

Условия предоставления услуг с использованием системы «Клиент-Сбербанк»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Обслуживание Банком Клиентов осуществляется на основании заключенных Договоров и в соответствии с Тарифами Банка.

1.2. Заключение Договора о предоставлении услуг с использованием системы «Клиент-Сбербанк» между Банком и Клиентом (далее – Договор) осуществляется путем присоединения Клиента к настоящим Условиям (акцепта Условий) в соответствии со статьей 428 Гражданского кодекса Российской Федерации и производится путем передачи Клиентом или его уполномоченным представителем в Банк Заявления на заключение Договора.

1.3. Настоящие Условия предоставления услуг с использованием системы «Клиент-Сбербанк», Тарифы Банка и Заявление на заключение Договора, надлежащим образом заполненное и подписанное Клиентом, в совокупности являются заключенным между Клиентом и Банком Договором.

1.4. Заключение Договора осуществляется после представления Клиентом в Банк всех документов и сведений, установленных действующим законодательством Российской Федерации.

1.5. Фактом заключения Договора является прием Банком от Клиента Заявления на заключение Договора.

1.6. Настоящие Условия регламентируют порядок и условия оказания услуг Клиентам с использованием Системы.

1.7. Банк предоставляет Клиенту на платной основе следующие услуги с использованием Системы:

- прием от Клиента электронных документов, защищенных ЭЦП, на выполнение операций по счетам Клиента, указанным в Заявлении на заключение Договора;
- предоставление Клиенту в виде электронных документов, защищенных ЭЦП, информации об операциях, совершенных по счетам Клиента, указанным в Заявлении на заключение Договора;
- прием от Клиента и предоставление Клиенту информации свободного формата в виде электронных служебно-информационных документов, защищенных ЭЦП.

1.8. Электронные документы передаются и принимаются с использованием Системы без их последующего представления на бумажном носителе, за исключением случая, предусмотренного п. 2.1.9 настоящих Условий. Заверенные копии электронных документов на бумажном носителе выдаются Клиенту по письменному запросу по счету(-ам), указанному(-ым) в Заявлении на заключение Договора, согласно условиям соответствующего Договора банковского счета.

1.9. При подаче Заявления на заключение Договора Клиент может выбрать один из следующих типов подключения по системе «Клиент-Сбербанк»:

- 1.9.1. Интернет соединение через локальную вычислительную сеть или телефонное подключение посредством модема.
- 1.9.2. Коммутируемое соединение посредством модема по линии телефонной сети общего пользования.

Клиент имеет возможность изменить тип подключения по Системе путем подачи соответствующим образом заполненного Заявления.

1.10. Специальные термины, применяемые в тексте настоящего Договора, используются в значениях, приведенных в Приложении 1 к настоящим Условиям.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Банк обязуется:

2.1.1. Предоставить Клиенту в порядке, предусмотренном в Приложении 2 к настоящим Условиям, на время действия настоящего Договора:

- Программное обеспечение, в т.ч.:
 - Приложение АРМ «Клиент» со встроенными средствами криптографической защиты информации «Бикрипт-КСБ-С» и документацию по Системе в электронном виде;

- Программный модуль ViewDoc.exe
- ИЗК и пароль к нему, предназначенные для подключения к VPN-сети, а также инструкцию по установке и подключению (при использовании типа подключения по Системе «интернет-соединение»). В случае совместного использования несколькими юридическими лицами одного ИЗК, предоставленного подразделением Банка по другому Договору, ИЗК не предоставляется;
- Открытый ключ ЭЦП Банка в виде электронного файла и его сертификат на бумажном носителе;
- Ключи шифрования;
- Сопроводительную документацию, в т.ч.:
 - Спецификацию минимальных требований к программно-аппаратным средствам для установки АРМ «Клиент»;
 - Требования по обеспечению безопасности в процессе эксплуатации АРМ «Клиент»;
 - Правила пользования СКЗИ «Бикрипт-КСБ-С»;
 - Результаты вычисления значений хэш-функции для модуля ViewDOC (по ГОСТ Р 34.11-94);
 - Рекомендуемую форму доверенности на право распоряжаться денежными средствами по расчетным счетам, указанным в Заявлении на заключение Договора;
 - Форму Доверенности на получение программного обеспечения и сопроводительной документации;
 - Форму Акта приема-передачи программного обеспечения и средств защиты автоматизированной системы «Клиент-Сбербанк»;
 - Форму Заявки на проведение работ по Договору;
 - Форму Заявления об использовании кодового слова при эксплуатации автоматизированной системы «Клиент-Сбербанк»;
 - Форму Акта готовности к эксплуатации автоматизированной системы «Клиент-Сбербанк».

2.1.2. По заявлению Клиента [Форма № 3 Сопроводительной Документации] в согласованный Сторонами срок проводить выезд специалиста Банка/Аутсорсинговой компании для оказания услуг, связанных с установкой/переустановкой АРМ «Клиент», Дополнительных и Наблюдательных рабочих мест и эксплуатацией Системы;

2.1.3. Обеспечить подключение Клиента к Системе в соответствии с порядком, указанным в Приложении 2 к настоящим Условиям.

2.1.4. Принимать к исполнению поступившие от Клиента электронные платежные документы, оформленные и переданные в Банк в соответствии с условиями настоящего Договора и подписанные корректной ЭЦП Клиента.

2.1.5. Не исполнять поступившие от Клиента электронные платежные документы, оформленные с нарушением требований действующего законодательства Российской Федерации, нормативных документов Банка России и условий настоящего Договора, а также при отсутствии или некорректности ЭЦП Клиента.

2.1.6. Предоставлять в виде электронного служебно-информационного документа, подписанного ЭЦП Банка, информацию об операциях по счету(-ам), указанному(-ым) в Заявлении на заключение Договора, а также квитанции, подтверждающие получение Банком электронных платежных документов Клиента, – не позднее тридцати минут с момента получения Банком соответствующего электронного документа Клиента.

2.1.7. Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и условиями настоящего Договора.

2.1.8. Поддерживать до помещения в электронные архивы системные журналы и текущие базы переданных и принятых файлов с электронными документами и ЭЦП на аппаратных средствах Системы в течение не менее тридцати дней после их получения, а в случае возникновения споров – до их разрешения. Обеспечить сохранность архивов переданных и принятых файлов, подписанных ЭЦП, открытых ключей ЭЦП Клиента, а также системных журналов в течение срока, установленного действующим законодательством Российской Федерации.

2.1.9. Заверять, в случае необходимости, на основании письменного заявления Клиента в срок не позднее 3 рабочих дней подписями должностных лиц Банка и оттиском штампа Банка распечатанные на бумажном носителе копии электронных документов, принятых Клиентом по Системе, подписанных корректной ЭЦП Банка.

2.1.10. Организовать внутренний режим функционирования установленных по месту нахождения Банка рабочих мест таким образом, чтобы исключить возможность использования Системы и ключей ЭЦП лицами, не имеющими допуска к работе с Системой.

2.2. Банк имеет право:

2.2.1. Требовать от Клиента замены (формирования) ключей ЭЦП при проведении периодической плановой замены ключей ЭЦП, смене лиц, уполномоченных распоряжаться счетами, указанными в Заявлении на заключение Договора, компрометации или подозрении на компрометацию закрытых ключей ЭЦП, нарушении Требований по обеспечению безопасности в процессе эксплуатации АРМ «Клиент», а также в случае замены программного обеспечения, предназначенного для вычисления значения хэш-функции, подтверждения авторства, целостности и обеспечения конфиденциальности электронных документов.

2.2.2. Блокировать использование ключей ЭЦП Клиента после окончания срока их действия или по истечению срока действия полномочий Владельца сертификата ключа подписи, устанавливаемого Банком на основании учредительных документов, распорядительного акта Клиента либо выданной им доверенности.

2.2.3. Требовать от Клиента предоставления ИЗК для обновления ключей VPN (при использовании типа подключения по Системе «интернет-соединение»). При совместном использовании несколькими юридическими лицами одного ИЗК, предоставленного данным подразделением Банка по другому Договору, – приостановить оказание услуг по Договору, в случае не предоставления в Банк ИЗК его владельцем для обновления ключей VPN.

2.2.4. При установлении возможности нарушения безопасности Системы, выявлении фактов или признаков таких нарушений, немедленно приостановить использование Системы и оповестить Клиента в порядке, предусмотренном п. 11 Приложения 2 к настоящим Условиям.

2.2.5. В одностороннем порядке вводить новые, изменять и дополнять действующие Тарифы на услуги Банка, порядок и сроки взимания платы, уведомив об этом Клиента не позднее 15 дней до даты вступления в силу соответствующих изменений. Уведомление об установлении Тарифов по настоящему Договору направляется Банком Клиенту в виде электронного служебно-информационного документа с использованием Системы.

На дату заключения настоящего Договора Банком установлены Тарифы, опубликованные в региональной части сайта Банка, либо в соответствии с Приложением № 5 к настоящим Условиям.

2.2.6. Отказывать Клиенту, после предварительного предупреждения, в приеме от него распоряжений на проведение операции по банковскому счету, подписанных корректной ЭЦП, в случае выявления сомнительных операций Клиента. При этом Банк принимает от Клиента только надлежащим образом оформленные расчетные документы на бумажном носителе.

2.2.7. Вводить ограничения или полностью прекратить предоставление Клиенту услуг по настоящему Договору в случае выявления попыток сканирования, атак информационных ресурсов Банка, нарушения контроля целостности программных средств АРМ «Клиент», а также иных признаков нарушения безопасности с использованием программно-аппаратных средств Клиента.

2.2.8. Разрабатывать новые версии программного обеспечения, инструкций по безопасности и использованию Системы и предоставлять их Клиенту путем передачи по Системе для последующей установки, обновления и применения.

2.2.9. Не осуществлять техническую поддержку АРМ «Клиент», Дополнительных/Наблюдательных рабочих мест «Клиент-Сбербанк», версия которых ниже двух последних, выпущенных Банком.

