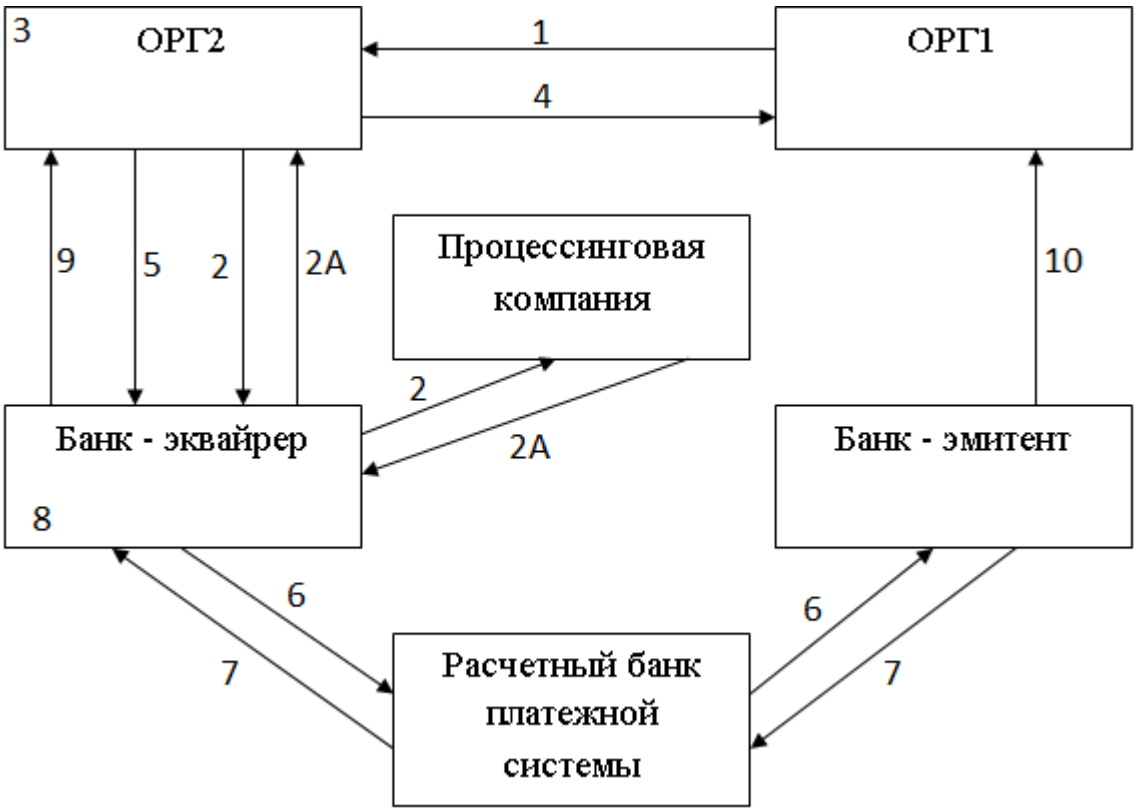

Рисунок 2 – Схема прохождения банковской транзакции

Одним из самых уязвимых мест прохождения банковской транзакции является приложение Клиента, установленное на персональном компьтере в организации, так как оно подвержено, как техническим угрозам информационной безопасности, так и человеческому фактору.

Систему Клиент – Банк в современном мире используют практических на каждой организации, так как она обеспечивает быстрый, удобный ввод информации, ее первичную обработку и любое внешнее воздействие банка с клиентами. В основе системы Клиент – Банк лежит программный продукт «Клиент», который реализует следующие важные функции:

– формирование базы платежных поручений клиента, а также ее автоматическое изменение по данным полученным из банка;

– осуществление модемной связи клиента с банком с целью передачи платежный поручений для списания сумм со счетов клиента;

– формирование и использование базы архивных платежных документов . [5,6]

2 АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ УДАЛЕННЫХ БАНКОВСКИХ ТРАНЗАКЦИЙ

2.1 Особенности информационной безопасности банков

Стратегия информационной безопасности банков весьма сильно отличается от аналогичных стратегий других компаний и организаций. Это связано с тем, что угрозы имеют специфический характер.

Информационная безопасность стандартной компании направлена на защиту информации от конкурентов, а также защиту информации от налоговых органов и преступных сообществ. Интересует такаяинформация узкий круг лиц и организаций и редко бывает ликвидна (обращение в денежную форму).

Хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги. Информация на компьютере служит основанием для проведения выплат, открытия кредитов, т.е. происходит оборот значительных сумм. Поэтому незаконные действия с данной информацией могут пагубно отразиться на всей деятельности компании.

Банковская информация затрагивает интересы многих людей и организаций — клиентов банка.Такая информация конфиденциальна, поэтому в обязанности банка входит обеспе чение секретности, за что несет ответственность перед клиентами.

На конкурентоспособность банка влияют многие обстоятельства:

– степень удобства работы с банком,

– широта спектра предоставляемых услуг, в т.ч.удаленные услуги и иные.

Информационная безопасность банка направлена, прежде всего, на обеспечение высокой надежности работы компьютерных систем, ведь на кону стоят денежные средства и банка и его клиентов.Банк осуществляет хранение важной информации о своих клиентах. Такой подход обеспечивает банку

возможность знать все о потенциальных злоумышленниках, которые заинтересованы в причинении вреда банку.

Преступления в банковской сфере отличаются специфическими чертами:

– достаточно большое количество финансовых преступлений не оглашается, по причине того, что руководители банка опасаются порчи своей репутации как надежного хранителя средств, что может привести к потере клиентуры.

– злоумышленники обычно являются клиентами этого банка, т.е. имеют собственные счета в нем. На этот счет переводятся похищенные суммы.

– чаще всего компьютерные преступления – мелкие.

– крупные же преступления, требуют проведения нескольких операций и большого терпения.

– большая часть преступников — клерки, руководство банка гораздо реже совершает такие преступления, но наносит значительный вред банку.

– преступления в компьютерной сфере не всегда высокотехнологичны. Чаще всего они связаны с подделкой данных, изменением параметров среды автоматизированных систем обработки информации банков (АСОИБ) и т.д., чаще всего преступники придумывают легенду о том, что они «берут в долг» деньги у банка, и затем не возвращают.

Задачи, которые решает АСОИБ делятся на:

– аналитические (задачи планирования, анализа счетов и т.д.). Это не оперативные задачи, для их решения необходимо много времени, и результат может оказать влияние на политику банка в отношении конкретного клиента или проекта. Решение таких задач предполагает использование не мощных вычислительных ресурсов (10-20 %мощности всей системы);

– повседневные. Это насущные задачи: корректировка счетов и выполнение платежей. От них зависит размер и мощность основной системы банка . Для того, чтобы их решить необходимо использовать большое количество ресурсов. Информация, при решении таких задач, имеет временный характер.[6]

2.2 Угрозы безопасности удаленных банковских транзакций

Угрозы безопасности можно разделить на:

- технические угрозы;
- человеческий фактор.

Человеческий фактор может возникнуть из – за ряда причин, например: уволенный сотрудники, решившие отомстить, случайное отключение электропитания, низкая квалификация, халатность.

К техническим угрозам можно отнести:

- компьютерные угрозы (вирусы, черви, и т. д.);
- DOS и DDos атаки;
- снифферы;
- технические средства съема информации;
- ошибки в программном обеспечении..

Также угрозы делятся на преднамеренные и непреднамеренные.

Преднамеренные:

- физическое воздействие на локальную сеть;
- вывод из строя подсистемы обеспечения;
- воздействие на персонал;
- хищение носителей информации;
- несанкционированное копирование информации и доступ к АРМ;
- незаконное получение паролей

Непреднамеренные:

- случайное отключение оборудования;
- ввод неверных данных;
- утрата или передача кому – либо личных данных;
- пересылка данных по ошибочному адресу;
- использование ненадежных сайтов;
- использование ненадежного программного обеспечения.

Остановимся поподробнее на технических преднамеренных угрозах.

Несанкционированным доступом (НСД) называют получение пользователем доступа к объекту, к которому он не имел права подключаться.

По характеру воздействия НСД это активное воздействие, использующее ошибки системы. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам в любом состоянии.

Для реализации НСД существует два способа:

– прекращение действия системы защиты различными способами;

– наблюдение за наборами данных, представляющих интерес для преступника (подбор пароля, например).

НСД может возникнуть по причине необоснованной системы защиты или плохого контроля, и небрежности в организации защиты своих данных.

Помимо вышеуказанного вида компьютерных нарушений существует незаконное использование привилегий. Этот способ предполагает использование злоумышленниками штатного программного обеспечения, функционирующего в нештатном режиме.

Такие средства необходимы, но они могут быть чрезвычайно опасными. Обычно эти средства используют администраторы, операторы, системные программисты и другие пользователи, выполняющие специальные функции.

Уменьшение риска от применения таких средств осуществляется с помощью определенных привилегий: обычные пользователи имеют минимальный набор, администраторы – максимальный. Несанкционированный захват привилегий может привести к несанкционированному выполнению определенной функции (НСД, реконфигурация системы).

Безусловно, каждый злоумышленник мечтает захватить максимальный набор привилегий, ведь это расширит его возможности.

Незаконный захват привилегий возможен либо при наличии ошибок в самой системе защиты, либо в случае халатности при управлении системой и привилегиями в частности.

“Скрытые каналы” - пути передачи информации между процессами системы, которые нарушают системную политику безопасности. В среде с разделением доступа к информации пользователю могут не дать доступ к обработке интересных для него данных. В этом случае он придумывает обманные пути: для этого ему необходимо проявлять наблюдательность и обладать знаниями в области связей.

“Скрытые каналы” реализуются различными путями, в частности при помощи программных закладок (“троянских коней”).

Атаки с использованием скрытых каналов обычно приводят к нарушениям конфиденциальности информации в АСОИБ. Это, как правило, пассивные атаки, нарушается только процесс передачи информации. Для того, чтобы организовать “скрытые каналы” могут использовать и штатное программное обеспечение, и специальные “троянские” или вирусные программы.

Примеры передачи информации по “скрытым каналам”: в итоговом отчете вместо слова “TOTAL” использовано слово “TOTALS”. Это сделано для того, чтобы при определенных условиях произойдет замена слов. Или проставление пробелов между двумя словами, значение третьей или четвертой цифры после запятой в какой-нибудь дроби (на которые никто не обращает внимания) и т.д.

Также можно отметить существование большого количества способов организации связи между двумя процессами системы. Большинство операционных систем имеют в своем распоряжении такие средства, так как они очень облегчают работу программистов и пользователей. Проблема состоит в том, что очень трудно отделить неразрешенные “скрытые каналы” от разрешенных, то есть тех, которые не запрещаются системной политикой безопасности. В конечном счете, все определяется ущербом, который может принести организация“скрытых каналов”.

Отличительные особенности “скрытых каналов”:

– малая пропускная способность (по ним обычно можно передавать только небольшое количество информации);

– трудности в их организации;

– ущерб, наносимый ими, как правило, небольшой или даже не заметен.

При “маскараде” один пользователь АСОИБ от имени другого выполняет определенные действия, причем чаще всего выполнение этих действий другой пользователь сам разрешает. Однако в этом случае запрещается использовать привилегии и присваивать права, в чем собственно и заключается нарушение.

Синонимами такого нарушения являются симуляция или моделирование. “Маскарад” направлен на то, чтобы скрыть какие-либо действия под именем другого пользователя или присво ить права и привилегии другого пользователя для доступа к его наборам данных или для использования его привилегий.

“Маскарад” совершается путем активных действий, а также является опосредованным воздействием, т.к. происходит использование возможностей других пользователей.

Самым ярким примером такого нарушения является использование чужого имени и пароля для осуществления входа в систему. Система защиты не способна распознать это нарушение. Для получения данных другого пользования обычно используют взлом системы.

Другим примером “маскарада” служит присвоение имени другого пользователя в процессе работы: например, у некоторых операционных систем есть возможность изменять имя пользователя в процессе работы или используют специально разработанные программы.

“Маскарадом” также называют передачу сообщений в сети от имени другого пользователя. Существуют различные способы смены идентификатора: ошибка в системе, особенности сетевых протоколов. Приемный узел воспринимает такое сообщение как корректное, и это может привести к серьезным нарушениям. Особенно это касается управляющих сообщений,

изменяющих конфигурацию сети, или сообщений, ведущих к выполнению привилегированных операций.

Самым опасным “маскарадом” является нарушение в банковских системах электронных платежей. Если здесь будет заменена идентификация клиента, возникают большие убытки. Особенно это касается платежей с помощью электронных банковских карт. Система идентификации с помощью персонального идентификатора (PIN) достаточно надежна, однако нарушения могут возникнуть вследствие ошибок его использования: потеря банковской карты, передача PIN недобросовестному лицу и т.д. именно поэтому клиенты обязаны строго соблюдать все рекомендации банка по выполнению такого рода платежей.

“Маскарад” - это достаточно серьезное нарушение, которое может привести к тяжелым последствиям: утечка информации, изменение конфигурации сети, нарушение работы АСОИБ и т.д.

Для того чтобы предотвратить “маскарад” следует использовать:

– проверенные методы идентификации и отождествления,

– блокировку попыток взлома системы,

– контроль входов в нее,

– фиксация всех событий, которые обладают признаками «маскарада» в системном журнале,

– анализ этих событий и т.д.

Следующим видом нарушений является “Сборка мусора”. Послетого, как работа окончена, обработанная информация не всегда полностью удаляется из памяти: какие-то данные остаются в оперативной памяти, на носителях информации.

Данные хранятся на носителе до перезаписи или уничтожения. Когда выполняются эти действия на освободившемся пространстве диска остаются какие-то их части. Эти данные, как правило, трудночитаемые, и для их опознавания необходимо использование специализированных программ. Этот

процесс и называется - “сборка мусора” и может привести к утечке важной информации.

“Сборка мусора” осуществляется с помощью активных действий: происходит непосредственное воздействие на объекты АСОИБ при их хранении с использованием доступа. Такое воздействие приводит к нарушению конфиденциальности информации.

Защита от “сборки мусора” осуществляется посредством специальных механизмов, реализующиеся в операционной системе и/или аппаратуре компьютера или в дополнительных программных (аппаратных) средствах. Примерами таких механизмов являются стирающий образец и меткаполноты:

– стирающий образец — это некоторая последовательность битов, записываемая на место, освобождаемое файлом. Менеджер или администратор безопасности АСОИБ может автоматически активизировать запись этой последовательности при каждом освобождении участка памяти, при этомстираемые данные уничтожаютсяфизически;

– метка полноты предотвращает чтение участков памяти, отведенных процессу для записи, но не использованных им. Верхняя граница адресов использованной памяти и есть метка полноты. Этот способ используется для защиты последовательных файлов исключительного доступа (результирующие файлы редакторов, компиляторов, компоновщиков т.д.). Для индексных и разделяемых последовательных файлов этот метод называется “стирание при размещении”, память очищается при выделении ее процессу.

“Взлом системы” это умышленное активное проникновение в систему с несанкционированными параметрами входа (имя пользователя и пароль). Как правило “Взлом системы” происходит в интерактивном режиме.

Обычно имя пользователя известно всем, оно не засекречивается в графе ввода, и поэтому объектом взлома практически всегда является пароль. Существует множество способов вскрытия пароля:

– перебор возможных паролей (обычно подбирают какие-то важные для настоящего пользователя символы),

– “маскарад” с использованием пароля другого пользователя,

– захват привилегий,

– использование ошибок программы входа.

Когда осуществляется взлом системы, основная нагрузка накладывается на программу входа. Программа входа должна бытьорганизована безупречно: алгоритм ввода имени и пароля, их шифрование (при необходимости), правила хранения и смены паролей не должны содержать ошибок.

«Взлом системы» можно предотвратить ограничением количества попыток неправильного ввода пароля с последующей блокировкой терминала и уведомлением оператора в случае нарушения.

Также оператор обязан регулярно контролировать активных пользователей системы: их имена, характер работы, время входа и выхода и т.д. Такие действия помогут своевременно установить факт “взлома” и позволят предпринять необходимые действия.

Следующим видом нарушения является “Люк” —скрытая, недокументированная точка входа в программный модуль. “Люк” вставляется в программу обычно на этапе отладки для облегчения работы: программный модуль можно вызывать в разных местах, что позволяет отлаживать отдельные его части независимо. Но в дальнейшем программист может забыть уничтожить “люк” или некорректно его заблокировать. Кроме того, “люк” может вставляться на этапе разработки для последующей связи данного модуля с другими модулями системы, но затем, в результате изменившихся условий данная точка входа оказывается ненужной.

Наличие “люка” позволяет вызывать программу необычным образом, что может серьезно сказаться на состоянии системы защиты (неизвестно, как в таком случае программа будет воспринимать данные, среду системы и т.д.). Кроме того, в таких ситуациях не всегда можно прогнозировать ее поведение.

«Люк» является угрозой, которая возникает по причине ошибок реализации какого-либо проекта (АСОИБ в целом, комплекса программ и т.д.). Поскольку использование “люков” может быть самым разным и зависит от

самой программы, классифицировать данную угрозу как-либо еще затруднительно.

“Люки” могут оказаться в программах по следующим причинам:

– их забыли убрать;

– для использования при дальнейшей отладке;

– для обеспечения поддержки готовой программы;

– для реализации тайного контроля доступа к данной программе после ее установки.

В первом случае «забывают» специально, намерено. Это может привести к сбою всей системы. Два следующих случая — серьезные испытания для системы безопасности, с которыми она может и не справиться. Четвертый случай может стать первым шагом преднамеренного проникновения с использованием данной программы.

Отметим, что программная ошибка “люком” не является. “Люк” — это достаточно широко используемый механизм отладки, корректировки и поддержки программ, который создается преднамеренно, хотя чаще всего и без злого умысла. Люк становится опасным, если он не замечен, оставлен и не предпринималось никаких мер по контролю за ним.

Большинство “люков”, особенно в программах операционной системы, компенсируется высокой сложностью их обнаружения. Если неизвестно заранее, что данная программа содержит “люк”, происходит обработка программного кода, чтобы найти его. Очевидно, что это не всегда реализуется, поэтому обнаруживаются “люки”, как правило, случайно. Защита от них предусматривает не допущениепоявления “люков” в программе, а при приемке программных продуктов, разработанных третьими производителями проведение анализа исходных текстов программ с целью обнаружения “люков”.

В последнее время отмечается все больше случаев воздействия на вычислительную систему с помощью специально созданных вредоносных программ – эти программы открыто или косвенно дезорганизуют процесс

обработки информации или способствуют утечке или искажению информации. Такие программы создают на основании данных о существующей системы, с ориентировкой на все ее особенности и защитные элементы.

Подобными программами являются: “троянский конь”, вирус, “червь”, “жадная” программа, “захватчик паролей”.

Программа “Троянский конь” выполня ет в дополнение к основным (проектным и документированным),не описаннымв документации, действия. Название эта программа получила по аналогиис древнегреческим “троянским конем”, и это вполне целесообразно, т.к. с виду программа не вызывает подозрений и кажется вполне обычной, однако состав данной программы является весьма угрожающимАСОИБ.

“Троянский конь” представляет собой активную угрозу, которая реализуется программными средствами, работающими в пакетном режиме. Он может нанести вред абсолютно любому объекту АСОИБ.

Наиболее сильную опасность представляетопосредованное воздействие, при котором “троянский конь” действует в рамках полномочий одного пользователя, но в интересах другого пользователя, установить личность которого порой невозможно.

Опасность “троянского коня” состоит в том, что создается дополнительный блок команд,который каким-то образом вставлен в исходную безвредную программу. Затем данная программа отправляется к пользователю АСОИБ – она может быть подарена, продана, подменена и т.д.

Для того чтобы этот закодированный блок сработал, необходимо чтобы были соблюдены определенные условия (наступление определенной даты, времени, запуск каких-то команд извне и т.д.) Как только программа запущена сразу возникает угроза для всей информации в системе и АСОИБ в целом.

Высокую опасность “троянский конь” несет, если запустивший ее пользователь обладает расширенным набором привилегий. В этом случае злоумышленник, составивший и внедривший “троянского коня”, и сам этими привилегиями не обладающий, может выполнить несанкционированные

привилегированные функции чужими руками. Или, например, злоумышленника очень интересуют наборы данных пользователя, запустившего такую программу. Последний может даже не обладать расширенным набором привилегий — это не помешает выполнению несанкционированных действий.

