ПРАВИЛА РАБОТЫ СИСТЕМЫ «КЛИЕНТ-БАНК»

г. Оренбург

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Система «Клиент-Банк» - Корпоративная информационная система дистанционного банковского обслуживания, организованная ОИКБ «РУСЬ» (ООО) (далее – Банк), включающая подсистему «Мобильный Клиент-Банк».

1.2. Настоящие Правила определяют порядок работы Клиента в рамках Системы «Клиент-Банк», регулируют отношения, возникающие в связи с этим между Банком и Клиентом.

1.3. Правила работы Системы «Клиент-Банк» разработаны в соответствии с действующим законодательством Российской Федерации, в том числе с положениями нормативных актов ФСТЭК России (Федеральной службы по техническому и экспортному контролю), ФСБ (Федеральной службы безопасности), Федерального закона от 06.04.2011 г. №63-ФЗ «Об электронной подписи» и других федеральных законов.

1.4. Настоящие Правила, включая все Приложения к ним, утверждаются Банком и размещаются на информационных стендах в структурных подразделениях Банка, в которых осуществляется обслуживание юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой, на официальном сайте Банка в сети Internet по адресу www.bankrus.ru.

1.5. Все изменения и дополнения в настоящие Правила и Приложения к ним вносятся Банком в одностороннем порядке. Информация об изменении/дополнении настоящих Правил и Приложений к ним доводится Банком до сведения Клиентов посредством уведомления не менее чем за 10 (Десять) календарных дней до даты вступления в силу таких изменений/дополнений. Уведомление осуществляется путем размещения соответствующей информации на официальном сайте Банка в сети Internet по адресу www.bankrus.ru, на информационных стендах в структурных подразделениях Банка, в которых осуществляется обслуживание юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой, а также путем направления Банком Клиенту соответствующего сообщения по Системе «Клиент-Банк».

1.6. Ознакомление Клиента с настоящими Правилами осуществляется до заключения между Банком и Клиентом договора об обмене электронными документами по Системе «Клиент-Банк».

1.7. Для заключения договора об обмене электронными документами по Системе «Клиент-Банк» Клиент предоставляет в Банк Заявление на подключение к Системе «Клиент–Банк» по форме, указанной в Приложении №1 к настоящим Правилам.

1.8. Клиент присоединяется к настоящим Правилам путем подписания договора об обмене электронными документами по Системе «Клиент-Банк», обязуется их выполнять и следить за всеми их изменениями и дополнениями. Условия настоящих Правил могут быть приняты Клиентом не иначе как путем присоединения к ним в целом. Настоящие Правила вступают в силу в отношении Клиента с момента заключения им с Банком договора об обмене электронными документами по Системе «Клиент-Банк».

1.9. Требования, предусмотренные настоящими Правилами, относятся к технологиям, системам и средствам обработки, передачи и хранения ЭД и предназначены для Клиентов Банка, принимающих участие в обмене ЭД по Системе «Клиент-Банк».

1.10. Безопасность технологии обработки ЭД обеспечивается созданием системы, включающей в себя комплекс технологических, организационных, аппаратных и программных мер и средств защиты на этапах подготовки, обработки, передачи и хранения ЭД.

1.11. Клиент обязуется соблюдать "Правила доступа к услугам дистанционного банковского обслуживания с указанием мер информационной безопасности", изложенные в Приложении №7 к настоящим Правилам.

1.12. Обязанности по администрированию программно-технических средств защиты ЭД рекомендуется возложить на одного из сотрудников, эксплуатирующих данную подсистему, с внесением соответствующих изменений в его должностные обязанности (Ответственный сотрудник Клиента).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированное рабочее место по обмену электронными документами (АРМ ОИ) – комплекс программных и аппаратных средств, включая средства криптографической защиты информации, используемых Сторонами для обмена ЭД.

Владелец сертификата ключа проверки электронной подписи (Владелец электронной подписи) – лицо, которому выдан сертификат ключа проверки электронной подписи.

Вредоносный код – компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование Банка и Клиента – пользователей систем дистанционного банковского обслуживания, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче любой информации в электронном виде, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

Клиент - юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающееся в установленном порядке частной практикой.

Ключевая информация – Ключ электронной подписи, Ключ проверки электронной подписи. Плановое обновление ключевой информации производится не реже 1 раза в течение 1 года 3 месяцев. Плановая смена ключей ЭП производится без смены Владельца электронной подписи, и типа носителя Ключевой информации.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с Ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Кодовое слово – секретный код, определяемый Клиентом и используемый для аутентификации Клиента в случае предоставления информации без личного присутствия Клиента (с использованием телефонной связи).

Компрометация ключа электронной подписи – событие, определенное Владельцем электронной подписи как ознакомление неуполномоченным лицом (лицами) с его ключом электронной подписи, а также утрата (хищение) ключа электронной подписи, утрата (хищение) ключа электронной подписи с последующим его обнаружением.

Ответственный сотрудник Клиента – полномочное лицо, назначенное Клиентом для организации:

- процедуры генерации Ключевой информации;
- мер, необходимых для обеспечения безопасности при обмене ЭД;
- обмена ЭД с использованием АРМ ОИ;
- взаимодействия с Банком по вопросам Ключевой информации и обмена ЭД.

Подсистема «Мобильный Клиент-Банк» (Мобильный Клиент-Банк) – подсистема Системы «Клиент-Банк», позволяющая осуществлять дистанционное банковское обслуживание средством Системы «Клиент-Банк», организованное Банком, в режиме реального времени с мобильных устройств, работающих на платформе iOS. Под управлением понимается полный функционал Системы «Клиент-Банк», определенный настоящими Правилами. «Мобильный Клиент-Банк» также позволяет использовать Систему «Клиент-Банк» с мобильных устройств на платформах Android в режиме просмотра, а именно, осуществление платежей и других действий со Счетом, требующих электронную подпись электронных документов, не осуществляется. При этом подсистема «Мобильный Клиент-Банк» в настоящем не рассматривается как отдельная система, и положения настоящего, применимые к Системе «Клиент-Банк», равно применимы к подсистеме «Мобильный Клиент-Банк», если не оговорено иное.

Актуальная версия руководства пользователя при работе с подсистемой «Мобильный Клиент-Банк» размещается Банком (либо указывается доступ к общедоступному ресурсу, где Клиент может получить документацию) на официальном сайте Банка www.bankrus.ru.

Подлинность электронного документа (подлинность ЭД) – положительный результат проверки ЭП зарегистрированного Владельца электронной подписи, устанавливающий факт неизменности содержания ЭД, включая все его реквизиты.

Подтверждение достоверности ЭД – процедура проверки правильности ЭП, позволяющая установить факт неизменности содержания электронного документа, включая все его реквизиты.

Правила – настоящие Правила работы Системы «Клиент-Банк».

Разработчик Системы – разработчик Системы Дистанционного Банковского Обслуживания BS-Client, включающая Систему «Банк-Клиент», Систему «Интернет-Клиент» и подсистему «Мобильный Клиент-Банк» - ООО «БСС», находящаяся по адресу 117105, г. Москва, Нагорный проезд, д. 5; Телефон/факс: +7 (495) 785-0494; E-mail: root@bssys.com; www.bssys.com.

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданный Банком и подтверждающий принадлежность Ключа проверки электронной подписи Владельцу электронной подписи.

Система «Клиент-Банк» – корпоративная информационная система дистанционного банковского обслуживания, организованная ОИКБ «Русь» (ООО) (далее – Банк), включающая подсистему «Мобильный Клиент-Банк», участники электронного взаимодействия в которой составляют определенный круг лиц.

СКЗИ – средства криптографической защиты информации.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка подлинности ЭП, создание Ключа электронной подписи и Ключа проверки электронной подписи.

Стороны – Банк и Клиент при совместном упоминании.

Счет – банковский счет в валюте Российской Федерации, иностранной валюте, открытый Банком Клиенту для осуществления банковских операций, в порядке и на условиях, предусмотренных договором банковского счета, внебалансовый счет по учету распоряжений, помещенных в очередь не исполненных в срок.

Тарифы - тарифы по обслуживанию юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой, утвержденные в порядке, установленном внутренними документами Банка.

Удостоверяющий центр – подразделение Банка, выполняющее функции регистрации и сертификации Ключей проверки электронной подписи Клиента и Банка.

Уполномоченный сотрудник Банка – сотрудник Банка, взаимодействующий с Клиентом в рамках работы по Системе «Клиент-Банк».

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому ЭД.

Электронный служебно-информационный документ (ЭСИД) – документ, в том числе и вложенный в виде отдельного файла, подписываемый ЭП, обеспечивающий обмен информацией с Банком (запросы, отчеты, другие документы) и имеющий равную юридическую силу с соответствующими документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати (при наличии), только при условии установления подлинности ЭСИД.

Электронный документ (ЭД) – электронный платежный документы и/или электронный служебно-информационный документ.

Электронный платежный документ (ЭПД) – документ, являющийся основанием для совершения операций по банковским счетам Клиента, открытым в Банке на основании договора банковского счета, подписанный ЭП и имеющий равную юридическую силу с распоряжениями на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати (при наличии), согласно заявленным образцам подписей и оттиска печати (при наличии), только при условии подтверждения подлинности ЭПД.

Электронное устройство – устройство Клиента, используемое в качестве удаленного рабочего места для целей дистанционного управления денежными средствами Клиента: персональный компьютер или планшетный компьютер.

Электронная подпись, ЭП – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. По классификации Федерального закона от 06.04.2011г. №63-ФЗ "Об электронной подписи" электронная подпись, используемая в системе "Банк-клиент" относится к усиленной неквалифицированной электронной подписи.

PIN-код – пароль доступа к следующим типам носителей Ключевой информации: USB-ключу eToken, смарт-карте eToken устройства Safe Touch, смарт-карте eToken устройства смарт-карт ридер для iPhone/iPad/iPod служит для дополнительной защиты. Пароль может содержать знаки (цифры, буквы, символа) на английской раскладке на клавиатуре, и быть не менее 4 знаков.

3. НОСИТЕЛИ КЛЮЧЕВОЙ ИНФОРМАЦИИ И ПОРЯДОК ОБРАЩЕНИЯ С НИМИ

3.1. В рамках работы Системы «Клиент-Банк» для записи Ключевой информации используются следующие типы носителей Ключевой информации:

3.1.1. USB-ключ eToken,

3.1.2. Смарт-карта eToken устройства Safe Touch,

3.1.2. Смарт-карта eToken устройства смарт-карт ридер для iPhone/iPad/iPod,

3.1.4. Гибкий диск 3,5"/USB-накопитель.

3.2. Клиент самостоятельно выбирает один из предлагаемых Банком в соответствии с Тарифами типов носителей Ключевой информации, который будет использоваться им в рамках работы в Системе «Клиент-Банк», путем подписания Заявления на подключение к Системе «Клиент–Банк» (Приложение № 1 к настоящим Правилам).

Клиент имеет право менять тип используемого носителя Ключевой информации на основании соответствующего заявления (Приложение № 2 к настоящим Правилам) в течение срока работы в Системе «Клиент-Банк».

3.3. Носители Ключевой информации рекомендуется маркировать и учитывать в журнале, в котором указывается Ф.И.О. сотрудника, сформировавшего Ключевую информацию (в случае формирования Ключевой информации на стороне Клиента), дата формирования, вид содержащейся на нем информации, срок действия носителя Ключевой информации, перечень лиц, допущенных к работе с данным носителем, дата и причину вывода носителя из действия.