2.2.10. Вносить в одностороннем порядке изменения в настоящие Условия и в Сопроводительную документацию в случае использования иных сертифицированных средств криптографической защиты, программного обеспечения, предназначенного для вычисления значения хэш-функции и для подтверждения авторства и целостности электронных документов, подписанных ЭЦП, программно-аппаратного комплекса для подключения к защищенной корпоративной VPN-сети, а также в порядок применения средств Системы с письменным уведомлением Клиента не позднее, чем за тридцать календарных дней до вступления в действие указанных изменений. При не поступлении от

Клиента в указанный выше срок заявления в письменной форме о расторжении настоящего Договора изменения считаются принятыми.

2.2.11. Привлекать сторонние организации/Аутсорсинговые компании для оказания Клиенту услуг, связанных с установкой и эксплуатацией Системы. В этом случае Банк несет ответственность за качество оказания данными организациями указанных услуг.

2.2.12. Использовать псевдоним Владельца сертификата ключа подписи – должностного лица Банка.

2.2.13. Уведомить Клиента о необходимости подачи корректирующего Заявления на заключение договора, в т.ч. посредством Системы, в срок, предусмотренный п. 2.3.19 настоящих Условий. Если корректирующее Заявление не будет подано Клиентом, Банк имеет право приостановить оказание услуги.

2.3. Клиент обязуется:

2.3.1. Получить после подписания настоящего Договора от Банка ИЗК (при использовании типа подключения по Системе «интернет-соединение»); кроме случаев совместного использования несколькими юридическими лицами одного ИЗК, предоставленного подразделением Банка по другому Договору), программные средства и сопроводительную документацию, указанную в п. 2.1.1 настоящих Условий.

2.3.2. Оплачивать услуги Банка на основании Тарифов в порядке и сроки, предусмотренные п. 3.1. настоящих Условий.

2.3.3. Представить в Банк документ, удостоверяющий личность уполномоченного лица Клиента, а также передать в Банк документы, подтверждающие права уполномоченного лица Клиента по распоряжению денежными средствами, находящимися на счете, используя ЭЦП или копии указанных документов, заверенные установленным порядком.

2.3.4. Обеспечить согласие физических лиц, персональные данные которых содержатся в представляемых Клиентом Банку документах в рамках настоящего Договора, на проверку и обработку (включая автоматизированную обработку) их персональных данных Банком в соответствии с требованиями действующего законодательства Российской Федерации, в том числе Федерального закона от 27 июля 2006 года № 152 – ФЗ «О персональных данных». Рекомендуемая форма заявления о согласии размещается на сайте Банка.

2.3.5. Обеспечить, при установке и обновлении собственными силами АРМ «Клиент», Дополнительного или Наблюдательного рабочего места «Клиент-Сбербанк», инсталляцию и настройку программного обеспечения, а также готовность к вводу в действие Системы в соответствии с п.п. 1 – 6 Приложения 2 к настоящим Условиям.

2.3.6. Предоставлять, в случае проведения работ специалистами Банка/Аутсорсинговой компании, рабочие площадки на своей территории, необходимые для подготовки к работе системы «Клиент-Сбербанк», обеспечить необходимые условия и соблюдение сроков проведения работ в соответствии с п.п. 1 – 9 Приложения 2 к настоящим Условиям.

2.3.7. В случае проведения работ специалистами Банка/Аутсорсинговой компании на рабочем месте Клиента, предоставлять в Банк Акт о проведении работ по заявке, заверенный подписью уполномоченного лица и оттиском печати Клиента, не позднее 5 рабочих дней со дня выполнения работ.

2.3.8. Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и условиями настоящего Договора.

2.3.9. При установлении возможности нарушения безопасности Системы, выявлении фактов или признаков таких нарушений, немедленно приостановить использование Системы и оповестить Банк в порядке, предусмотренном п. 11 Приложения 2 к настоящим Условиям.

2.3.10. Подписывать электронные платежные документы ЭЦП уполномоченных лиц в соответствии с требованиями действующего законодательства Российской Федерации¹ и Банка России и в количестве, указанном в Акте готовности к эксплуатации автоматизированной системы «Клиент-Сбербанк».

2.3.11. Поддерживать до помещения в электронные архивы системные журналы и текущие базы переданных и принятых файлов с электронными документами и ЭЦП на собственных аппаратных

¹ Федеральный закон «О бухгалтерском учете» №129-ФЗ от 21.11.1996г.

средствах в течение не менее 30 дней после их получения, а в случае возникновения споров – до их разрешения. Обеспечить сохранность архивов переданных и принятых файлов, подписанных ЭЦП, открытых ключей ЭЦП Банка, а также системных журналов в течение срока, установленного действующим законодательством Российской Федерации.

2.3.12. Организовывать внутренний режим функционирования рабочих мест уполномоченных лиц таким образом, чтобы исключить возможность использования Системы и ключей ЭЦП лицами, не имеющими допуска к работе с Системой.

2.3.13. Соблюдать Требования по обеспечению безопасности в процессе эксплуатации АРМ «Клиент».

2.3.14. Производить замену ключей ЭЦП уполномоченных лиц в случаях, предусмотренных п. 2.2.1 настоящих Условий.

2.3.15. Предоставлять Банку ИЗК для обновления ключей VPN (при использовании типа подключения по Системе «интернет-соединение»; кроме случаев совместного использования несколькими юридическими лицами одного ИЗК, предоставленного подразделением Банка по другому Договору).

2.3.16. Передать Банку в срок не позднее следующего рабочего дня с даты его обращения распечатанную на бумажном носителе и заверенную подписями уполномоченных лиц Клиента и оттиском печати Клиента копию электронного документа, принятого Банком от Клиента по Системе, подписанного корректной ЭЦП уполномоченного лица Клиента.

2.3.17. Использовать предоставленные в соответствии с п. 2.1.1 настоящего Договора документацию и инструкции по Системе, ИЗК (при использовании типа подключения по Системе «интернет-соединение»; кроме случаев совместного использования несколькими юридическими лицами одного ИЗК, предоставленного подразделением Банка по другому Договору) и программные средства, в т.ч. используемые в Системе шифровальные средства, только в рамках Системы, без права их отчуждения и/или передачи в пользование другим физическим и/или юридическим лицам, за исключением перечня клиентов, для которых допускается совместное использование ИЗК по Договорам о предоставлении услуг с использованием системы «Клиент-Сбербанк» и перечисленных в Заявлении на заключение договора, а также случаев, прямо предусмотренных действующим законодательством Российской Федерации.

2.3.18. После расторжения настоящего Договора или прекращения его действия прекратить использование и уничтожить программное обеспечение, включая средства защиты, предоставленное Клиенту согласно п. 2.1.1 настоящих Условий.

2.3.19. При изменении формы Заявления на заключение договора, требующем от Клиента заполнения дополнительных полей, без которых невозможно дальнейшее обслуживание по Системе, в течение 10 (десяти) рабочих дней с момента получения уведомления Банка в установленном порядке подать корректирующее Заявление на заключение договора.

2.4. Клиент имеет право:

2.4.1. В случае возникновения у Клиента претензий, связанных с принятием или непринятием и/или исполнением или неисполнением Банком электронного документа, требовать от Банка проведения технической экспертизы в соответствии с Приложением 3 к настоящим Условиям.

2.4.2. В любое время производить замену ключей ЭЦП Клиента.

2.4.3. Отозвать ранее переданный электронный платежный документ, имеющий корректную ЭЦП Клиента, путем направления в Банк по Системе соответствующего уведомления в виде электронного служебно-информационного документа, защищенного ЭЦП, при условии, что Банк к моменту получения уведомления Клиента не произвел списание со счета Клиента денежных средств во исполнение ранее полученного от Клиента электронного платежного документа.

2.4.4. Приостановить на срок до шести месяцев предоставление услуг по настоящему Договору, путем направления не менее, чем за два дня письменного уведомления с указанием даты начала и даты окончания приостановки предоставления услуг, заверенного руководителем Клиента или лицом, наделенным правом подписывать Договор(ы) финансово-банковских услуг, а также оттиском печати Клиента.

3. УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ И ОПЛАТЫ УСЛУГ

3.1. Плата за услуги Банка по Договору списывается Банком в безакцептном порядке со счета Клиента, указанного в Заявлении на заключение договора.

- Платы за организацию расчетно-кассового обслуживания с использованием системы «Клиент-Сбербанк», за восстановление программного обеспечения АРМ «Клиент», нарушенного по вине клиента, за замену идентификатора для записи ключей VPN-сети, выведенного из строя клиентом (при использовании типа подключения по Системе «интернет-соединение»; кроме случаев совместного использования несколькими юридическими лицами одного ИЗК, предоставленного подразделением Банка по другому Договору), взимаются Банком не ранее дня подписания Сторонами Акта приема-передачи программного обеспечения и средств защиты автоматизированной системы «Клиент-Сбербанк» в соответствии с Тарифами Банка.
- Ежемесячная плата за предоставление услуг с использованием системы «Клиент-Сбербанк» взимается Банком в соответствии с Тарифами, начиная с даты ввода в действие Системы, не ранее последнего рабочего дня месяца, в котором услуга была предоставлена.
- Ежемесячная плата за предоставление услуг с использованием системы «Клиент-Сбербанк» по Дополнительному/Наблюдательному рабочему месту «Клиент-Сбербанк», имеющему локальную базу документов, взимается Банком в соответствии с Тарифами, начиная с даты ввода в действие указанного Дополнительного/Наблюдательного рабочего места «Клиент-Сбербанк», не ранее последнего рабочего дня месяца, в котором услуга была предоставлена.

3.2. Общие условия предоставления услуг и обслуживания Системы, а также порядок ввода в действие Системы изложены в Приложении 2 к настоящим Условиям.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

4.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Договору виновная Сторона несет ответственность в соответствии с действующим законодательством Российской Федерации.