“Троянский конь” — одна из наиболее опасных угроз безопасности АСОИБ. Для того чтобы эффективно бороться с этой программой необходимо создать замкнутую среду исполнения программ.

Необходимо разделить внешние сети(особенно Интернет) и внутренние сети, по крайней мере, на уровне протоколов, а еще лучше — на физическом уровне.

Кроме того, стоит организовать работу привилегированным и непривилегированны м пользователям с разными экземплярами прикладных программ, которые должны храниться и защищаться индивидуально. При соблюдении этих мер вероятность внедрения программ подобного рода будет достаточно низкой.

Далее поговорим о вирусе. Это программа, обладающая способностью к заражению других программ посредством включения в них своей, возможно измененной, копии. Стоит отметить, что вирусная программа сохраняет способность к дальнейшему размножению. Вирусу присущи следующие особенности:

– способность к самовоспроизведению – в то время как вирус существует и действует на компьютере, он обязательно воспроизводит минимум один раз свою копию на долговременном носителе;

– способность к вмешательству (получению управления) в вычислительный процесс. В этом случае вирус действуют как «паразит» - внедряется в систему и поражает ее отдельные свойства, что в конечном итоге приводит к сбоям в системе, потери важной информации и т.д.Это свойство является аналогом “паразитирования” в живой природе, которое свойственно биологическим вирусам.

По аналогии с “троянским конем” вирус осуществляется путем активного программного воздействия. Классификация вирусов, используемые ими методы заражения, способы борьбы с ними достаточно хорошо изучены и описаны. Эта проблема в нашей стране стала особенно актуальной, поэтому очень многие занимаются ею.

Проблема защиты от вирусов может рассматриваться с двух сторон: как самостоятельная проблема, и как одна из сторон проблемы общей защиты АСОИБ. И тот, и другой подходы имеют свои отличительные особенности и, соответственно, свои собственные методы решения проблемы.

В последнее время удалось более или менее ограничить масштабы заражений и разрушений. Тут сыграли свою роль и превентивные меры, и новые антивирусные средства, и пропаганда всех этих мер.

В целом проблема вирусов может стать тем толчком, который приведет к новому осмыслению как концепций защиты, так и принципов автоматизированной обработки информации в целом.

“Червем” называют программу, которая распространяется через сеть и (в отличие от вируса) не оставляет своей копии на магнитном носителе. “Червь” использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Наиболее известным представителем этого класса выступает вирус Морриса (“червь Морриса”), поразивший сеть Internet в 1988 г.

Наиболее благоприятной средой для распространения “червя” является сеть, в которой взаимодействие пользователей основано на дружественных связях и доверии. Кроме того, если в сети нет механизма осуществления защиты, то «червь» будет распространяться крайне быстро.

Самым эффективным способом защиты сети от «червя» являются меры предосторожности против несанкционированного доступа к сети.

Захватчиками паролей являются программы, которые специально созданы для того, чтобы взламывать и воровать пароли.

Суть действия данной программы заключается в том, что, когда осуществляется попытка входа, происходит имитация ввода имени и пароля, пересылаемые владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе.

Пользователь по началу думает, что допустил ошибку в пароле, и затем , осуществив последующий вход в систему, получает к ней доступ. Однако программа-захватчик уже считала его данные и может ими свободно пользоваться в дальнейшем. Кроме того, считывание пароля может осуществляться и другим способом - с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Для предотвращения этой угрозы перед входом в систему необходимо убедиться, что ввод имени и пароля осуществляется именно в системную программу входа, а не в какую-то другую. Помимо этого, обязательным условием соблюдения безопасности является соблюдение правил использования паролей и работы с системой. Это связано с тем, что большинство взломов осуществляется именно по причине обычной небрежности самого пользователя.

Эти простые действияпомогут избежать захвата пароля:

– не рекомендуется покидать рабочее место, не выйдя из системы,

– следует постоянно проверять сообщения о дате и времени последнего входа и количестве ошибочных входов,

– не следует записывать команды, которые содержат пароль, в командные процедуры,

– необходимо избегать явного объявления пароля при запросе доступа по сети (так как возможно отслеживать такие ситуации и осуществить захват пароля),

– не стоит использовать один и тот же пароль для доступа к разным узлам.

Кроме уже описанных способов компрометации пароля существуют и другие возможности. Не следует записывать команды, содержащие пароль, в командные процедуры, надо избегать явного объявления пароля при запросе доступа по сети: эти ситуации можно отследить и захватить пароль. Не стоит использовать один и тот же пароль для доступа к разным узлам.

Соблюдение правил использования паролей — необходимое условие надежной защиты.[7]

2.3 Безопасность удаленных электронных платежей

Особенностью защитных мероприятий для банковских систем является специальная форма обмена электронными данными - электронных платежей. В современном мире ни один банк не может существовать без этой формы обмена.

Обменом электронными данными (ОЭД) называют межкомпьютерный обмен деловыми, коммерческими, финансовыми электронными документами (заказы, платежные инструкции, контрактные предложения, накладные, квитанции и т.д.)

ОЭД направлено на обеспечение оперативного взаимодействия торговых партнеров (клиентов, поставщиков, торговых посредников и др.) на каждом этапе подготовки торговой сделки, заключения контракта и реализации поставки. Этап оплаты контракта и перевода денежных средств предполагает, что ОЭД, как правило, приводит к электронному обмену финансовыми документами. Осуществляется создание эффективной среды для торгово-платежных операций:

- торговые партнеры знакомятся с предложениями товаров и услуг, выбирают необходимый товар/услугу, уточняют коммерческие условия (стоимость и сроки поставки, торговые скидки, гарантийные и сервисные обязательства);
- осуществляется заказ товара/услуг или запрашивается контрактное предложение;
- производство оперативного контроля поставки товара, получение по электронной почте сопроводительных документов (накладных, фактур, комплектующих ведомостей и т.д.);
- подтверждение завершения поставки товара/услуги, выставление и оплата счетов;
- выполнение банковских кредитных и платежных операций.

ОЭД имеет ряд достоинств:

– за счет перехода на безбумажную технологию уменьшается стоимость операций;

– повышенная скорость расчета и оборота денег;

– высокое удобство расчетов.

Когда сообщение пересылается по линиям связи, оно содержит информацию о выполнении отправителем соответствующих операций над своим счетом, а также обязанность получателя в свою очередь совершить определенные действия. Обычно такие сообщения служат основанием открытия кредита, платы покупок и услуг и т.д.

Подобные сообщения именуются электронными деньгами, а банковские операции, на которых основаны такие операции - это электронные платежи. При производстве электронных платежей необходимо обеспечить качественную и надежную защиту от различных неблагоприятных влияний.

Для того чтобы осуществить пересылку денег по системе электронных платежей, необходимо пройти несколько этапов:

– в системе первого банка уменьшается счет на требуемую сумму;

– в системе второго банка счет увеличивается на эту сумму;

– первый банк отправляет второму сообщение, которое содержит информацию о выполняемых действиях (идентификаторы счетов, сумма, дата, условия и т.д.), как правило, такая информация защищена средствами шифрования;

– второй банк направляет первому уведомление о том, что произведены необходимые корректировки счета (тоже шифруется);

– для того чтобы предотвратить возможные конфликты, ведется протокол обмена, который содержит все действия сторон.

Для передачи информации могут создаваться специальные посредники - клиринговые центры, банки-посредники в передаче информации и т.п.

Чтобы определить проблемы защиты удаленных транзакций, проводится 3 этапа действий:

– документ подготавливается к отправке;

– документ передается по каналу связи;

– документ принимается и обратно преобразуется.

Однако в системе удаленных платежей существует масса уязвимых мест:

– пересылка платежных и других сообщений между банками или между банком и клиентом;

– обработка информации внутри организаций отправителя и получателя;

– доступ клиента к средствам, аккумулированным на счете.

В процессе осуществления пересылки платежных и других сообщений могут возникнуть проблемы:

– системы получателя и отправителя должны быть приспособлены к получению (отправке) электронных документов

– получатель и отправитель взаимодействуют через канал связи, т.е. опосредовано. Здесь могут возникнуть проблемы установления тождества при установлении соединения, доказательства отправления/доставки документа и т.д.;

– обычно отправитель и получатель документа независимы друг от друга, поэтому часто может возникнуть недоверие в части обеспечения исполнения документа.

При пересылке платежных и иных сообщений могут возникнуть следующие проблемы:

– осуществляется неправомерный доступ к ресурсам и данным системы. Например, могут взламывать эту систему или подбирать пароль к входным данным;

– перехватывают и подменяют трафик, например, посредством подделки платежных поручений, атаки типа "человек посередине";

– IP-спуфинг (заключается в подмене сетевых адресов);

– отказывают в обслуживании;

– производят атаку на уровне приложений;

– сканируют сети или сетевую разведку;

– используют отношения доверия в сети.

Основные виды атак на финансовые сообщения и финансовые транзакции:

– вскрытие информации;

– представление документа от имени другого участника;

– несанкционированное изменение;

– повтор переданной информации.

Существует четыре основныеформы удаленного банковского обслуживания клиентов:

– домашнее (телефонное) обслуживание. В этом случае клиент пользуется услугами банка, не выходя из дома;

– расчет с помощью автоматического кассового аппарата (банкомата, АКА). Банкомат – специальное устройство, которое обслуживает клиента при отсутствии персонала. Как правило, АКА выполняет следующие функции – выдача наличных денег, проверка состояния счета, изменение его состояния, осуществление различных платежей, предоставление различной информации, важной для клиента;

– расчет в точке продажи(point-of-sale, POS). Терминалы, которые подключены к таким системам, размещены на предприятиях торговли (супермаркеты, торговые центры и т.д.) Это связано с большим количеством совершения покупок в таких местах. Услуги, предоставляемые системами POS – проверка и подтверждение чеков, проверка и обслуживание дебетовых карточек, системы электронного расчета.

– финансовый сервис с использованием всемирной сети Интернет.[8]

2.4 Проблемы идентификации при удаленном обслуживании

Персональный номер (идентификатор) (PIN) –представляет собой последовательность цифр, которую используют для идентификации клиента. Для ввода PIN как в АКА, так и в терминалах систем POS предусмотрена цифровая клавиатура, аналогичная телефонной. Выделяют следующие типы PIN:

- назначаемые выведенные PIN;
- назначаемые случайные PIN;
- PIN, выбираемые пользователем.

В связи с тем, что PIN предназначен для идентификации и отождествления клиента, он должен обеспечить безопасность этого PIN. То есть его необходимо запомнить, никому не передавать и сохранять иными способами.

Когда сам банк вручает PIN, это не очень удобно, даже при небольшом их количестве. Человеку сложно запомнить большое число цифр, и поэтому чаще всего их записывают. Однако для удобства клиент чаще всего использует PIN, который он сам создает или выбирает. Так, клиент может использовать один PIN для различных целей и создавать такую их последовательность, которую ему удобнее запомнить.

PIN обычно состоит из четырех или шести цифр. Если злоумышленник планирует произвести подбор PIN или перебор всех возможных комбинаций, их будет 10 000. При сильной заинтересованности такой перебор возможен за короткое время. Поэтому важно обеспечить защиту PIN от перебора.

ПроверяютPIN двумя способами: алгоритмическим и неалгоритмическим.

Алгоритмический способ проверки заключается в том, что у пользователя запрашивается PIN, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением PIN, хранившемся на карточке. Достоинством этого метода проверки является:

– на главном компьютере нет в наличии PIN, что делает невозможным узнать его персоналу банка;

– отсутствие передачи PIN между АКА и главным компьютером банка, что исключает его перехват злоумышленником или навязывание результатов сравнения;

– облегчение работы по созданию программного обеспечения системы, так как уже нет необходимости действий в реальном масштабе времени.

Неалгоритмический способ проверки PIN, как это следует из его названия, не требует применения специальных алгоритмов. Проверка PIN осуществляется путем прямого сравнения полученного PIN со значениями, хранимыми в базе данных.

Часто сама база данных со значениями PIN шифруется прозрачным образом, чтобы не затруднять процесс сравнения, но повысить ее защищенность.

Идентификация клиента с использованием PIN работает только в следующих случаях:

– отсутствует перехват карточки и/или PIN при передаче от банка клиенту;

– банковские карточки не воруют, не теряют и их невозможно подделать;

– PIN невозможно узнать при доступе к системе другим пользователем;

– PIN иным образом не может быть скомпрометирован;

– в электронной системе банка отсутствуют сбои и ошибки;

– в самом банке нет мошенников.

В качестве альтернативы PIN предлагается применять устройства идентификации, основанные на биометрическом принципе. Их широкое применение сдерживается высокой стоимостью.

2.5 Основные требования обеспечения безопасности удаленных транзакций

Чтобы рассмотреть проблему защиты удаленных транзакций с технической стороны, необходимо выделить пару механизмов, которые обеспечивают безопасность электронных банковских систем. Такие службы, например как Value-AddedNetworkиVAN обеспечивают действие данных механизмов. Можно охарактеризовать функции данных служб. К ним относятся:

– обеспечение защиты от случайных и умышленных ошибок;

– обеспечение адаптации к частым изменениям количества пользователей, типов оборудования, способов доступа, объемов трафика, топологии;

– поддержка различных типов аппаратного и программного обеспечения, которое поставляют различные производители;

– осуществление управления и поддержки сети для того чтобы работа была непрерывной и быстро обеспечивалась диагностика нарушений;

– реализация полного спектра прикладных задач ОЭД, в т.ч. электронную почту;

– реализация большинства требований партнеров.

Для того чтобы защиты была обеспечена и на отдельных узлах системы и на уровнях протоколов, создается и обеспечивается ряд действий.

1. Происходит равноправие при отождествлении абонентов.
2. Отправитель или получатель не могут отказаться от принадлежности к ним отправленного сообщения.
3. Обязательное условия защиты - обеспечение контроля за сохранностью сообщения.
4. Сообщение должно быть строго секретным, для защиты от проникновения злоумшленников.

5. Обязательно осуществляется контроль за доступом на оконечных системах.

6. Доставка сообщения должна быть гарантирована и должна отслеживаться.

7. До того момента пока не приняты меры по сообщению – невозможно отказать.

8. Порядок сообщений обязательно регистрируется и проверяется сохранность такой последовательности.

Также, хотелось бы добавить, что решение проблемы защиты обмена электронными документами однозначно зависит от правильного выбора системы шифрования. Такую систему можно назвать совокупностью алгоритмов и методов шифрования ключей. Если выбрать правильный, то:

– происходит скрытие содержания всего документа от посторонних лиц посредством шифра;

– необходимо обеспечить использование документа целой группой пользователей с помощью криптографического разделения информации, а также с помощью протокола разделения ключей. То есть, если лицо не входит в данную группу, то документ будет от него скрыт;

– при помощи криптографического контрольного признака можно во время обнаружить подделку документа, а также его искажение;

– существует возможность идентифицировать личность, то есть удостовериться в том, что абонент действительно является тем, за кого себя выдает.

Необходимо обратить внимание на то, что при защите систем важно обеспечить целостность и идентификацию абонентов во время проведения сеанса связи. Можно сказать, что механизм шифрования играет так называемую вспомогательную роль в данном процессе.

Как известно, хакерские нападения наиболее часто совершаются именно на общедоступные сети. Дадим понятие людям, которые этим занимаются. Хакеры – это высококвалифицированные специалисты, которые в состоянии

вывести из строя серверы АБС, а также причинить им вред или проникнуть в их системы безопасности. Нападения чаще всего совершаются одним специалистом, но если имеются более сложные и тяжелые нарушения, то они работают объединенной группой. Стоит отметить, что хакер это не всегда посторонний человек, зачастую это обычный сотрудник.

Обычно защита системы от проникновения осуществляется следующими способами:

1. Зашифровываетсяинформация составляющая содержание документа;
2. Осуществляется проверка через специализированные программы на заимствование (плагиат);
3. Обеспечивается всестороннийконтроль за целостностью документа;
4. Пронумеровываются страницы документа;
5. Проводятся сеансы на уровне защиты информации;
6. Осуществляется динамическаяидентификация;
7. Обеспечивается сохранность секретных ключей;
8. Проводится процедура проверки клиента при регистрации в прикладной системе;
9. Используетсяэлектронный сертификата клиента;
10. Создается защищенное соединение клиента с сервером.

Стоит сказать, что необходимо использовать целый комплекс средств защиты сервисов Интернет:

– межсетевой экран - программная и/или аппаратная реализация;
– системы обнаружения и блокировка атак на сетевом уровне;
– антивирусные средства и программы;
– защищенные операционные системы, обеспечивающие уровень;
– защита на уровне приложений: протоколы безопасности, шифрования, ЭЦП, цифровые сертификаты, системы контроля целостности;
– защита средствами системы управления БД;

– защита передаваемых по сети компонентов программного обеспечения;

– проверка безопасности и выявление попыток вторжения, адаптивная защита сетей, активный аудит действий пользователей;

– обманные системы;

– корректное управление политикой безопасности.

Для проведения безопасных банковских транзакций проводится:

– идентификация документа в момент его создания;

– защита документа, когда он передается;

– идентификация документа при обработке, хранении и исполнении;

– защита документа при доступе к нему из внешней среды.[9]

2.6 Протоколы защиты удаленных банковских транзакций SSL и SET

Начнем с понятия протокола. Протокол – это алгоритм, который определяет порядок взаимодействия участников транзакции(например владельца карты, центра сертификации и обслуживающего банка) и форматы сообщений, с помощью которых участники транзакции обмениваются между собой для обеспечения процесса авторизации и расчета.

Под устойчивым протоколом подразумевается, то что, он позволяет:

– отождествить владельца карты другими участниками операции;

– идентифицировать торговую точку другими участниками транзакции;

– идентифицировать обслуживающий банк торговой точкой.

Кроме того устойчивость протокола проявляется вего:

– тайномхарактере сообщений между участниками транзакции через Интернет;

– тайном характере информации о реквизитах карты для торговой точки;

– сохранностиобмениваемых участниками транзакции данных;

– защите от транзакции – наличие для каждого участника транзакции электронного достоверного и неопровержимого доказательства факта совершения транзакции.

Далее поговорим о проколе SSL, который является наиболее распространенным и известным. Его распространенность обусловлена рядом причин:

– такой протокол является составной частью практически всех известных браузеров и веб-серверов.

– любой человек, который обладает картой и доступом в Интернет может произвести транзакцию при помощи этого протокола.

– протокол SSL достаточно прост в использовании, не нужно применять особых усилий для пользования им.

– достаточно высокая скорость проведения транзакций.

Безусловно протокол SSLне идеален в использовании, он также имеет несколько значительных недостатков.

Все электронные протоколы, которые основаны на SSLне поддерживают отождествление клиента в Интернет-магазине, так как сертификаты клиента фактически не используются в данных протоколах.

Многие клиенты используют динамическийIPадрес. Естественно в таком случае сертификат может быть без труда использован мошенниками и поэтому он автоматически мало чем полезен при проведении транзакции. Чтобы значение сертификата клиента возросло, необходимо чтобы при проведении транзакции могла устанавливаться связь между банком и номером карты клиента. Также очень важно установить возможность владельца карты проверить проведение покупки в любом Интернет магазине, например с помощью банка, обслуживающего его.

Таким образом, данный сертификат необходимо получать в банке-эмитенте. Также большой объем информации должен быть оговорен между всеми участниками транзакции. Для развития обеспечения взаимного отождествления участников транзакции необходимо создать точную иерархическую инфраструктуру центров сертификации. Без нее обеспечение отождествления невозможно.

Наиболее существенным недостатком протокола SSL является то, что в нем отсутствует клиент. Мошенникам удобно знать только реквизиты, ведь именно так они могут проводить необходимые им операции. Помимо этого, SSLпротокол не позволяет идентифицировать клиента, обслуживающим его банком.