3.4. Создание Ключевой информации необходимо проводить на выделенном Электронном устройстве, программное обеспечение которого должно выполнять только функции, регламентированные технологическим процессом формирования криптографических ключей. При этом электронное устройство рекомендуется размещать в отдельном, выделенном только для этой цели помещении.

3.5. Электронное устройство, вырабатывающее Ключевую информацию, должно быть оснащено программно-аппаратными системами защиты информации от несанкционированного доступа, имеющими сертификат ФСТЭК.

3.6. Доступ посторонних (неуполномоченных) лиц к носителям с Ключевой информацией должен быть исключен. Не допускается:

- снимать несанкционированные копии с носителей Ключевой информации;
- знакомить с содержанием носителей Ключевой информации или передавать носители Ключевой информации лицам, в обязанности которых не входит работа в Системе "Клиент-Банк" (в том числе не передавать носители IT-специалистам, обслуживающим АРМ ОИ):
- выводить ключи электронной подписи /закрытые ключи шифрования на дисплей (монитор) или принтер;
- устанавливать носитель Ключевой информации в считывающее устройство Электронного устройства в режимах, не предусмотренных функционированием системы обработки и обмена ЭД, а также в другие Электронные устройства;
- записывать на носитель Ключевой информации постороннюю информацию.

3.7. Клиент обязан присоединять носитель Ключевой информации к Электронному устройству непосредственно перед началом работы с Системой «Клиент – Банк». По окончании работы извлекать носитель Ключевой информации из Электронного устройства.

3.8. В случае прекращения по тем или иным причинам полномочий сотрудника Клиента, имевшего доступ к Системе «Клиент-Банк», Клиенту необходимо в кратчайшие сроки произвести смену паролей, перегенерацию закрытых ключей шифрования и ключей электронной подписи, бывших в распоряжении данного сотрудника.

3.9. Срок действия Ключевой информации– 1 год 3 месяца. После ввода в действие новых ключей ЭП / закрытых ключей шифрования недействительные (старые) ключи ЭП / закрытые ключи шифрования уничтожаются Клиентом самостоятельно с составлением акта. Ключи проверки ЭП / открытые ключи шифрования хранятся Клиентом в течение всего

срока хранения ЭД, для подтверждения подлинности которых могут быть использованы. Уничтожение ключей проверки ЭП / открытых ключей шифрования после истечения срока их хранения осуществляется Клиентом самостоятельно с составлением акта.

3.10. В случае если Банк производит генерацию (перегенерацию) ключа(ей) электронной подписи на следующих типах носителей ключей информации: USB-ключа eToken, смарт-карты eToken устройства Safe Touch. смарт-карты eToken устройства смарт-карт ридер для iPhone/iPad/iPod Банк устанавливает по умолчанию PIN-код на USB-ключа eToken - 1234567890, на смарт-карты eToken устройства Safe Touch и смарт-карты eToken устройства смарт-карт ридер для iPhone/iPad/iPod – 123456.

Клиент обязан провести смену PIN-кода Владельца электронной подписи не позднее рабочего дня, следующего за днем получения «Сертификата ключа проверки электронной подписи», указанного в Договоре об обмене электронными документами по Системе «Клиент-Банк».

При неправильном вводе PIN – кода 3 (Три) раза подряд USB-ключ eToken, смарт – карта eToken устройства Safe Touch, смарт-карта eToken устройства смарт-карт ридер для iPhone/iPad/iPod блокируется. В этом случае Клиент должен обратиться в Банк для проведения процедуры перегенерации ключей ЭП в порядке, указанном в Договоре об обмене электронными документами по Системе «Клиент-Банк».

4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДГОТОВКЕ, ОБРАБОТКЕ И ПЕРЕДАЧИ ЭД

4.1. На АРМ ОИ рекомендуется устанавливать только лицензионное программное обеспечение. АРМ ОИ в обязательном порядке должно быть оснащено средствами антивирусной защиты, а также желательно программно-аппаратными системами защиты от несанкционированного доступа.

4.2. Конфиденциальность ЭД обеспечивается на основе использования средств криптографической защиты информации.

4.3. При эксплуатации СКЗИ необходимо соблюдать требования и рекомендации эксплуатационной документации на СКЗИ.

4.4. Клиент должен четко регламентировать порядок использования Электронного устройства, с которого осуществляется взаимодействие с Системой «Клиент – Банк», в том числе список лиц и порядок доступа к Электронному устройству.

4.5. Не рекомендуется использовать на АРМ ОИ средства удаленного (дистанционного) доступа, которые часто применяют IT-специалисты для удалённой поддержки.

4.6. Не рекомендуется использовать АРМ ОИ для доступа к посторонним сайтам.

4.7. Не рекомендуется устанавливать на АРМ ОИ постороннее программное обеспечение, например программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Доказано, что подобные программы передают информацию о содержимом просматриваемых страниц посторонним лицам.

4.8. Не рекомендуется запускать на АРМ ОИ программы, полученные из не заслуживающих доверия источников.

4.9. Клиент должен перед вводом своего логина и пароля убедиться, что установлено соединение с легальным сайтом Системы "Клиент-Банк" ОИКБ "Русь" (ООО). Необходимо проверить правильность указания адреса сайта, наличие сертификата безопасности.

4.10. Клиент должен всегда явным образом завершать сеанс работы с Системой «Клиент – Банк», используя пункт меню «Выход».

4.11. Клиент не должен совершать доступ к Системе «Клиент – Банк» с использованием постороннего Электронного устройства.

4.12. При заключении договора об обмене электронными документами по Системе "Клиент-Банк" Клиент в Заявлении по форме, указанной в Приложении №1 к настоящим Правилам, по желанию может указать IP-адреса и MAC-адреса Электронного устройства на установку в Банке фильтра для вашего АРМ ОИ. Это позволит исключить возможность входа под вашим логином/паролем с Электронного устройства злоумышленников.

4.13. В случае обнаружения подозрительных сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов ОИКБ "Русь" (ООО), Банк рекомендует сообщить об этом по электронной почте bankrus@bankrus.ru.

4.14. В случае использования системы защиты Safe Touch Клиент обязан перед наложением ЭП и отправкой ЭПД проверять реквизиты получателя ЭПД, отображаемые на экране устройства Safe Touch с использованием смарт-карты eToken, на соответствие реквизитам получателя ЭПД, которому направляется перевод денежных средств. Если реквизиты получателя ЭПД, отображаемые на экране устройства Safe Touch, не соответствуют реквизитам получателя ЭПД, которому направляется перевод денежных средств, Клиент обязан не отправляя (не подтверждая) в Банк ЭПД, предпринять самостоятельно меры по выяснению, устранению причины указания неверных данных, в случае подозрения на компрометацию ключевой информации, действовать в порядке, указанном в разделе 13 настоящих Правил.

5. ПРАВИЛА АНТИВИРУСНОЙ ЗАЩИТЫ АРМ ОИ

5.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

5.2. Клиент должен производить регулярную антивирусную проверку и регулярное обновление антивирусных баз.

5.3. При возникновении подозрения на наличие Вредоносного кода/компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) или обнаружении компьютерных вирусов (выдается сообщение от антивируса об обнаружении вируса) должны быть приняты все меры для их удаления, после этого необходимо сменить пароль в Систему «Клиент-Банк» (в т.ч. Мобильный Клиент-Банк) и проконтролировать состояние банковского счёта (путем просмотра Выписки по Счету).

5.4. В случае обнаружения вирусов категории Trojan-Banker (вредоносные программы, предназначенные для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт), Trojan-Spy (вредоносные программы, предназначенные для ведение электронного шпионажа за пользователем), Backdoor (вредоносные программы, предназначенные для скрытого удалённого управления злоумышленником пораженным Электронным устройством) необходимо незамедлительно обратиться в Банк, предпринять все меры для прекращения любых операций с электронными документами с использованием ключей ЭП / закрытых ключей шифрования и произвести их смену. Категорически запрещается работать на Электронном устройстве с финансовыми документами при наличии вирусов.

5.5. Клиент должен незамедлительно обратиться в Банк в случае:

- подозрительной активности на Электронном устройстве (самопроизвольное сворачивание или открывание окон, движение курсора, запуск различных программ и прочее) в период неактивности пользователя;
- появления каких-либо дополнительных окон или сообщений при попытке доступа в Систему «Клиент-Банк» (в т.ч. Мобильный Клиент-Банк) либо в процессе работы в Системе «Клиент-Банк» (в т.ч. Мобильный Клиент-Банк);
- невозможности получения доступа к Системе «Клиент-Банк» (в т.ч. Мобильный Клиент-Банк) и т. д.

5.6. Банк не несет ответственность в случае финансовых потерь, понесенных Клиентом, в связи с нарушением и (или) ненадлежащим исполнением им требований по защите от Вредоносного кода/компьютерного вируса клиентских автоматизированных рабочих мест систем дистанционного банковского обслуживания.

6. ПРАВИЛА ПАРОЛЬНОЙ ЗАЩИТЫ

6.1. На учетные записи пользователей АРМ ОИ необходимо устанавливать пароль и для мобильных устройств пароль на разблокировку экрана.

6.2. Полная плановая смена паролей пользователей АРМ ОИ должна проводиться регулярно, не реже одного раза в 30 (Тридцать) дней.

6.3. Личные пароли должны генерироваться пользователями самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих паролей;
- пользователь не имеет права сообщать личный пароль другим лицам.

6.4. Внеплановая полная смена паролей пользователей АРМ ОИ должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) пользователя АРМ ОИ.

6.5. В случае компрометации личного пароля одного из пользователей АРМ ОИ, должна быть произведена внеплановая полная смена паролей всех пользователей данного АРМ ОИ.

6.6. Клиент не должен использовать функцию запоминания логина и пароля в браузерах.

6.7. Клиент не должен использовать одинаковые логин и пароль для доступа к различным системам.

7. РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ

7.1 Разделы 3-6 настоящих Правил определяют защитные меры по снижению рисков нарушения информационной безопасности при использовании Клиентом Системы «Клиент – Банк».

При этом Клиент обязан учитывать то, что:

- сеть Internet не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Internet могут обеспечить только те услуги, которые реализуются непосредственно ими;
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Internet;

- существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из сети Internet.;
- гарантии по обеспечению информационной безопасности при использовании сети Internet никаким органом/учреждением/организацией не предоставляются;
- меры по нейтрализации злоумышленных действий могут быть эффективными только в течение первых часов после инцидента.

7.2. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы «Клиент – Банк». Содержимое журнала Системы «Клиент – Банк» используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования злоумышленных действий.

7.3. При несоблюдении настоящих Правил Клиент несет риски потери носителя Ключевой информации, раскрытия, искажения и несанкционированного использования ключей ЭП.

7.4. Вследствие несанкционированного использования злоумышленниками Ключевой информации возможно нанесение материального ущерба Клиенту или нанесение ущерба его деловой репутации.

7.5. В случае утраты Клиентом носителя Ключевой информации Банк не восстанавливает ключи электронной подписи/шифрования. Информация Клиента, зашифрованная при помощи утерянного носителя Ключевой информации, восстановлению не подлежит.

7.6. При повторном получении Сертификата информация, зашифрованная с использованием старого носителя Ключевой информации, в случае его уничтожения, восстановлению не подлежит.

8. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К ЗАПОЛНЕНИЮ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

При подготовке ЭД Клиент должен осуществлять контроль на уникальность номера документа (ненулевое значение), правильность указания даты, наличие заполненных реквизитов.