4.2. В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих или препятствующих осуществлению Сторонами своих функций по Договору и иных обстоятельств, не зависящих от волеизъявления Сторон, Стороны по настоящему Договору освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

При наступлении обстоятельств непреодолимой силы Сторона должна без промедления известить о них другую Сторону в порядке, предусмотренном п. 11 Приложения 2 к настоящим Условиям. Извещение должно содержать данные о характере обстоятельств, а также оценку их влияния на возможность исполнения Стороной обязательств по настоящему Договору.

По прекращении указанных выше обстоятельств Сторона должна без промедления известить об этом другую Сторону в порядке, предусмотренном п. 11 Приложения 2 к настоящим Условиям. В извещении должен быть указан срок, в течение которого предполагается исполнить обязательства по настоящему Договору.

4.3. В случае неоплаты Банку предоставленных услуг (в том числе по причине отсутствия достаточной суммы средств на счете(ах) Клиента или невозможности списания средств в связи с приостановлением расходных операций по счету(ам) или наложением ареста на денежные средства, находящиеся на счете(ах)), Банк имеет право приостановить на срок до одного месяца предоставление услуг по настоящему Договору, а в случае неоплаты по истечении указанного срока – расторгнуть Договор в одностороннем порядке без соблюдения срока, установленного п. 6.3 настоящих Условий. При этом Клиенту направляется письменное уведомление о расторжении Договора.

4.4. Стороны несут ответственность за содержание электронных документов, подписанных ЭЦП их уполномоченных лиц, и не отвечают за правильность заполнения и оформления электронных документов другой Стороной.

4.5. Банк не несет ответственности за ущерб, возникший вследствие разглашения уполномоченными лицами Клиента собственного закрытого ключа ЭЦП, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.

4.6. Банк не несет ответственности за последствия исполнения электронного платежного документа, защищенного корректной ЭЦП Клиента, в т.ч. в случае использования ключей ЭЦП и программно-аппаратных средств клиентской части Системы неуполномоченным лицом.

4.7. Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к части Системы, установленной у Клиента, и криптографическим ключам Клиента, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

4.8. Банк не несет ответственности за неработоспособность оборудования и программных средств Клиента и третьих лиц, повлекшую за собой невозможность доступа Клиента к банковской части Системы и возникшие в результате задержки в осуществлении платежей Клиента, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах Клиента, подключенных к сети Интернет для обеспечения предоставления услуг по Договору.

5. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

5.1. При возникновении разногласий и споров в связи с обменом электронными документами с помощью Системы с целью установления фактических обстоятельств, послуживших основанием для их возникновения, а также для проверки целостности и подтверждения авторства электронного документа, Стороны обязаны провести техническую экспертизу, процедура и сроки проведения которой установлены Приложением 3 к настоящему Договору. Споры, по которым не достигнуто соглашение Сторон после проведения технической экспертизы, разрешаются в Арбитражном суде по месту заключения Договора в соответствии с действующим законодательством Российской Федерации.

6. СРОК ДЕЙСТВИЯ ДОГОВОРА

6.1. Договор вступает в силу с даты приема Банком Заявления на заключение договора и действует в течение 1 (Одного) года.

6.2. Договор считается пролонгированным на каждый следующий срок, если ни одна из Сторон не предупредит другую Сторону о прекращении использования Системы не менее чем за 30 дней до даты окончания срока действия Договора.

6.3. Договор может быть расторгнут досрочно любой из Сторон в одностороннем порядке путем предварительного письменного уведомления другой Стороны не менее чем за 30 дней до даты расторжения Договора.

6.4. С момента прекращения действия/расторжения Договора Банк прекращает предоставление услуг, указанных в п. 1.7 настоящих Условий, блокируя доступ к банковской части Системы с рабочих мест Клиента.

6.5. Все приложения, на которые даны ссылки в тексте настоящих Условий, являются его неотъемлемыми частями.

Приложение 1
к Условиям предоставления услуг
с использованием системы «Клиент-Сбербанк»

Термины и определения

Специальные термины, применяемые в тексте настоящих Условий, используются в следующем значении:

Автоматизированная система «Клиент-Сбербанк» (Система) – корпоративная информационная система Клиент-Банк ОАО «Сбербанк России», включающая в себя совокупность программно-аппаратных средств, устанавливаемых у Клиента и Банка с целью обеспечения подготовки, защиты, отправки, приема, проверки и обработки документов в электронном виде.

Система состоит из:

- программных и аппаратных средств, соответствующих требованиям Банка, комплектуемых и эксплуатируемых Клиентом за свой счет;
- аппаратных средств Банка, эксплуатируемых Банком за свой счет;
- программных средств Системы, устанавливаемых в соответствующих частях на аппаратных средствах Клиента и Банка и самостоятельно эксплуатируемых Сторонами;
- программных и аппаратных средств связи, обеспечивающих обмен электронными документами между Сторонами.

Автоматизированное рабочее место «Клиент-Сбербанк» (АРМ «Клиент») – составная часть Системы, устанавливаемая на территории Клиента, используемая Клиентом для предоставления в Банк и получения от Банка электронных документов. АРМ «Клиент» является основным рабочим местом Клиента в Системе.

Авторство ЭД – принадлежность ЭД создавшей его Стороне.

Аутсорсинговая компания – организация, с которой Банком заключен соответствующий договор на оказание услуг по установке и сопровождению установленных у Клиентов компонент Системы.

Бикрипт-КСБ-С – программное обеспечение – средство криптографической защиты информации, используемое для генерации закрытых и открытых ключей ЭЦП, формирования и проверки ЭЦП.

Владелец сертификата ключа подписи – уполномоченный сотрудник Клиента или Банка, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и который владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Договор – совокупность следующих документов: «Условия предоставления услуг с использованием системы «Клиент-Сбербанк» и «Заявление на заключение договора о предоставлении услуг с использованием системы «Клиент-Сбербанк».

Дополнительное рабочее место «Клиент-Сбербанк» – составная часть Системы, устанавливаемая на программно-аппаратных средствах Клиента, используемая Клиентом для предоставления в Банк и получения от Банка электронных документов. Дополнительное рабочее место «Клиент-Сбербанк» может иметь общую базу документов с АРМ «Клиент» или иметь локальную базу документов. Дополнительное рабочее место «Клиент-Сбербанк» имеющее локальную базу документов функционально идентично АРМ «Клиент».

Закрытый ключ ЭЦП – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Заявление на заключение договора - Заявление на заключение договора о предоставлении услуг с использованием системы «Клиент-Сбербанк», являющееся акцептом предложенной Банком оферты на заключение Договора.

Идентификатор для записи ключей VPN-сети (ИЗК) – электронный идентификатор на базе USB-Key, устанавливаемый на компьютере Клиента, предназначенный для записи ключей VPN (Virtual Private Network) сети и подключения к защищенной корпоративной VPN-сети ОАО «Сбербанк России».

Допускается совместное использование ИЗК для приема/передачи информации, несколькими юридическими лицами - клиентами банка, заключившими Договор(-ы) о предоставлении услуг с использованием системы «Клиент-Сбербанк» и указанными в Заявлении на заключение Договора, при условии, что соответствующие АРМ «Клиент» установлены на одном компьютере и эксплуатируются одним и тем же персоналом. В случае совместного использования несколькими юридическими лицами одного ИЗК, предоставленного подразделением Банка по настоящему Договору Перечень Клиентов, для которых допускается совместное использование ИЗК указывается в Заявлении на заключение Договора.

В случае совместного использования Клиентом ИЗК, предоставленного данным подразделением Банка другому юридическому лицу в Заявлении на заключение Договора указываются реквизиты Договора о предоставлении услуг с использованием системы «Клиент-Сбербанк», заключенного владельцем ИЗК с Банком.

Ключи шифрования – ключи, изготавливаемые Банком с использованием средств Системы и предназначенные для защиты ЭД Сторон при их передаче по каналам связи. Передача ключей шифрования Банком Клиенту отражается в Акте приема-передачи программного обеспечения и средств защиты автоматизированной системы «Клиент-Сбербанк», который подписывается Сторонами.

Корректная электронная цифровая подпись – электронная цифровая подпись, дающая положительный результат ее проверки программно-аппаратными средствами Системы, с использованием действующего на момент подписания открытого ключа подписи его владельца.

Наблюдательное рабочее место «Клиент-Сбербанк» – составная часть Системы, устанавливаемая на территории Клиента, используемая им для получения от Банка сведений об остатках, движении денежных средств по счету(-ам), указанным в Заявлении на заключение Договора.

Открытый ключ ЭЦП – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, и предназначенная для проверки корректности ЭЦП электронных документов. Открытый ключ подписи считается принадлежащим участнику Системы, если он был зарегистрирован в Системе в соответствии с изложенным в п. 16 Приложения 2 к настоящим Условиям порядком. Открытый ключ является недействующим на момент подписания, если он не зарегистрирован или выведен из действия.

Пароль ИЗК – пароль, необходимый для получения доступа к функциям ИЗК.

Сертификат ключа подписи – документ на бумажном носителе, который включает в себя открытый ключ электронной цифровой подписи и который выдается Удостоверяющим центром участнику Системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Удостоверяющий центр – орган, выполняющий в Системе функции, предусмотренные Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

Уполномоченное лицо Клиента – сотрудник Клиента, уполномоченный распоряжаться денежными средствами, находящимися на счете, и совершать иные действия, предусмотренные разделом 1 настоящих Условий, используя электронную цифровую подпись.

Условия – Условия предоставления услуг с использованием системы «Клиент-Сбербанк».

Уполномоченное лицо Банка – физическое лицо Банка, уполномоченное предоставлять Клиенту информацию об операциях, совершенных по счету(-ам), и остатках средств по счету(-ам) Клиента, и совершать иные действия, предусмотренные разделом 1 настоящих Условий, используя электронную цифровую подпись.

