ДОГОВОР
ОБ ИСПОЛЬЗОВАНИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ СИСТЕМЕ УДАЛЁННОГО КЛИЕНТСКОГО ОБСЛУЖИВАНИЯ В ВИДЕ ПУБЛИЧНОЙ ОФЕРТЫ

г. Москва

ООО "СПЕЦСТРОЙБАНК", имеющее Лицензию ФСБ Российской Федерации ЛЗ №0013803 Рег.№15386Н Х от 22.08.2016 г., являющееся организатором системы электронного документооборота, именуемое в дальнейшем Банк, в лице Председателя Правления Хацернова Ильи Марковича, действующего на основании Устава, публикует настоящий договор (далее - Договор), являющийся публичным Договором (офертой) в адрес юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в соответствии с пунктом 2 статьи 437 Гражданского кодекса Российской Федерации. В случае согласия с изложенными ниже условиями предоставления услуг и их оплатой, юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой по установленной Банком форме производят письменный акцепт оферты (в соответствии с пунктом 3 статьи 438 ГК РФ акцепт оферты равносилен заключению договора на условиях, изложенных в оферте). После открытия расчётного счёта, подписания заявления на подключение к электронной системе удалённого клиентского обслуживания (далее Система) и оплаты подключения к Системе в соответствии с действующими Тарифами Банка лицо, совершившее акцепт оферты, становится Клиентом Банка. Банк и Клиент совместно именуются Стороны.

В связи с применением в Системе сертифицированных ФСБ России шифровальных средств (средств криптографической защиты информации, далее - СКЗИ) Стороны признают необходимость обеспечения безопасности эксплуатации СКЗИ и обязуются строго выполнять требования Договора.

В соответствии с Договором Банк осуществляет обслуживание счетов Клиента, открытых в Банке на основании договоров банковского счёта, с использованием системы "Банк-Клиент", позволяющей посредством электронной связи отправлять в Банк расчётные и иные документы, а также самостоятельно получать информацию о текущем состоянии счетов.

1. Общие положения

1.1. Стороны принимают к использованию для осуществления электронной передачи документов в Системе программное средство криптографической защиты информации "Крипто-Про CSP", сертифицированное ФСБ России.
1.2. Стороны признают, что используемые во взаимоотношениях между Банком и Клиентом электронные документы, заверенные электронной подписью (далее - ЭП), подготовленные и переданные с помощью программного обеспечения Системы в соответствии со всеми процедурами защиты информации, предусмотренными Договором, эквивалентны документам на бумажном носителе и имеют юридическую силу наравне с документами, подписанными должностными лицами и заверенными печатями Банка и Клиента традиционным способом.
1.3. Стороны признают, что используемая ими система защиты информации, которая обеспечивает шифрование, контроль целостности и ЭП, достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства электронных документов, а также разбора конфликтных ситуаций по ним.
1.4. Секретные ключи обеих Сторон, используемые для передачи и защиты информации, а также материалы разбора конфликтных ситуаций являются конфиденциальной информацией и не подлежат разглашению Банком и Клиентом ни при каких обстоятельствах, кроме установленных законом.
1.5. Стороны считают, что электронные документы: "платёжное поручение", "заявление на перевод" и другие платёжные документы Клиента, заверенные ЭП Клиента, а также произвольные документы Банка юридически эквивалентны соответствующим документам на бумажном носителе, подписанным уполномоченным(и) представителем(ями) Клиента и Банка и имеющим оттиск печати (при её наличии), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами.

2. Порядок подключения Клиента к системе и формирования ключей шифрования и ЭП Клиента