Кроме того, описываемый протокол отличается тем, что в нем не используется цифровая подпись. Это значительно затрудняет процесс разрешения возникающих споров при работе платежной системы. Ведь при разрешении споров для того чтобы доказать факт транзакции нужно либо хранить бумажные копии документов, которые подтверждают получение

товара, либо хранить в электронном виде целый диалог клиента и магазина. Второй способ редко используется на практике, так как это очень дорогостоящий и энергоемкий процесс.

Также, когда используется SSLневозможно обеспечить конфиденциальность данных. Прежде всего это касается реквизитов карты для какой-либо торговой точки. Еще необходимо сказать, что данный протокол не является устойчивым. [10]

Для операций с кредитными карточками используется протокол SET (SecureElectronictransactions). В отличие от SSL протокол SET является узкоспециализированным. Целью SET считается обеспечение и поддержание необходимого уровня безопасности для платежного механизма, в котором участвует три или более субъектов. При этом предполагается, что транзакция происходит через Интернет, то есть удаленно.

SETосуществляет совокупность важнейший функций:

– функция идентификации. Участники участники кредитных операций имеют собственную неповторимую электронную подпись, с помощью которой происходит их отождествление;

– функция обеспечения тайного характера. Все операции производимые участниками шифруются;

– функция сохранности сообщений. Информация не может быть подвергнута изменению по дороге иначе это будет сразу известно;

– функция присоединения. SET позволяет подключить к базовому сообщению дополнительный текст и послать его одному из партнеров;

– функция безопасности. Протокол должен обеспечить максимально возможную безопасность операции, которая возможна в имеющихся условиях;

– функция совместимости. Должна быть предусмотрена совместимость с любыми программными продуктами и с любыми сервис-провайдерами.

На более высоком уровне протокол SET поддерживает все возможности, которые предоставляются современными кредитными карточками:

– учет держателя карточки;
– учет данных продавца;
– запрос покупки;
– фиксирование платежа;
– перевод денег;
– операции по кредиту;
– восстановление денег;
– отмену кредита;
– дебитные операции.

Необходимым условием создания глобальной системы отождествления, которая основывается на использовании асимметричных алгоритмов шифрования, является наличие иерархической однокорневой системы центров сертификации, которая отсутствует в протоколе SSL. Основные функции системы центра сертификации – генерация и распределение сертификатов открытых ключей, обновление сертификатов, а также генерация и распределение списков отозванных ключей.

В протоколе SET центр сертификации имеет четырехуровневую архитектуру основанную на использовании протокола X.509.

На самом верхнем уровне располагается Корневой центр сертификации (RootCertificateAuthority, RCA), который отвечает за генерацию сертификатов для центров сертификации следующего нижележащего уровня.

На втором уровне расположения системы центра сертификации находятся центры сертификации платежных систем.

В настоящее время такие центры сертификации созданы в платежных системах VISA, Europay/MasterCard, AmericanExpress. Центр сертификации уровня BCA отвечает за генерацию сертификатов для центров сертификации следующих уровней – GCA, CCA, MCA, PCA, а также за генерацию, поддержку и распространение CRL для сертификатов, ранее подписанных данным BCA. Оператором BCA является соответствующая платежная система.

На третьем уровне системы центра сертификатов SET располагается Геополитический центр сертификации.

Наличие центра сертификации уровня GCA позволяет платежной системе проводить более гибкую политику генерации и распределения сертификатов ключей для центров сертификации уровня CCA, MCA, PCA в отдельных геополитических зонах земного шара, а также повышать эффективность процедур генерации, поддержания и распространения CRL по сертификатам, эмитированным GCA.

Оператор центра сертификации уровня GCA определяется правилами соответствующей платежной, системы. Например, по правилам систем VISA и MasterCard оператором GCA может быть либо сама платежная система, либо GroupMember — банк, имеющий статус Группового участника платежной системы.

На четвертом, нижнем уровне системы центра сертификации SET располагаются три так называемых оконечных (End-Entity) типа центра сертификации. [10]

Центры сертификации уровня End-Entity отвечают за генерацию сертификатов для основных участников транзакции — для владельца карты, торговой точки и платежного шлюза. В этом смысле все остальные центры сертификации играют вспомогательную роль, обеспечивая единую общую инфраструктуру центров доверия, позволяющую любым двум непосредственным участникам транзакции надежно идентифицировать друг друга. Кратко остановимся на основных функциях центра сертификации уровня End-Entity.

Центр сертификации уровня CCA отвечает за создание и доставку сертификатов открытых ключей владельцев карт. По электронной почте или через веб-страницы от владельцев карт поступают запросы на получение сертификатов. Эмитент карты определяет и поддерживает необходимую процедуру отождествления клиента для создания сертификата владельца. CCA также отвечает за распространение среди владельцев карт списков CRL,

сгенерированных RCA, BCA, ССД, PCA. Оператором CCA могут являться банк-эмитент карточек, для которых выпускаются сертификаты, платежная система или третья сторона, которая определяется правилами конкретной платежной системы.

Центр сертификации уровня MCA отвечает за создание и доставку сертификатов открытых ключей торговых точек. Запросы на получение сертификатов поступают в MCA от торговых точек либо через Web-страницы, либо по электронной почте.

Для генерации сертификата торговой точки MCA должен поддерживать специальную процедуру идентификации торговой точки, определенную обслуживающим банком данной торговой точки. MCA также отвечает за распространение в адрес торговой точки списков CRL, сгенерированных RCA, BCA, GCA, PCA. Оператором MCA могут являться обслуживающий банк торговой точки, платежная система или третья сторона, определяемая правилами конкретной платежной системы.

Центр сертификации уровня PCA отвечает за создание и доставку сертификатов открытых ключей платежным шлюзам. PCA также отвечает за генерацию и распространение списка CRL, содержащего ранее эмитированные данным PCA сертификаты открытых ключей, для которых соответствующие им закрытые ключи оказались скомпрометированными на момент рассылки CRL.

PCA отвечает за распространение в адрес платежных шлюзов листов CRL, сгенерированных RCA, BCA, GCA, PCA. Оператором PCA могут являться обслуживающий банк, платежная система или третья сторона, определяемая правилами рассматриваемой платежной системы.

Сам процесс регистрации должен пройти шесть расстояний. Он начинается с отправки начального запроса и завершается получением сертификата. От методов, которые использует платежная система очень сильно зависит эффективность сертификата. На данном этапе еще не используется цифровая подпись, поэтому это довольно таки трудоемкий процесс.

Рисунок 3 – Регистрация владельца карты в центре сертификации

Сертификаты у владельцев карт можно считать так называемым электронным представлением самих платежных карт. Их не может изменить третья сторона, из-за того, что они подписаны цифровым способом. На сертификате владельца не указан номер счета и срок действия карты. Но зато, на нем имеется кодировка с помощью современных технологий, которая несет в себе информацию о счете, а также секретный код, который известен исключительно программе владельца карты. Если вдруг становятся известны номера счета, срок его действия, а также секретный код, то необходимо произвести проверку корректности сертификата. При этом извлечь вышеперечисленную информацию из сертификата, зная хотя бы часть параметров, указанных выше невозможно. Владелец карты передает секретный код и другую информацию о счете в расчетный центр. А уже там данная информация подтверждается.

Если финансовая организация, которая занимается выпуском карт одобрит сертификат, то тогда он посылается владельцу карты. Наличие запроса

сертификата обозначает, что собственник карты желает выполнить какую-либо коммерческую операцию. Сертификат, который получил владелец карты передается продавцу вместе с инструкциями по платежам в рамках запроса конкретной покупки. Если продавец получил сертификат собственника карты, он должен быть уверен, что счет владельца карты действительно существует. И что этот факт подтверждает агент или эмитент карты. Среди протокола SETданные сертификаты сохранены, а также оставлены на усмотрение платежной системы.

Когда в сертификационный центр приходит запрос от собственника карты, он вскрывает цифровой конверт и получает всю необходимую информацию о счете, а также секретный код, который генерируется программой собственника карты. При помощи симметричного ключа открывается запрос сертификата. После этого сертификационный центр начинает использовать общедоступный ключ, который присылается в запросе. Это делается для того, чтобы проверить подпись которая формируется с помощью секретного ключа владельца карты.

Если подписи совпали, процесс продолжается и переходит на следующую стадию. Следующей стадией является проверка самого запроса. Для этого начинает привлекаться информация о счете. Здесь сертификационный центр начинает взаимодействовать с эмитентом карты. Данное взаимодействие никак не регламентируется протоколом SET. Возможны случаи, когда на данной стадии для проверки запроса привлекаются возможности платежной системы. В случае, если проверка прошла успешно, то сертификат создается и пересылается собственнику карты.

Для начала сертификационный центр создает случайное число. Оно комбинируется ср12азу с секретным кодом, который в свою очередь присылается в запросе. Данный код необходимо использовать для защиты информации о счете собственника карты. [11]

Секретный код, номер счета и срок его действия преобразуются при помощи специального алгоритма. Данный результат помещают в сертификат.

Если стали известны секретный код, номер счета и срок его действия, то сертификат можно подтверждать.

После всех этих произведенных действий сертификационный центр подписывает сертификат с помощью цифровой подписи. Сертификационный центр определяет срок действия сертификата. Но иногда срок действия сертификата равен сроку работы платежной карты. Также случаются случаи, когда время действия платежа гораздо меньше, чем срок работы платежной карты.[12]

Ответное сообщение от сертификационного центра содержит в себе сам сертификат, секретный код, который также сформировал сертификационный центр, а также логотип платежной системы. Данную информацию засекречивают ключом, который присылается в запросе. Процедуры, которые мы упоминали выше будут рассмотрены далее гораздо подробнее.

Поддержку платежной системы создают сертификаты продавца. Это связанно с тем, что данные сертификаты наделены цифровой подписью. Сертификаты продавца не могут быть изменены третьей стороной.

Сертификаты продавца должен одобрить банк продавца, а также предоставить гарантию официального соглашения со своим банком. Для того, чтобы работать в среде SETу продавца должны находиться хотя бы пара сертификатов для каждого вида платежной системы, которые он поддерживает.

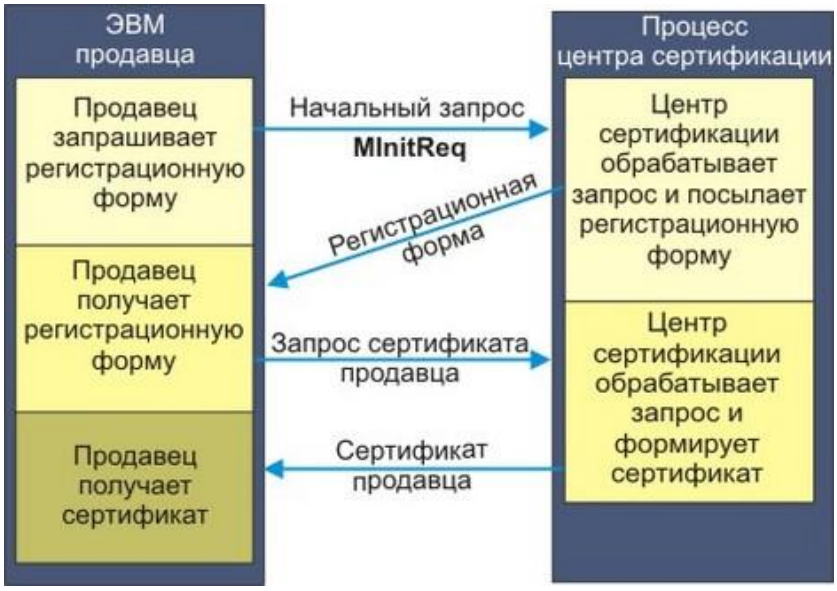

Рисунок 4 – Регистрация продавца

Безусловно до того момента, как продавец получит инструкции по платежу от собственника карты, а также будет участвовать в транзакциях с расчетным центром он обязательно должен зарегистрироваться в сертификационном центре. Сначала продавец должен получить общедоступный ключ, а еще потом отправлять запрос в сертификационный центр.

Продавец должен скопировать форму регистрации собственном банке и отождествить получателя в запросе, который посылается в сертификационный центр. Процедура регистрации начинается как только направляется запрос сертификата, в котором содержится общедоступный ключ и соответствующая форма регистрации.

Сертификационный центр отождествляет банк продавца и ищет соответствующую регистрационную форму. В ответ сертификационного центра прикладывается регистрационная форма, а также сертификат, который содержит общедоступный ключ. Данный сертификат потом используется продавцом в процессе регистрации.

Так как программа продавца имеет копию САсертификата, то продавец имеет возможность воспринимать инструкции по платежу, а также обрабатывать транзакции SET. Перед обработкой сертификата продавец обязан установить контакт со своим банком или получателем.

У продавца должно обязательно быть несколько пар общедоступных ключей, т.к. в дальнейшем происходит обмен ключами. Помимо этого наличие таких ключей влияет на цифровую подпись. Формируют такие ключи на основе и с помощью программы продавца.

Регистрация требует указания продавцом определенных данных: имени, адреса, идентификатора в регистрационную форму. Помимо этого необходимо направить в сертификационный центр общедоступный ключ продавца. Затем программой создается случайный ключ, используемый для сокрытия запроса сертификационного центра. Ключ возможно скрыть при помощи общедоступного ключа сертификационного центра, и затем его отправляют

цифровой конверт. Сгенерированное таким образом сообщение отправляется в сертификационный центр.

После того как продавец направил запрос в сертификационный центр, тот осуществляет раскрытие конверта и извлекает оттуда ключ, используемый для расшифровки запроса. Кроме того, сертификационным центром может быть использован данный ключ для того, чтобы проверить цифровую подпись. Подпись должна быть обязательно проведена соответствующим секретным ключом. Совпадение цифровой подписи означает продолжение процесса. В обратном случае, продавец должен оповестить сертификационный центр об этом.

Далее осуществляется проверка сертификационным центром информации регистрационного запроса. Для этого он использует известные данные о продавце, которые получены в процессе обмена между сертификационным центром и банком продавца (получателем).

Если данные успешно подтверждены, формируется и подписывается цифровой подписью сертификат продавца. Время действия сертификата определяет сертификационный центр, однако оно не должно превышать времени, на который заключен контракт между продавцом и его банком. Сертификат должен быть зашифрован сгенерированным новым симметричным ключом, который в свою очередь шифруется общедоступным ключом продавца. Полученный код образует цифровой конверт отклика. Сообщение-отклик посылается продавцу.

Когда программа продавца получает отклик от сертификационного центра, она дешифрует цифровой конверт и получает симметричный ключ для дешифрования регистрационного отклика, содержащего сертификат продавца.

Протокол SET взаимодействует с несколькими субъектами, а именно таковыми являются:

- владелец кредитной карты;
- банк, выпустивший эту карту;
- продавец;

– банк, где помещен счет продавца.

Эти субъекты являются основными, функциональными. Кроме них могут участвовать центры сертификации. Основная задача, стоящая перед ними заключается в проверке подлинности предъявляемых параметров отождествления. Если речь идет о крупной сделке, то каждый из функциональных субъектов должен взаимодействовать с такими центрами.

Спецификация SET определяет функции и технику реализации этапов пять, шесть, семь и девять. Таким образом, работа протокола SET инициализируется владельцем карты. Владельцем карты может быть как частное лицо, так и корпоративный клиент, работающие на своих рабочих станциях.

Многие современные WEB-браузеры поддерживают протокол SET. Что позволяет осуществлять торговлю товарами и услугами с использованием WWW-технологии. Номер кредитной карточки имеет определенную структуру (это не случайное число). Первые четыре цифры - код банка, выпустившего карточку. Последняя цифра представляет собой контрольную сумму номера.

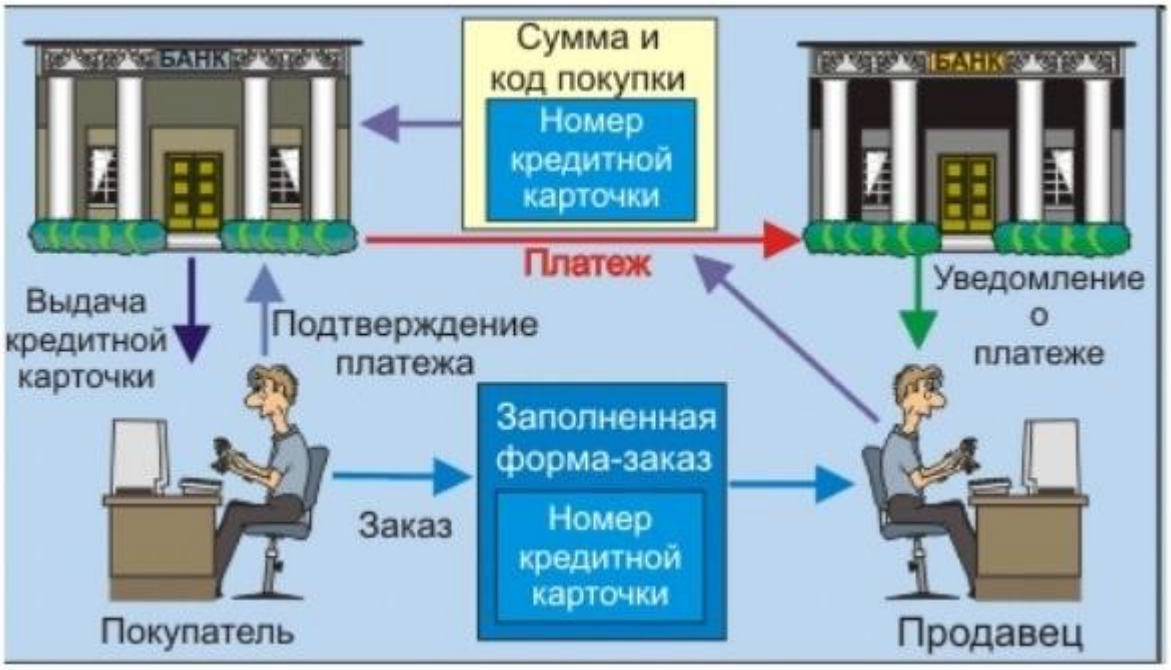

Рисунок 5 – Взаимодействие субъектов протокола SET

Покупатель является инициатором покупки. При этом покупатель выбирает продавца, просматривает его WEB-сайт, принимает решение о

покупке, заполняет бланк заказа. Все это делается до вступления в дело протокола SET. Реально взаимодействие участников сделки регламентируется протоколом IOTP. SET начинает свою работу, когда покупатель нажимает клавишу оплаты. При этом сервер посылает ЭВМ-покупателя сообщение, которое и запускает соответствующую программу. Процедура эта может быть реализована с помощью PHP- или CGI-скрипта, или JAVA-аплета.[13]

Программа клиента посылает заказ и информацию об оплате. Для этого формируется два сообщения, одно содержит данные о полной стоимости покупки и номере заказа, второе - номер кредитной карточки покупателя и банковскую информацию. Сообщение о заказе шифруется с использованием симметричного метода (например, DES) и вкладывается в цифровой конверт, где используется общедоступный ключ продавца. Сообщение об оплате шифруется с привлечением общедоступного ключа банка (эмитента кредитной карты). Таким образом продавец не получает доступа к номеру кредитной карточки покупателя. Программа генерирует хэш-дайджест (SHA1) обоих сообщений с использованием секретного ключа покупателя. Это позволяет продавцу и банкиру проконтролировать целостность сообщения, но препятствует прочтению части, ему не предназначенной (например, номера кредитной карты продавцом).

Продавец выделяет часть, адресованную банкиру, и направляет ее по месту назначения. Программа SET WEB-сервера продавца генерирует запрос авторизации серверу банка, где находится счет продавца.

При формировании запроса авторизации используется электронная подпись продавца, базирующаяся на его секретном ключе, что позволяет однозначно его идентифицировать.

Этот запрос шифруется с помощью ключа сессии и вкладывается в цифровой конверт, где используется общедоступный ключ банка.

Банк проверяет действительность кредитной карточки, дешифрует запрос авторизации продавца и идентифицирует продавца. После этого осуществляется проверка авторизации покупателя. При этом посылается запрос

авторизации, снабженный электронной подписью, банку, выпустившему кредитную карточку.

Банк, выпустивший карточку, выполняет авторизацию и подписывает чек, если кредитная карточка покупателя в порядке. Отклик, снабженный соответствующей подписью, посылается банку продавца.