В соответствии с указаниями Регионального центра информатизации Главного управления Банка России по Оренбургской области Клиент должен контролировать реквизиты ЭД на наличие недопустимых спецсимволов:

Перечень десятичных кодов запрещенных спецсимволов: **0-31, 126-175, 241-255.**

9. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ЭЛЕКТРОННЫМ УСТРОЙСТВАМ ДЛЯ ОРГАНИЗАЦИИ АРМ ОИ КЛИЕНТА

9.1. Установка программных средств АРМ ОИ может быть произведена на Электронном устройстве, которое должно соответствовать следующим требованиям:

Для стационарных и портативных устройств, за исключением подсистемы Мобильный Клиент-Банк:

- технические характеристики устройства не ниже уровня Pentium-II-250, ОЗУ 32Mb, 100Mb свободного места на HDD, наличие видеосистемы (видеоадаптер VGA, монитор VGA) с поддержкой видеорежимов не ниже 1024*766, 256 цветов;
- работающий под управлением операционной системы WinNT/2000/XP и выше, установленным интернет браузером Internet Explorer версии 7.0 и выше, установленным текстовым процессором Microsoft Word версии XP/2003 и выше или OpenOffice версии 2.3 и выше.
- иметь доступ к сети интернет на скорости не ниже 256 кб/с (по предварительному согласованию с банком, возможно подключение через коммутируемые линии связи общего пользования (телефонные линии), при этом используемый модем (не WIN модем) должен иметь характеристики не хуже чем 19200bps, Hayes-совместимый);
- для печати документов необходим принтер, совместимый с программными средствами Windows;

Требования к рабочим станциям пользователей подсистемы Мобильный Клиент-Банк

Требования к программному окружению

Операционная система: iOS 6 и выше, Android 2.3.3 - 2.3.7, 4.0.3 - 4.0.4, 4.1, 4.2 и выше

Требования к аппаратному обеспечению

Устройство, используемое пользователем для работы с подсистемой Мобильный Клиент-Банк, должно обладать следующими характеристиками:

диагональ экрана не менее 5.5";

объем свободного места на диске 50Mb;

разрешение экрана, соответствующее указанному в следующей таблице:

Платформа / ОС	**Разрешение экрана (пикселей)**									
	1024x768	2048x1536	1024x600	1280x768	1280x800	1920x1200	720x1280	800x1280	800x480	800x600
iOS	+	+	-	-	-	-	-	-	-	-
Android	-	-	+	+	+	+	+	+	+	+

10. ПОРЯДОК ДЕЙСТВИЙ КЛИЕНТА В СЛУЧАЕ ВЫЯВЛЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

10.1. В случае выявления хищения денежных средств в Системе «Клиент–Банк» (в т.ч. Мобильный Клиент-Банк) Клиент обязан:

10.1.1. немедленно прекратить любые действия с Электронным устройством, на котором организовано АРМ ОИ, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь аккумуляторную батарею из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Internet, USB, Wi-Fi и др.) или перевести в режим гибернации (режим пониженного потребления электроэнергии, все открытые документы и программы сохраняются на жестком диске, затем Электронное устройство выключается).

10.1.2. незамедлительно проинформировать Банк о выявленном факте хищения денежных средств в порядке и сроки, предусмотренные Разделом 13 настоящих Правил.

10.1.3. произвести фотосъёмку рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) Электронного устройства как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.), и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры Электронного устройства, следует поместить его в непрозрачный пакет (мешок) и опечатать горловину. При необходимости ведения хозяйственной деятельности – задействовать другое Электронное устройство.

10.1.4. предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Internet (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

10.1.5. провести сбор записей с межсетевых экранов, серверов баз данных и иных компонент клиентского приложения Системы «Клиент-Банк», систем авторизации пользователей (AD, NDS и т.д.), Электронных устройств, используемых для управления денежными средствами через Систему «Клиент-Банк», устройств, которые могут использоваться для удалённого управления указанными Электронными устройствами.

10.1.6. зафиксировать в протокольной форме значимые действия и события (в том числе действия с Электронным устройством, на котором организовано АРМ ОИ), предшествовавшие факту хищения денежных средств, подготовить объяснения Клиента (сотрудников Клиента) об использовании Электронного устройства в целях, отличных от осуществления операций в Системе «Клиент–Банк», посещаемых сайтах, о странностях при работе Электронного устройства, перебоях или отказах Электронного устройства, обращениях в ИТ-службы, в Банк, о сторонних лицах, побывавших в месте расположения Электронного устройства и т.д.

10.2. Клиент не должен предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности Электронного устройства, отправлять Электронное устройство в сервисные службы для восстановления работоспособности.

10.3. Все действия, указанные в п.10.1.1., 10.1.3., 10.1.4.,10.1.5.,10.1.6. настоящих Правил, сотрудникам Клиента необходимо производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъёмки.

10.4. Клиент имеет право в течение одного дня с момента обнаружения факта утери, кражи, компрометации Ключевой информации, незаконном использовании Ключевой информации, обратиться:

10.4.1. к Интернет-провайдеру с письменным заявлением о предоставлении журналов соединения (логов) для получения в электронной форме журналов соединений с Internet Электронного устройства Клиента или из его локально-вычислительной сети как минимум за три месяца, предшествовавшие факту хищения денежных средств. Рекомендуемая форма заявления указана в Приложении № 4 к настоящим Правилам.

10.4.2. в правоохранительные органы с письменным заявлением о возбуждении уголовного дела по факту хищения денежных средств. Рекомендуемая форма заявления указана в Приложении № 5 к настоящим Правилам.

10.5. Клиенту рекомендуется составить обращение в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона КУСП (из книги учета сообщений о преступлениях), содержащую отметку правоохранительного органа о его приеме.

10.6. Клиент должен предоставить в Банк перечень документов, указанный в Приложении № 6 к настоящим Правилам, копии заявлений, направленных Интернет – провайдеру и в правоохранительные органы в соответствии с п. 10.4. настоящих Правил в случае их направления.

10.7. Для продолжения работы в Системе «Клиент-Банк» Клиент должен обратиться в Банк для внеплановой замены Ключевой информации.

11. ПОРЯДОК РАЗРЕШЕНИЯ РАЗНОГЛАСИЙ ПРИ ОБМЕНЕ ЭД В СИСТЕМЕ «КЛИЕНТ-БАНК»

11.1. Разногласия, возникающие между Сторонами в рамках работы в Системе «Банк-Клиент», разрешаются уполномоченными представителями Сторон в рамках согласительной комиссии (далее – Комиссия).

11.2. При возникновении разногласий при обмене ЭД Сторона, заявляющая разногласие (Сторона-инициатор), обязана в срок, не превышающий пяти дней, направить другой Стороне заявление о разногласиях, подписанное руководителем Стороны, с подробным изложением причин разногласий и предложением создать Комиссию с целью установления авторства и подлинности спорного документа в электронном виде. Заявление должно содержать фамилии представителей Стороны-инициатора, которые будут участвовать в работе Комиссии, место, время и дату сбора Комиссии (не позднее 7 дней со дня

отправления заявления). В состав Комиссии включаются представители Клиента, представители Банка, а в случае необходимости (при несогласии Клиента с результатами разрешения разногласий и предоставления соответствующего заявления) - независимые эксперты, обладающие специальными знаниями в области средств криптографической защиты информации и информационной безопасности, представители компании - Разработчика Системы. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате их услуг. Выбор членов Комиссии осуществляется по согласованию со всеми участниками. При невозможности согласованного выбора, последний проводится случайно (по жребию). Комиссия создается организационно-распорядительным документом Банка. В состав Комиссии должно входить равное количество полномочных представителей от каждой Стороны. Состав Комиссии фиксируется в акте, который является итоговым документом, отражающим результаты работы Комиссии.

До подачи заявления Стороне-инициатору рекомендуется убедиться в целостности своего программного обеспечения, неизменности используемой Ключевой информации, отсутствии воздействия различного рода вредоносного программного обеспечения, а также отсутствии несанкционированных действий со стороны персонала, обслуживающего собственный АРМ ОИ, и внешних нарушителей.

11.3. Целью работы созданной Комиссии является установление подлинности созданного ЭД. Сторонами принимаются к рассмотрению только надлежащим образом оформленные ЭД.

11.4. Срок работы Комиссии - не более 5 (Пяти) рабочих дней. В особо сложных ситуациях этот срок может быть увеличен до 30 (Тридцати) дней.

11.5. На время разрешения спорной ситуации Банк имеет право приостановить работу Клиента в Системе «Клиент-Банк» с последующим уведомлением Клиента.

11.6. При возникновении спорной ситуации в отношении подлинности документа в электронном виде и принадлежности ЭП, Стороны не исполняют указанный документ до разрешения спорной ситуации.

11.7. Стороны способствуют работе Комиссии и не допускают отказа от предоставления необходимых документов. В противном случае заинтересованная Сторона имеет право составить акт в одностороннем порядке и направить его другой Стороне для сведения.

11.8. Комиссия принимает в качестве исходных электронных документов файлы, формируемые Системой «Клиент–Банк», установленной на расположенном в Банке сервере, из архивных баз данных ЭД Банка, подлинность которых удостоверяется проверкой ЭП Владельца электронной подписи и формированием полученного результата проверки ЭП Клиента.

11.9. Комиссия использует для проверки подлинности ЭД в качестве эталонного программное обеспечение Банка, установленное на Электронном устройстве по обработке ЭД Клиентов. Комиссия применяет следующий порядок проверки подлинности ЭД:

- на выделенном Банком Электронном устройстве создаётся каталог C:\BSS;
- необходимо установить крипто - провайдер Crypto-Pro 1.1 build 85, или более новый, из имеющегося в Банке дистрибутивного комплекта данного программного обеспечения;
- в каталог C:\BSS копируется эталонное программное обеспечение: файлы CRPROTST.EXE, SIGNCHCK.EXE;
- на сервере ДБО Банка выполняется процедура выгрузки документа в текстовый файл;
- после того, как выгрузка документа в текстовый файл завершена, необходимо выполнить преобразование текстового файла в MIME формат. Преобразование осуществляется модулем signchck.exe в следующем порядке: необходимо запустить signchck.exe, передав ему в качестве параметра имя текстового файла, в который был выгружен документ (см. предыдущее действие):
  signchck.exe <имя текстового файла>.
  В результате образуется файл с тем же именем, но с расширением *.1. Новый файл содержит в конце электронную подпись Клиента (или несколько электронных подписей);

для проверки электронной подписи необходимо выполнить следующую команду:

CrProtst.exe <имя файла с расширением *.1 для проверки>.

Если в результате исполнения программа выдает сообщение: «The verify is Ok!», то результат проверки ЭП считается положительным.

Если в результате исполнения программа выдает сообщения: “Verification sign failed”, “file <имя файла с расширением *.1 для проверки> is not contain signed data from BSS system” (где: <имя файла с расширением *.1 для проверки> - имя файла для проверки), то результат проверки ЭП считается отрицательным.

В результате исполнения программа выдает дополнительную информацию.

11.10. При выполнении всех перечисленных условий Комиссия выносит заключение о подлинности ЭД и составляет акт о результатах проведения процедуры проверки подлинности ЭД.

11.11. Составленный Комиссией акт является основанием для выработки Сторонами окончательного решения по спорному вопросу. Данное решение должно быть подписано полномочными представителями Сторон на позднее 10 (Десять) календарных дней с момента окончания работы Комиссии.