2.1. Клиент собственноручно в присутствии представителя Банка заполняет и подписывает заявление на подключение к Системе.
2.2. Клиент обеспечивает комплектование аппаратного обеспечения для программного комплекса Системы в оборудованном помещении с учётом требований Приложения № 1 к Договору.
2.3. Формирование ключей шифрования и ЭП Клиента является непременным элементом процедуры его подключения к Системе и осуществляется после подписания Договора.
2.4. Полномочия лиц, осуществляющих формирование индивидуальной ключевой информации и оформление регистрационных карточек открытых ключей, определяются на основании Доверенности. При её отсутствии – без ограничений.
2.5. Формирование ключей шифрования и электронной подписи Клиента осуществляется на автоматизированном рабочем месте Администратора безопасности Банка при помощи программного обеспечения СКЗИ "Крипто-Про CSP".
2.6. При подключении Клиента к Системе вырабатывается рабочий комплект ключевой информации.
2.7. Секретные ключи ЭП и шифрования записываются на USB Flash Drive (далее - ключевой носитель) предоставляемый в Банк Клиентом вместе с заявлением на подключение к Системе.
2.8. Банком распечатывается в двух экземплярах сертификат ключа проверки ЭП в системе ДБО (далее сертификат).
2.9. Сертификат подписывается надлежаще уполномоченными на то лицами Сторон. Заверенные экземпляры сертификата хранятся по одному у Клиента и Банка.
2.10. Сертификат считается удостоверенным, если на нём присутствуют подписи уполномоченных лиц и печати Клиента (при наличии) и Банка.
2.11. Банк передаёт Клиенту секретные ключи ЭП и шифрования, а также необходимое программное обеспечение клиентской части Системы.

2.12. Банк осуществляет консультирование по телефону: (495) 755-5666 (доб.148) сотрудников Клиента по установке, настройке, вводу в эксплуатацию и работе с клиентской частью Системы и СКЗИ "Крипто-Про CSP".
2.13. Банк передаёт Клиенту необходимую документацию в электронном виде.
2.14. Уполномоченные должностные лица Клиента и Банка оформляют акт формирования и передачи ключей в одном экземпляре, который хранится в Банке.

3. Права и обязанности Клиента

3.1. Клиент обязуется использовать предоставленные шифровальные средства только в Системе, без права их продажи или передачи каким-либо другим способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны лицензирующего органа за соблюдением требований и условий осуществления лицензионной деятельности.
3.2. Клиент представляет и передаёт на хранение Банку оформленные в соответствии с действующим законодательством документы, материалы и информацию, необходимые для подключения к Системе.
3.3. Клиент назначает своих ответственных должностных лиц, имеющих право работать с СКЗИ "Крипто-Про CSP", с указанием их полномочий и срока действия таких полномочий.
3.4. Клиент обязан:
- соблюдать положения документов, регламентирующих функционирование Системы с встроенными средствами криптографической защиты информации. Эксплуатировать сертифицированные ФСБ России СКЗИ в соответствии с условиями сертификатов на данные средства. Выполнять условия и требования эксплуатационной документации на СКЗИ;
- Клиент обязан регулярно производить оплату за пользование Системой в соответствии с Тарифами;
- оплачивать услуги Банка в соответствии с действующими Тарифами;
- допускать к эксплуатации СКЗИ только сотрудников, прошедших необходимую подготовку по применению данных средств и допущенных к работе с ними на основании приказов руководителей организации Клиента;
- учитывать требования к помещению, перечисленные в Приложении № 1 к Договору;
- обеспечивать сохранность и целостность программного комплекса Системы, включая СКЗИ "Крипто-Про CSP". Сохранять конфиденциальность и подлинность своих секретных ключей и паролей для оповещения о фактах компрометации ключей;
- сообщать Банку об обнаружении попытки несанкционированного доступа к Системе или к своим секретным ключам в день её обнаружения и блокировать свою работу в Системе, направив в Банк соответствующее уведомление в произвольном виде по факсу или на бумажном носителе. Клиент несёт риск всех последствий, связанных с несанкционированным доступом к Системе или ключам ЭП Клиента.
- извещать Банк обо всех случаях компрометации криптографических ключей Клиента;
- в случае прекращения использования Системы уничтожить программное обеспечение Системы, включая СКЗИ (кроме открытых ключей СКЗИ и данных архива оригиналов принятых и отправленных документов), и официально уведомить об этом Банк;

3.5. Клиент имеет право с использованием Системы самостоятельно получать информацию о состоянии своего счёта.