Банк продавца авторизует данную операцию, и посылает подтверждение, подписанное электронным образом, WEB-серверу продавца.

WEB-сервер продавца завершает операцию, выдавая клиенту подтверждение на экран, и заносит результат операции в соответствующую базу данных.

Продавец осуществляет подтверждение выполнения операции своему банку, Деньги покупателя переводятся на счет продавца.

Банк, выпустивший карточку, посылает счет покупателю и SET уведомляет покупателя об изменениях на его счету (раз в месяц).

Итак, видно, что каждый шаг реализации протокола SET сопровождается идентификацией. Это препятствует какому-то внешнему субъекту стать посредником и видоизменять сообщения. Для нормальной работы протокола SET все участники должны зарегистрироваться и снабдить партнеров своим общедоступным ключом.

Протокол SET может использоваться не только в рамках Интернет, но и при заказах по почте или телефону MOTO (MailOrder/TelephoneOrder). Для понимания основополагающих принципов вышеизложенного могло бы быть достаточно.

Более того, квалифицированный программист мог бы написать программы, которые эти принципы реализовали для некоторой замкнутой системы покупатель-банки-продавец.

Но функция SET шире, этот протокол рассчитан на международную ничем не ограниченную систему платежей. По этой причине ниже будут приведены некоторые, наиболее важные детали работы протокола, регламентирующие его функционирование.

SET может работать в режиме, когда участники не имеют сертификатов и не прошли идентификацию. Такой режим сопоставим с использованием SSL для пересылки номера карточки продавцу, и не может рассматриваться как удовлетворительный.

Протокол SET призван защищатьисключительно финансовую информацию, которая непосредственно сопряжена с платежной транзакцией. Так, например информацию, которая содержится в заказе, SET не регламентирует.

В SET под владельцем платежной карты подразумевается программа, работающая на рабочей станции клиента-покупателя. Эта программа обеспечивает доступ к серверам продавцов, если требуется, поддерживает диалог между покупателем и продавцом, и реализует платежный процесс. При этом посылается заказ, получается отклик на этот заказ, осуществляются, если требуется, дополнительные информационные запросы и получаются данные о ходе реализации транзакции.

Эта программа выполняет опосредованную связь с получателем. Зашифрованные платежные данные через систему продавца поступают в расчетный центр, где они дешифруются.

Программа продавца предоставляет интерфейс для взаимодействия с программой владельца платежной карты, с программой получателя (Acquirer - банк продавца) и с центром сертификации.

Эта программа авторизует транзакцию, инициированную владельцем карты. Выполнение криптографических операций может производиться на аппаратном уровне. Такие криптографические модули могут быть снабжены также аппаратными устройствами генерации и запоминания секретных ключей (например, смарт-карты).

Важной функцией расчетных центров помимо реализации платежей является поддержка списков аннулированных сертификатов CRL (CertificateRevocationList). Это крайне важно для вовлеченных финансовых

организаций и фирм предоставляющих платежные средства (например, таких как VISA или MasterCard).

Сертификаты расчетного центра (РЦ) пересылаются банку продавца (получателю) и служат для обработки сообщений авторизации и платежей. Ключ шифрования расчетного центра, который получает владелец карты из сертификата РЦ, используется для защиты информации о счетах владельца карты.

Банку продавца (получателю) необходимо иметь сертификаты с целью взаимодействия с сертификационным центром. Он в свою очередь способен получать и обрабатывать запросы, которые поступают от продавцов. Банк продавца получает свои сертификаты из платежной системы.

Организации, которые выпускают карты должны владеть сертификатами, для того чтобы взаимодействовать с сертификационным центром, который может получать и обрабатывать запросы, которые поступают непосредственно от владельцев карт. Эмитент получает сертификаты также из платежной системы.

Цифровая подпись создана для того чтобы отождествить (установить соответствие между подписанными данными и уникальным секретным ключом подписанта). Подпись является особенной неповторимой, что гарантирует защиту от подделки подписи.

Секретный ключ математически связан с общедоступным ключом, и таким образом, связывает данные и общедоступный ключ. Фундаментальной целью сертификата является установление соответствия между общедоступным ключом и уникальным идентификатором объекта (или субъекта), гарантируя отсутствие подмены.

Следует помнить, что общедоступные ключи пересылаются по незащищенным каналам Интернет. В случае держателя карты сертификат подписи устанавливает соответствие между его общедоступным ключом и индивидуальным кодом PAN (PrimaryAccountNumber).

Цифровая подпись в сочетании с хэшированием сообщения (вычислением его цифрового дайджеста) гарантирует, кроме того, целостность данного сообщения, блокируя возможность его изменить в процессе пересылки. Механизм пересылки сообщений между объектами SET не регламентируется. Предполагается, что приложения SET могут работать в одном из двух режимов.

Интерактивном, когда объекты взаимодействуют в реальном масштабе времени с малыми задержками между запросами и откликами (например, в рамках технологии WWW).

Не интерактивном, когда задержки между запросом и откликом велики, например, при использовании электронной почты.

SET использует усовершенствованный Матиасом и Джонсоном метод хэширования, улучшающий технику OAEP.

Деятельность протокола SET основана на базовых процедурах: посылке и приеме сообщений. Процесс отправки сообщения представлен в таблице 1.

Таблица 1 – Процесс отправки сообщения

Шаг	Действие
1	Генерация сообщения SET
2	Вложение кода текущей версии в MessageWrapper (цифровой конверт, сейчас 1 или 0)
3	Вложить код даты, включая время.
4	Заполнить MessageID из полей TransID в Message. Если MessageID в Message отсутствует, поле опускается.
5	Вводится RRPID. Если это запрос, генерируется RRPID и запоминается для последующего сравнения с соответствующим кодом отклика. Если посылается отклик, то RRPID копируется из запроса.
6	Вводится SWIdent. Это строка, которая идентифицирует разработчика и версию программного продукта

Процесс обработки входящего сообщения представлен в таблице 2.

Таблица 2

Шаг	Действие
1	Извлекается цифровой конверт сообщения
2	Проверяется формат и содержимое полей цифрового конверта сообщения: версия, субверсия, дата/время, тип сообщения. Если обнаружена ошибка, возвращается отклик Error с ErrorCode.
3	Используя RRPID, производится сравнение и актуализация контрольного журнала на предмет выявления повторных сообщений
4	Произвести DER-декодирование сообщения
5	Если сообщение содержит SignedData, произвести следующее: Актуализовать системный кэш с учетом полученных CRL. Для каждого полученного сертификата, произвести верификацию цепочки сертификатов Проверить подпись сообщения
6	Если сообщение содержит инкапсулированные данные, выполняется извлечение вложенных данных согласно типу вложенного содержимого, включая шаг 5, если вложенные данные содержат SignedData
7	Извлечь идентификаторы BrandCRLIdentifier, включенные в сообщение и актуализовать системный кэш, проверить, что все CRL, идентифицированные BCI, находятся в системном кэше. В противном случае обработка сообщения прерывается.
8	Обработать сообщение
9	Актуализовать системный журнал с учетом состояния транзакции

На практике предполагается, что процесс верификации будет остановлен на уровне, который был успешно пройден ранее. Все приложения SET помимо самих сертификатов контролируют их дату пригодности. Процедура верификации представлена в таблице 3.

Таблица 3

Шаг	Действие
1	Верифицировать каждый сертификат в цепи согласно правилам X.509
2	Проверить то, что расширения KeyUsage, CertificatePolicies, PriviteKeyUsage и AuthorityKeyIdentifier находятся в согласии с X.509.
3	Если получено новое значение BCI: - проверить его подпись, используя сертификат CRL центра сертификации платежной системы - проверить, что BrandName в BCI соответствует тому, что проверено в цепочке сертификации - проверить, что дата NotAfter меньше текущей даты Проверить SequenceNum. Если оно больше чем SequenceNum из кэша BCI запомнить BCI и проверить, что все CRL, содержащиеся в BCI находятся в кэше CRL. Запомнить любой CRL, который пока нет в кэше
4	Провести верификацию для каждого нового полученного CRL,
5	Проверить каждый сертификат

Протокол SET обладает рядом особенностей:

– во-первых, это самый устойчивый протокол. Он представляет собой наиболее совершенный способ для защиты карточных платежей. Сегодня не существует никакого другого (кроме SET) опубликованного устойчивого протокола.

– во-вторых, для того чтобы данный протокол функционировал достаточно эффективно, необходимо наладить механизм его взаимодействия с другими субъектами. Для этого необходимо создать специальную сетевую инфраструктуру;

– в-третьих, данный протокол гарантирует абсолютнуюконфидециальность платежной информации на карточке;

– в-четвертых, пользователи должны быть уверены, что их информация сохраниться в таком виде, в котором была прежде;

– в-пятых, в описываемом проколе используется аутентификация (установление подлинности) данных владельца для сохранения информации от посторонних влияний.

Таким образом, протокол SET в настоящее время – это единственный открытый и устойчивый протокол в электронной коммерции.[14, 15]

2.7 Модель угроз информационной безопасности

В организации объектами защиты являются платежная информация, банковский платежный технологический процесс, информация ограниченного доступа, персональные данные и иная информация подлежащая защите в соответствии с законодательством Российской Федерации

При обеспечении конфиденциальности информации угрозами являются:

– разглашение информации;

– утечка информации как результат хищения информации и средств ее обработки;

– утрата информации и средств ее обработки.

При обеспечении доступности информации угрозами являются:

– блокировка доступа к информации;

– уничтожени информации и средств ее обработки.

При обеспечении целостности информации угрозами являются:

– изменение информации;

– отрицание подлинности информации;

– навязывание ложной информации.

Источниками угроз могут быть как субъекты, так и объективные проявления. Источники угроз могут быть как внутри защищамой системы, так и вне ее – внешние источники.

Источниками угроз являются:

– внешние: лица разрабатывающие вредоносное ПО; лица организующие DOS, DDosатаки и другие виды атак; лица осуществляющие попытки НСД;

– внутренние: персонал, имеющий права доступа к аппаратному оборудованию, администраторы серверов, сетевых приложений и т.п.;

– комбинированные источники угроз: внутренние и внешние, действующие сообща;

– сбои, отказы программных и технических средств;

– форс – мажорные обстоятельства: стихийное бедствие, военное действие, забастовки.

Классификация угроз и нарушителей безопасности информации приведена в таблице 4. [16]

Таблица 4

Характер угроз	Вид воздействия угрозы	Источники угроз		Объекты угроз		Объекты защиты
Технологические	Физические	Человек	Внутренние нарушители	На оборудование и канал связи		1. Банковский платежный технологический процесс; 2. Платежная информация; 3. Информация, отнесенная к защищаемой информации в соответствии с пунктом 2.1 Положения Банка России от 09.06.2012 № 382-П [3]; 4. Иная значимая для Банка информация, разглашение или модификация которой может привести к негативным последствиям для Банка.
			Внешние нарушители			
		Форс-мажорные обстоятельства		На ресурс		
				На канал связи		
		Сбои, отказ оборудования и внутренних систем обеспечения		На ресурс		
				На канал связи		
	Программные (логические)	Внутренние нарушители		На ресурс	На операционную систему	
					На программное обеспечение	
					На информацию	
		Внешние нарушители		На ресурс	На информационную систему	
					На сетевые службы	
					На информацию, обрабатываемую сетевыми службами	
				На канал связи	На сетевое оборудование	
					На протоколы связи	
Организационные	Воздействие на персонал	Внешний нарушитель	Физическое воздействие на персонал с целью получения информации или нарушения непрерывности ведения бизнеса	На информацию или канал связи		
				На непрерывность ведения бизнеса		
			Психологическое воздействие на персонал с целью получения информации или нарушения непрерывности ведения бизнеса	На информацию или канал связи		
				На непрерывность ведения бизнеса		
	Действие персонала	Внутренний нарушитель	Умышленные действия (шпионаж)	На информацию или канал связи		
			Неумышленные действия	На информацию		
				На непрерывность ведения бизнеса		

3 МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИЕ «КЛИЕНТ – БАНК»

3.1. Газпромбанк

3.1.1. При первом входе в систему необходимо сменить пароль выданный администратором системы безопасности Газпромбанка, который будет известен только пользователю системы, и не будет доступен третьим лицам.

3.1.2 Необходимо не реже 1 раза в 50 дней изменять свой пароль, который должен быть не менее 8 символов, и содержать в себе как цифры, так и большие и маленькие буквы английского алфавита.

3.1.3. Крайне не рекомендуется разглашать свой пароль. Даже сотрудники банка не имеют права требовать пароль пользователя для входа в систему. Также не рекомендуется пересылать файлы с ключевой информацией для работы в системе «Клиент – Банк» по электронной почте.

3.1.4. Если кто – либо обратился с просьбой сообщить ему пароль от системы «Клиент – Банк», необходимо сообщить об этом в Службу безопасности Газпромбанк.

3.1.5. Закрытый ключ электронно – цифровой подписи должен храниться на сменном носителе информации, таком как USB–flashнакопитель или USB–ключи e-token. Если ключевая информация расположена на жестком диске, то повышается риск получения этой информации третьими лицами.

3.1.6. Сменный носитель ключевой информации должен храниться в месте, недоступном третьим лицам, например: сейф или опечатываемый бокс.

3.1.7. Рекомендуется вставлять сменный носитель ключевой информации в считывающее устройство только на время проведения платежной операции и/или операций обмена с банком.

3.1.8. Никакой иной информации не должно храниться на носителе ключевой информации.

3.1.9. Компьютер, на котором установлена система «Клиент – Банк» должен быть оборудован программным или аппаратным средством межсетевого экранирования.

3.1.10. В случае передачи сторонним лицам компьютера (ноутбука), на котором ранее была установлена система «Клиент – Банк», необходимо произвести очистку всей информации, в том числе следы работы в системе, которая может быть получена третьими лицами с целью нанести вред финансовой деятельности или имиджу компании.

3.1.11. Если в процессе работы невозможно войти в систему под ранее известным рабочим паролем, необходимо незамедлительно сообщить в Службу безопасности Газпромбанк.

Недостатки системы «Клиент – Банк» bs – clientv. 3:

– Дата создания версии клиента 01.01.2001. Вот уже 16 лет версия не обновляется.

– Передача данных происходит через открытый канал связи, что не может обеспечивать должного уровня защиты от злоумышленников.

– Для входа в систему используется один и тот же пароль для всех организаций. В случае, если администратор безопасности захочет изменить этот пароль, ему придется создавать новую базу данных.

– Для того, чтобы подписать документ необходимо ввести пароль, что, конечно же, с одной стороны является плюсом, но в настройках системы можно установить сохранение пароля для того, чтобы больше не приходилось его вводить, а это уже является большим минусом.[17]

Рекомендации по повышению уровня безопасности работы в системе:

– Необходимо использовать шифрованный канал связи для передачи данных, либо сделать невозможным запуск системы без работающего крипто шлюза.

– Для входа в систему «Клиент – Банк» в паре с паролем использовать e-tokenc ограничением срока действия согласно сроку действия договора.

– Запретить сохранение пароля для подписи документов.

3.2. Сбербанк

3.2.1. Ключи электронной подписи изготавливаются самими владельцами при помощи соответствующей функции в системе «Клиент»

3.2.2. Идентификатор электронной подписи должен содержать не более 32 символов. Он предоставляется в формате YYYYNNNNsФИО должность, где YYYY – уникальный четырехразрядный буквенно-цифровой код Клиента, который присваивается системой корневого Удостоверяющего центра; s– признак принадлежности ключа электронной подписи организации, которая является клиентом ПАО «Сбербанк России» ;NNNN–четырехразрядный порядковый номер ключа электронной подписи; ФИО (фамилия и инициалы) – обязательный параметр; должность – узнаваемое сокращение должности владельца сертификата и название фирмы.

3.2.3. Не рекомендуется использовать в идентификаторе электронной подписи более одного пробела подряд, а также какие – либо символы: кавычки, точки, запятые и т.д.

3.2.4. Необходимо для каждого ключа проверки электронной подписи оформить и заверить рукописной подписью владельца сертификата распечатку проекта сертификата ключа. Это будет являться доказательством принадлежности изготовленных ключей, уполномоченным лицам.

3.2.5. Распечатка проекта сертификата ключа должна включать в себя:

– полное название организации;

– ФИО уполномоченного лица клиента;

– занимаемую должность уполномоченного лица в организации;

– идентификатор ключа электронной подписи;

– шестнадцатеричное представление ключа проверки электронной подписи;

– сведения о средствах электронной подписи;

– рукописную подпись владельца электронной подписи;

– рукописную подпись руководителя или доверенного лица, наделенного полномочиями подписывать договоры финансово – банковских услуг, оттиск печати Клиента.

3.2.6. Для того чтобы провести сертификацию ключей проверки электронной подписи, необходимо передать по системе файлы с ключами, а также заверенные копии сертификатов ключей проверки электронной подписи на бумажном носителе нужно передать в отделение «Сбербанк России», с которым заключен договор на обслуживание.

3.2.7. ПАО «Сбербанк России» проверяет полномочия владельцев сертификатов, оформление проектов сертификатов, и соответствуют ли подписи оттискам печати. Далее проекты передаются в удостоверяющий центр.

3.2.8. Ключи Клиента вступают в силу только после изготовления удостоверяющим центром сертификата ключа проверки электронной подписи и регистрации в соответствующей криптосети.

3.2.9. Сертификаты ключей проверки электронной подписи Клиента с подписью уполномоченного лица и оттиском печати удостоверяющего центра передаются Клиенту через функциональное подразделение ОАО «Сбербанк России».

3.2.10. По истечению срока действия ключей, определенного в сертификате, необходимо произвести их замену. Процедуру замены ключей желательно производить заблаговременно, чтобы избежать приостановки работы системы.

3.2.11. Срок действия ключа не может быть более одного года и трех месяцев.

3.2.12. Процедура входа в систему состоит из трех этапов:

1. Необходимо вставить электронный ключ в считыватель информации;

2. Вход в VPN. Требуется ввод логина и пароля;

3. Вход в программу Клиент «Сбербанк Бизнес – онлайн». Требуется ввод логина и пароля

3.2.13. Для подписи документа, помимо ключа электронной подписи, также требуется ввод пароля, который знает только владелец ключа, или доверенное лицо.

3.2.14. Данные в системе «Клиент – Банк» передаются по шифрованному каналу, используя порт 443.

Недостатки системы «Сбербанк Бизнес – онлайн»:

– Возможность использования сторонних интернет порталов во время работы с системой;

– Авторизация путем ввода логина и пароля с клавиатуры.[18]

Рекомендации по повышению уровня безопасности работы в системе:

– так как сторонние сайты не блокируются во время работы с системой, необходимо использовать только лицензионное антивирусное программное обеспечение;

– использовать крипто шлюз для обеспечения информационной безопасности, а также для защиты информационных сетей от вторжения со стороны сетей передачи данных, обеспечения конфиденциальности информации припередачи через открытый канал связи;

– запретить использование клавиатуры для ввода пароля. Использовать только экранную клавиатуру.

3.3. ВТБ

3.3.1. Система Клиент – Банк, именуемая «Клиент – ТелеБанк», в своей основе использует программный комплекс Inter – Prокак средство криптографической защиты информации.

3.3.2. Запуск системы «Клиент –ТелеБанк» невозможен без запуска программного комплекса Inter – ProClient.

3.3.3. Программный комплекс Inter – ProClientблокируетсторонние порталы, работа возможна только в системе «Клиент –ТелеБанк».

3.3.4. При первом входе в систему необходимо сменить технический пароль, выданный администратором безопасности. Без смены пароля доступ в систему будет заблокирован.

3.3.5. В случае неправильного ввода пароля, предоставляется еще четыре попытки, по истечению которых логин блокируется в системе.

3.3.6. Пароль обязательно должен состоять не менее чем из восьми символов.

3.3.7. USB–ключи электронной подписи обладают функцией, которая делает невозможным изъятие ключевой информации. Это повышает устойчивость к несанкционированному доступу к счетам клиентов.

3.3.8. Система «Клиент –ТелеБанк» обладает двухфакторной аутентификацией:

– Ввод логина и пароля для входа в систему;

– Ввод кода доступа, отправленный на мобильный телефон. Используется сервис SMS – OTP. Код доступа не может быть использован при повторном входе в систему, так как является одноразовым.