ФПСУ-IP – программно-аппаратный комплекс, устанавливаемый в Банке и предназначенный для организации доступа Клиента к защищенной корпоративной сети ОАО «Сбербанк России» (VPN-сети) и обеспечения конфиденциальности передаваемых по сети общего пользования документов.

Хэш-функция – однонаправленное отображение (свертка) содержимого файла или блока данных произвольного размера в блок данных фиксированного размера, обладающее заданными математическими свойствами; используется при формировании и проверке ЭЦП, а также для контроля целостности программного обеспечения и данных.

Электронная цифровая подпись (ЭЦП) – контрольное значение электронного документа, предназначенное для защиты его от подделки, полученное в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющее идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронный документ (ЭД) – электронный образ документа (платежного или иного), представленный в согласованном Сторонами формате, определяемом программными средствами создания документа. ЭД передается между Сторонами в составе файла, подписанного ЭЦП. В состав файла может входить несколько ЭД. Если файл имеет корректную ЭЦП, то каждый электронный документ, входящий в файл, считается подписанным ЭЦП.

Электронный платежный документ (ЭПД) – электронный документ (платежное поручение Клиента), являющийся основанием для совершения Банком операций по банковскому счету Клиента. ЭПД, защищенные корректной ЭЦП, имеют равную юридическую силу с расчетными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

Электронный служебно-информационный документ (ЭСИД) – электронный документ, защищенный корректной ЭЦП и обеспечивающий обмен информацией между Банком и Клиентом при совершении расчетов и проведении операций по счету Клиента.

ЭЦП Стороны (ЭЦП Банка или Клиента) – ЭЦП любого уполномоченного лица Стороны.

ViewDoc.exe – программное обеспечение (модуль), предназначенное для подтверждения авторства и целостности электронных документов, подписанных ЭЦП, а также для вычисления значения хэш-функции по ГОСТ Р 34.11-94.

Приложение 2

к Условиям предоставления услуг
с использованием системы «Клиент-Сбербанк»

Порядок ввода в действие Системы и Общие условия предоставления услуг и обслуживания Системы

1. Программное обеспечение, открытые ключи ЭЦП Банка и сопроводительная документация, перечисленные в п. 2.1.1. настоящих Условий, Банк предоставляет Клиенту на носителе цифровой информации или через сайт Банка. Стороны оформляют Акт приема-передачи программного обеспечения и средств защиты автоматизированной системы «Клиент-Сбербанк», в котором отражается факт получения Клиентом от Банка ИЗК (при использовании типа подключения по Системе «интернет-соединение»; кроме случаев совместного использования несколькими юридическими лицами одного ИЗК, предоставленного подразделением Банка по другому Договору), Ключей шифрования и, в случае предоставления на носителе цифровой информации, программного обеспечения, открытого ключа ЭЦП Банка и сопроводительной документации.

2. Клиент самостоятельно проводит установку, переустановку и настройку переданного Банком программного обеспечения, в соответствии с предоставленными инструкциями, на своих аппаратных средствах, отвечающих требованиям спецификации (СПЕЦИФИКАЦИЯ аппаратных и программных средств для установки АРМ «Клиент» АС «Клиент-Сбербанк» Сопроводительной документации).

3. Для регистрации программного обеспечения на каждую процедуру установки, переустановки или переноса АРМ «Клиент» на иные аппаратные средства, а также в случаях, когда производятся действия, связанные с изменениями конфигурации программно-аппаратных средств, Клиент предоставляет в Банк кодовое слово [Форма №4 Сопроводительной документации] не позднее рабочего дня, предшествующего дню проведения работ.

4. В случае невозможности проведения самостоятельной установки, переустановки или обновления АРМ «Клиент» силами Клиента, по письменной заявке [Форма №3 Сопроводительной документации] Банк или Аутсорсинговая компания в согласованный Сторонами срок после получения заявки устанавливает на технических средствах Клиента необходимое программное обеспечение и подготавливает его к работе.

5. По окончании работ по установке и настройке программного обеспечения Клиент производит вычисление значений и печать хэш-функции каждого установленного приложения АРМ «Клиент». Уполномоченные лица Клиента самостоятельно формируют закрытый и открытый ключи ЭЦП и производят распечатку сертификатов ключа подписи на бумажном носителе.

6. По окончании работ в соответствии с п.п. 2 – 5 настоящего Приложения Клиент одновременно передает Банку:

– Акт готовности к эксплуатации автоматизированной системы «Клиент-Сбербанк», подписанный и заверенный оттиском печати Клиента (в двух экземплярах);

– документ(-ы) подтверждающий(-ие) права уполномоченных лиц(-а) распоряжаться денежными средствами на счете с использованием ЭЦП с правами первой и второй подписи;

– распечатки проектов сертификатов ключей подписи, заверенные собственноручной подписью владельца сертификата ключа подписи, руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг и оттиском печати Клиента (по три экземпляра для каждого открытого ключа ЭЦП);

– распечатанные и заверенные подписью уполномоченного лица и оттиском печати Клиента значения хэш-функции программного обеспечения;

– электронные файлы открытых ключей Клиента и значения хэш-функции программного обеспечения каждого установленного приложения АРМ «Клиент», подписанные ЭЦП Клиента²;

– Акт о проведении работ по заявке, заверенный подписью уполномоченного лица и оттиском печати Клиента, в случае установки Системы работниками Банка или Аутсорсинговой компании.

7. При отсутствии замечаний по оформлению представленных документов и корректности произведенной установки программного обеспечения руководитель или лицо, наделенное правом от

² Передача значений хэш-функции АРМ «Клиент» производится системой в автоматическом режиме

имени Банка подписывать договор(-ы) о предоставлении услуг с использованием системы «Клиент-Сбербанк», подписывает Акт готовности к эксплуатации автоматизированной системы «Клиент-Сбербанк». Один экземпляр Акта и один экземпляр сертификатов ключей подписи Клиента передается Клиенту.

Дата подписания указанного Акта является датой ввода Системы в действие.

8. При замене ключей ЭЦП в соответствии с условиями настоящего Договора Клиент предоставляет в Банк распечатки проектов сертификатов ключей подписи и документ(-ы) подтверждающий(-ие) полномочия указанного в сертификате лица на право распоряжения денежными средствами на счете с использованием ЭЦП.

9. Все документы, предоставляемые Клиентом Банку или подписываемые Сторонами по итогам проведения работ в соответствии с п.п. 2 – 5 настоящего Приложения, должны быть составлены по формам, приведенным в Сопроводительной Документации к настоящему Договору.

10. С целью исполнения условий настоящего Договора Банк передает во владение Клиенту на время действия Договора программный модуль ViewDoc.exe, предназначенный для проверки ЭЦП электронных документов при проведении процедуры технической экспертизы в соответствии с Приложением 3 к настоящим Условиям и для вычисления значений хэш-функции.

11. При выходе из строя аппаратных или программных средств Системы или их элементов, а также в иных случаях невозможности предоставления (получения) услуг, указанных в разделе 1. Условий и, соответственно, приостановлении использования Системы, Сторона обязана в течение трех часов известить другую Сторону любым доступным способом, а в течение суток дать письменное сообщение о готовности и сроках возобновления обмена документами в электронном виде. На период приостановления использования Системы обмен документами между Сторонами осуществляется на бумажных носителях или с использованием иных, предусмотренных Договором банковского счета, систем и средств связи.

12. Стороны признают, что программные средства, обеспечивающие шифрование, изготовление закрытых и открытых ключей ЭЦП, а также формирование и проверку ЭЦП, реализуют алгоритмы в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

13. Клиент признает, что получение Банком электронных документов, подписанных корректной ЭЦП Клиента, равнозначно получению документов на бумажном носителе, подписанных собственноручной подписью уполномоченных(-ого) лиц(-а) и заверенных оттиском печати Клиента.

14. Банк признает, что получение Клиентом электронных документов, подписанных корректной ЭЦП Банка, равнозначно получению документов на бумажном носителе, подписанных собственноручной подписью уполномоченных(-ого) лиц(-а) и заверенных оттиском штампа Банка.

15. Стороны признают, что:

- используемая Сторонами в соответствии с настоящим Договором система защиты информации, которая реализует подписание ЭЦП и шифрование электронных документов, достаточна для обеспечения конфиденциальности, а также подтверждения авторства и контроля целостности электронных документов;
- после подписания электронного документа ЭЦП любое изменение, добавление или удаление символов документа делает ЭЦП некорректной, т.е. проверка подписи с открытым ключом ЭЦП Стороны, подписавшей электронный документ, дает отрицательный результат;
- создание корректной ЭЦП электронного документа возможно исключительно с использованием закрытого ключа ЭЦП;
- по содержанию электронных документов, подписанных ЭЦП, и открытых ключей ЭЦП невозможно определить закрытые ключи ЭЦП;
- каждая Сторона несет полную ответственность за обеспечение безопасности и сохранность своих закрытых ключей ЭЦП, а также за действия своего персонала;
- целостность программных средств АРМ «Клиент» может быть проверена путем вычисления значений хэш-функции по ГОСТ Р 34.11-94 и сравнения их со значениями хэш-функции, вычисленными при установке или обновлении программного обеспечения;

- предоставление в Банк распечатки проекта сертификата ключа подписи на бумажном носителе, сформированной на АРМ «Клиент» и заверенной собственноручной подписью владельца сертификата ключа подписи, руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг, и оттиском печати Клиента, эквивалентно подаче в Удостоверяющий центр заявления на выдачу сертификата ключа подписи уполномоченного лица Клиента.