4. Права и обязанности Банка

4.1. Банк назначает своих ответственных должностных лиц, имеющих право обслуживать программно-технические средства Системы, а также устанавливать и обслуживать программное обеспечение СКЗИ у Пользователя.
4.2. Банк обязан:
- исполнять принятые от Клиента электронные документы, подписанные подлинной ЭП Клиента, в соответствии с условиями Договора, договоров банковского счёта и действующим законодательством;
- сохранять конфиденциальность и подлинность используемых секретных ключей и паролей для оповещения о фактах компрометации ключей;
- протоколировать все случаи и попытки нарушения безопасности Системы. При возникновении таких случаев принимать все возможные меры для предотвращения и/или ликвидации их последствий вплоть до приостановления функционирования Системы;
- в случае компрометации ключей Клиента заблокировать открытые ключи Клиента и провести внеплановую смену ключей Клиента;
- обеспечивать сохранность и конфиденциальность информации, доверенной ему Клиентом в ходе практической деятельности в рамках Договора, в соответствии с действующим законодательством;
- своевременно информировать Клиента об изменениях порядка осуществления приёма/передачи электронных документов и другой информации по Системе. Оказывать консультационные услуги Пользователю по вопросам функционирования Системы;
- соблюдать положения документов, регламентирующих функционирование Системы.

4.3. Банк имеет право не обрабатывать документы Клиента в случаях, предусмотренных договором банковского счёта, а также в следующих случаях:
- нарушения Клиентом законодательных и нормативных документов, регламентирующих расчёты;
- несоответствия содержимого документа требованиям системы защиты от НСД и/или электронной подписи Клиента;
- неверно указанного номера счёта и/или ИНН Клиента;
- отсутствия или неверного указания платёжных реквизитов получателя;
- отсутствия назначения платежа, соответствующего установленным требованиям;
- несоответствия проводимой Клиентом операции действующему законодательству, в том числе валютному;
- непредставления документов, необходимых Банку для осуществления функций агента валютного контроля.

4.4. Банк имеет право оформлять от имени Клиента бумажные платёжные поручения на основе полученных Банком по каналам связи электронных документов, заверять их штампом и подписью уполномоченного лица Банка и проводить соответствующий платёж с указанного в платёжном поручении счёта Клиента в Банке.
4.5. Банк имеет право отказывать Клиенту в приёме от него распоряжений на проведение операции по банковскому счёту, подписанных аналогом собственноручной подписи, в случае признания её подозрительной/сомнительной. В этом случае Банк принимает от Клиента надлежащим образом оформленные расчётные документы на бумажном носителе в порядке, предусмотренном Договором банковского счёта.
4.6. Банк имеет право приостановить и/или прекратить приём, регистрацию и исполнение, а также передачу Клиенту электронных документов посредством системы "Банк-Клиент" в случае непредставления (неполного представления) запрошенных Банком документов, при выявлении Банком факта поддельности представленных Клиентом документов, а также в случаях, предусмотренных

законодательством Российской Федерации. При этом Банк принимает разумные меры для оповещения Клиента о таком факте. Наряду с этим Банк вправе принимать от Клиентов только надлежащим образом оформленные расчётные документы на бумажном носителе, а также запрашивать подтверждающие операцию документы в соответствии с законодательством Российской Федерации.
4.7. Банк имеет право использовать подсистему "Произвольные документы для клиентов" электронной системы удалённого клиентского обслуживания ООО "СПЕЦСТРОЙБАНК" для формирования информационных сообщений Клиенту (письма, уведомления, предупреждения, предписания о приостановлении операций по счёту и т.д.). Сообщение считается принятым Клиентом при следующем входе последнего в Систему после формирования данного сообщения на стороне Банка.
4.8. Банк имеет право расторгнуть Договор в одностороннем порядке в случае невнесения платы за пользование Системой в соответствии с Тарифами в течение 3 (трёх) календарных месяцев без предварительного уведомления.
4.9. Банк имеет право без согласия и дополнительного распоряжения Клиента взимать плату за Систему (стоимость ЭП, программы, её установка, стоимость повторного изготовления, абонентская плата и т.п.) согласно Тарифам Банка со счетов, обслуживающихся с использованием Системы. В случае образования задолженности Клиента перед Банком, Клиент предоставляет право списания без согласия и дополнительного распоряжения Клиента суммы задолженности с любых счетов Клиента, открытых в Банке.
4.10. Банк не несёт ответственности за состояние программного обеспечения, а также аппаратного и компьютерного оборудования Клиента, возможные помехи в телефонных линиях связи, прекращение работы Системы из-за отключения электроэнергии, сбои в работе провайдеров, предоставляющих доступ в Интернет, действия компьютерных вирусов, если возникновение указанных обстоятельств не вызвано действиями Банка.