3.3.9. Доступ в систему «Клиент –ТелеБанк» предоставляется только с фиксированных IP–адресов. Необходимо сообщить в отделение банка внешний IP – адрес узла, с которого будет разрешен доступ пользователей в систему.

3.3.10. Ключевые носители с электронной подписью должны использовать только их владельцы. Передача ключа владельцем другим пользователям ведет к компрометации ключа.

3.3.11. Копии с ключевых носителей электронной подписи, возможно, сделать только на специализированном программном обеспечении, которое можно получить в филиале. Запрещается создание несанкционированных копий информации с ключевых носителей электронной подписи, в том числе копирование на локальный жесткий диск компьютера.

3.3.12. Для хранения ключей электронной подписи рекомендуется использовать сейфы, оборудованные надежными запирающими механизмами.

3.3.13. Необходимо регулярно обновлять системное и прикладное программное обеспечение, используемое при работе в системе.

3.3.14. Ключевые носители должны быть вставлены в считыватели информации только на время работы с системой.

3.3.15.Рабочая станция, на которой происходит работа с системой дистанционного банковского обслуживания, должна быть оборудованаантивирусным программным обеспечением с обновленными базами данных, а также средствами защиты от несанкционированного доступа.

3.3.16. Рекомендуется отключить автозаполнение в настройках браузера. Это поможет не сохранять данные, такие как пароль или имя пользователя.

3.3.17. На стартовой странице системы указана дата последнего посещения, с помощью чего можно контролировать посещение системы «Клиент – ТелеБанк».[19]

Программный комплекс "Inter-PRO" предназначен для защиты Интернет-приложений, построенных по технологии "клиент-сервер" на базе протокола HTTP (Web-браузер - на стороне клиента и Web-сервер - на стороне сервера).Для защищенного обмена информацией между Web-браузером и Web-сервером комплекс "Inter-PRO" использует протокол SSL.

В настоящее время протокол SSL поддерживается программным обеспечением серверов и браузеров, выпускаемых рядом западных компаний, в частности, компаниями Netscape и Microsoft (NetscapeNavigator, MicrosoftExplorer, NetsiteCommerceServer и др.). Однако из-за экспортных ограничений подавляющее большинство этих продуктов доступны в России только в усеченном варианте (с длиной сеансового ключа 40 бит для одноключевых алгоритмов шифрования и параметром 512 бит для алгоритма RSA, используемого на этапе установления SSL-сессии). Данные ограничения практически исключают возможность построения систем с приемлемым уровнем защиты на базе этих продуктов.

Программный комплекс "Inter-PRO" восполняет этот пробел. Выполненный по proxy-технологии, "Inter-PRO" позволяет использовать встроенную в него реализацию протокола SSL без экспортных ограничений на длину криптографических ключей. Помимо этого, стандартный протокол SSL дополнен отечественными криптографическими алгоритмами и реализует возможность формирования и проверки цифровой подписи пользователяпод HTML-формами.Комплекс "Inter-
PRO" включаетпрограммныемодули "Inter-PROServer" и "Inter-PROClient".[20]

Недостатки системы «Клиент – ТелеБанк»:

– Авторизация путем ввода логина и пароля с клавиатуры.

Рекомендации по повышению уровня безопасности работы в системе:

– Ввод логина и пароля должен осуществляться с экранной клавиатуры.

3.4. Федеральное Казначейство РФ

3.4.1. Технические средства, на которые устанавливаются средства электронной подписи, должны быть оборудованы исключительно лицензионным программным обеспечением фирм – изготовителей.

3.4.2. Программное обеспечение средств электронной подписи необходимо устанавливать только с дистрибутива, полученного в Удостоверяющем центре Федерального казначейства.

3.4.3. На технических средствах с установленными средствами электронной подписи запрещается устанавливать средства разработки программного обеспечения и отладчики. Если они все-таки необходимы для технологических потребностей пользователя, то это должно быть санкционированно с администратором безопасности.

3.4.4. Необходимо исключить возможность изменения аппаратной части рабочего места, например, опечатав системный блок и разъемы.

3.4.5. На рабочей машине, использующей средства электронной подписи и средства криптографической защиты, необходимо исключить возможности, позволяющие:

- модифицировать собственный код и код других программ;
- модифицировать память, выделенную для других программ;
- модифицировать содержимое произвольных областей памяти;
- повышать предоставленные привилегии;
- изменять настройки операционной системы;
- несанкционированно изменять файлы, содержащие исполняемые коды при их хранении на жестком диске.

3.4.6. Ключи электронной подписи на ключевом носителе защищаются паролем. Его формирует лицо, занимающееся процедурой генерации ключей, в соответствии с требованиями на используемое средство электронной подписи.

3.4.6. Минимальная длина пароля – шесть символов.

3.4.7. При смене пароля, новый пароль должен отличаться от старого не менее чем на четыре позиции.

3.4.8. Личный пароль запрещается разглашать кому – либо, в том числе сотрудникам Федерального казначейства.

3.4.9. Смена пароля должна происходить не реже чем один раз в девяноста дней.

3.4.10. Запрещается оставлять электронный ключ в считывателе информации, если работа с техническими средствами электронной подписи закончена.

3.4.11. Без согласования с администратором безопасности запрещается копирование ключевой информации с электронных носителей.

3.4.12. Запрещается записывать на ключевые носители постороннюю информацию.

3.4.13. Необходимо исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной системы, а

также исключить возможность удаленного администрирования операционной системы.

3.4.14. Только администратор безопасности обладает право установки и настройки операционной системы, а также средств электронной подписи и криптографической защиты.

3.4.15. Все неиспользуемые ресурсы системы во время работы с электронными подписями необходимо отключить.

3.4.16. На рабочей станции должна быть включена подсистема регистрации событий информационной безопасности.

3.4.17.Обязательным условием для работы в системе – это настроенный аппаратно – программный комплекс криптографической защиты трафика данных (крипто шлюз).

3.4.18. Для запуска аппаратно – программного комплекса шифрования трафика требуется пройти авторизации, в связи с чем можно сделать вывод: для того чтобы войти в систему для работы с электронными подписями, необходимо пройти авторизацию из двух этапов: авторизация в системе крипто шлюз; авторизация в самой системе для работы с электронными подписями.[21]

АПКШ «Континент» — аппаратно-программный комплекс, позволяющий обеспечить защиту информационных сетей организации от вторжения со стороны сетей передачи данных (Интернет), конфиденциальность при передаче информации по открытым каналам связи (VPN), организовать безопасный доступ пользователей VPN к ресурсам сетей общего пользования, а также защищенное взаимодействие сетей различных организаций.

Программа объединяет межсетевой экран и средство построения VPN-сетей. Является сертифицированным продуктом и обладает сертификатами ФСТЭК и ФСБ.

Программа предназначена для объединения через Интернет локальных сетей предприятия в единую сеть VPN. Поддерживает подключение удалённых и мобильных пользователей к VPN по защищённому каналу, разделение доступа между информационными подсистемами организации, безопасное

удалённое управление маршрутизаторами. Может использоваться для организации защищённого взаимодействия со сторонними организациями.

Является одной из немногих российских сертифицированных программ с высокой производительностью (в режиме VPN — 800 Мбит/сек). Входит в число наиболее популярных VPN-продуктов в России.[22]

Недостатки системы безопасности:

– возможность сохранить пароль для входа в систему АПКШ;

– однофакторная аутентификация при входе в саму систему.

Рекомендации по повышению уровня безопасности работы в системе:

– исключить возможность сохранения пароля для входа в систему АПКШ;

– добавить SMS – OTPсервис, благодаря которому, в случае, если пара логин и пароль попадут к злоумышленнику, он не сможет войти в систему без ввода кода доступа, который поступает на номер телефона, указанный в договоре;

– для ввода пароля использовать только экранную клавиатуру.

3.5. Новикомбанк

3.5.1. Для хранения ключей электронных подписей используются только флеш – накопители или USB–Token.

3.5.2. Доступ к ключевым носителям электронной подписи должен быть строго ограничен.

3.5.3. Запрещается записывать постороннюю информацию на ключи, содержащие электронную подпись.

3.5.4. Носители электронной подписи должны включаться в компьютер только на время подписи, и даже если работа в системе дистанционного банковского обслуживания продолжается, необходимо отключить ключи от компьютера.

3.5.5. Минимальная длина пароль составляет шесть символов.

3.5.6. Не реже чем один раз в месяц производить смену пароля.

3.5.7. Запрещается сообщать пароль от системы дистанционного банковского обслуживания третьим лицам, в том числе администраторам безопасности и сотрудникам банка.

3.5.8. Ограничить физический доступ к компьютеру, на котором осуществляется работа с системой дистанционного банковского обслуживания.

3.5.9. Запретить доступ под учетной записьюWindows, обладающей правами администратора. Необходимо использовать учетную запись с ограниченными правами.

3.5.10. Активировать на компьютере, с установленной системой дистанционного банковского обслуживания системный аудит, регистрирующий возникающие ошибки.

3.5.11. Обеспечить своевременную загрузку и установку последних обновлений, поступающих с официального сайта Microsoft.

3.5.12. Регулярно производить обновление установленного лицензионного антивирусного программного обеспечения. Настроить регулярное сканирование оперативной памяти и жестких дисков на наличие вредоносных программ.

3.5.13. Во время настройки межсетевого оборудования необходимо заблокировать несанкционированный исходящий и входящий сетевой трафик по всем TCPи UDPпортам для всех адресов, как внешней, так и внутренней локальной сети организации.

3.5.14. Обязательное наличие электронного ключа владельца электронной подписи в считывателе информации во время входа в систему.

3.5.15. Двухфакторная аутентификация для входа в систему:

– логин и пароль используется для входа в систему;

– уникальный пин – код владельца электронной подписи, чей ключ находится в считывателе информации.

3.5.16. Для подписи документа необходимо ввести пароль только в том случае, если изначально вход в систему выполнялся другим пользователем.

Недостатки системы безопасности:

– возможность пользоваться сторонними интернет порталами во время работы в системе дистанционного банковского обслуживания.

Рекомендации по повышению уровня безопасности работы в системе:

– использование программных или программно – аппаратных средств криптографической защиты информации;

– использование сервиса SMS – OTP для получения дополнительного одноразового кода доступа, который присылается на номер телефона, указанный в договоре на дистанционное банковское обслуживание.

4 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ АДМИНИСТРИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

4.1 Общие положения

К эксплуатации средств вычислительно техники и перифирийного оборудования допускается только специально обученый персонал, возраст которого не может быть моложе 18 лет, пригодный по состоянию здоровья и квалификации к выполнению указанных работ .

Один раз в шесть месяцев необходимо производить инструктаж по тезнике безопасности с показом рациональных и безопасных приемов работы. К работе допускать только после прохождения инструктажа. Внеплановый инструктаж может проводиться в случаях изменения правил по охране труда или в случаях нарущения персоналом правил техники безопасности.

В тех помещениях, где проходит работа с персональными компьютерами и перифирийными устройствами, должна быть вывешена инструкция по технике безопасности с указанием действий персонала в случаях возникновения пожара, аварии или травм.

Ответственность за организацию правильной и безопасной эксплуатации средств вычислительной техники и перифирийного оборудования лежит на руководителях структурных подразделений.

4.2 Виды опасных и вредных факторов

При эксплуатации средств вычислительной техники и перифирийного оборудования персонал может подвергаться опасным и вредным воздействиям, подразделяющиеся на следующие группы:

- механические повреждения;
- электромагнитное излучение;
- поражение электрическим током;

– инфракрасное излучение;

– опасность пожара;

– повышенный уровень шума и вибрации.

4.3 Требования электробезопасности

Во время использования средств вычислительной техники и периферийных устройств каждый работник должен внимательно и осторожно обращаться с электропроводкой, приборами и аппаратами.

Во избежание поражения электрическим током необходимо выполнять следующие правила безопасного пользования электроэнергией:

– на своем рабочем месте необходимо следить за исправностью выключателей, проводов, штепсельных розеток и заземлений. О любых неисправностях стоит немедленно доложить администрации и обесточить оборудование;

– чтобы избежать повреждения изоляции проводов и возникновения коротких замыканий запрещается:

1) что – либо вешать на провода;
2) убирать провода и шнуры за водопроводные и газовые трубы;
3) закрашивать и белить провода и шнуры;
4) выдергивать вилку из розетки, держась за шнур.

– воизбежание поражения электрическим током запрещается:

1) часто включать и выключать компьютер, если нет такой необходимости;
2) работать за компьютером и с перифирийным устройством мокрыми руками;
3) трогать экран и тыльную сторону системного блока компьютера;
4) работать за компьютером, имеющий внешние механические повреждения, нарушение изоляции проводов и признаки электрического напряжения на корпусе;
5) класть посторонние предметы на компьютер или периферийное оборудование.

– запрещается очищать от пыли и загрязнений оборудование, которое находится под напряжением;

– запрещается самостоятельно ремонтировать электрооборудование. Этим должны заниматься специалисты – техники;

– при использовании электрооборудования запрещается касаться одновременно каких – либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей;

– при обнаружении оборвавшегося провода необходимо немедленно сообщить администрации, а также принять необходимые меры по исключению контакта провода с людьми;

В случаях, если все таки произошло поражение электрическим током кого - либо, необходимо вызвать врач, а до его прибытия оказывать первую помощь пострадавшему.

4.4 Требования по обеспечению пожарной безопасности

Запрещается иметь огнеопасные вещества на рабочем месте.

В помещениях запрещается:

– разжигать огонь;

– включать электрооборудование, если в помещених пахнет газом;

– курить;

– сушить что – либо на отопительных приборах;

– закрывать вентиляционные отверстия в электрооборудование.

Источниками пожара могут быть:

– искра от электрооборудования;

– искра от удара и трения;

– искра при разряде статического электричества;

– открытое пламя.

В случаях возникновения пожара, персонал вынужден немедленно вызвать пожарную команду, принять меры по ликвидации пожара и оповестить администрацию.[23]

ЗАКЛЮЧЕНИЕ

Система «Клиент – ТелеБанк» является самой защищенной на сегодняшний день. Она использует в своей основе программный комплекс криптографической защиты информации, который, помимо защиты данных, передаваемых по каналу клиент – банк, также блокирует сторонние интернет – порталы. Использование двухфакторной аутентификации также является большим плюсом, так как даже в том случае, если логин и пароль попадет к злоумышленнику, он не сможет войти в систему без ввода кода доступа, который придет на телефон, номер которого привязан к системе. Для подписи документа в системе, помимо token-а в считывателе информации, необходимо ввести пароль, что является немаловажной защитой от несанкционированного доступа.

Таблица 4 – Сравнительная характеристика методов защиты

Методы/Банки	Газпромбанк	ВТБ	Сбербанк	Новиком	Казначейство
Использование 2х факторной аутентификации		✓	✓	✓	
Использование протокола https		✓	✓	✓	
Использование программного или АП комплекса криптографической защиты		✓			✓
Обязательно наличие token – а в считывателе для подписи документов	✓	✓	✓	✓	✓
Запрос пароля для подписи документов	✓	✓	✓	✓	✓

Результаты исследования:

В результате расчетов были получены следующие данные (число хищений на 1000 клиентов):

При этом использовалась следующая формула:

(число отзывов о хищении/ общее число отзывов)*1000 = число хищений на 1000 клиентов

Газпромбанк – 41/988*1000 = 41,5

Новикомбанк – 24/2058*1000 = 11,66

Казначейство - 5/838*1000 = 5,97

Сбербанк – 7/1277*1000 = 5,48

ВТБ – 5/1330*1000 = 3,76 [24]

СПИСОК ИСПОЛЬЗУЕМОЙЛИТЕРАТУРЫ

1. Статистика краж денег[электронный ресурс] //РБК; ред. Александра Краснова, Антон Баев - режим доступа: http://money.rbc.ru, свободный. (Дата обращения: 10.11.2016 г.).

2.Схемы мошенничества с картами [электронный ресурс]//finanz.ru; ред. Краснов А. В. – режим доступа: http://www.finanz.ru, свободный. (Дата обращения: 10.11.2016 г.).

3. История появления электронных денег [электронный ресурс]//Информационный сайт о форексе; ред. Портнов С. К. – режим доступа: http://www.niceforex.ru, свободный. (Дата обращения: 15.11.2016 г.)

4. Статистика денежных потерь банков из – за деятельности интернет - мошенников [электронный ресурс]// «Своя Компания».Бизнес журнал; ред. Лаптева А. А. – режим доступа: http://www.company-mag.ru, свободный. (Дата обращения: 15.11.2016 г.)

5. Автоматизированные информационные системы в экономике [электронный ресурс]// Учебные материалы; ред. Ясенев В. Н. – режим доступа http://www.works.doklad.ru, свободный. (Дата обращения: 17.11.2016 г.)

6. Модель программно – аппаратного комплекса для эмуляции уязвимостей систем ДБО [электронный ресурс]// «Студенческий научный форум – 2015»; ред. Абрамов Е. С. – режим доступа http://www.scienceforum.ru, свободный. (Дата обращения: 17.11. 2016 г.)

7.Защита информации в электронных платежных системах [электронный ресурс]//Slidehare; ред. Прудник А. М. – режим доступа: http://www.slideshare.net, свободный. (Дата обращения: 05.12.2016 г.).

8. Защита банковских транзакций и электронной торговли [электронный ресурс]//Информзащита. Учебный центр; ред. Дыбова Ольга – режим доступа: http://www.itsecurity.ru, свободный. (Дата обращения: 07.12.2016 г.)

9.Информационная банковская безопасность и ее необходимость [электронный ресурс]//Финэксперт24; ред. Колобков В. Н. – режим доступа: http://www.finexpert24.com, свободный. (Дата обращения: 07.12.2016 г.)

10. Что такое протокол SSLи зачем он нужен [электронный ресурс]//INTERFACE; ред. АйяЗагуль – режим доступа: http://www.interface.ru, свободный (Дата обращения: 10.12.2016 г.)

11. SETдругие системы осуществления платежей [электронный ресурс]//CITFORUM; ред. Семёнов Ю. А. – режим доступа: http://www.citforum.ru, свободный. (Дата обращения: 10.12.2016 г.).

12. Регистрация владельца карты [электронный ресурс]//Защита информационных банковских сетей. Хрестоматия; ред. Семёнов Ю. А. – режим доступа: http://www.eos.ibi.spb.ru, свободный. (Дата обращения: 12.12.2016 г.).

13. Банковское дело [электронный ресурс]//сравни.ru; ред. Кудряшов В. Н. – режим доступа: http://www.sravni.ru, свободный. (Дата обращения: 17.12.2016 г.)

14. Протокол SET[электронный ресурс]//Общие принципы потроения каналов передачи данных и сетей; ред. Семенов Ю. А. – режим доступа: http://www.book.itep.ru, свободный. (Дата обращения: 17.12.2016 г.)

15. Безопасность электронных платежных систем [электронный ресурс]//Учебник по сайтостроению; ред. Колесников Д. Г. – режим доступа: http://www.protect.htmlweb.ru, свободный. (Дата обращения: 05.01.2017 г.)

16. Построение модели угроз безопсности информации кредитной организации [электронный ресурс]//CYBERLENINKA; ред. Коновалова Ю. Н. – режим доступа http://www.cyberleninka.ru, свободный. (Дата обращения: 05.01.2017 г.)

17. Система «ДБО BS – Clientv.3». Руководство по использованию [электронный ресурс]//Банк’с софт системс; ред. Корольков М. В. – режим доступа: http://www.tfb.ru, свободный. (Дата обращения: 10.01.2017 г.)

18. Инструкция по работе с корпоративными картами дляинтернет – клиентов Сбербанк [электронный ресурс]//Система Сбербанк Бизнес Онлайн; ред. Семшов А. Г. – режим доступа http://www.sberbank.ru, свободный. (Дата обращения: 10.01.2017 г.)

19. Инструкция по работе с системой Клиент – Телебанк[электронный ресурс]//ВТБ северо – западный региональный центр; ред. Глазырин В. М. – режим доступа http://www.szrcvtb.ru, свободный. (Дата обращения: 10.01.2017 г.)