11.12. В случае если на предложение Стороны-инициатора о создании Комиссии ответ другой Стороны не был получен или получен отказ от участия в работе Комиссии, или если другой Стороной чинились препятствия в работе Комиссии, Сторона-инициатор вправе составить акт в одностороннем порядке с указанием причины его составления. В акте приводится обоснование выводов о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого ЭД. Указанный акт

составляется в двух экземплярах, подписывается уполномоченным должностным лицом, и один экземпляр направляется другой Стороне.

11.13. В случае, когда Банк предъявляет ЭД Комиссии, корректность ЭП Клиента признана Комиссией, принадлежность Клиенту открытых ключей Клиента подтверждена, Банк от Клиента по выполненным операциям со Счетом Клиента претензий не принимает.

11.14. В том случае, если Банк исполнил ЭД, заверенный ЭП, подлинность которого не подтверждена Комиссией, претензии Клиента к Банку, связанные с последствиями исполнения данного ЭД, могут быть признаны обоснованными. В случае принятия Комиссией решения о необходимости возмещения Клиенту денежных средств по операциям, совершенным без его согласия, уполномоченный член Комиссии на основании акта не позднее 7 (Семи) календарных дней формирует соответствующее распоряжение о возмещении Клиенту суммы операции по спорному ЭД.

12. ПОРЯДОК ИНФОРМИРОВАНИЯ КЛИЕНТОВ ОБ ОПЕРАЦИЯХ ПО СЧЕТУ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ «КЛИЕНТ–БАНК»

12.1. Банк уведомляет Клиента, использующего Систему «Клиент-Банк», обо всех проводимых по Счету операциях ежедневно в рабочие дни путем формирования и предоставления Клиенту с использованием Системы «Клиент-Банк» выписки по Счету, содержащей информацию об операциях, проведенных по Счету Клиента в предшествующий день:

- по Счетам в рублях Российской Федерации – не позднее **9-00** часов местного времени рабочего дня, следующего за днем проведения операций по Счету;
- по Счетам в иностранной валюте - не позднее **12-00** часов местного времени рабочего дня, следующего за днем проведения операций по Счету;

Временем и датой получения Клиентом уведомления, указанного в настоящем пункте Правил, **считается время и дата формирования и предоставления Банком Клиенту доступа к выписке по Счету**. **Время и дата уведомления фиксируются в электронном протоколе, который ведется Банком.**

Клиент обязан ежедневно проверять уведомления, полученные от Банка в соответствии с настоящим пунктом Правил путем входа в Систему «Клиент – Банк».

12.2. Дополнительно к уведомлениям, указанным в п.12.1. Правил, Банк уведомляет Клиента о поступлении распоряжения Клиента о проведении расходной операции по Счету с использованием Системы «Клиент-Банк» (далее – Уведомление), одним из следующих способов:

- путем направления SMS–сообщений на номер мобильного телефона Клиента,
- путем направления E-mail сообщений на адрес электронной почты Клиента.

12.3. Клиент самостоятельно определяет способ получения Уведомлений Банка в соответствии с п.12.2. Правил при подключении к Системе «Клиент–Банк», а также может его изменять в течение срока действия договора об обмене электронными документами по Системе «Клиент-Банк» путем оформления соответствующего заявления (Приложения №1, №2 к настоящим Правилам).

Клиент также может изменять номер мобильного телефона/адрес электронной почты, на который Банком осуществляется отправка Уведомлений, в течение срока действия договора об обмене электронными документами по Системе «Клиент-Банк» путем оформления соответствующего заявления (Приложение №2 настоящим Правилам).

12.4. Уведомление, указанное в п.12.2. настоящих Правил, направляется Банком Клиенту в течение 10 (Десяти) минут с момента поступления распоряжения Клиента о проведении расходной операции по Счету с использованием Системы «Клиент-Банк».

12.5. Клиент самостоятельно обеспечивает все необходимые мероприятия для получения от Банка SMS и E-mail сообщений в соответствии с указанной Клиентом в заявлении информацией, в том числе, но неисключительно: поддержание в рабочем состоянии мобильного телефона, функции получения SMS-сообщений (в т.ч. в роуминге), обеспечение доступа в Интернет, работоспособности указанного в заявлении почтового ящика для осуществления контроля за входящими e-mail сообщениями и т.п.

12.6. **Временем и датой получения Клиентом Уведомления**, направленного Банком Клиенту в виде SMS или E-mail сообщения, **считается время и дата его отправления Банком**, указанные **в электронном протоколе передачи SMS или E-mail сообщения, который ведется Банком.** История отправления SMS/ E-mail сообщений фиксируется на сервере Банка и хранится не менее 3 (Трех) лет.

12.7. Уведомление Банка составляется латинскими символами, либо на русском языке и должно содержать следующую информацию:

- наименование Банка и указание на проведение операции с использованием Системы «Клиент-Банк»,
- дата и время распоряжения Клиента – дд.мм.гггг чч:мм,
- номер Счета, по которому Клиентом направлено распоряжение на списание денежных средств, - 20 знаков номера Счета,
- сумма списания денежных средств согласно распоряжению Клиента – указывается в валюте счета (рубли - RUR, доллары США - USD, Евро – EURO),
- номер Счета, на который перечисляются денежные средства согласно распоряжению Клиента, - 20 знаков номера Счета,

- при необходимости другая информация.

Пример СМС - Уведомления:

ОНСВ”RUS”Klient-Bank, 12.10.2012 13:54, с 40702810000000001234 rashod 120,900.12RUR na 40817810000000004321.

Пример Email – Уведомления:

Банк ”Русь” Клиент-Банк,12.10.2012 13:54 для списания со счета 40702810000000001234 поступил документ на сумму 120,900.12 рублей на счет 40817810000000004321. Получатель «ООО «XXX»»

12.8. Клиент должен использовать собственные программно-технические средства (мобильный телефон, Электронное устройство и т.п.) для получения Уведомлений Банка и самостоятельно оплачивать все расходы, связанные с использованием сетей связи.

12.9. Клиент несет ответственность за обеспечение доступа к мобильному телефону/адресу электронной почты только полномочных лиц Клиента.

12.10. Клиент должен незамедлительно уведомить Банк в письменной форме в случае смены номера мобильного телефона/электронного адреса, утери, кражи, пропажи и иных случаях утраты мобильного телефона, SIM–карты, утраты доступа к электронной почте, также смены SIM-карт или их передачи третьим лицам по любым основаниям.

12.11.Банк производит изменение номера мобильного телефона/адреса электронной почты для отправки Клиенту Уведомлений не позднее одного рабочего дня, следующего за днем получения Банком соответствующего заявления (Приложение №2 к настоящим Правилам).

12.12.Банк не несет ответственности за качество доставки (факт доставки, скорость передачи и т.д.) SMS и E-mail сообщений, в том числе вызванных авариями и иными неполадками в оборудовании, сетях и линиях связи третьих лиц, а также не гарантирует конфиденциальности и целостности передачи информации.

12.13.Клиент признает, что передача информации в объеме и порядке, предусмотренном настоящими Правилами, является правомерным раскрытием информации и производится с его согласия и по его поручению. Клиент осознает и в полном объеме принимает на себя все риски, связанные с возможным раскрытием информации, предаваемой посредством SMS и E-mail сообщений.

12.14. Банк не несет ответственности за не доставленные либо доставленные не полностью/не в срок SMS и E-mail сообщения, если это произошло по причинам, не зависящим от Банка.

12.15. Банк не несет ответственность за действия по направлению уведомлений в случае нарушения Клиентом условий пункта 12.10. настоящих Правил.

13. ПОРЯДОК ИНФОРМИРОВАНИЯ БАНКА КЛИЕНТОМ О КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ, НЕСОГЛАСИИ КЛИЕНТА С ПРОВЕДЕННОЙ РАСХОДНОЙ ОПЕРАЦИЕЙ ПО СЧЕТУ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ «КЛИЕНТ-БАНК»

13.1. В случае компрометации Ключевой информации, если Клиент подозревает возможность возникновения подобных ситуаций, а также в случае несогласия Клиента с расходной операцией по Счету, проведенной с использованием Системы «Клиент-Банк», Клиент обязан незамедлительно уведомить об этом Банк по телефону, указанному в Разделе 15 настоящих Правил.

При обращении в Банк по телефону Клиент должен сообщить наименование Клиента, номер Счета, Кодовое слово.

13.2. Кодовое слово предоставляется Клиентом в Банк в заявлении по форме Приложений №1, № 2 к настоящим Правилам. При наличии дополнительного соглашения к договору банковского счета о предоставлении информации о состоянии Счета, Клиент может использовать данное кодовое слово для извещения Банка о выявленном факте.

Клиент обязан хранить Кодовое слово в тайне, обеспечить нераспространение его третьим лицам и исключить возможность использования кодового слова неуполномоченными лицами. Риск негативных последствий такого использования несет Клиент.

13.3. В случае если Клиент не назвал Кодовое слово или сеанс связи Клиента с Банком был прерван, Уполномоченный сотрудник Банка перезванивает Клиенту на номер телефона, указанный в хранящемся в Банке досье Клиента.

13.4. Датой и временем получения Банком от Клиента сообщения о факте, указанном в п.13.1. Правил, считается дата и время получения устного сообщения Клиента по телефону, указанному в разделе 15 настоящих Правил, или при отсутствии устного сообщения – дата и время получения Банком письменного заявления Клиента по форме Приложения № 3 к настоящим Правилам.

13.5. Устное сообщение Клиента должно быть в обязательном порядке подтверждено письменным заявлением по форме Приложения № 3 к настоящим Правилам, переданным в Банк в течение одного рабочего дня после устного сообщения.

В случае предоставления Клиентом данного заявления для разрешения спорной ситуации организационно-распорядительным документом Банка создается Комиссия, порядок работы которой указан в разделе 11 настоящих Правил.

14. ОСОБЫЕ УСЛОВИЯ

14.1. Банк имеет право направлять Клиенту по Системе «Клиент-Банк», на номера мобильных телефонов и адреса электронной почты, представляемые Клиентом Банку в рамках настоящих Правил, сообщения информационного и рекламного характера.

14.2. Банк имеет право проводить запись телефонных переговоров между Уполномоченным сотрудником Банка и Клиентом.

14.3. Банк имеет право приостановить или прекратить использование Клиентом Системы «Клиент-Банк» при нарушении Клиентом настоящих Правил и/или договора об обмене электронными документами по Системе «Клиент-Банк», заключенного между Банком и Клиентом.

14.4. Во всем, что прямо не предусмотрено настоящими Правилами и Приложениями к ним, Стороны руководствуются договором об обмене электронными документами по Системе «Клиент-Банк», заключенным между Банком и Клиентом, а также действующим законодательством Российской Федерации.