5. Срок действия ключей ЭП

5.1. Управление секретными ключами ЭП в течение всего срока действия Договора осуществляется Банком и регламентируется Договором.
5.2. Плановый срок действия секретных ключей ЭП определяется Банком и составляет 1 (один) год с момента изготовления. Дата изготовления секретных ключей ЭП фиксируется в акте формирования, передачи ключей и регистрационных карточек ключей.
5.3. Плановая смена секретных ключей ЭП производится по инициативе Банка и возможна только в период действия секретных ключей ЭП. Расходы по плановой смене ключей ЭП возлагаются на Банк.
5.4. Для безотказной работы за 30 (тридцать) календарных дней до окончания планового срока действия секретных ключей ЭП, Система автоматически ежедневно выводит Клиенту сообщение с предложением плановой смены ключей. Клиенту необходимо в указанный срок (тридцать календарных дней) ответить согласием (нажатие клавиши "Ок") на предложение плановой смены ключей и запустить процесс перегенерации. В случае отказа Клиента (нажатие клавиши "Отмена") от плановой смены ключей и запуска процесса перегенерации, секретные ключи ЭП после окончания срока действия становятся недействительными. Последующая смена ключей в данном случае будет являться внеплановой.
5.5. Банк не несёт ответственность за несвоевременное исполнение Клиентом процедур плановой смены секретных ключей ЭП Клиента в случае истечения её срока действия.
5.6. Внеплановая смена секретных ключей ЭП производится по инициативе Клиента путём изготовления нового комплекта секретных ключей ЭП. Расходы по внеплановой смене ключей возлагаются на Клиента согласно Тарифам Банка.
5.7. При смене ключей, как плановой, так и внеплановой, Клиент обязан в течение 5 (пяти) рабочих дней подписать и предоставить в Банк акт формирования, передачи ключей и регистрационных карточек ключей и сертификат для обмена сообщениями. В случае непредставления Клиентом в Банк указанных выше документов, Банк имеет право заблокировать секретные ключи ЭП Клиента и приостановить его обслуживание по Договору.

6. Права и обязанности Сторон

6.1. Стороны обязуются обеспечить условия сохранения ключевых носителей и условия хранения и использования программного обеспечения СКЗИ, исключающие порчу и утрату ключевых носителей, а также их использование посторонними лицами.
6.2. Сторона, допустившая утрату контроля за ключевых носителей, независимо от наличия или отсутствия сведений о её несанкционированном использовании, незамедлительно сообщает об этом другой Стороне и прекращает работу с использованием СКЗИ до момента регистрации и ввода в действие новых ключей. Вышедший из-под контроля ключевой носитель не подлежит дальнейшему использованию. Замена ключевых носителей осуществляется в порядке, изложенном в документации на СКЗИ "Крипто-Про CSP".

7. Порядок разрешения споров

7.1. В случае возникновения между Сторонами споров или разногласий, вытекающих из Договора или связанных с ним, Стороны примут все меры к разрешению их путём переговоров в соответствии с порядком разбора конфликтных ситуаций (Приложение № 2).
7.2. Если Сторонам не удастся разрешить путём переговоров споры и/или разногласия в течение 30 (тридцати) дней с момента их возникновения, то такие споры и/или разногласия подлежат передаче на рассмотрение в Арбитражный суд в соответствии с действующим законодательством Российской Федерации.

8. Прочие условия

8.1. Для создания рабочего места Системы Клиенту необходимо следующее:
- предназначенный для функционирования системы "Клиент-Банк" IBM-совместимый персональный компьютер с установленной операционной системой Microsoft Windows 7; 8; 10 и оборудованный USB-портом для чтения ключевых носителей;
- доступ к сети Интернет.

8.2. Для предотвращения несанкционированного доступа к защищаемой информации и минимизации рисков финансовых потерь, клиентам рекомендуется выполнение ряда мер, изложенных в Приложении № 3 к настоящему договору.