20. Руководство пользователя InterPRO [электронный ресурс]//ЗАО «Сиггнал – Ком»; ред. Москвин С. Л. – режим доступа http://www.lghost.ru, свободный. (Дата обращения: 12.01.2017 г.)

21. Руководство пользовался Автоматизированной системой Федерального Казначейства (СУФД) [электронный ресурс]// Официальный сайта Казначейства РФ; ред. Ткаченко В. В. – режим доступа http://www.roskazna.ru, свободный. (Дата обращения: 19.01.2017 г.)

22. АПКШ – Континент [электронный ресурс]// Wikipedia – режим доступа https://ru.wikipedia.org, свободный. (Дата обращения: 19.01.2017 г.)

23. Безопасность жизнедеятельности [электронный ресурс]// Инструкция по технике безопасности при работе за компьютером; ред. Мочалов А. В. – режим доступа:http://www.web.vrn.ru, свободный. (Дата обращения: 20.01.2017 г.)

24. Рейтинг безопасности банков [электронный ресурс]//banki.ru; ред. Измайлов В. Н. – режим доступа: http://www.banki.ru/, свободный. (Дата обращения: 20.01.2017 г.)

ПРИЛОЖЕНИЕ А

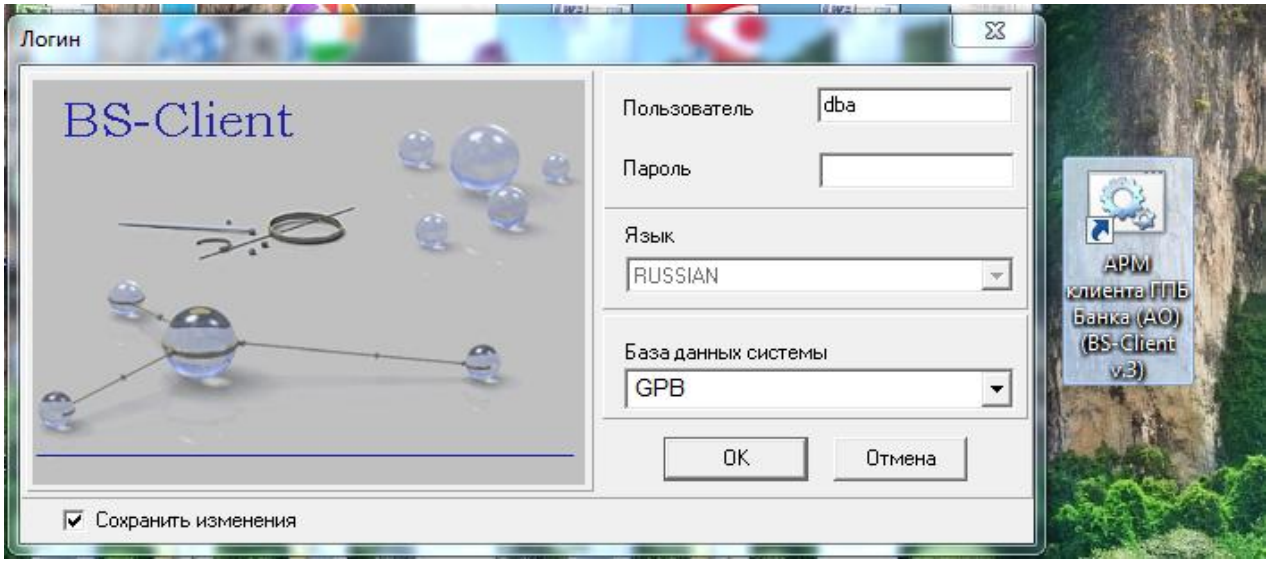

Рисунок А1 – Окно авторизации в системе Газпромбанк

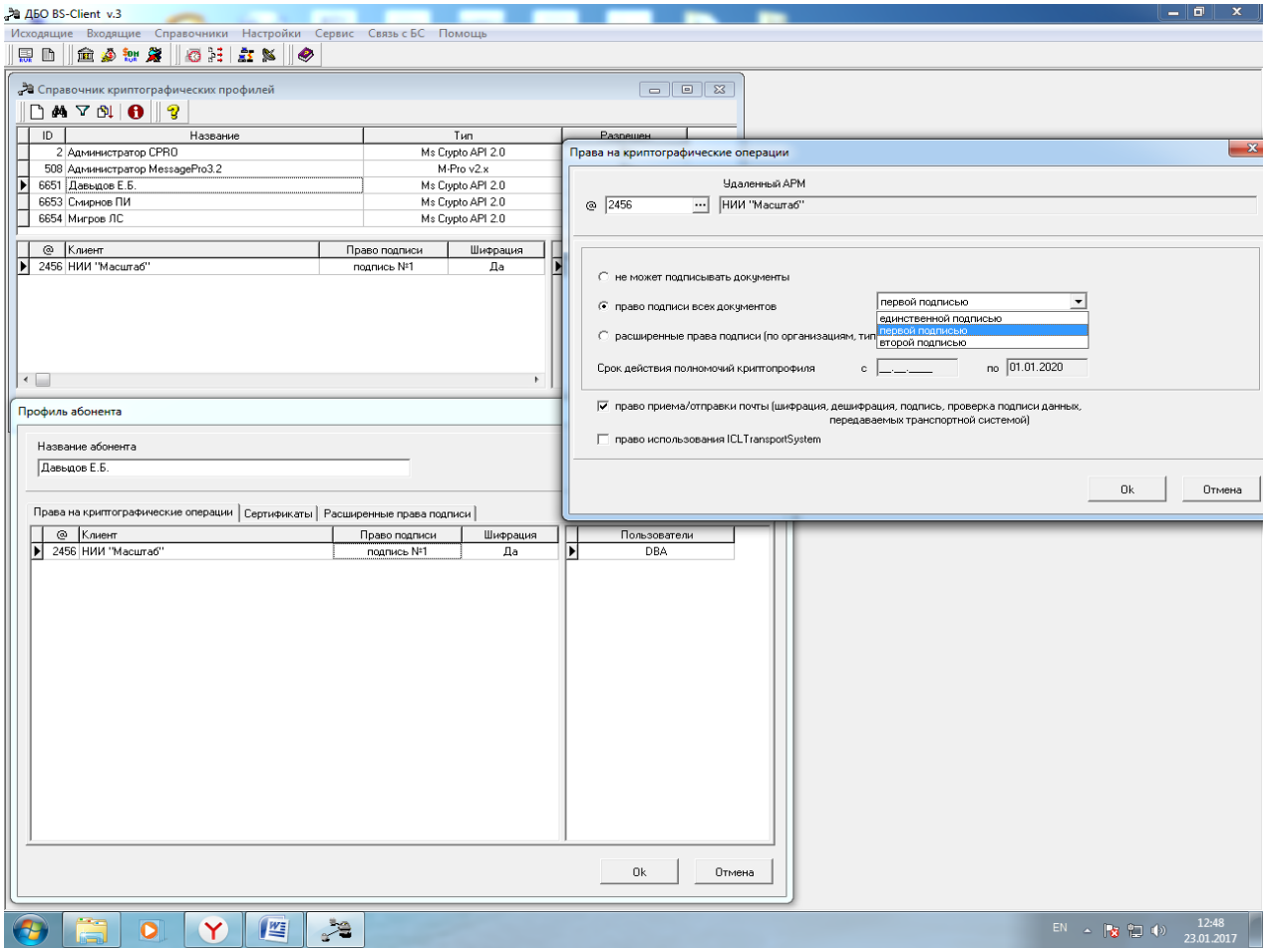

Рисунок А2 – Окно разделения прав подписи Газпромбанк

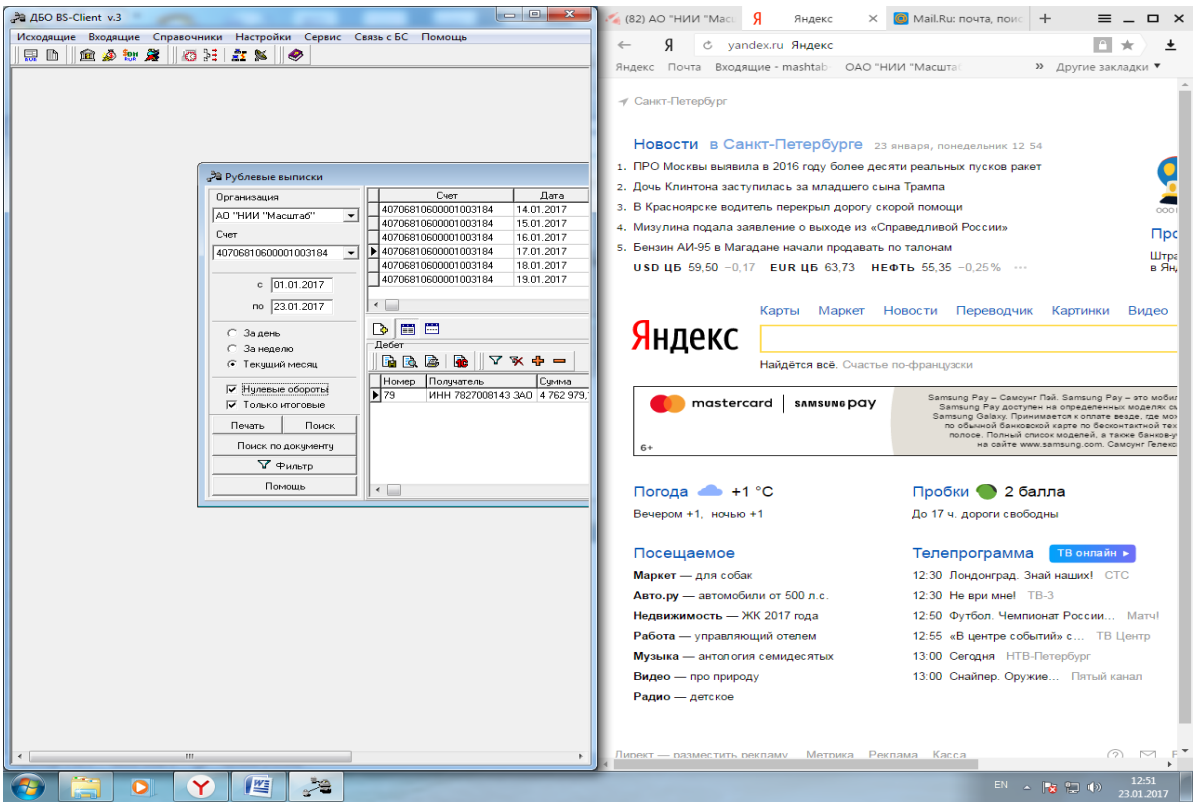

Рисунок А3 – Работа в сети интернет возможна при работе в системе Банк – Клиент Газпромбанк