16. Порядок применения средств Системы предусматривает, что:

- функции Удостоверяющего центра по настоящему Договору выполняет Банк;
- каждая Сторона может иметь несколько закрытых ключей ЭЦП, каждому закрытому ключу ЭЦП соответствует собственный открытый ключ ЭЦП;
- каждая Сторона самостоятельно формирует (изготавливает) свои закрытые и открытые ключи ЭЦП;

- Клиент предоставляет Банку каждый собственный открытый ключ подписи одновременно в виде электронного файла и в виде распечатки проекта сертификата на бумажном носителе, заверенной собственноручной подписью владельца сертификата ключа подписи, руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг, и оттиском печати Клиента, в трех экземплярах. В случае, когда уполномоченное лицо Клиента является руководителем или лицом, наделенным правом подписывать Договор(ы) финансово-банковских услуг, проект сертификата ключа подписи на бумажном носителе заверяется одной подписью уполномоченного лица Клиента и оттиском печати Клиента;

- Удостоверяющий центр не позднее трех рабочих дней осуществляет проверку уникальности идентификатора ключа подписи, корректности и соответствия открытого ключа в распечатке проекта сертификата электронному файлу и оформляет сертификаты ключа подписи на бумажном носителе с указанием сроков действия ключа подписи. Один экземпляр сертификата передается Клиенту;

- Клиент предоставляет Банку документы (доверенность или распоряжение), подтверждающие права уполномоченных лиц на распоряжение денежными средствами, находящимися на счетах Клиента и передачу иных документов по счетам Клиента с использованием ЭЦП. В случае изменения в составе уполномоченных лиц Клиент обязан представить соответствующие документы, подтверждающие изменения. Банк устанавливает личности уполномоченных лиц Клиента на основании документов, удостоверяющих их личность;

- Стороны предоставляют друг другу собственные открытые ключи подписи в виде электронного файла и в виде сертификата на бумажном носителе, заверенном подписью уполномоченного лица и оттиском печати Удостоверяющего центра;

- представленный Клиентом открытый ключ подписи вводится в действие с даты, указанной в его сертификате;

- предоставленный Клиентом открытый ключ подписи может быть временно заблокирован Банком в случае окончания полномочий Владельца сертификата ключа подписи до предоставления Клиентом в Банк документов, подтверждающих пролонгацию полномочий Владельца сертификата ключа подписи;

- при компрометации или подозрении на компрометацию закрытого ключа ЭЦП или ключа шифрования одной из Сторон (т.е. при ознакомлении или подозрении на ознакомление неуполномоченного лица с закрытым ключом ЭЦП или с ключом шифрования, а также при несанкционированном использовании или подозрении на несанкционированное использование закрытого ключа ЭЦП или ключа шифрования) другая Сторона извещается передачей электронного служебно-информационного документа по Системе или иным доступным способом о прекращении действия соответствующего ключа ЭЦП. С момента уведомления Стороны прекращают передачу электронных документов с использованием указанного ключа ЭЦП, и выводят из действия соответствующий открытый ключ ЭЦП. Скомпрометированные ключи уничтожаются Сторонами самостоятельно;

- Сторона, получившая по Системе сообщение о компрометации и/или замене ключа ЭЦП, выводит соответствующий открытый ключ из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о компрометации;

– Количество различных ключей ЭЦП, используемых Клиентом для подписания передаваемых Банку электронных платежных документов, определяется действующим законодательством Российской Федерации³ и требованиями Банка России и указывается в Акте готовности к эксплуатации автоматизированной системы «Клиент-Сбербанк». При использовании 2-х ЭЦП электронный документ признается имеющим корректную ЭЦП, если корректны и принадлежат разным лицам, имеющим право первой и второй подписи, обе ЭЦП, которыми он подписан;

при использовании типа подключения по Системе «интернет-соединение»:

– Клиент самостоятельно выбирает организацию – провайдера, обеспечивающую доступ к сети Интернет, и осуществляет подключение к сети Интернет за счет собственных средств. Все расходы, связанные с подключением к сети Интернет, эксплуатацией и обменом данными по Системе через сеть Интернет, осуществляются Клиентом за счет собственных средств;

– Клиент по предоставленным Банком спецификациям для обеспечения защищенной связи по сети Интернет самостоятельно обеспечивает необходимую настройку телекоммуникационного и другого оборудования (коммутаторы, маршрутизаторы, прокси-сервера, сетевые экраны и пр.) в своей локальной сети;

– Клиент полностью несет все риски, связанные с подключением его вычислительных средств к сети Интернет. Клиент самостоятельно обеспечивает защиту собственных вычислительных средств и криптографических ключей от несанкционированного доступа и вирусных атак из сети Интернет. Стороны также признают, что выход из строя АРМ «Клиент» в результате вмешательства из сети Интернет рассматривается как выход из строя по вине Клиента и восстановление работоспособности Системы осуществляется в соответствии с действующими тарифами Банка.

17. Исходя из изложенного в п.п. 12 – 16 настоящего Приложения Стороны признают аутентификационные свойства средств ЭЦП, применяемых ими. Электронный документ, подписанный корректной ЭЦП одной из Сторон, признается другой Стороной как эквивалентный документу на бумажном носителе, составленному и оформленному в соответствии с законодательством Российской Федерации, а также нормативными документами Банка России, и порождает права и обязанности Сторон при выполнении взаимных обязательств по настоящему Договору и договору(-ам), дополнительным соглашениям и всем приложениям к ним по счету(-ам), указанному(-ым) в Заявлении на заключение Договора.

18. Стороны признают в качестве единой шкалы времени при работе в Системе местное поясное время по месту ведения счета. Контрольным является время системных часов аппаратных средств Банка.

19. Стороны установили, что моментом получения электронного документа принимающей Стороной в Системе является текущее время по системным часам принимающей Стороны в момент помещения информации в архив входящих сообщений принимающей Стороны.

20. Банк исполняет поступившие от Клиента в пределах операционного времени Банка по месту ведения счета электронные платежные документы, имеющие корректную ЭЦП, на совершение операций по счетам Клиента, указанным в Заявлении на заключение Договора, текущим рабочим днем, а поступившие в послеоперационное время – следующим рабочим днем.

21. На дату заключения настоящего Договора Банком установлено операционное время, опубликованное в региональной части сайта Банка, либо в соответствии с Приложением № 5 к настоящим Условиям расчетно-кассового обслуживания.

³ Федеральный закон «О бухгалтерском учете» №129-ФЗ от 21.11.1996г.

Приложение 3

к Условиям предоставления услуг с использованием системы «Клиент-Сбербанк»

ПРОЦЕДУРА ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ СПОРНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПРИНЯТИЕМ ИЛИ НЕПРИНЯТИЕМ, ИСПОЛНЕНИЕМ ИЛИ НЕИСПОЛНЕНИЕМ БАНКОМ ЭЛЕКТРОННОГО ДОКУМЕНТА КЛИЕНТА

1. При возникновении разногласий Сторон в связи с обменом документами в электронном виде с помощью системы «Клиент-Сбербанк», а также в иных случаях возникновения спорных ситуаций в связи с эксплуатацией системы, обмен документами в электронном виде с использованием системы «Клиент-Сбербанк» между Сторонами немедленно прекращается.

2. Сторона, заявляющая разногласие, (инициатор спора) обязана направить другой Стороне заявление о разногласиях, подписанное руководителем или лицом Стороны, наделенным правом подписывать Договор(ы) финансово-банковских услуг, с предложением создать согласительную комиссию и изложением причин разногласий, в объеме, необходимом для исполнения настоящей Процедуры. Заявление должно содержать фамилии, имена, отчества и иные сведения о представителях Стороны - инициатора спора, которые будут участвовать в работе комиссии, место, время и дату сбора комиссии. Дата сбора комиссии должна быть не позднее десяти дней со дня получения другой Стороной заявления.

3. В состав комиссии должно входить равное количество представителей от Клиента и Банка (до трех человек от каждой из Сторон), полномочия которых удостоверяются доверенностями, оформленными в соответствии с действующим законодательством Российской Федерации. При необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно введены эксперты третьей стороны. Состав комиссии должен быть зафиксирован в акте, который является итоговым документом, отражающим результаты работы комиссии.

Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке.

Срок работы комиссии – не более пяти рабочих дней.

В исключительных ситуациях этот срок может быть увеличен по взаимной договоренности Сторон.

4. Стороны должны способствовать работе комиссии и не допускать отказа от предоставления необходимых документов. При необходимости Стороны обязаны предоставить комиссии возможность ознакомиться с условиями и порядком работы Системы.

5. При возникновении у Клиента претензий к Банку по поводу корректности действий, совершенных в рамках выполнения обязательств по п.п. 2.1.4 – 2.1.6 Условий, комиссия должна:

- проверить авторство предъявляемого Банком полученного им от Клиента электронного документа, в соответствии с которым совершены действия;
- проверить, что совершенные Банком действия соответствуют содержанию электронного документа.

6. При возникновении у Клиента претензий к Банку по поводу неисполнения направленных электронных платежных документов, в рамках выполнения обязательств в соответствии с п. 2.1.4 Условий, комиссия должна:

- проверить авторство предъявляемого Клиентом полученного им от Банка электронного документа, подтверждающего прием или проводку ЭПД, по которому не совершены необходимые действия;
- при необходимости проверить авторство предъявляемого Банком документа, содержащего поручение.

7. Для проверки авторства электронного документа выполняются следующие действия:

7.1. Определяется файл, содержащий электронный документ, авторство которого должно быть проверено в связи со спорной ситуацией на основе проверки корректности ЭЦП файла, содержащего оспариваемый документ.

7.2. Из электронного архива Стороны, получившей электронный документ, комиссии предъявляется файл с ЭЦП, содержащий оспариваемый электронный документ.

7.3. Сторона, получившая оспариваемый документ, предъявляет комиссии действующую на момент подписания базу сертификатов ключей подписи, либо сертификат ключа подписи, либо открытый ключ ЭЦП, переданный ей противоположной Стороной и предназначенный для проверки корректности ЭЦП файла, содержащего оспариваемый документ.

7.4. Проверяется целостность программного модуля ViewDOC.exe, предъявляемого любой из Сторон. Проверка целостности осуществляется путем вычисления значения хэш-функции и сравнения его со значением, соответствующим версии предъявленного модуля ViewDOC.exe, переданным Банком в соответствии с п. 2.1.1 Условий или опубликованным на сайте Банка.