9. Срок действия Договора и порядок его прекращения

9.1. Договор вступает в силу с момента акцепта оферты Клиентом и действует до окончания действия договора банковского счёта либо до наступления условий, предусмотренных Договором или договором банковского счёта
9.2. Договор в период его действия может быть дополнен или изменён Сторонами. Все изменения и дополнения оформляются дополнительными соглашениями, которые будут являться неотъемлемыми частями Договора.

9.3. Договор может быть расторгнут в порядке, предусмотренном действующим законодательством Российской Федерации (статья 859 Гражданского Кодекса Российской Федерации), при этом обязательства Банка по исполнению Договора прекращаются со дня направления Клиенту уведомления о расторжении Договора.

10. Сведения о Банке

10.1. Полное наименование и реквизиты:
Общество с ограниченной ответственностью Коммерческий Банк развития специального строительства "СПЕЦСТРОЙБАНК". Лицензия Банка России на совершение банковских операций № 236 выдана 21.05.2012 г., ИНН 7706074938, КПП 770901001, БИК 044525728, к/с 30101810045250000728 в ГУ Банка России по Центральному федеральному округу.
10.2. Местонахождение:
109004, г. Москва, ул. Александра Солженицына, 12, стр.4.
10.3. Телефон, адрес официального сайта и адрес электронной почты:
8(495)755-5666, http://ssb.msk.ru, bank@ssb.msk.ru

Приложение № 1

**ТРЕБОВАНИЯ К ОРГАНИЗАЦИЯМ,
ОСУЩЕСТВЛЯЮЩИМ ЭКСПЛУАТАЦИЮ СЕРТИФИЦИРОВАННЫХ ФСБ РОССИИ СРЕДСТВ
КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ)**

В целях обеспечения безопасности СКЗИ и ключей, пользователям рекомендуется следовать настоящим требованиям.

Данные требования распространяются на СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

1. Требования по организационному обеспечению безопасности СКЗИ

1.1. В организации Клиента руководством должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ.
1.2. Вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утверждённых руководством предприятия, с учётом эксплуатационной документации на СКЗИ.

2. Требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ

2.1. Размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее помещения), должны обеспечивать безопасность информации, СКЗИ и шифрключей, сведены к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.
2.2. Порядок допуска в помещения определяется внутренней инструкцией, которая разрабатывается с учётом специфики и условий функционирования конкретной структуры организации.
2.3. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решётками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, на которые устанавливаются надёжные замки.
2.4. Для хранения шифрключей, нормативной и эксплуатационной документации помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством организации.
2.5. Устанавливаемый руководителем организации порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.
2.6. Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

3. Требования по обеспечению безопасности шифрключей

3.1. Клиент обеспечивает защиту собственных вычислительных средств от несанкционированного доступа и вредоносного программного обеспечения.
3.2. Все поступающие для использования шифрключи должны браться на предприятии на поэкземплярный учёт в выделенных для этих целей журналах.
3.3. Учёт и хранение носителей шифрключей, непосредственная работа с ними поручается руководством организации специально выделенным работникам организации. Эти работники несут персональную ответственность за сохранность шифрключей.
3.4. Учёт шифрключей, регистрация их выдачи для работы и обратного возврата, а также уничтожения ведётся в организации Пользователя.
3.5. Хранение шифрключей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение. Наряду с этим должна быть предусмотрена возможность раздельного безопасного хранения рабочих и резервных шифрключей, предназначенных для использования в случае компрометации рабочих шифрключей в соответствии с правилами пользования СКЗИ.
3.6. При пересылке шифрключей должны быть обеспечены условия транспортировки, сводящие к минимуму возможность физических повреждений и внешнего воздействия на записанную ключевую информацию.
3.7. В случае отсутствия у оператора СКЗИ индивидуального хранилища, шифрключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.
3.8. Уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

4. Требования к сотрудникам, осуществляющим эксплуатацию СКЗИ

4.1. К работе с СКЗИ допускаются решением руководства предприятия только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию.
4.2. Руководитель организации или лицо, уполномоченное на руководство эксплуатацией шифровальных средств, должно иметь представление о возможных угрозах информации при её обработке, передаче, хранении, методах и средствах защиты информации.