15. КОНТАКТНАЯ ИНФОРМАЦИЯ БАНКА

г. Оренбург
пер. Сакмарский, д.4.
Телефоны: (3532) 445-700 (добавочно 1272, 1273, 1274, 1275, 1276, 1277, 1278, 1279)
(3532) 445-762, 445-763, 445-764, 445-765, 445-767, 445-768, 445-769, 445-771

ул. 8 Марта, д.35.
Отдел пластиковых карт
Телефоны: (3532) 445-772 (добавочно 1321,1322,1323)

г. Бузулук
ул. 1-й мкр-н, д.16в,
Телефоны: (35342) 7-99-48, 7-99-30 (вн. 1801, 1802)
Режим работы: понедельник-пятница с 08.30. до 17.30, перерыв на обед с 13.00. до 14.00

г. Орск
пр-т Мира, д.26, встроенное помещение № 3
Телефон: (3537) 203-140, 203-138 (вн. 1605)
Режим работы: понедельник-пятница с 08.30. до 17.30, перерыв на обед с 13.00. до 14.00

Телефон (3532) 445-735 - по которому можно связаться с дежурными специалистами Банка в указанные часы:
в понедельник – четверг с 13.00. до 14.00, с 17.30. до 19.00,
пятница с 13.00. до 14.00, с 16.30 до 19.00
суббота с 09.00 до 17.00

Приложение №1

к Правилам работы Системы «Клиент-Банк»

В ОИКБ «Русь» (ООО) (далее – Банк)

Юридический адрес: 460014, г. Оренбург, пер. Шевченко,7

от _____

Наименование Клиента

_____

ИНН Клиента

Контактные телефоны: _____

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ К СИСТЕМЕ «КЛИЕНТ-БАНК»

1. Прошу заключить с _____ (далее – Клиент)

полное наименование Клиента

договор об обмене электронными документами по Системе «Клиент-Банк».

2. Подтверждаю, что с Правилами работы Системы «Клиент-Банк» (далее – Правила) в действующей редакции ознакомился и согласен с их условиями, при заключении с Банком договора об обмене электронными документами по Системе «Клиент-Банк» обязуюсь исполнять Правила, а также следить за всеми их изменениями и дополнениями.

3. Прошу предоставить доступ к Системе «Клиент-Банк»

- ☐ **с использованием Мобильного Банк-Клиента.**
- ☐ **без использования Мобильного Банк-Клиента.**

4. Для работы в Системе «Клиент-Банк» прошу предоставить в качестве носителя Ключевой информации:

- ☐ **USB-ключ eToken** в количестве ___ штук.
- ☐ **Смарт-карту eToken для Safe Touch** в количестве ___ штук.
- ☐ **Смарт-карту eToken для** Смарт-карт ридера для iPhone/iPad/iPod в количестве ___ штук.
- ☐ **USB-накопитель** в количестве ___ штук.

5. В целях обеспечения контроля доступа, прошу:

☐ **не устанавливать** фильтрацию IP-адреса и MAC-адреса Электронного устройства, с которого осуществляется работа Клиента в Системе «Клиент – Банк»

☐ **установить** фильтрацию перечисленных ниже IP-адреса и MAC-адреса Электронного устройства, с которого осуществляется работа Клиента в Системе «Клиент – Банк».

Список доступных адресов:

№ п/п	IP-адрес	MAC-адрес
1		
2		
3		

6*. **Прошу Банк направлять Уведомления** на условиях, в порядке и в сроки, предусмотренные Правилами, следующим способом:

- ☐ **SMS-сообщения на номер:**

7										

(номер мобильного телефона в федеральном формате)

- ☐ **E-mail сообщения на электронный адрес:**

_____

(адрес электронной почты)

Прошу использовать вышеуказанный **номер мобильного телефона / адрес электронной почты** *(ненужное зачеркнуть)* для направления Банком Клиенту Уведомлений согласно настоящему заявлению по всем имеющимся у Клиента на дату его составления, а также по всем вновь открываемым Клиенту банковским счетам.

Прошу Банк не направлять Уведомления на условиях, в порядке и в сроки, предусмотренные Правилами _____

Подпись Клиента

7. **Прошу установить кодовое слово** для использования его в экстренных случаях при обращении в Банк в соответствии с Правилами, в том числе при возникновении несанкционированных списаний с расчетного счета Клиента, утере, хищении, компрометации Ключевой информации и т.п. в рамках использования Системы «Клиент-Банк»:

+7										

Прошу использовать вышеуказанный **номер мобильного телефона Владельца ключевой информации** в экстренных случаях при обращении в Банк в соответствии с Правилами, в том числе при утере, хищении, компрометации Ключевой информации и т.п. в рамках использования Системы «Клиент-Банк».

8. Сокращенное наименование Клиента латинскими буквами - _____

* Данный пункт не заполняется Клиентами, не имеющими Счет в Банке (которые намерены использовать Систему «Клиент-Банк» только для обмена реестрами).

9. Прошу списать предусмотренные тарифами Банка комиссии, связанные с подключением Клиента к работе в Системе «Клиент-Банк», с любого расчетного счета Клиента, открытого в Банке.

Вся информация, указанная в настоящем заявлении, проверена и является достоверной.

_____ _____ /_____/
(должность) *(подпись)* *(фамилия, имя, отчество полностью)*

_____ _____ /_____/
(должность) *(подпись)* *(фамилия, имя, отчество полностью)*

м.п.

«____» _____20__г.
(дата заполнения заявления)

ОТМЕТКИ БАНКА (*заполняется сотрудником Банка)*
Личность(-и) Клиента/представителей Клиента мною проверена(-ы) и удостоверена(-ы).
"___"_____ 20__ г. _____ _____ _____
дата *должность, подразделение* *подпись* *расшифровка подписи*

Приложение №2

к Правилам работы Системы «Клиент-Банк»

В ОИКБ «Русь» (ООО) (далее – Банк)

Юридический адрес: 460014, г. Оренбург, пер. Шевченко,7

от _____

Наименование Клиента

_____

ИНН Клиента

Контактные телефоны: _____

ЗАЯВЛЕНИЕ НА ИЗМЕНЕНИЕ ПАРАМЕТРОВ РАБОТЫ В РАМКАХ СИСТЕМЫ «КЛИЕНТ-БАНК»*

1. Прошу предоставить доступ к Системе «Клиент-Банк»
   - ☐ **с использованием Мобильного Клиент-Банка.**
   - ☐ **без использования Мобильного Клиент-Банка**

2. Для работы в Системе «Клиент-Банк» прошу предоставить в качестве носителя Ключевой информации:
   - ☐ **USB-ключ eToken** в количестве ___ штук.
   - ☐ **Смарт-карту eToken для Safe Touch** в количестве ___ штук.
   - ☐ **Смарт-карту eToken для** Смарт-карт ридера для iPhone/iPad/iPod в количестве ___ штук.
   - ☐ **USB-накопитель** в количестве ___ штук.

ИЛИ

- ☐ **.Для работы в Системе «Клиент-Банк» прошу сгенерировать Ключевую информацию на ранее выданном носителе**

ИЛИ

- ☐ **Оставить ранее зарегистрированную электронную подпись**

3.* Прошу Банк направлять Уведомления на условиях, в порядке и в сроки, предусмотренные Правилами, следующим способом:

- ☐ **SMS-сообщения на номер:**

7										

(номер мобильного телефона в федеральном формате)

- ☐ **E-mail сообщения на электронный адрес:**

_____

(адрес электронной почты)

Прошу использовать вышеуказанный **номер мобильного телефона / адрес электронной почты** *(ненужное зачеркнуть)* для направления Банком Клиенту Уведомлений согласно настоящему заявлению по всем имеющимся у Клиента на дату его составления, а также по всем вновь открываемым Клиенту банковским счетам.

4. **Прошу установить кодовое слово** для использования его в экстренных случаях при обращении в Банк в соответствии с Правилами, в том числе при возникновении несанкционированных списаний с расчетного счета Клиента, утере, хищении, компрометации Ключевой информации и т.п. в рамках использования Системы «Клиент-Банк»:

+7										

Прошу использовать вышеуказанный **номер мобильного телефона** в экстренных случаях при обращении в Банк в соответствии с Правилами, в том числе при утере, хищении, компрометации Ключевой информации и т.п. в рамках использования Системы «Клиент-Банк»

5. В целях обеспечения контроля доступа, прошу:
   - ☐ **не устанавливать** фильтрацию IP-адреса и MAC-адреса Электронного устройства, с которого осуществляется работа Клиента в Системе «Клиент – Банк»
   - ☐ **установить** фильтрацию перечисленных ниже IP-адреса и MAC-адреса Электронного устройства, с которого осуществляется работа Клиента в Системе «Клиент – Банк».

Список доступных адресов:

№ п/п	IP-адрес	MAC-адрес
1		
2		
3		

6. Сокращенное наименование Клиента латинскими буквами - _____

7. Прошу списать предусмотренные тарифами Банка комиссии, связанные с изменением параметров подключения Клиента к работе в Системе «Клиент-Банк», с любого расчетного счета Клиента, открытого в Банке.

Вся информация, указанная в настоящем заявлении, проверена и является достоверной.

* Данный пункт не заполняется Клиентами, не имеющими Счет в Банке (которые намерены использовать Систему «Клиент-Банк» только для обмена реестрами).

_____ _____ /_____/
(должность) *(подпись)* *(фамилия, имя, отчество полностью)*

_____ _____ /_____/
(должность) *(подпись)* *(фамилия, имя, отчество полностью)*

м.п.

«____» _____20__г.
(дата заполнения заявления)

ОТМЕТКИ БАНКА (*заполняется сотрудником Банка)*

Личность(-и) Клиента/представителей Клиента мною проверена(-ы) и удостоверена(-ы).

"___"_____ 20__ г. _____ _____ _____

дата *должность, подразделение* *подпись* *расшифровка подписи*

***Пункты заявления, не требующие изменений, перечеркиваются**

Приложение №3

к Правилам работы Системы «Клиент-Банк»

В ОИКБ «Русь» (ООО) (далее – Банк)
Юридический адрес: 460014, г. Оренбург, пер. Шевченко,7
от _____
наименование Клиента
_____
ИНН Клиента

ЗАЯВЛЕНИЕ ОБ ИСПОЛЬЗОВАНИИ НОСИТЕЛЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ БЕЗ СОГЛАСИЯ КЛИЕНТА

«___» _____ 201__ года с нашего расчетного счета № _____, открытого в Банке, по Системе «Клиент-Банк» была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами платежа:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Дополнительно сообщаю:
Количество электронных устройств настроенных для доступа в Систему «Клиент-Банк»: _____.
Для доступа в Систему «Клиент-Банк» хотя бы раз использовались:
☐ корпоративные электронные устройства
☐ личные электронные устройства
☐ электронного устройства, находящиеся в общественном пользовании
Периодичность смены пароля Системы «Клиент-Банк»: _____
Применяемые элементы безопасности электронного устройства включают:
☐ соблюден порядок подготовки электронного устройства к установке Системы «Клиент-Банк»
☐ используется только программное обеспечение для работы Системы «Клиент-Банк»
☐ используется только лицензионное программное обеспечение
☐ операционная система и приложения обновляются в автоматическом режиме
☐ используется антивирусное программное обеспечение: _____
☐ антивирусное программное обеспечение обновляется ежедневно
☐ из числа съемных носителей информации на электронном устройстве используются только ключевые носители
☐ передача файлов и обмен сообщениями электронной почты на электронном устройстве ограничены
☐ целостность исполняемых файлов и файлов конфигураций контролируется с периодичностью _____
☐ используются средства сетевой защиты: _____
☐ на электронном устройстве запрещены входящие соединения из сети Интернет
☐ с электронного устройства разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений программного обеспечения, число разрешенных сайтов составляет _____
☐ обеспечивается возможность доступа к электронному устройству только уполномоченных лиц
☐ обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц

Иная информация, имеющая отношение к инциденту: _____
_____
_____

Прошу заблокировать нашу учетную запись в Системе «Клиент-Банк», провести процедуру компрометации всех ключей электронной подписи и оказать содействие в возврате денежных средств.

☐ Я намерен обратиться в правоохранительные органы по факту хищения денежных средств.