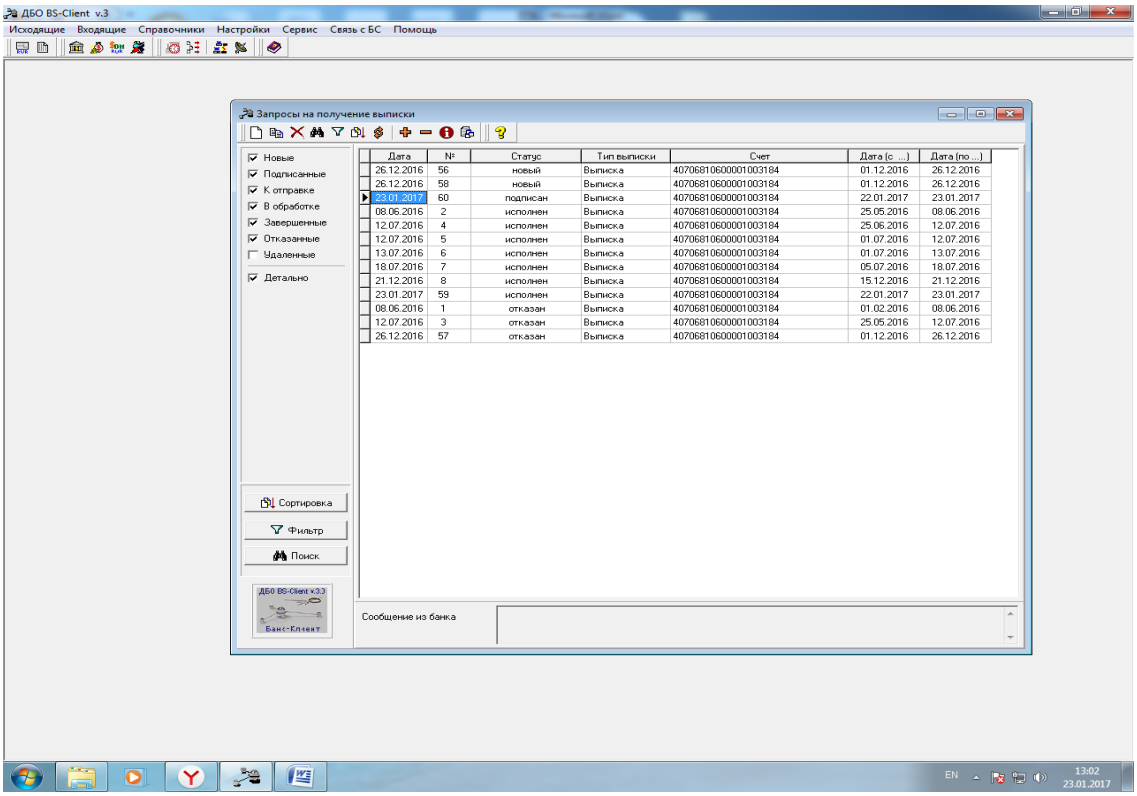

Рисунок А4 – Документ подписан без ввода пароля

ПРИЛОЖЕНИЕ Б

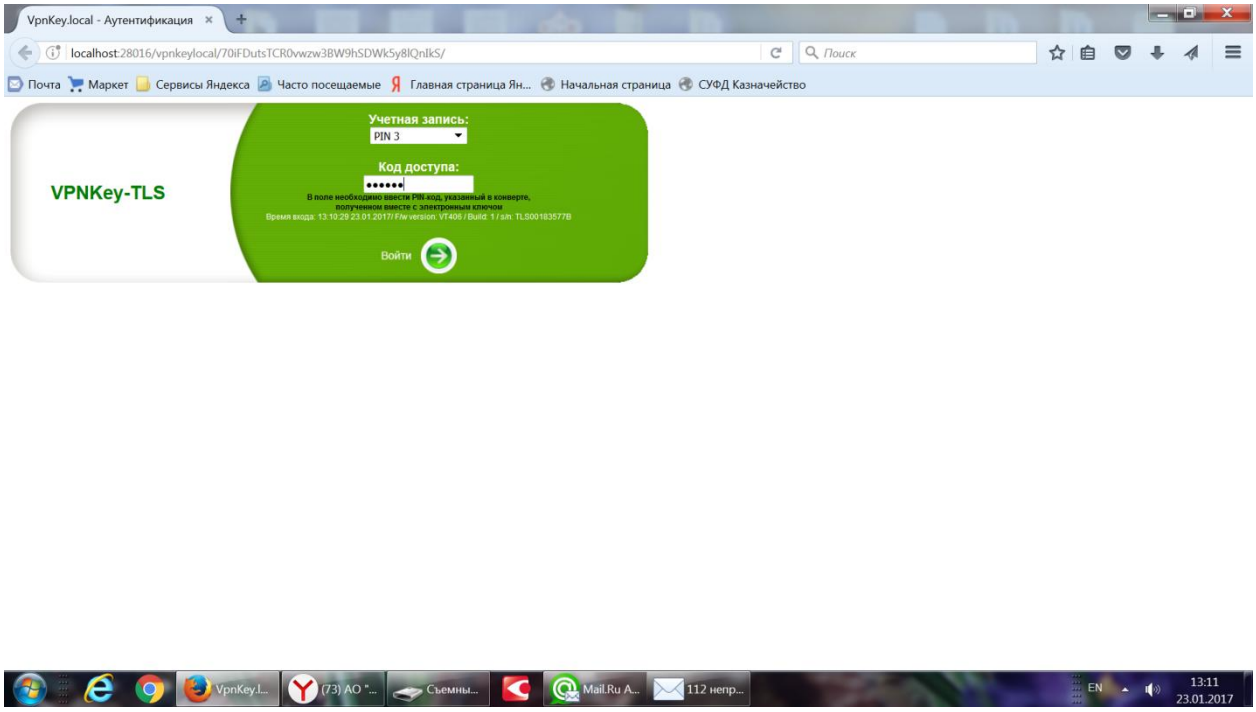

Рисунок Б1 – Окно авторизации в VPNСбербанк

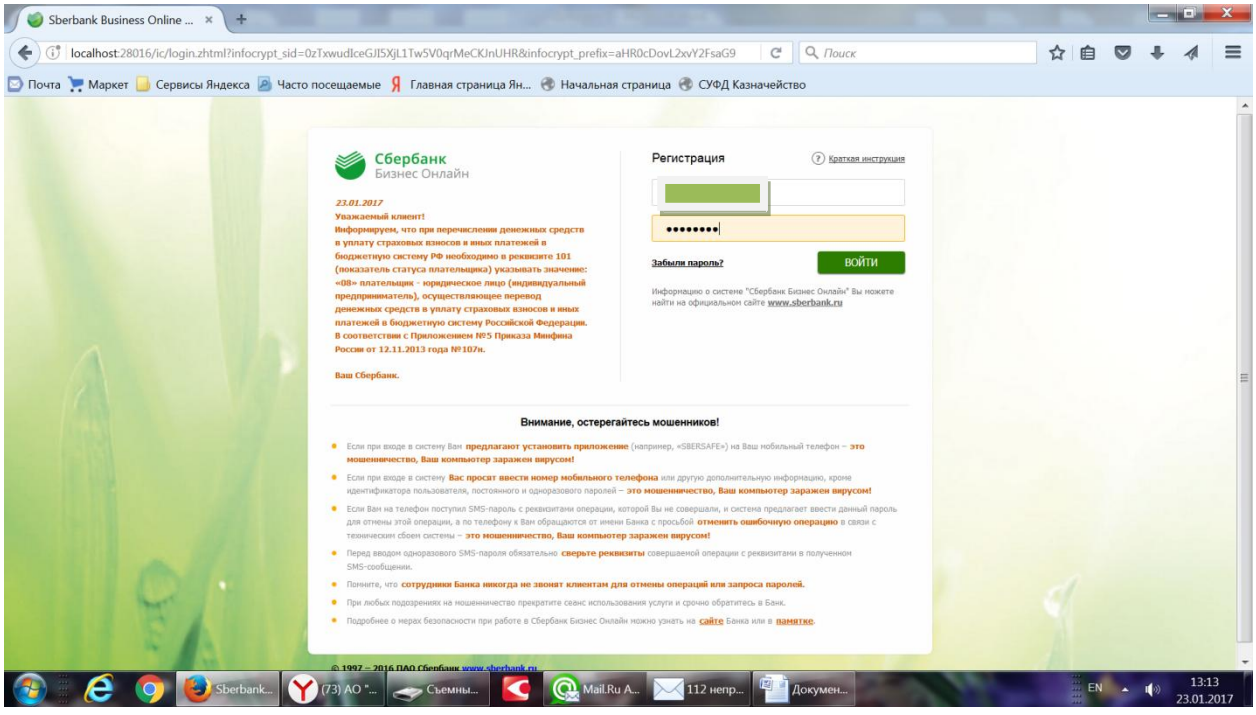

Рисунок Б2 – Окно авторизации в системе Сбербанк Бизнес Онлайн

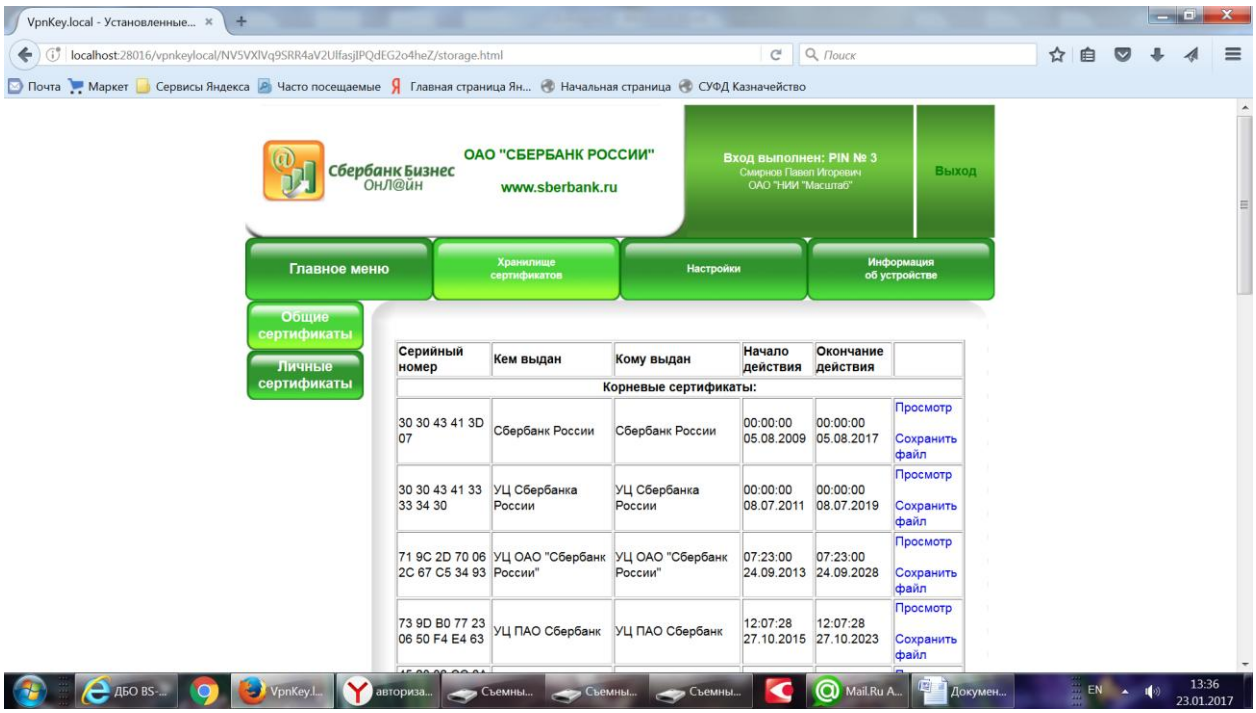

Рисунок Б3 – Хранилище сертификатов

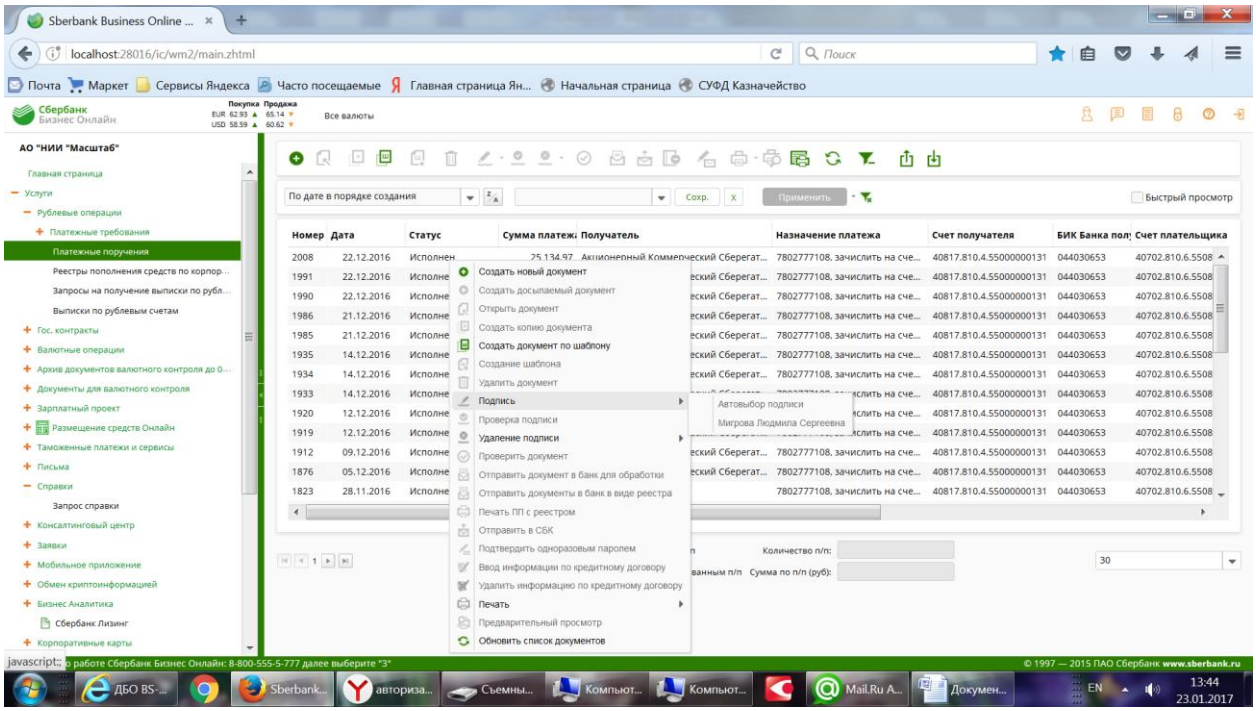

Рисунок Б4 – Подпись платежного поручения

ПРИЛОЖЕНИЕ В

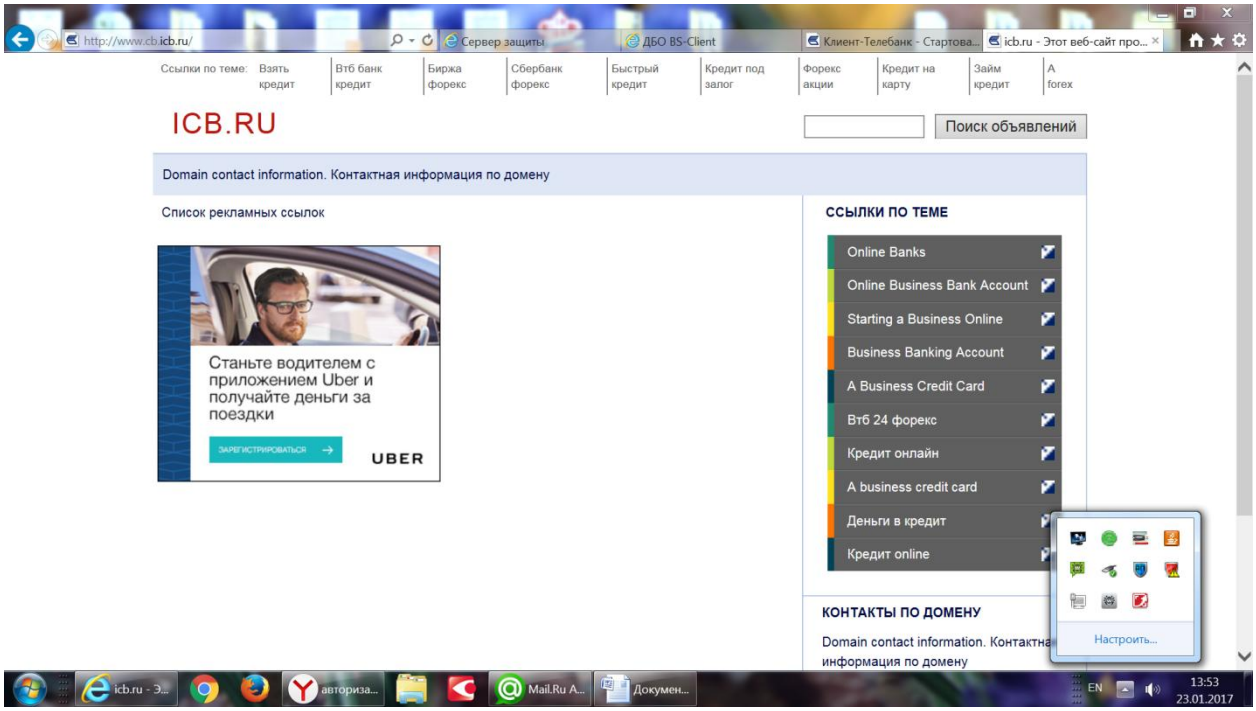

Рисунок В1 – Стартовая страница банка, если не активирован Inter – PROClient

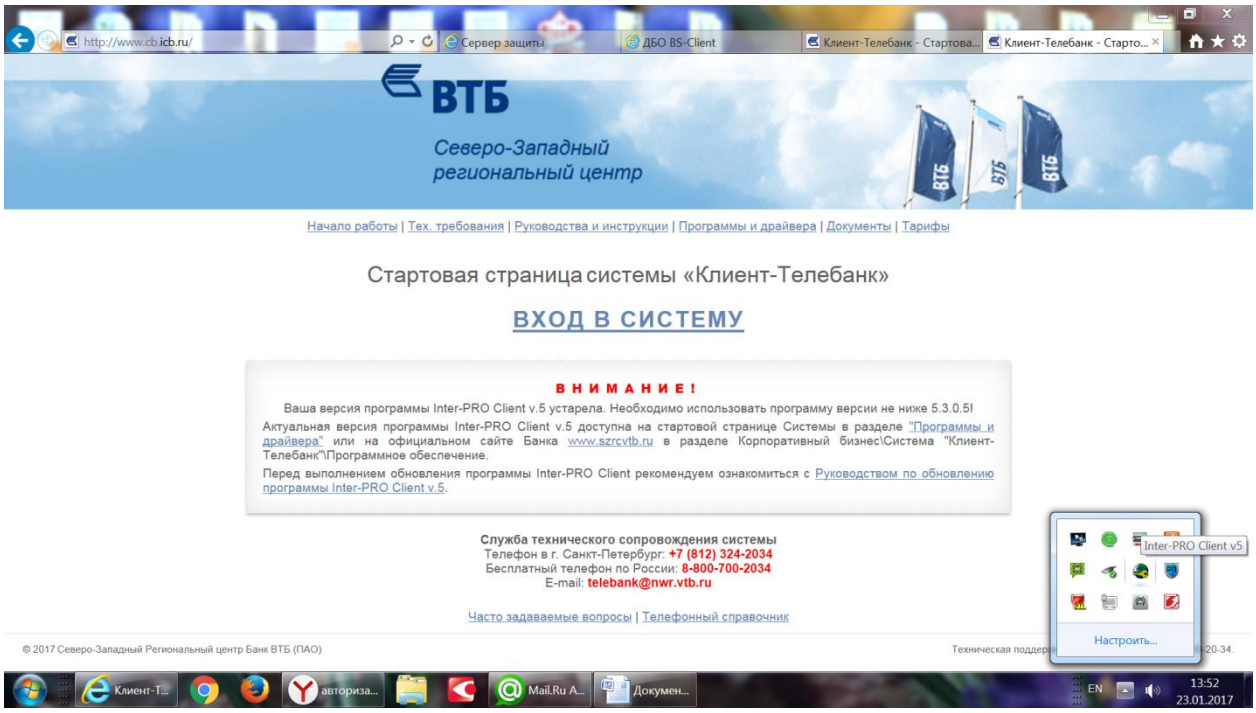

Рисунок В2 – Стартовая страница банка с активированным Inter – PROClient

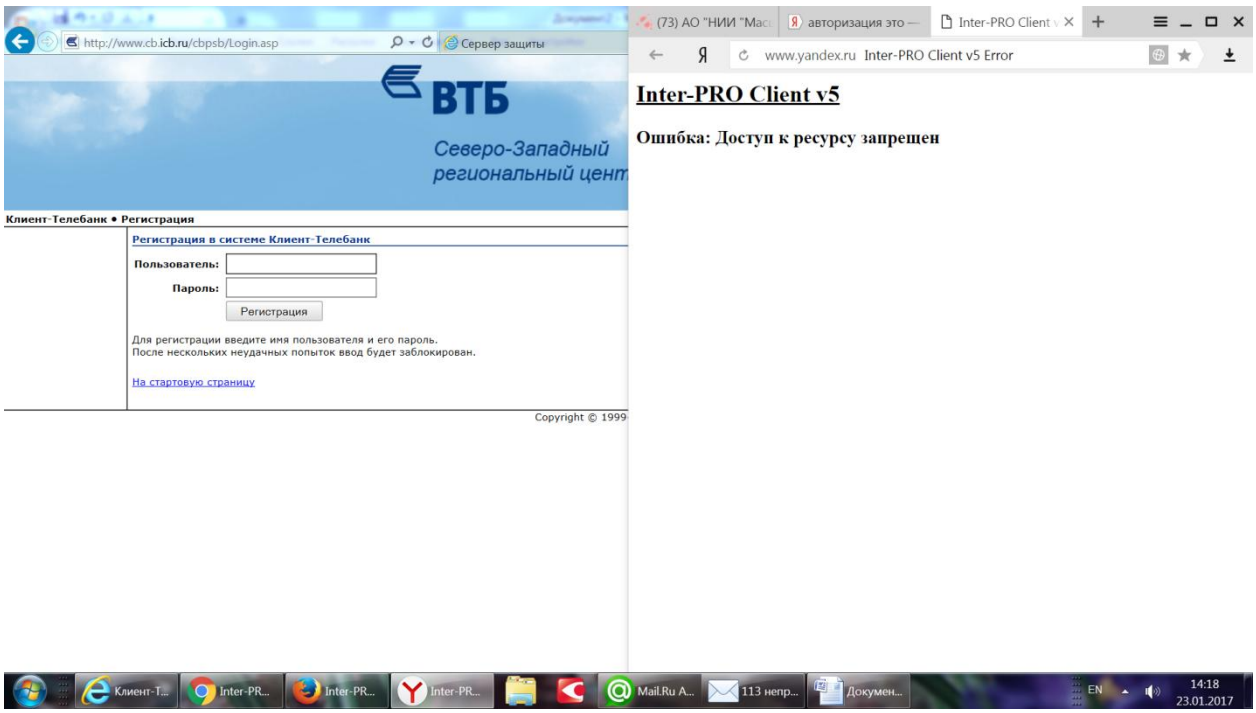

Рисунок В3 – Окно авторизации в системе

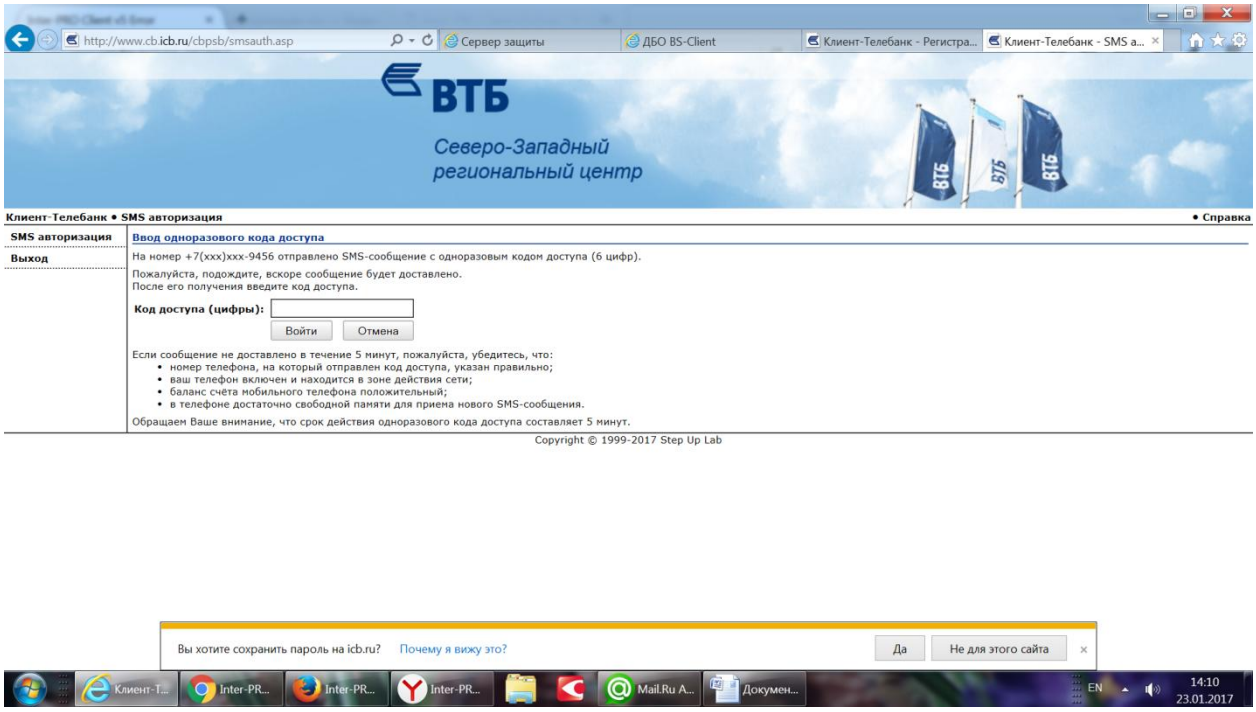

Рисунок В4 – Ввод кода доступа, присланного на телефон