Приложение № 2

ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ЭП

1. Общие положения

1.1. В приложении описана процедура предъявления претензий и разрешения споров по вопросам оспаривания Сторонами авторства и/или содержимого документа, подписанного электронной цифровой подписью.
1.2. Разбор конфликтной ситуации выполняется по инициативе любой из Сторон и состоит из:
- предъявления претензии одной из сторон другой;
- формирования комиссии для рассмотрения конфликтной ситуации;
- разбора конфликтной ситуации.

1.3. Претензии друг к другу рассматриваются Сторонами на основании официально вручённых уведомлений в письменном виде.
1.4. Стороны вправе решать возникающие претензии в рабочем порядке. По факту претензии Стороны проводят внутреннее расследование и официально информируют друг друга о его результатах в течении 14 календарных дней с даты получения претензии.
1.5. Сторона, предъявившая претензию, в срок 5 рабочих дней после получения результатов расследования от другой Стороны, должна рассмотреть достаточность представленных объяснений и направить официальное уведомление о снятии претензии или предложение о создании комиссии по разрешению спорной ситуации.
1.6. В случае, если хотя бы одна из Сторон при возникновении спора не удовлетворена результатами рассмотрения претензии в рабочем порядке, то Стороны обязаны сформировать комиссию для рассмотрения конфликтной ситуации. Целью работы комиссии является установление правомерности и обоснованности претензии, а также установление, если необходимо, подлинности и авторства спорного документа.
1.7. В состав конфликтной комиссии входит равное количество, но не менее двух представителей от каждой из Сторон, определяемых Сторонами самостоятельно. При необходимости, по согласованию Сторон, к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты.
1.8. Право представлять соответствующую Сторону в комиссии должно подтверждаться доверенностью, выданной каждому представителю на согласованный Сторонами срок работы комиссии.
1.9. Стороны договариваются, что для разбора конфликтных ситуаций комиссия принимает на рассмотрение электронные документы и подтверждения по ним и обязана использовать следующие, признаваемые сторонами, эталонные данные:
- данные архива оригиналов принятых, отправленных документов;
- подписанные сторонами оригиналы регистрационных бланков с открытыми ключами Сторон;
- хранимое у Банка программное обеспечение Системы с встроенным СКЗИ "Крипто-Про CSP".

1.10.Результат работы комиссии оформляется Актом, в котором определяются последующие действия Сторон. Оспаривание результатов работы комиссии и возмещение пострадавшей стороне принесённого ущерба выполняется в установленном действующим законодательством Российской Федерации порядке.
1.11.Принимая во внимание математические свойства алгоритма ЭП, реализованного в соответствии с требованиями стандартов Российской Федерации ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, гарантирующими невозможность подделки значения сертифицированной ЭП любым лицом, не обладающим секретным ключом подписи, Стороны признают, что разбор конфликтной ситуации в отношении авторства электронного документа заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем.

2. Порядок разбора конфликтной ситуации

2.1. Проверка подписанного электронного документа включает в себя выполнение следующих действий:
- проверка действительности регистрационной карточки открытого ключа ЭП, необходимой для проверки ЭП;
- проверка ЭП электронного документа с использованием открытого ключа ЭП из регистрационной карточки;
- определение даты формирования ЭП для данного электронного документа;
- проверка действительности ключа на момент формирования ЭП;
- проверка наличия сообщения о компрометации соответствующего секретного ключа ЭП.

Если ключ был скомпрометирован, то комиссия принимает решение о действительности ЭП документа, используя дату создания документа и дату сообщения о компрометации.

При положительном результате проверки ЭП документа, установлении того, что ключ был действующим и не было сообщения о его компрометации, авторство подписи под документом считается установленным.
2.2. Случаи невозможности проверки значения ЭП:
- при не обнаружении в архиве акта признания открытого ключа Клиента, выполнившего ЭП, доказать авторство документа невозможно.

Приложение № 3

ПАМЯТКА
О ВОЗМОЖНЫХ РИСКАХ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ООО "СПЕЦСТРОЙБАНК" С ЦЕЛЬЮ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

ООО "СПЕЦСТРОЙБАНК" (далее – Банк) предлагает Вашему вниманию информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемые меры по снижению этих рисков. Документ также содержит рекомендации по защите информации от воздействия вредоносного кода.