ИЛИ

Заявление в правоохранительные органы приняты в ОВД_____
_____
район, город, иные идентифицирующие ОВД данные
и зарегистрировано за № _____в КУСП (книге учета сообщений о преступлениях).

ИЛИ

☐ Я не намерен обращаться в правоохранительные органы по факту хищения денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелицензированного и контрафактного программного обеспечения в соответствии со статьей 146 УК Российской Федерации предупрежден.

_____ _____ _____

должность подпись расшифровка подписи

«___» _____ 20__г.

Исп. _____

Фамилия И.О.

тел. _____

Приложение №4

к Правилам работы Системы «Клиент-Банк»

Рекомендуемая форма заявления к Интернет-провайдеру

_____
должность руководителя

_____
наименование организации

_____
ФИО руководителя

от _____
_____
_____
указываются реквизиты Клиента (для организаций: наименование, ИНН, должность и ФИО руководителя, юридический адрес и контактные телефоны)

Уважаемый(ая) _____,
имя, отчество руководителя

«____» _____ 20___ года в ___:___ по местному времени по Системе «Клиент–Банк» был осуществлен несанкционированный перевод денежных средств. Электронное устройство, с которого осуществляется подключение к Системе «Клиент–Банк», располагается по адресу _____ и использует IP-адрес ___.___.___.___.

Вероятной причиной несанкционированного перевода могло послужить заражение Электронного устройства вредоносным программным обеспечением, кража логина, пароля и ключей электронной подписи/шифрования Системы «Клиент–Банк».

«____» _____ 20__ года между _____ и вами был заключен договор № _____ об оказании _____ услуг.

Для выявления обстоятельств несанкционированного перевода прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с «____» _____ 20___ года по «____» _____ 20__ года с указанием времени соединения, IP и MAC адресов.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение №5

к Правилам работы Системы «Клиент-Банк»

Рекомендуемая форма заявления в правоохранительные органы

Начальнику _____
наименование подразделения полиции

от _____

_____

_____
указываются реквизиты Клиента (для организаций: наименование, ИНН, должность и ФИО руководителя, юридический адрес и контактные телефоны)

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

ЗАЯВЛЕНИЕ

Прошу провести проверку по факту незаконного завладения, принадлежащими _____
наименование Клиента

денежными средствами (кражи) с использованием Системы «Клиент-Банк» ОИКБ «Русь» (ООО).

_____ 201__г. неизвестными лицами по Системе «Клиент-Банк» был осуществлен несанкционированный перевод денежных средств со следующими реквизитами:

Дата платежа: _____
Номер платежного поручения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____

Оснований для данного денежного перевода нет, с получателем платежа отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним, перевод расцениваю как хищение денежных средств.

Признаком хищения является то, что этот перевод не был осуществлен уполномоченными лицами.

Факт появления этого перевода был установлен «____» _____ 201__г. _____
ФИО лица, установившего факт несанкционированного перевода, должность, наименование организации

при _____.
обстоятельства обнаружения факта несанкционированного перевода

Электронное устройство, с которого осуществляется подключение к Системе «Клиент-Банк», располагается по адресу _____, доступ к электронному устройству ограничен, прямая кража реквизитов доступа (учетной записи, пароля и секретных ключей) маловероятна.

Вероятной причиной этого несанкционированного перевода считаю ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, поскольку данному событию сопутствовали следующие обстоятельства:

1. _____;
обстоятельства, снижающие вероятность прямого хищения реквизитов доступа в Систему «Клиент-Банк»

2. _____.
наблюдавшиеся сбои, нехарактерное поведение Системы «Клиент-Банк» и рабочего места Системы «Клиент-Банк»

3. _____.
иное

На основании изложенного, прошу Вас провести необходимые оперативно-розыскные мероприятия для выявления виновных лиц и привлечь их к уголовной ответственности в соответствии с действующим законодательством.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__ г.

Исполнитель:

_____/_____/
Подпись Ф.И.О.

«___» _____ 20__г.

Приложение №6

к Правилам работы Системы «Клиент-Банк»

ПЕРЕЧЕНЬ ДОКУМЕНТОВ ДЛЯ ПРЕДЪЯВЛЕНИЯ В БАНК КЛИЕНТОМ В СЛУЧАЕ ВЫЯВЛЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

1. Копия лицензии на операционную систему ПК.

2. Копия чека на приобретение операционной системы ПК.

3. Описание используемого ПО (перечень использованного лицензионного ПО на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).

4. Копия договора на оказание телематических услуг информационно–телекоммуникационной сети Интернет.

5. Описание организации доступа в сеть Интернет на рабочем месте.

6. Копия чека на оказание доступа в сеть Интернет на повременной основе.

7. Копия заявления в правоохранительные органы, Интернет – провайдеру (в случае направления).

8. Копия лицензии на антивирусное ПО.

9. Копия чека на антивирусное ПО.

10. Описание по антивирусной защите рабочего места (наличие установленного на жестком диске автоматизированного рабочего места клиента антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на автоматизированном рабочем месте клиента вредоносных программ).

11. Описание системы защиты информации (наличие или отсутствие персонального межсетевого экрана у клиента, сведения об использовании рабочего места в иных целях, кроме осуществления платежно-расчетных операций, в частности – интернет-серфинга, сведения о порядке хранения и использования ключевых носителей).

Приложение №7

к Правилам работы Системы «Клиент-Банк»

Правила доступа Клиентов ОИКБ «Русь» (ООО) к услугам дистанционного банковского обслуживания с указанием мер информационной безопасности.

Уважаемые Клиенты, пользователи Системы «Клиент-Банк» ОИКБ «Русь» (ООО), пожалуйста, прочитайте настоящие правила доступа. Они помогут Вам в работе с Системой «Клиент-Банк» и позволят снизить Ваши риски.

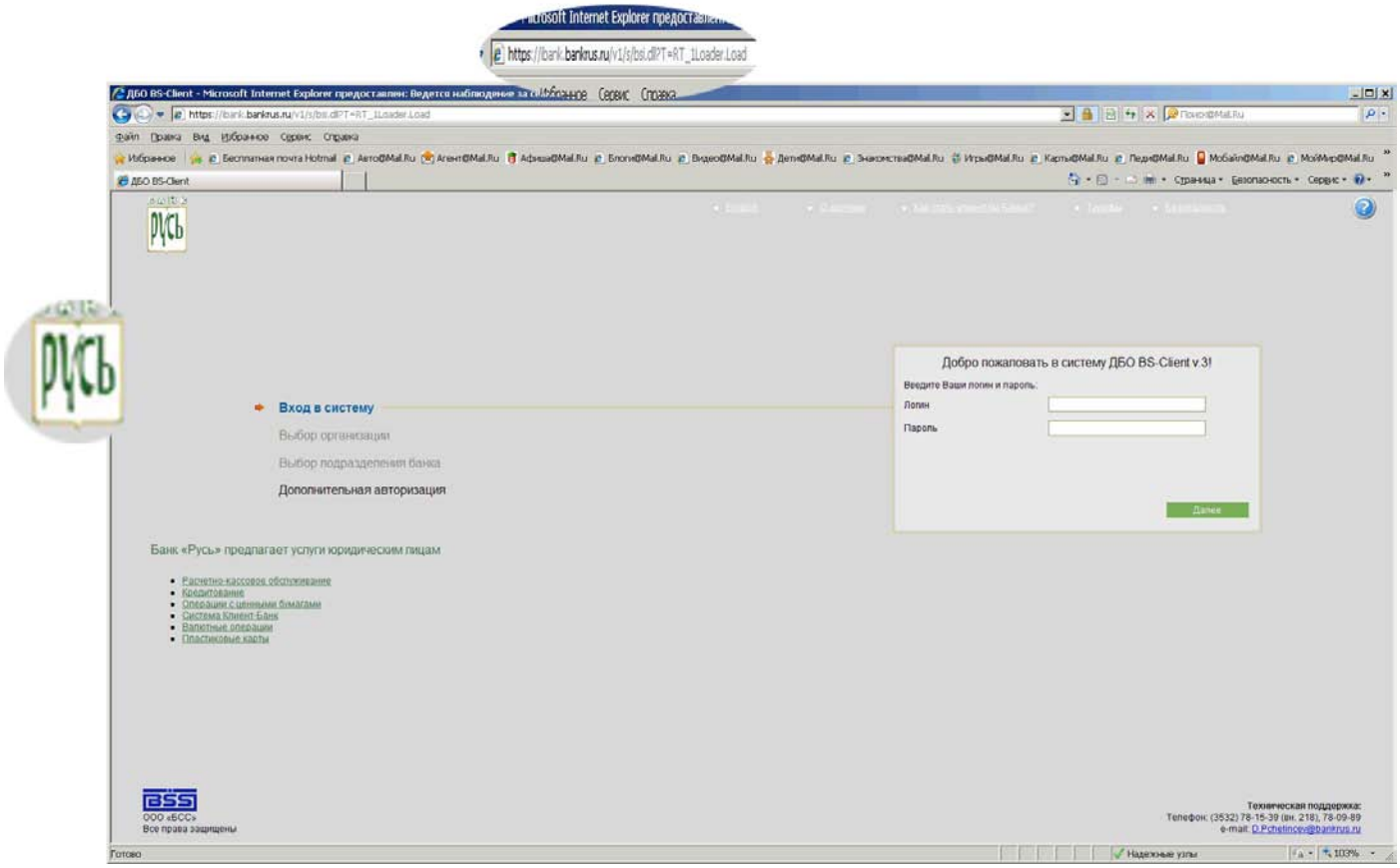
Просим принять к сведению, что за последний год существенно увеличилось количество фактов мошенничества (попыток хищения денежных средств со Счетов юридических лиц) путем совершения платежей с использованием реквизитов учетных записей и ключей электронной подписи систем удаленного доступа (Система «Клиент-Банк»). Появилось вредоносное программное обеспечение (вирусы и пр.), действия которого направлено именно на системы удаленного доступа (Система «Клиент-Банк») различных Банков (кража логинов, паролей и ключей электронной подписи).

Технологии защиты операций в системах дистанционного банковского обслуживания ОИКБ «Русь» (ООО) используют современные механизмы обеспечения безопасности и предоставляют удобство пользования услугой, обеспечивая при этом высокий уровень ее надежности и безопасности. Вместе с тем эффективность данных механизмов зависит также от соблюдения Вами мер безопасности.