7.5. Проверяется корректность электронной цифровой подписи файла, содержащего оспариваемый электронный документ, с помощью программного модуля ViewDOC.exe.

7.6. По требованию Стороны, открытый ключ которой предъявлен второй Стороной, может быть проверена принадлежность предъявленного открытого ключа первой Стороне. Открытый ключ признается принадлежащим первой Стороне, если открытый ключ, представленный комиссии в виде файла, соответствует открытому ключу, содержащемуся в сертификате на бумажном носителе, выданном Удостоверяющим центром в соответствии с условиями Договора.

Если предъявленный в виде файла ключ не соответствует открытому ключу, содержащемуся в сертификате на бумажном носителе, либо период действия предъявленного ключа не соответствует времени получения оспариваемого документа, то комиссия признает, что открытый ключ не был представлен Стороной, получившей оспариваемый документ.

8. Если в результате проведенной проверки корректности ЭЦП файла, содержащего оспариваемый документ, по открытому ключу ЭЦП, предъявленному Стороной, получившей оспариваемый документ, ЭЦП признана корректной, то авторство оспариваемого электронного документа признается комиссией установленным.

Если авторство оспариваемого электронного документа признано комиссией установленным и действия Стороны, к которой предъявляются претензии, соответствуют содержанию оспариваемого документа, то претензии инициатора спора признаются необоснованными.

Если авторство оспариваемого электронного документа признано комиссией установленным, а действия Стороны, к которой предъявляются претензии, не соответствуют содержанию оспариваемого документа, то претензии инициатора спора признаются обоснованными.

9. Если в результате проведенной проверки корректности ЭЦП файла, содержащего оспариваемый документ, по открытому ключу ЭЦП, предъявленному Стороной, получившей оспариваемый документ, ЭЦП признана некорректной, то предъявленный для проверки авторства электронный документ признается комиссией ложным.

Если Сторона, представившая ложный электронный документ, является инициатором спора, то претензии данной Стороны к другой Стороне признаются необоснованными.

Если Сторона, к которой предъявляются претензии, представила ложный электронный документ, то претензии к данной Стороне признаются обоснованными.

10. Претензии инициатора спора к противоположной Стороне признаются необоснованными, если инициатор спора был обязан в соответствии с п. 7.2. настоящей Процедуры предъявить, но не предъявил комиссии полученный им файл, содержащий оспариваемый документ, или не предъявил в соответствии с п. 7.3. настоящей Процедуры открытый ключ подписи противоположной Стороны.

11. С целью выяснения причин и обстоятельств возникновения спорной ситуации комиссией при необходимости проводится исследование внутренних архивов, протоколов и системных журналов рабочего места Клиента.

12. Отсутствие на клиентском рабочем месте Системы признаков отправки электронного документа, принятого Банком с корректной ЭЦП данного Клиента, не является основанием для отказа Клиента от авторства данного документа.

13. По итогам работы комиссии составляется акт, в котором в обязательном порядке отражаются:

- состав комиссии;

- действия членов комиссии;
- установленные обстоятельства;
- основания, которые послужили для формирования выводов;
- выводы, влияющие на возможность установления подлинности оспариваемого документа.

В этом случае акт признается Сторонами надлежащим.

14. В случае, если предложение о создании комиссии оставлено другой Стороной без ответа, либо Сторона отказывается от участия в комиссии или препятствует работе комиссии, а также отказывается от подписания акта, заинтересованная Сторона самостоятельно составляет акт, в котором указываются сведения о причинах его составления в одностороннем порядке. В данном акте фиксируются обстоятельства, позволяющие сделать вывод о том, что оспариваемый электронный документ является корректным, либо формулируется вывод об обратном. Указанный акт направляется другой Стороне для сведения.

При рассмотрении в суде споров о наличии документа, исполненного с помощью Системы или подписанного электронной цифровой подписью, заинтересованная Сторона обязана предоставить суду акт, составленный в соответствии с настоящей Процедурой.

15. Составленный комиссией акт является основанием для выработки Сторонами окончательного решения комиссии. Данное решение должно быть подписано Сторонами не позднее десяти дней с момента окончания работы комиссии. В случае, если решение не будет подписано в указанный срок, заинтересованная Сторона вправе обратиться в Арбитражный суд и без выработанного Сторонами решения, а в качестве доказательства представить акт, составленный в соответствии с настоящей Процедурой.

Приложение 4

к Условиям предоставления услуг с использованием системы «Клиент-Сбербанк»

Сопроводительная документация к Договору о предоставлении услуг с использованием системы «Клиент – Сбербанк»

СПЕЦИФИКАЦИЯ аппаратных и программных средств для установки АРМ «Клиент» АС «Клиент-Сбербанк»

1. Персональный компьютер x86 в следующей конфигурации:
 - Процессор x86 – Intel 486/AMD K6 и старше;
 - Видеоадаптер SVGA с разрешением 800x600 и выше;
 - Цветной дисплей (в соответствии с видеоадаптером);
 - Клавиатура со 101 клавишей, русско-латинская;
 - Оперативная память – не менее объема, рекомендуемого производителем соответствующей операционной системы;
 - Свободное пространство на накопителе на жестких магнитных дисках (НЖМД) – не менее 120 Мбайт;
 - Устройство для чтения CD-ROM дисков для инсталляции программного обеспечения;
 - Подключенный русифицированный принтер (обязательно наличие описания принтера);
 - USB порт для подключения ИЗК для доступа через Интернет.
2. Операционная система MS Windows с поддержкой русского языка:
 - при коммутiruемом доступе – MS Windows 98, NT, 2000, XP, Vista, Windows 7;
 - при доступе через Интернет – MS Windows 2000, XP, Vista, Windows 7.
3. Устройство для чтения ключевой информации. В случае хранения ключей:
 - на дискетах – дисковод накопителя на гибких магнитных дисках 3.5» емкостью 1.44 Мб;
 - на электронных идентификаторах Touch Memory – считыватель информации с Touch Memory;
 - на сменных носителях (USB флэш-диск) – USB порт.
4. Подключенное устройство для приема и передачи информации:
 - при коммутiruемом доступе – Hayes-совместимый Dialup модем (рекомендуется применять модемы ZyXEL или US Robotics)
 - при доступе через Интернет – настроенное подключение по локальной вычислительной сети или телефонное подключение через модем (Dialup, xDSL) или адаптер ISDN;
5. Телефонная коммутiruемая линия телефонной сети общего пользования при коммутiruемом доступе или при подключении к Интернет через модем.

ДОВЕРЕННОСТЬ № _____

г. _____

« _____ » _____ 20__ г.

(полное наименование юридического лица в соответствии с Уставом, Положением)

в лице _____,
(должность, фамилия, имя, отчество уполномоченного лица - полностью)

действующего(-ей) на основании _____,
(Устава, Положения, Доверенности⁴)

уполномочивает _____,
(Фамилия, имя, отчество лица, которому выдается доверенность)

(документ, удостоверяющий личность доверенного лица: номер (серия) документа, каким органом и когда выдан)

распоряжаться денежными средствами по расчетным счетам, указанным в Приложении 1 к Договору о предоставлении услуг с использованием системы «Клиент-Сбербанк» № _____, заключенного « _____ » _____ 20__ г. между _____ и _____ ОАО «Сбербанк России» (далее по тексту –

(наименование юридического лица) (наименование подразделения)

Договор), и наделяет его правом _____ подписи.

(первой/второй)

_____, имеет право совершать от имени _____
(фамилия, инициалы уполномоченного лица) (полное наименование юридического лица)

все необходимые действия по распоряжению денежными средствами на счетах, указанных в Приложении 1 к Договору о предоставлении услуг с использованием системы «Клиент-Сбербанк» № _____ от « _____ » _____ 20__ г., предусмотренные законодательством Российской Федерации, банковскими правилами и соответствующими договорами банковского счета.

_____, имеет право подписывать от имени _____
(фамилия, инициалы уполномоченного лица) (полное наименование юридического лица)

все предусмотренные законодательством Российской Федерации, банковскими правилами и договорами банковских счетов расчетные и кассовые документы в качестве лица, наделенного правом _____ подписи,
(первой/второй)

в том числе, используя электронную цифровую подпись.

Образец подписи _____ удостоверяю.
(подпись) (фамилия, инициалы уполномоченного лица)

Настоящая доверенность действует с « _____ » _____ 20__ г. по « _____ » _____ 20__ г. включительно.

(подпись) / _____ /
(расшифровка подписи должность лица, выдавшего доверенность)

М.П.

⁴ В соответствии с п.3 ст.187 Гражданского кодекса Российской Федерации Доверенность, выдаваемая в порядке передоверия, т.е. лицом, действующим на основании доверенности, должна быть нотариально удостоверена.

ДОВЕРЕННОСТЬ № ____

г. _____

« ____ » _____ 20 ____ г.

(полное наименование юридического лица в соответствии с Уставом, Положением)

в лице _____,
(должность, фамилия, имя, отчество уполномоченного лица - полностью)

действующего(-ей) на основании _____,
(Устава, Положения, Доверенности⁵)

доверяет _____
(Фамилия, имя, отчество лица, которому выдается доверенность)

(документ, удостоверяющий личность доверенного лица: номер (серия) документа, каким органом и когда выдан)

совершать все юридические действия, связанные с получением, проверкой и обменом в

(наименование подразделения ОАО «Сбербанк России»)

ОАО «Сбербанк России» программного обеспечения системы «Клиент-Сбербанк», ключей шифрования, открытых ключей Банка, инструкций по установке и безопасности в соответствии с п.2.1.1 Договора о предоставлении услуг с использованием системы «Клиент-Сбербанк» № _____ от « ____ » _____ 20 ____ г. в том числе подписывать Акт приема-передачи программного обеспечения и средств защиты автоматизированной системы «Клиент-Сбербанк» и другие документы.