1. Рекомендуемые меры по снижению рисков компрометации ключей электронной подписи
Компрометация ключей электронной подписи – факт (а также подозрение на такой факт) доступа постороннего лица к информации, содержащей (закрытый) ключ электронной подписи (далее – ЭП).
Ключ может быть скомпрометирован в следующих ситуациях, создания которых следует избегать:
- физическая утеря носителя информации, на котором хранится файл ключа ЭП;
- передача файла ключа ЭП по открытым каналам связи (т.е. без использования шифрования);
- использование ключа ЭП лицом, отличным от того, для кого генерировалась ЭП;
- несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом; подозрение, что данные факты имели место (срабатывание сигнализации, повреждение устройств контроля несанкционированного доступа (слепков печатей), взлом учётной записи пользователя и т.п.);
- сознательная передача носителей и файла ключа ЭП постороннему лицу;
- перехват информации вредоносным программным обеспечением (компьютерными вирусами, троянскими программами).

2. Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации при утрате или компрометации устройства, с использованием которого клиентом осуществлялся перевод денежных средств (компьютер, USB-flash, USB-токен и т.п.)
Рекомендуется выполнять следующие меры для снижения риска несанкционированного доступа к защищаемой информации:
- для работы с системой "Банк-Клиент" используйте отдельный компьютер, доступ к которому имеют только лица, осуществляющие платежи в системе "Банк-Клиент";
- на компьютере, с которого осуществляется работа в системе "Банк-Клиент", используйте только лицензионное системное и прикладное программное обеспечение (далее – ПО), оперативно его обновляйте;
- не реже 1 раза в день осуществляйте проверку компьютера, на котором установлено ПО "Банк-Клиент" на наличие вредоносных программ при помощи установленных средств антивирусной защиты;
- в качестве хранилища ключей ЭП используйте только носители, полученные в Банке. Не копируйте свои ключи ЭП на другие носители;
- не передавайте ключ ЭП третьим лицам (т.к. электронные документы, заверенные ЭП юридически эквивалентны документам на бумажном носителе, заверенным подписями лиц из карточки с образцами подписей и оттиска печати);
- не храните на устройстве, с использованием которого клиентом осуществлялся перевод денежных средств (компьютер, USB-flash и т.п.), пароль от входа в систему "Банк-Клиент" (включая Интернет-браузер с использованием которого осуществляется доступ к системе);

3. Информация для клиентов о возможных рисках получения несанкционированного доступа к защищаемой информации путём использования ложных ресурсов сети Интернет
При осуществлении переводов денежных средств через сеть Интернет существует риск получения несанкционированного доступа к защищаемой информации (персональные данные, данные о платежах и т.п.) путём использования ложных ресурсов сети Интернет лицами, не обладающими правом распоряжения этими денежными средствами (злоумышленниками). При этом сайт-копия будет выглядеть как копия сайта платёжного сервиса, но при вводе данных, они будут отправляться злоумышленнику. Попадание на такой сайт-копию возможно, например, с различных внешних ссылок, на которых установлена переадресация на сайт злоумышленника. С целью снижения указанного риска, защиты от него, а также защиты от вредоносного кода, который может присутствовать на таких сайтах-копиях, рекомендуется выполнять следующие действия:
- используйте на компьютере с которого осуществляете платежи только лицензионное программное обеспечение, происхождение которого не вызывает у Вас сомнений;
- по возможности старайтесь использовать этот компьютер только для осуществления платежей (работы в системе "Банк-Клиент"). Не осуществляйте работу с этого компьютера с сомнительными Интернет-ресурсами. Пользуйтесь функциями безопасного браузинга.
- переходите на сайт системы "Банк-Клиент", набрав его название собственноручно в адресной строке – https://bc.ssb.msk.ru (резервный сайт https://bank-client.ssb.msk.ru); после перехода на сайт, прежде чем ввести имя и пароль, всегда проверяйте подлинность сайта по данным SSL-сертификата (в адресной строке около названия сайта будет отображён значок закрытого замочка зелёного цвета 