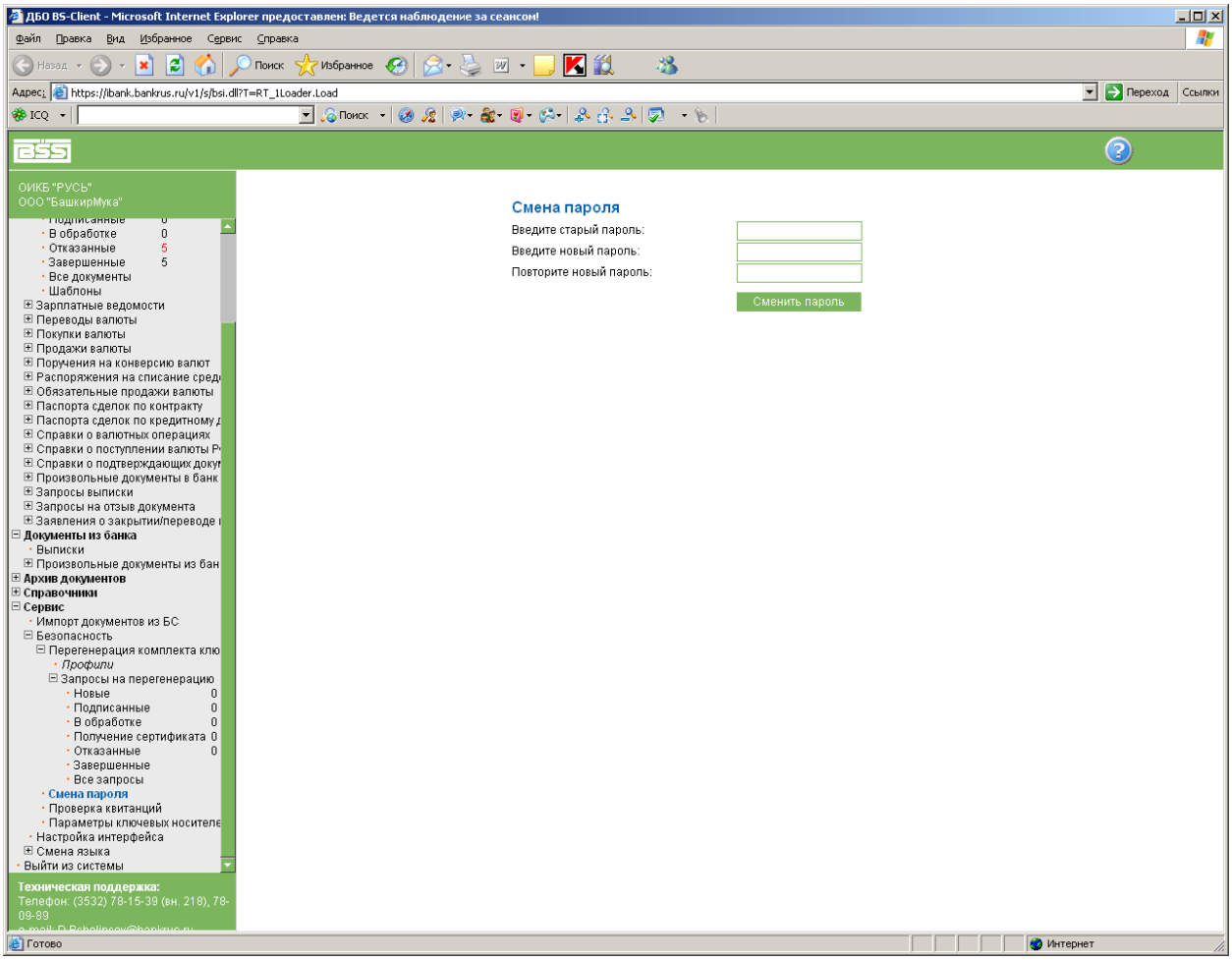
Для получения доступа к Системе «Клиент-Банк», Клиенту необходимо пройти процедуру идентификации и аутентификации в системе. Идентификация считается успешно пройденной в случае, если введенный Клиентом логин соответствует логину, содержащемуся в Системе «Клиент-Банк». Аутентификация Клиента в Системе «Клиент-Банк» осуществляется на основании введенного Клиентом пароля. Процедура Аутентификации считается пройденной успешно в случае соответствия введенного пароля логину Клиента. Настоятельно рекомендуем Вам работать в Системе «Клиент-Банк», соблюдая следующие меры безопасности, позволяющие снизить Ваши риски:

1. **ПАРОЛЬ ДЛЯ ВХОДА** в Систему «Клиент-Банк» это Ваша личная **КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ**, ни при каких обстоятельствах не раскрывайте свой пароль кому-либо. При первом входе в Систему «Клиент-Банк» обязательно измените выданный Вам нашим администратором пароль на **СВОЙ**, известный только Вам.
2. **НЕ СОХРАНЯЙТЕ** Ваш **ПАРОЛЬ В БРАУЗЕРЕ, ТЕКСТОВЫХ ФАЙЛАХ** на компьютере, либо на других электронных носителях информации, потому что это может привести к его краже и компрометации. Не оставляйте записанные на бумаге пароли в легкодоступных местах (на рабочем столе и т. д.), не передавайте пароли неуполномоченным лицам.
3. **ИСПОЛЬЗУЙТЕ** современное **АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ** и следите за его регулярным обновлением**.**
4. **РЕГУЛЯРНО ВЫПОЛНЯЙТЕ АНТИВИРУСНУЮ ПРОВЕРКУ** на своем компьютере лицензионной антивирусной программой для своевременного обнаружения вредоносных программ. В случае обнаружения вирусов должны быть приняты все меры для их удаления, после этого необходимо сменить пароль в Систему «Клиент-Банк» и проконтролировать состояние счёта (путем просмотра выписки). В случае обнаружения вирусов категории Trojan-Banker (вредоносные программы, предназначенные для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт), Trojan-Spy (вредоносные программы, предназначенные для ведение электронного шпионажа за пользователем), Backdoor (вредоносные программы, предназначенные для скрытого удалённого управления злоумышленником пораженным компьютером.) следует незамедлительно обратиться в Банк, предпринять все меры для **ПРЕКРАЩЕНИЯ ЛЮБЫХ ОПЕРАЦИЙ** с электронными документами с использованием ключей электронных подписей и произвести их смену. Категорически не рекомендуется работать на компьютере с финансовыми документами при наличии вирусов.
5. **НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАЙТЕСЬ** в Банк в случае:
   - подозрительной активности на компьютере (самопроизвольное сворачивание или открывание окон, движение курсора, запуск различных программ и прочее) в период неактивности пользователя;
   - появления каких-либо дополнительных окон или сообщений при попытке доступа в Систему «Клиент-Банк», либо в процессе работы в Системе «Клиент-Банк»;
   - невозможности получения доступа к Системе «Клиент-Банк» и т. д.
6. Используйте дополнительное программное обеспечение, позволяющее **ПОВЫСИТЬ УРОВЕНЬ ЗАЩИТЫ ВАШЕГО КОМПЬЮТЕРА** – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок, системы защиты информации от несанкционированного доступа и т. д.
7. **ИСПОЛЬЗУЙТЕ** лицензионное программное обеспечение. Своевременно **ОБНОВЛЯЙТЕ** операционные системы, браузеры и т. д. (устанавливайте патчи, критичные обновления) в целях устранения выявленных в них уязвимостей.
8. **ВКЛЮЧИТЕ** системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически **ПРОСМАТРИВАЙТЕ** журнал и **РЕАГИРУЙТЕ** на ошибки.
9. **НЕ ОТКРЫВАЙТЕ** неизвестные письма и файлы, пришедшие по почте, **НЕ ЗАХОДИТЕ** по ссылкам в почте, прежде чем не будете уверены в благонадежности источника, даже если там написано что-то, кажущееся важным.
10. При работе в сети «Интернет» **НЕ СОГЛАШАЙТЕСЬ** на установку каких-либо дополнительных программ.

11. **ПРОВЕРЯЙТЕ** антивирусом любые программы и файлы, полученные из сети «Интернет», по электронной почте или на внешних носителях (дискеты, USB носители, CD, DVD – диски и т. д.).
12. **ПРОВЕРЯЙТЕ**, что защищенное **SSL-СОЕДИНЕНИЕ** установлено именно с **ОФИЦИАЛЬНЫМ САЙТОМ УСЛУГИ** (**https://ibank.bankrus.ru/**), настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официальных ресурсов Банка, например, www.bankrus.ru) или из поступивших по электронной почте писем:



13. **УБЕДИТЕСЬ** в наличии символа замка в статусной строке окна браузера (в правом нижнем углу веб-страницы или справа/слева от адресной строки). Этот символ указывает на то, что веб-сайт работает в защищенном режиме. Щелкнув два раза мышкой по этому символу, можно просмотреть информацию о серверном сертификате. Таким образом, при установлении защищенной сессии возможна визуальная Аутентификация сервера.
14. **ИСПОЛЬЗУЙТЕ** криптографические средства защиты информации в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.
15. **ПЕРВОНАЧАЛЬНАЯ СТРАНИЦА** доступа в Систему «Клиент-Банк» **СОДЕРЖИТ ТОЛЬКО ПОЛЯ ВВОДА ЛОГИНА И ПАРОЛЯ**. В случае если на данной странице от Вас требуется ввод любой другой персональной информации (номеров банковских карт, мобильного телефона, других личных данных), следует прекратить пользование услугой и связаться с Банком.
16. **НЕ РЕЖЕ ОДНОГО РАЗА В МЕСЯЦ** настоятельно рекомендуем проводить **СМЕНУ ПАРОЛЯ** на вход в Систему «Клиент-Банк», выбрав пункт меню: «Сервис» - «Безопасность» - «Смена пароля». При смене пароля новое значение должно отличаться от предыдущих. Пароль должен составлять **МИНИМУМ 10** символов. Пароль может содержать цифры, большие и маленькие буквы английского алфавита. Символы паролей должны вводиться в режиме латинской раскладки клавиатуры. Мы крайне не рекомендуем Вам использовать простые пароли (например, имена, фамилии, номера телефонов, года рождения и т.д.). Используйте пароли, которые трудно угадать и которые знаете только вы:



17. При работе в операционной системе Windows **НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ** установить ограничения на **ПРАВА ПОЛЬЗОВАТЕЛЕЙ**, работающих на данном компьютере. **НЕ ДОПУСКАЙТЕ** работу под учётной записью Windows, имеющей права администратора.
18. **УСТАНАВЛИВАЙТЕ** пароли на вход в операционную систему и **РЕГУЛЯРНО ПРОИЗВОДИТЕ** плановую смена паролей пользователей, не реже одного раза в течение 30 дней. При смене пароля новое значение должно отличаться от предыдущих, пароль должен быть не менее 6 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.), символы паролей должны вводиться в режиме латинской раскладки клавиатуры, пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования ПЭВМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).
19. Пользователь Гость (Guest) обязательно должен быть заблокирован.
20. **НЕ ИСПОЛЬЗУЙТЕ** на компьютерах, на которых осуществляется подготовка и отправка документов в Банк, средства удаленного (дистанционного) доступа, которые часто применяют IT-специалисты для удалённой поддержки.

Обеспечение безопасности ключевой информации

1. На Вашем предприятии должен быть **ОПРЕДЕЛЕН** и **УТВЕРЖДЕН** порядок учета, хранения и использования носителей ключевой информации (ключевых дискет, usb-носителей и т. д.) с ключами электронных подписей, который должен полностью исключать возможность несанкционированного доступа к ним.
2. Рекомендуется использовать **ПРИНЦИП РАЗДЕЛЕНИЯ** электронных подписей ответственных лиц, которые осуществляют установку электронной подписи под электронным документом, путем использования двух разных электронных подписей (например, один для руководителя, второй для главного бухгалтера).
3. Для хранения носителей ключевой информации в помещениях должны устанавливаться хранилища (сейфы), оборудованные надежными запирающими устройствами и приспособлением для опечатывания. **ДОСТУП НЕУПОЛНОМОЧЕННЫХ ЛИЦ** к носителям ключевой информации должен быть исключен.
4. По завершению сеанса работы с Системой «Клиент-Банк» **ИЗВЛЕКАЙТЕ КЛЮЧЕВОЙ НОСИТЕЛЬ** из считывающих устройств компьютера и помещайте его в опечатанный контейнер в хранилище (сейф).
5. **НЕ ОСТАВЛЯЙТЕ** включенным без присмотра компьютер, не активизировав средства защиты от

несанкционированного доступа (временную блокировку экрана и клавиатуры).