Образец подписи _____
(подпись)

_____ удостоверяю.
(Фамилия, имя, отчество лица, которому выдается доверенность)

Настоящая доверенность действует по « ____ » _____ 20 ____ г. включительно.

(подпись) / _____ /
(расшифровка подписи должность лица, выдавшего доверенность)

М.П.

⁵ В соответствии с п.3 ст.187 Гражданского кодекса Российской Федерации Доверенность, выдаваемая в порядке передоверия, т.е. лицом, действующим на основании доверенности, должна быть нотариально удостоверена.

Акт приема-передачи программного обеспечения и средств защиты автоматизированной системы «Клиент-Сбербанк»

г. _____ «__» _____ 20__ г.

(наименование подразделения ОАО «Сбербанк России»)

именуем __ в дальнейшем «Банк», в лице _____
(должность, ф.и.о. полностью)

действующего на основании _____, с одной стороны, и

(наименование организации)

именуем __ в дальнейшем «Клиент», в лице _____
(должность, ф.и.о. полностью)

действующего на основании _____, с другой стороны, совместно именуемые «Стороны», составили настоящий Акт в том, что «__» _____ 20__ г. в соответствии с Договором о предоставлении услуг с использованием системы «Клиент-Сбербанк» № _____ от «__» _____ 20__ г. Банк передал, а Клиент принял Дистрибутивный комплект № _____ в составе:

№ п/п	Наименование	Кол-во
1.	<p><i>Магнитооптический носитель (компакт-диск)*:</i></p> <ul style="list-style-type: none"> • Программное обеспечение Рабочее место «Клиент» со встроенным программным средством криптографической защиты информации • Инструкция по установке Рабочего места «Клиент» • Руководство пользователя Рабочего места «Клиент» • Руководство Администратора Рабочего места «Клиент» • Руководство по установке и эксплуатации комплекса ФПСУ-IP/Клиент при подключении к автоматизированным системам Сбербанка России через сеть Интернет • Открытый(-ые) ключ(-и) ЭЦП Банка и сертификат(-ы) ключей ЭЦП Банка • Сопроводительная документация, в том числе с шаблонами документов, создаваемых в процессе установки и эксплуатации Системы и Результатами вычисления значений хеш-функции для модуля ViewDOC (по ГОСТ Р34.11-94) • Файл формата Abode PDF «Сертификат соответствия на СКЗИ «Бикрипт-КСБ-С» (Windows) №СФ/124-1522 от 15.08.2010 г., №СФ/124-1524 от 15.08.2010 г.» • Файл формата Abode PDF «Средство криптографической защиты информации «Бикрипт-КСБ-С». Формуляр. ИНФК.11485466.4012.009.30 • Файл формата Abode PDF «Средство криптографической защиты информации «Бикрипт-КСБ-С». Правила пользования. ИНФК.11485466.4012.009.31» 	1 компакт диск
2.	Ключ шифрования номер _____ на носителе (при необходимости)	1 шт.
3.	Параметры дистрибутивного комплекта на бумажном носителе	1 лист
4.	Идентификатор для записи ключей VPN-сети Сбербанка России ** (ИЗК) серийный номер _____ и конверт с PIN-кодами к нему	1 шт.

Стороны претензий друг к другу не имеют.

От Банка

От Клиента

_____/_____/_____

_____/_____/_____

М.П.

* содержимое носителя может предоставляться Клиенту, использующему канал связи интернет, через сайт Банка

** Включается в дистрибутивный комплект, в случае использования канала связи интернет

ЗАЯВКА на проведение работ
по Договору о предоставлении услуг с использованием системы «Клиент-Сбербанк»
 № _____ от «__» _____ 20__ г.

Настоящим _____,

(полное наименование организации, учреждения, предприятия)

просит произвести _____
(установку, переустановку, настройку АРМ «Клиент», первичный инструктаж и т.п.)

по адресу: _____

Ответственный исполнитель: _____

Контактный телефон: _____

Организация располагает следующими аппаратно-программными средствами⁶:

Персональный компьютер в следующей конфигурации:

- процессор _____;
- цветной дисплей с адаптером SVGA и выше;
- устройство для чтения CD ROM дисков;
- клавиатура со 101 клавишей, русско-латинская;
- оперативная память _____;
- накопитель на жестких магнитных дисках (НЖМД) _____;
- порт для подключения принтера;
- USB порт для подключения ИЗК;
- порт для подключения устройства для приема и передачи информации (модема и т.д.).

Под управлением операционной системы _____ с поддержкой русского языка.

Русифицированный принтер _____;

Модем Hayes-совместимый _____;

Телефонная коммутируемая линия телефонной сети общего пользования или выделенная линия для подключения к Интернет: номер телефона _____, IP адрес подключения _____.

_____/_____/_____
 подпись / ФИО, должность

«__» _____ 20__ г.

М.П.

АКТ о проведении работ по Заявке

Работы по Заявке выполнены

- † в полном объеме в согласованные с Клиентом сроки;
- † не выполнены, в связи с отсутствием технической возможности;
- † не выполнены, в связи с _____;
указать причину

_____.

От Клиента

_____/_____/_____
 подпись / должность / ФИО

«__» _____ 20__ г.

М. П.

⁶ Вместо информации о конфигурации рабочей станции допускается указывать фразу: "Аппаратно-программные средства соответствуют требованиям, указанным в сопроводительной документации для установки АРМ «Клиент»"

ЗАЯВЛЕНИЕ об использовании кодового слова при эксплуатации АС «Клиент-Сбербанк»

к Договору о предоставлении услуг с использованием системы «Клиент-Сбербанк» № _____ от «___»
_____ 20__ г.

Настоящим _____,

(полное наименование организации, учреждения, предприятия)

просит использовать приведенное ниже кодовое слово при дальнейшей эксплуатации автоматизированной системы «Клиент-Сбербанк».

Кодовое слово:

--	--	--	--	--	--	--	--	--	--	--	--

(заполняется прописными печатными буквами русского алфавита и цифрами)

Сотрудники, уполномоченные использовать кодовое слово, проинструктированы о правилах его использования.

Дата заполнения: _____

от Клиента

(должность руководителя)

_____ (_____)

(подпись, Ф.И.О. руководителя)

М.П.

АКТ готовности к эксплуатации автоматизированной системы «Клиент-Сбербанк»

Открытое акционерное общество «Сбербанк России», именуемый в дальнейшем Банк, в лице _____ и _____, именуем _____ в дальнейшем Клиент, в лице _____, совместно именуемые стороны, в соответствии с условиями «Договора о предоставлении услуг с использованием системы «Клиент-Сбербанк»» № _____ от «___» _____ 20__ г. (далее Договор) составили настоящий Акт о нижеследующем:

1. Клиент использует для работы с Банком собственные аппаратные и общесистемные программные средства (компьютер, модем, операционная система, вспомогательные программы).
2. Установку программных средств, переданных Банком во временное пользование на период действия Договора, на аппаратных средствах Клиента выполнил __ (Клиент или Банк или Аутсорсинговая компания)__. Комплектность и содержание установленных программных средств, а также используемого вместе с ним вспомогательного программного обеспечения Клиента закреплено путем вычисления хэш-функции средствами Системы.
3. Банк предоставил Клиенту документацию на АРМ «Клиент» и инструкции, достаточные для работы Клиента в соответствии с Договором, включая обеспечение информационной безопасности. Перечень документации по Договору приведен в Акте приема-передачи программного обеспечения и средств защиты автоматизированной системы «Клиент-Сбербанк» от «___» _____ 20__ г.
4. Руководство Клиента и лица, осуществляющие эксплуатацию рабочего места «Клиент», с требованиями по обеспечению безопасности при эксплуатации рабочего места «Клиент» ознакомились.
5. Руководство Клиента назначило сотрудника (сотрудников), в чьи функции входит организация и контроль выполнения требований по обеспечению безопасности в процессе эксплуатации рабочего места «Клиент», а также взаимодействие со Службой безопасности Банка.
6. Руководство Клиента назначило лиц, уполномоченных от имени Клиента подписывать ЭЦП электронные документы. Генерация закрытых ключей ЭЦП уполномоченных лиц Клиента осуществлена на (дискеты/электронные идентификаторы Touch Memory/ сменные носители (USB флэш-диск)). Ключам ЭЦП присвоен идентификатор в соответствии с установленным Удостоверяющим центром форматом.
7. Передаваемые Клиентом в Банк электронные документы будут заверяться __ (одной, двумя) __ ЭЦП. Передаваемые Банком электронные документы будут заверяться одной ЭЦП.
8. Вычисленные значения хэш-функции и открытые ключи ЭЦП переданы Банку в виде распечаток на бумажных носителях и направлены в виде электронных файлов по Системе.
9. Работоспособность рабочего места «Клиент» проверена. Рабочее место «Клиент» системы «Клиент-Сбербанк» готово к эксплуатации. Стороны не имеют взаимных претензий по факту выполненных работ.

От Банка:

От Клиента:

(должность руководителя)

(должность руководителя)

(подпись, Ф.И.О. руководителя)

(подпись, Ф.И.О. руководителя)

М.П.

М.П.

«___» _____ 20__ г.

«___» _____ 20__ г.