; чтобы увидеть детали SSL-сертификата, необходимо сделать двойной щелчок мыши по закрытому замочку);
- проверяйте информацию о предыдущем сеансе работы при каждом входе на сайт (дату последнего посещения сайта и т.п.);
- не переводите денежные средства по просьбам, озвученным по телефону, присланным в SMS-сообщениях, в сообщениях из социальных сетей, а также людям, которые обещают различные подарки, выигрыши, компенсации и т.п.;
- не используйте функции автозаполнения в настройках специализированных программ для просмотра веб-страниц в сети Интернет (Интернет-браузеров). Использование данной функции приводит к сохранению конфиденциальной информации (пароля и имени пользователя и др.) в памяти Интернет-браузера, что в свою очередь может привести к использованию данных злоумышленниками. Регулярно удаляйте случайно сохранённые в памяти браузера пароли и имена пользователя; Работайте с системой "Банк-Клиент" в

"приватном" режиме – это обеспечит затирание конфиденциальной информации (пароля и имени пользователя и др.) из памяти Интернет-браузера после окончания сеанса работы с системой;

- храните пароль от входа в платёжный сервис отдельно, в недоступном для посторонних лиц месте. Не храните пароль в компьютере. Записав пароль, не делайте комментариев к записи. Не используйте в качестве пароля имена и фамилии родственников и знакомых, элементы адреса местожительства и памятных дат, клички животных и другие простые и известные окружающим слова и словосочетания. Используйте пароль не короче 6 символов, включающий бессмысленное сочетание букв и цифр. Меняйте пароль не реже 1 раза в месяц.

В качестве радикальной меры для защиты от хищений секретных ключей ЭП, паролей и параметров доступа к системе "Банк-Клиент" ООО "СПЕЦСТРОЙБАНК" предлагает своим клиентам воспользоваться дополнительной БЕСПЛАТНОЙ услугой "IP фильтрации", т.е. ограничить возможности подключения к системе "Банк-Клиент" только IP-адресами, указанными Клиентом заранее. Это существенно сузит возможности злоумышленника по несанкционированному переводу денежных средств. Обсудите эту возможность с системным администратором, обслуживающим Вашу организацию.

4. Рекомендации клиентам по организации антивирусной защиты информации

Создания ограничения по физическому доступу к компьютеру с которого Вы осуществляете платежи (работаете в системе "Банк-Клиент"). Любой компьютер, с которого осуществляется выход в сеть Интернета, подвержен риску заражения вирусом (вредоносный код, способный нарушить целостность используемой информации, что может привести к несанкционированному переводу денежных средств, к краже персональных данных, сбоям в работе компьютера и т.п.), поэтому рекомендуется придерживаться следующих правил безопасной работы в сети Интернет:

- не работайте со съёмными носителями других систем и компьютеров, которые ранее были заражены вирусом;
- не посещайте непроверенные и небезопасные сайты (возможна непреднамеренная загрузка на свой компьютер вирусов и шпионских программ);
- не скачивайте информацию из сети Интернета на диск своего компьютера;
- не нажимайте на всплывающие окна, содержащие рекламу;
- не открывайте вложения и не переходите по ссылкам при получении электронного сообщения с неизвестным вложением или со ссылкой на неизвестный ресурс сети Интернет;
- не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных, ни при каких обстоятельствах не сообщайте свой пароль никому, включая людей, представляющихся сотрудниками Банка;
- максимально ограничьте использование интернет-коммуникаторов (ICQ, Skype и т.п.) на данном компьютере;
- будьте внимательны к странным и непонятным сообщениям и поведению системы (нетипичная работа ПО, появление графических и звуковых эффектов, искажение данных, исчезновение файлов, частое появление сообщений об ошибках, замедление работы компьютера и сети и т.п.);
- не используйте непроверенное и неизвестное ПО (такое ПО маожет быть мошенническим и провоцировать на выполнение действий, нужных мошенникам: устанавливать вредоносное ПО для кражи персональных данных; отображать всплывающие окна с ложными уведомлениями об угрозах; снижать производительность компьютера, повреждать файлы; отключать обновления операционной системы или антивирусных программ; блокировать посещение веб-сайтов разработчиков антивирусных программ и др.).

Рекомендуется осуществлять проверку компьютера на наличие вредоносных программ при помощи лицензионных антивирусных программ (программы, которые способны находить, лечить, а также полностью удалять вирусы из системы, а также моментально предупреждать о том, что на той или иной странице Интернета есть вирус и система может быть им заражена): Антивирус Касперского, Dr. Web и др. Используйте и оперативно обновляйте антивирусное ПО.