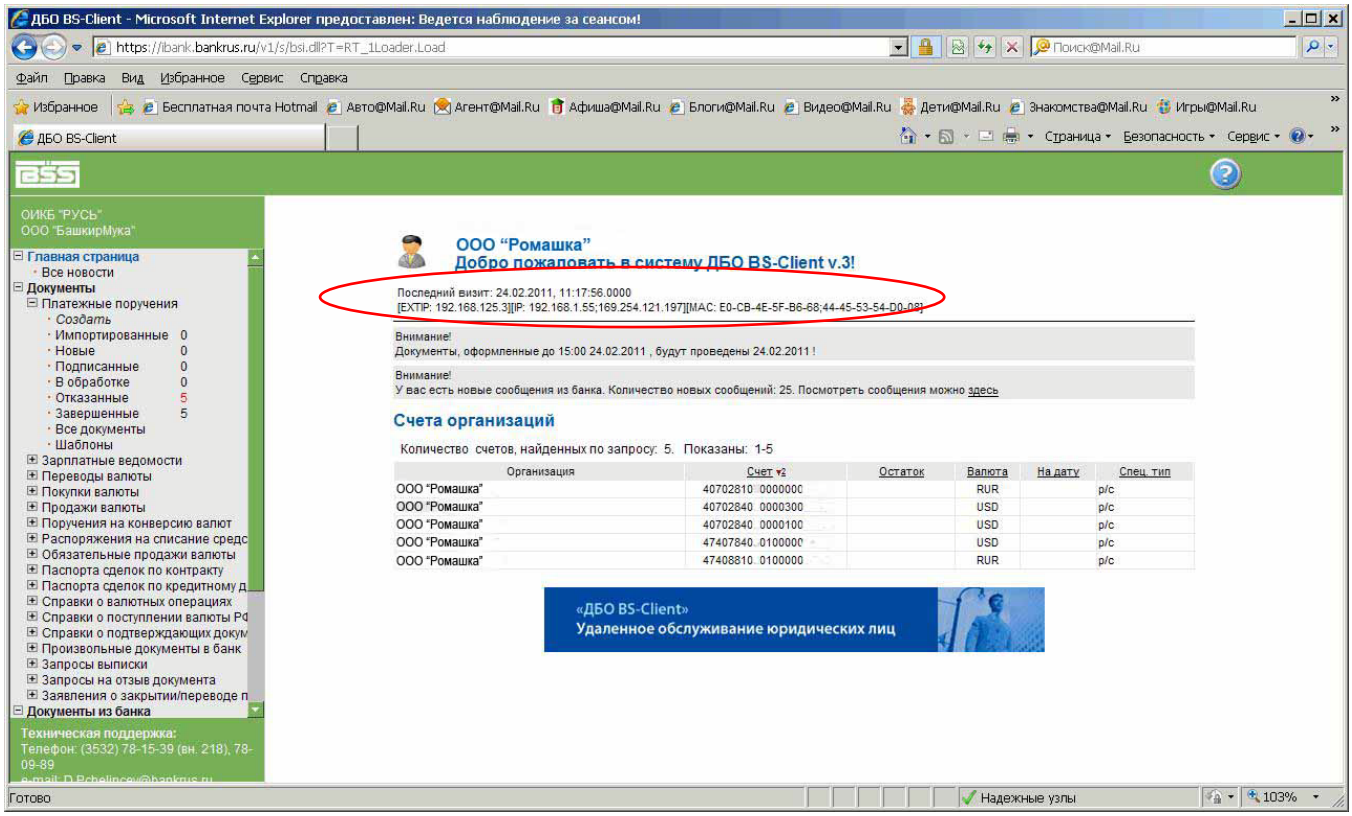
6. **НЕ ОБРАБАТЫВАЙТЕ** конфиденциальную информацию с отключенными средствами защиты информации (о чем свидетельствует отсутствие значков антивируса, firewall и т.д. в системном трее на панели задач).
7. **НЕ УСТАНАВЛИВАЙТЕ КЛЮЧЕВОЙ НОСИТЕЛЬ** в считывающее устройство компьютера в режимах, не предусмотренных функционированием системы обработки и обмена электронных документов с Банком (внезапная перезагрузка, нетипичное поведение программ, появление сообщений об ошибках, любые проблемы в работе программного и аппаратного обеспечения и т. д.).
8. **НЕ ЗАПИСЫВАЙТЕ НА КЛЮЧЕВОЙ НОСИТЕЛЬ** постороннюю информацию.
9. **НЕ ЗАПИСЫВАЙТЕ и НЕ СОХРАНЯЙТЕ** информацию с ключевого носителя на жесткий диск.
10. **НЕ ОСТАВЛЯЙТЕ** без контроля ключевые носители на столах, в шкафах и других местах, в которых они могут стать доступными лицам, не имеющим права работать с данными ключевыми носителями, хотя бы и кратковременно.
11. **НЕ ОСУЩЕСТВЛЯЙТЕ** обработку конфиденциальных данных в присутствии посторонних (не допущенных к данной информации) лиц.
12. **НЕ РАЗМЕЩАЙТЕ** мониторы так, чтобы с них существовала возможность визуального считывания информации посторонними лицами.
13. **ПРИ УВОЛЬНЕНИИ ИЛИ ПЕРЕВОДЕ** (на другую должность), изменении функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям, **ДОЛЖНА БЫТЬ ПРОВЕДЕНА СМЕНА КЛЮЧЕЙ электронных подписей**, к которым он имел доступ.
14. **ПРИ КОМПРОМЕТАЦИИ КЛЮЧА электронной подписи** необходимо предпринять все меры для **ПРЕКРАЩЕНИЯ ЛЮБЫХ ОПЕРАЦИЙ** с электронными документами с использованием этого ключа электронной подписи, а также проинформировать Банк о факте компрометации.
15. **РЕГУЛЯРНО КОНТРОЛИРУЙТЕ** состояние счёта (путем просмотра выписки).
16. При работе на компьютерах необходимо использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.
17. На компьютере с установленной Системой «Клиент-Банк»:
    - должны быть отключены службы и процессы операционной системы Windows такие как: службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски C$ и т.д.).
18. Настоятельно рекомендуем **НЕ СОВЕРШАТЬ** с компьютером, на котором установлена Система «Клиент-Банк» следующие действия:
    - просматривать посторонние (не относящихся к Системе «Клиент-Банк») Интернет сайты;
    - работать с электронной почтой (особенно через общедоступные почтовые сервера: Mail.ru и т.д.);
    - устанавливать на него игры и любые программы с пиратских дисков;
    - загружать и устанавливать программы из сети «Интернет»;
    - открывать и редактировать непроверенные антивирусом DOC, XLS, PDF и др. файлы.

    Желательно использовать отдельный компьютер для работы только с Системой «Клиент-Банк»!
19. Если у Вас Система «Клиент-Банк» установлена на ноутбук, постарайтесь не подключать ноутбук к сетям общего доступа в местах свободного доступа в сеть «Интернет» (Интернет-кафе, гостиницы, офисные центры и т.д.).
20. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в Систему «Клиент-Банк», или компьютер, с установленным Системой «Клиент-Банк» внезапно вышел из строя (нет доступа, невозможно войти в систему, возникли ошибки при загрузке операционной системы и т.д.), незамедлительно сообщите об этом в ОИКБ «Русь» (ООО).
21. В случае передачи (списания, выброса) сторонним лицам стационарного компьютера (ноутбука), на котором ранее была установлена Система «Клиент-Банк», необходимо гарантированно удалить с него всю информацию (в том числе следы работы в Системе «Клиент-Банк»), использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Вашей организации.

Дополнительные меры обеспечения безопасности при работе с Системой «Клиент-Банк».

1. Для клиентов, использующих **СТАТИЧЕСКИЙ** IP-адрес (список адресов) при работе в сети «Интернет», **НАСТОЯТЕЛЬНО** рекомендуем на стороне Банка использовать дополнительную фильтрацию по IP-адресу. **Услуга Банком предоставляется бесплатно в нижеуказанном порядке.**
2. Для контроля входа в Систему «Клиент-Банк» с **КОНКРЕТНОГО** компьютера **НАСТОЯТЕЛЬНО** рекомендуем на стороне Банка использовать дополнительную фильтрацию по MAC-адресам компьютера (компьютеров).
   Услуга Банком предоставляется бесплатно в нижеуказанном порядке.

MAC-адрес и статический IP-адрес отображаются на главной странице при входе в Систему «Клиент-Банк»:



Установка дополнительной фильтрации с указанием MAC и IP адресов осуществляется на основании заявления Клиента на подключение к Системе «Клиент-Банк», согласно приложению №1 к Правилам работы Системы «Клиент-Банк». Заявление направляется в Банк **НА БУМАЖНОМ НОСИТЕЛЕ**, заверяется печатью (при наличии) и подписями лиц, обладающими правом подписи на основании оформленной Карточки с образцами подписей. После получения заявки сотрудник Банка осуществляет звонок клиенту и подтверждает установку дополнительной фильтрации.

***Обращаем Ваше внимание**, что после установки дополнительной фильтрации на стороне Банка, вход в систему с компьютеров, параметры которых не соответствуют указанным фильтрам в заявке, будет **НЕВОЗМОЖЕН**.*

Отмена фильтрации осуществляется на основании письменного обращения клиента в Банк в свободной форме, заверенной печатью (при наличии) и подписями лиц, обладающими правом подписи на основании оформленной Карточки с образцами подписей.

Изменение IP или MAC-адресов осуществляется на основании заявления на изменение параметров работы в рамках системы «Клиент-Банк», согласно приложению №2 к Правилам работы Системы «Клиент-Банк». Заявление направляется в Банк **НА БУМАЖНОМ НОСИТЕЛЕ,** заверяется печатью (при наличии) и подписями лиц, обладающими правом подписи на основании оформленной Карточки с образцами подписей. **При этом ранее направленная заявка считается недействующей в части IP или MAC-адресов с момента установки фильтрации по новой заявке и направления в Ваш адрес сообщения Системы «Клиент-Банк».**

Хищение денежных средств со Счетов при получении злоумышленниками доступа к электронной подписи, предположительно, могут осуществлять:

- Ответственные сотрудники организации, работающие или уволенные, ранее имевшие доступ к электронным подписям: директора, бухгалтеры или их заместители и т. д.
- Штатные IT-сотрудники компании, имеющие доступ к носителям с электронными подписями.
- Нештатные IT-специалисты, обслуживающие компьютеры организации.
- Другие злоумышленники, получившие доступ к электронным подписям путем заражения компьютера вирусами (через сеть «Интернет» или почту).

ОИКБ «Русь» (ООО) еще раз напоминает Вам, что:

- Ни при каких условиях мы не просим предоставить нам Ваши пароли или ключи электронных подписей.
- Ответственность за сохранность Ваших ключей электронных подписей лежит на владельцах этих ключей электронных подписей.
- Мы не осуществляем рассылку сообщений с просьбой что-либо прислать по электронной почте. Вся важная корреспонденция отправляется по Системе «Клиент-Банк», заверенная электронной подписью Банка.

При любых подозрениях на компрометацию пароля или ключа электронной подписи и выполнении несанкционированных Вами операций, следует незамедлительно обратиться в Банк.

По всем вопросам и дополнительным разъяснениям просьба обращаться к специалистам Банка по следующим телефонам:

- отдел продаж корпоративных продуктов: (3532) 44-57-55

- служба технической поддержки: (3532) 44-57-44

Надеемся на Ваше понимание и взаимовыгодное сотрудничество.