Заявление на приостановление/возобновление обслуживания в Системе

НАИМЕНОВАНИЕ КЛИЕНТА				
ДОГОВОР О ПРЕДОСТАВЛЕНИИ УСЛУГ С ИСПОЛЬЗОВАНИЕМ АС «КЛИЕНТ-СБЕРБАНК»	от		№	

1. ПРИОСТАНОВЛЕНИЕ ОБСЛУЖИВАНИЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ:

<input type="checkbox"/>	просим приостановить обслуживание с использованием Системы
ДАТА ПРИОСТАНОВЛЕНИЯ ОБСЛУЖИВАНИЯ	

2. ВОЗОБНОВЛЕНИЕ ОБСЛУЖИВАНИЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ:

<input type="checkbox"/>	просим возобновить обслуживание с использованием Системы
ДАТА ВОЗОБНОВЛЕНИЯ ОБСЛУЖИВАНИЯ	

_____ / _____
 подпись / ФИО, должность
 М.П.
 «__» _____ 20__ г.

**РЕЗУЛЬТАТЫ вычисления значений хэш-функции для модуля ViewDOC
(по ГОСТ Р 34.11-94)**

При вычислении значений хэш-функции использованы следующие параметры алгоритма:

1. Заполнение узлов замены

```
char uz[4][16]=  
{  
{0xA5,0x74,0x77,0xD1,0x4F,0xFA,0x66,0xE3,0x54,0xC7,0x42,0x4A,0x60,0xEC,0xB4,0x19},  
{0x82,0x90,0x9D,0x75,0x1D,0x4F,0xC9,0x0B,0x3B,0x12,0x2F,0x54,0x79,0x08,0xA0,0xAF},  
{0xD1,0x3E,0x1A,0x38,0xC7,0xB1,0x81,0xC6,0xE6,0x56,0x05,0x87,0x03,0x25,0xEB,0xFE},  
{0x9C,0x6D,0xF8,0x6D,0x2E,0xAB,0xDE,0x20,0xBA,0x89,0x3C,0x92,0xF8,0xD3,0x53,0xBC}  
};
```

2. Начальный вектор хэширования

```
char iv[2][16]=  
{  
{0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0},  
{0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0}  
};
```

Результаты вычисления:

bcry32.dll

impborl.dll

viewdoc.exe

От Банка

_____/_____
м.п.

От Клиента

_____/_____
м.п.

ТРЕБОВАНИЯ
по обеспечению безопасности в процессе эксплуатации АРМ «Клиент»

Согласно Сертификатам соответствия (№СФ/124-1522 и №СФ/124-1524 от 15.08.2010 г., формуляр ИНФК.11485466.4012.009.30) СКЗИ «Бикрипт-КСБ-С» удовлетворяет требованиям к стойкости СКЗИ класса КС1, а при использовании на ПЭВМ сертифицированного средства защиты от НСД ПАК «Аккорд/АМДЗ» - класса КС2.

Необходимый уровень защищенности АРМ «Клиент» (соответствие классу КС1 или классу КС2) определяется Клиентом самостоятельно.

Со стороны Банка уровень защиты банковской части системы обеспечивается по классу КС2. Клиентам рекомендуется обеспечивать тот же уровень для защиты АРМ «Клиент».

Эксплуатация АРМ «Клиент» и обеспечение его безопасности организационными и техническими мерами должны осуществляться в соответствии с Правилами пользования СКЗИ «Бикрипт-КСБ-С» (ИНФК.11485466.4012.009.31).

Распоряжением руководителя Клиента должны быть назначены работники, в чьи функции входит организация и контроль выполнения требований по обеспечению безопасности в процессе эксплуатации Рабочего места «Клиент», а также взаимодействие со Службой безопасности ОАО «Сбербанк России».

При генерации уполномоченными лицами Клиента ключей ЭЦП формат идентификатора ключа должен соответствовать рекомендациям, изложенным в Правилах изготовления и сертификации ключей ЭЦП Клиента.

При организации доступа в Банк по сети Интернет хранение и использование носителей ключей VPN сети (ИЗК) должно производиться аналогично порядку, предусмотренному в Правилах пользования для ключей шифрования СКЗИ «Бикрипт-КСБ-С».

ПРАВИЛА ИЗГОТОВЛЕНИЯ И СЕРТИФИКАЦИИ КЛЮЧЕЙ ЭЦП КЛИЕНТА

1. Изготовление ключей ЭЦП

1.1. Ключи ЭЦП изготавливаются их владельцами самостоятельно с помощью соответствующей функции АРМ «Клиент».

1.2. Идентификатор ЭЦП не может содержать более 32 символов (вкл. пробелы) и должен соответствовать формату:

YYYYNNNNsФИО должность

где **YYYY** – уникальный четырехразрядный буквенно-цифровой код Клиента, присваиваемый автоматизированной системой корневого Удостоверяющего центра (код Удостоверяющего центра, КУЦ)⁷; **NNNN** – уникальный (для каждого ключа ЭЦП данного Клиента, включая случаи регенерации ключа) четырехразрядный порядковый номер ключа ЭЦП; **s** – признак принадлежности ключа ЭЦП организации, являющейся Клиентом ОАО «Сбербанк России»; **ФИО** (фамилия и инициалы) – обязательный параметр; **должность** – узнаваемое сокращение должности владельца ЭЦП и названия фирмы, в случае отсутствия свободных разрядов должность и название фирмы допускается не указывать.

1.3. Во избежание технических осложнений не следует использовать в идентификаторе ЭЦП более одного пробела подряд, специальных символов, точек, кавычек и т.п.

Пример: A9G40001sПетровИА ГенДир КБСалют

A9G40002sСидороваАИ ГлБухКБСалют

1.4. Для подтверждения принадлежности изготовленных ключей ЭЦП уполномоченным лицам Клиента необходимо, в трех экземплярах для каждого открытого ключа ЭЦП, оформить и заверить рукописной подписью владельца сертификата ключа подписи, руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг, и оттиском печати Клиента распечатку проекта сертификата ключа подписи.

1.5. Распечатка проекта сертификата ключа подписи создаваемая средствами АРМ «Клиент» должна включать в себя:

- Полное наименование организации Клиента
- Фамилию, имя и отчество уполномоченного лица Клиента (Владельца сертификата ключа подписи)
- Занимаемую должность уполномоченного лица в штатной структуре Клиента
- Шестнадцатеричное представление открытого ключа ЭЦП уполномоченного лица Клиента
- Идентификатор ключа ЭЦП
- Сведения о средствах ЭЦП
- Рукописную подпись Владельца сертификата ключа подписи
- Рукописную подпись руководителя или лица, наделенного правом подписывать Договор(ы) финансово-банковских услуг, и оттиск печати Клиента

⁷ КУЦ указан в информационном листе с параметрами дистрибутивного комплекта, переданным по Акту приема-передачи; в АРМ «Клиент» КУЦ известен и автоматически используется при создании идентификатора ЭЦП

Пример:

**УЦ ОАО «Сбербанк России»
Сертификат ключа электронной цифровой подписи
Владелец сертификата ключа электронной цифровой подписи**

Фамилия, имя и отчество: Сидорова Алла Игнатьевна

Должность: Главный бухгалтер

Организация: АО «Салютик-ТМ»

Дата начала действия ключа*: _____

Дата окончания действия ключа *: _____

* - заполняется работником УЦ

Открытый ключ

12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78
12 34 56 78 12 34 56 78 12 34 56 78 12 34 56 78

Идентификатор: A9G40002sСидороваАИ ГлБухАОСалют

Область действия сертификата ключа подписи

Электронный документооборот по системе «Клиент-Сбербанк» ОАО «Сбербанк России» в соответствии с договором о предоставлении услуг с использованием системы «Клиент-Сбербанк»

Сведения о средствах электронной цифровой подписи

Средство криптографической защиты информации «Бикрипт-КСБ-С»

Разработчик – ООО Фирма «ИнфоКрипт»

Алгоритм ЭЦП: ГОСТ Р 34.10-2001 Хэш-функция: ГОСТ Р 34.11-94

Подпись владельца

Подпись и полномочия Сидоровой

Сертификата ключа подписи

Аллы Игнатьевны
(ФИО владельца ключа)
удостоверяю:

Уполномоченное лицо
удостоверяющего центра

(М.П.)

Руководитель клиента

(М.П.)

2. Сертификация и регистрация ключей ЭЦП

2.1. Для сертификации ключей ЭЦП следует передать по Системе файлы с открытыми ключами ЭЦП Клиента⁸, а заверенные распечатки сертификатов ключей подписей на бумажном носителе в функциональное подразделение ОАО «Сбербанк России», заключившее с Клиентом Договор о предоставлении услуг с использованием автоматизированных систем дистанционного обслуживания.

2.2. Функциональное подразделение ОАО «Сбербанк России» проверяет полномочия Владельцев сертификатов ключей подписи, оформление проектов сертификатов, соответствие подписей и оттиска печати и передает распечатки проектов сертификатов ключей подписи Клиента в УЦ в соответствии с внутренними правилами, установленными в банке.

2.3. Ключи ЭЦП Клиента вступают в силу после изготовления УЦ сертификата ключа подписи на основе открытого ключа ЭЦП Клиента и регистрации их в соответствующей криптосети ОАО «Сбербанк России».

2.4. Возможность использования новых ключей ЭЦП подтверждается получением сертификата ключа подписи на бумажном носителе или получением через функциональное подразделение соответствующего уведомления (по телефону, электронной почте или другими доступными способами).

2.5. Сертификаты ключей подписей Клиента с подписью уполномоченного лица и оттиском печати Удостоверяющего центра, передаются Клиенту через функциональное подразделение, заключившее с ним договор о предоставлении услуг с использованием автоматизированных систем дистанционного обслуживания.

3. Замена ключей ЭЦП

3.1. Срок действия ключей ЭЦП определен сертификатом Удостоверяющего центра и не может превышать одного года и трех месяцев. По истечении этого срока ключи ЭЦП подлежат замене. Для обеспечения непрерывности работы процедуру замены ключей ЭЦП следует проводить заблаговременно. По истечению срока действия ключи и соответствующие им электронные сертификаты ключей подписи автоматически блокируются в Системе. Банк не несет ответственности за несвоевременную смену ключей ЭЦП Клиентами.

3.2. Процедура замены ключей ЭЦП включает в себя все операции, изложенные в первых двух разделах настоящего документа.

⁸ При создании ЭЦП в АРМ «Клиент» файл автоматически формируется и направляется в Банк при очередном сеансе связи после создания ЭЦП