ПРИЛОЖЕНИЕ Г

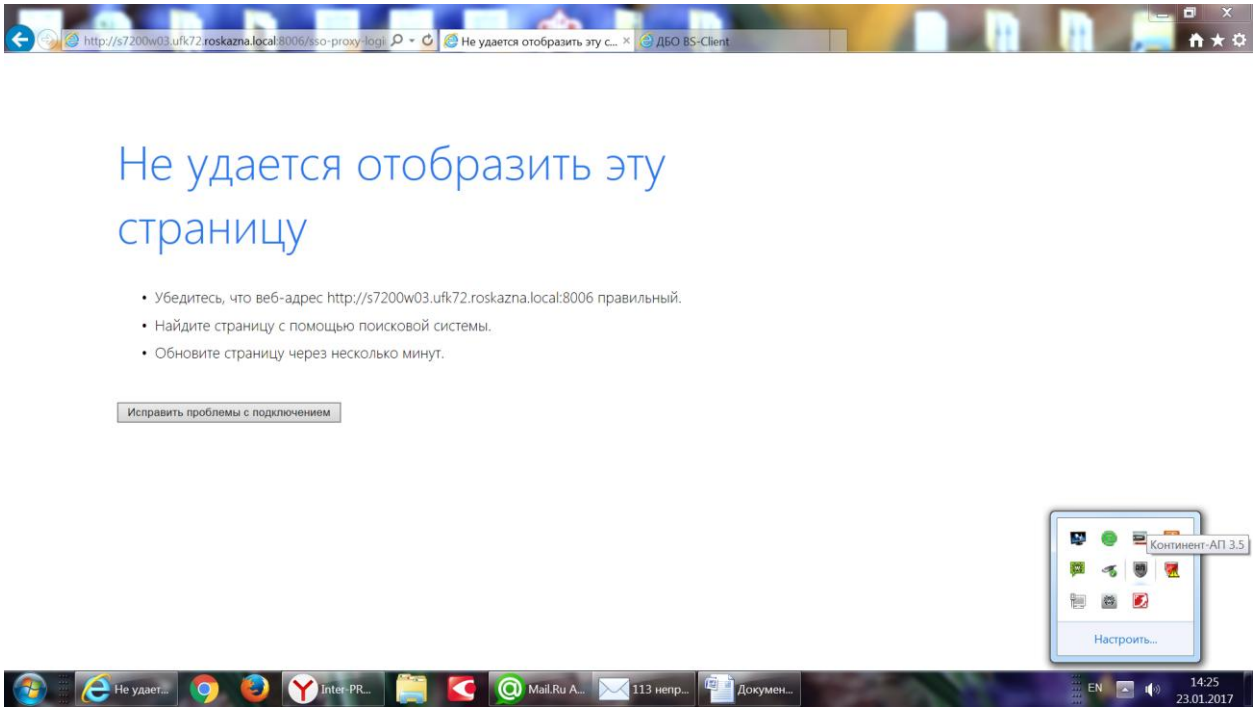

Рисунок Г1 – Невозможен запуск системе с отключенным АПКШ Континент

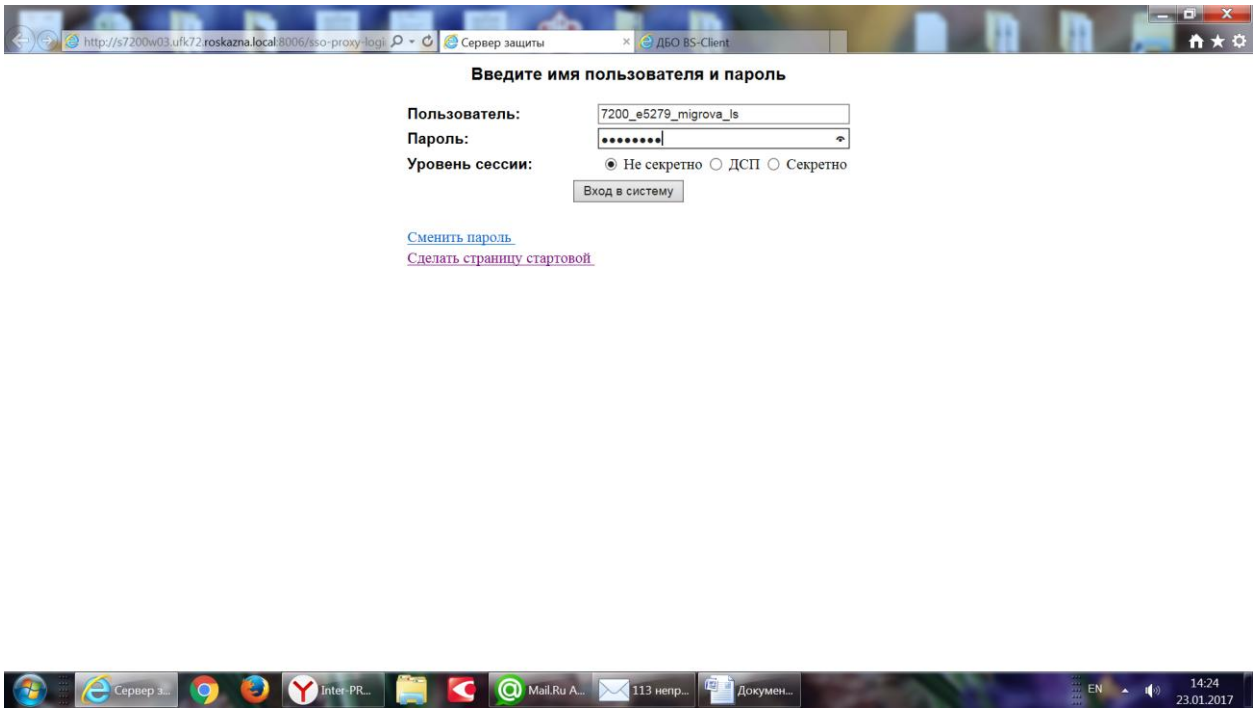

Рисунок Г2 – Окно авторизации в системе

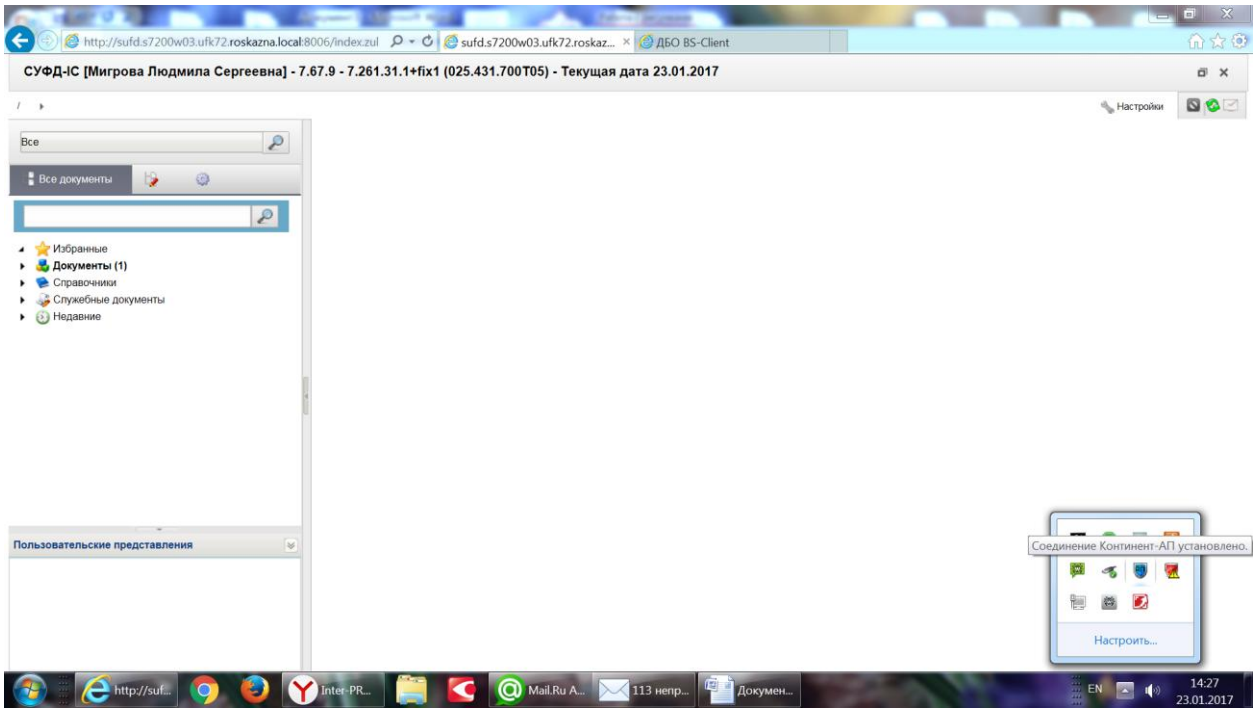

Рисунок Г3 – Главное окно системы. АПКШ активен

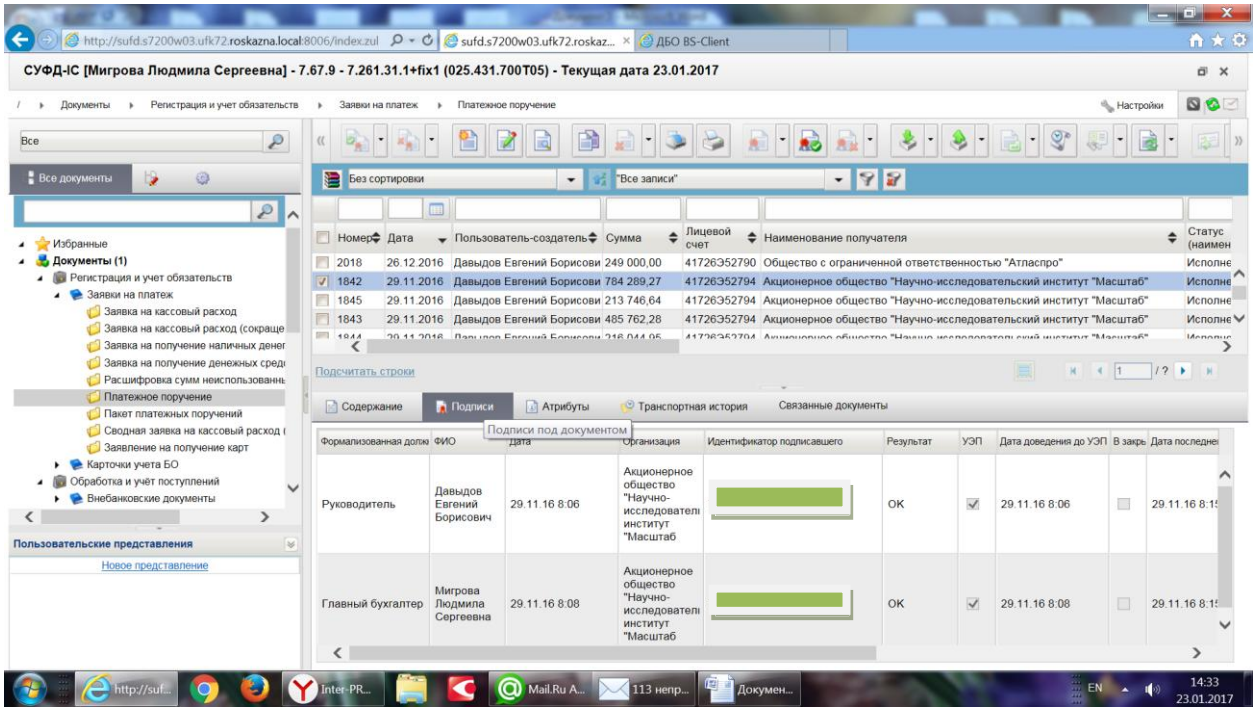

Рисунок Г4 – Подпись платежного поручения

ПРИЛОЖЕНИЕ Д

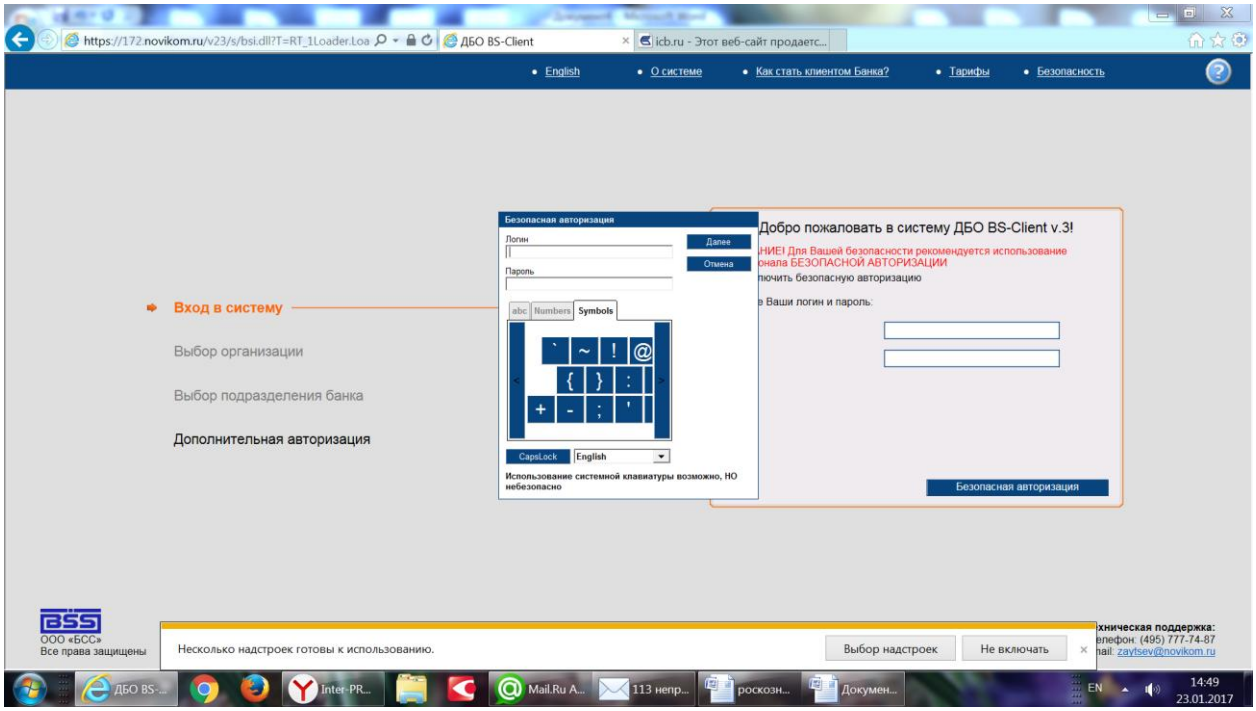

Рисунок Д1 – Окно авторизации в системе, ввода данных экранной клавиатуры

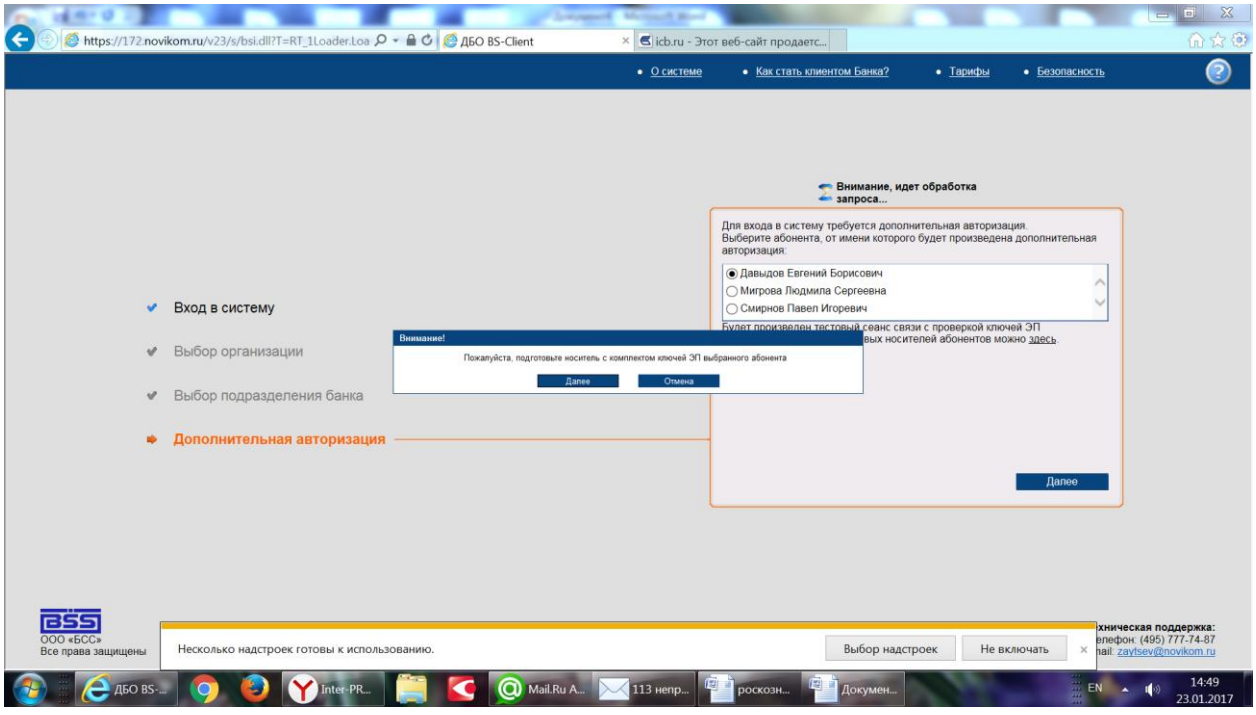

Рисунок Д2 – Запрос носителя с комплектом ключей электронной подписи выбранного пользователя

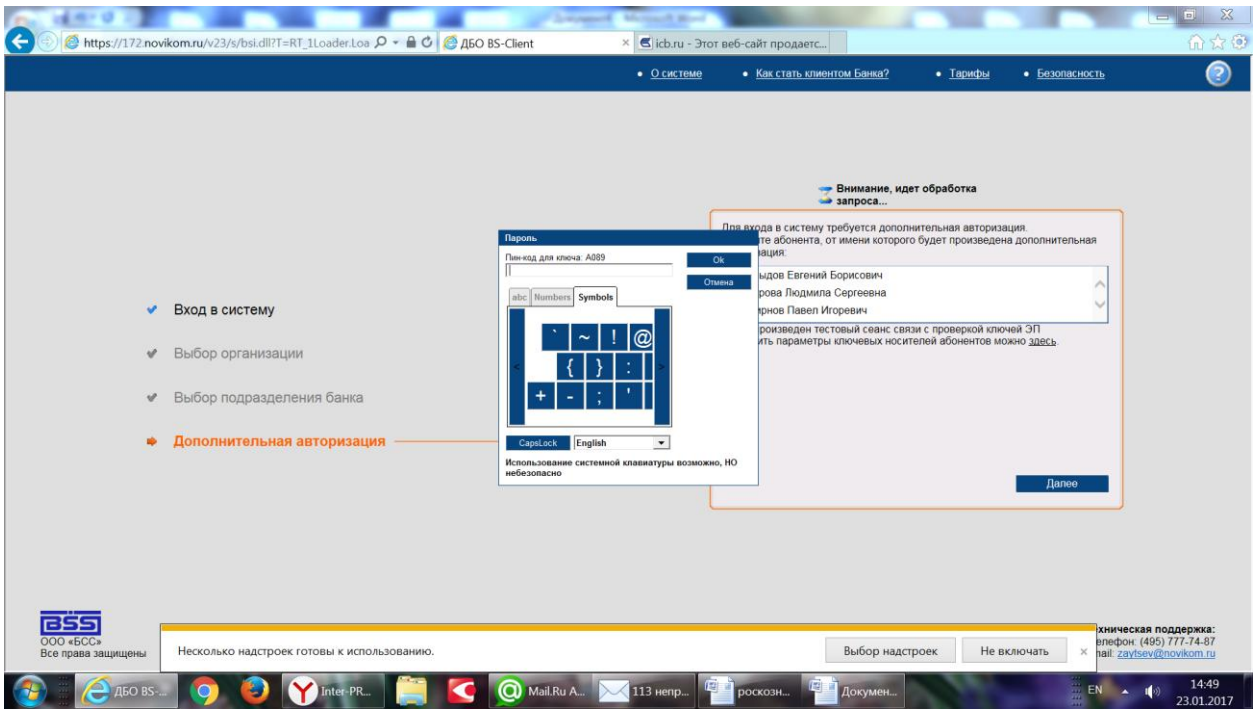

Рисунок Д3 – Запрос пин – кода пользователя, чей носитель с комплектом ключей ЭП находится в считывателе

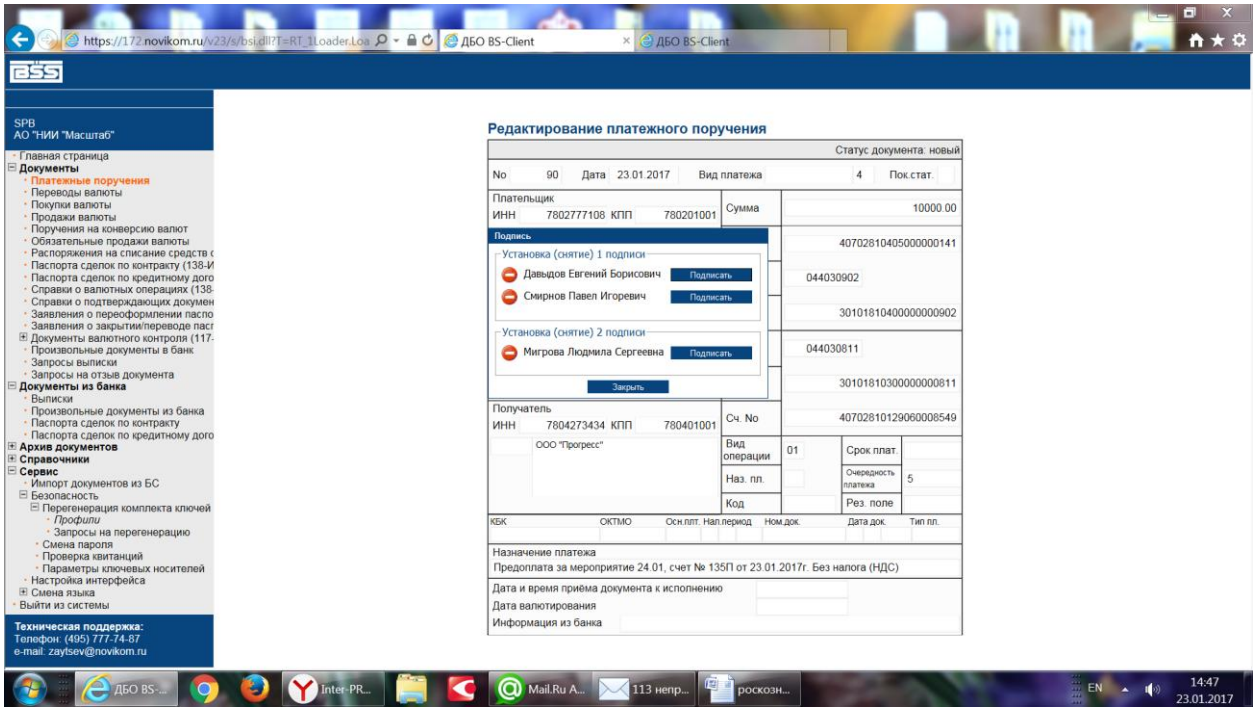

Рисунок Д4 – Подпись платежного поручения