



СБЕРБАНК РОССИИ

Основан в 1841 году

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «СБЕРБАНК РОССИИ»

*Условия предоставления услуг с использованием системы дистанционного банковского обслуживания
ОАО «Сбербанк России» юридическим лицам, индивидуальным предпринимателям и физическим лицам,
занимающимся частной практикой в порядке, установленном законодательством Российской Федерации*

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины «Электронная подпись» (ЭП), «Ключ электронной подписи», «Ключ проверки электронной подписи», «Сертификат ключа проверки электронной подписи», «Владелец сертификата ключа проверки электронной подписи» («Владелец сертификата»), «Удостоверяющий центр» (УЦ) применяются в настоящем Договоре в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

Авторство электронных документов (Авторство ЭД) - принадлежность ЭД создавшей его Стороне.

Аналог собственноручной подписи (АСП) – значение Хэш-функции, вычисленное по всем реквизитам электронного документа (номер лицевого счета, номер телефона, номер обязательства и т.д.), паролю, введенному Клиентом при входе в Систему, и одноразовому паролю, подтверждающему реквизиты получателя средств и/или реквизиты плательщика, если он использовался при совершении операции.

Банк – Открытое акционерное общество «Сбербанк России», ОАО «Сбербанк России».

Браузер – программное обеспечение для просмотра веб-сайтов, для запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой.

Бюджет (строки бюджета) – набор аналитических признаков (строк), выделенный Головной компанией по счетам Клиента с указанием следующих параметров:

- лимит/отсутствие лимита;
- период планирования.

Владелец сертификата ключа шифрования – уполномоченный работник Клиента, на имя которого УЦ выдан Сертификат ключа шифрования и который владеет соответствующей закрытой компонентой Ключа шифрования.

Головная компания – Клиент или иное юридическое лицо/ индивидуальный предприниматель или физическое лицо, занимающееся частной практикой в порядке, установленном законодательством Российской Федерации, которое осуществляет функции контроля движения денежных средств по открытым в Банке счетам Клиента, в соответствии данным в договоре банковского счета поручением Клиента Банку.

Дистрибутивный комплект – инициализированный Электронный ключ и комплект программных и аппаратных средств для установки Рабочего места «Клиент».

Документы, связанные с проведением валютных операций:

- документы, являющиеся основанием для проведения валютных операций, включая договоры (соглашения, контракты) и дополнения и (или) изменения к ним;
- документы, подтверждающие факт передачи товаров (выполнения работ, оказания услуг), информации и результатов интеллектуальной деятельности, в том числе исключительных прав на них;
- таможенные декларации, документы, подтверждающие ввоз в РФ и вывоз из РФ товаров;
- уведомление налогового органа об открытии счета (вклада) в банке за пределами территории РФ;
- паспорт сделки.

Договор – совокупность следующих документов: «Условия предоставления услуг с использованием системы дистанционного банковского обслуживания ОАО «Сбербанк России» юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся частной практикой в порядке, установленном законодательством Российской Федерации» и «Заявление на заключение договора о предоставлении услуг с использованием дистанционного банковского обслуживания ОАО «Сбербанк России».

Заявление на заключение договора - Заявление на заключение договора о предоставлении услуг с использованием дистанционного банковского обслуживания ОАО «Сбербанк России», являющееся акцептом предложенной Банком оферты на заключение Договора.

Идентификатор – логин, являющийся именем Представителя Клиента в Системе.

Клиент - Юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся частной практикой в порядке, установленном действующим законодательством Российской Федерации, заключившее с Банком Договор о предоставлении услуг с использованием Системы.

Ключи шифрования - ключи, самостоятельно изготавливаемые участниками Системы с использованием средств Системы и предназначенные для обеспечения конфиденциальности ЭД участников Системы при их передаче по сети Интернет путем шифрования. Ключ шифрования состоит из уникальных однозначно взаимосвязанных открытой и закрытой компонент.

Корректная ЭП – электронная подпись, дающая положительный результат ее проверки соответствующим сертифицированным средством ЭП, с использованием действующего на момент подписания ключа проверки ЭП его Владельца.

Мобильное приложение Сбербанк Бизнес Онлайн (мобильное приложение) – один из каналов отправки ЭД в банк, требующий установки специализированного программного обеспечения на мобильное устройство Клиента

Мобильное устройство - переносное мобильное устройство Клиента, такое как смартфон или планшетный компьютер на базе операционных систем iOS или Android

Ответственное лицо – сотрудник Банка, имеющий право совершать от имени уполномоченного банка ОАО «Сбербанк России» как агента валютного контроля действия по валютному контролю, предусмотренные нормативно-правовыми актами валютного законодательства РФ (далее – НПА ВЗ).

Подпись Ответственного лица – паспорта сделок (далее – ПС), ведомости банковского контроля (далее – ВБК), справки о валютных операциях (далее – СВО) и справки о подтверждающих документах (далее – СПД) (файлы с ПС, ВБК, СВО и СПД), направляемые банком Клиенту в соответствии с НПА ВЗ и настоящим документом, имеют в электронном виде аналог собственноручной подписи (далее – АСП) Ответственного лица, формируемый и применяемый на основании полномочий Ответственного лица и в соответствии с правилами, установленными Банком.

Факт проставления АСП Ответственного лица подтверждается проставлением Ф.И.О. Ответственного лица в печатных формах ПС, ВБК, СВО и СПД и именах вложенных файлов.

Рабочее место «Клиент» - составная часть Системы, устанавливаемая на стороне Клиента при выборе им в качестве канала доступа «Сбербанк Бизнес».

«Сбербанк Бизнес» – один из каналов отправки ЭД в банк, требующий локальной установки специализированного программного обеспечения на рабочее место Клиента.

«Сбербанк Бизнес Онлайн» – один из каналов отправки ЭД в банк, не требующий установки специализированного программного обеспечения на рабочее место Клиента, работа Клиента в Системе производится по средствам браузера

«Сбербанк Интеграция» – один из каналов отправки ЭД в банк, требующий разработки специализированного программного обеспечения для рабочего места Клиента, собственными силами клиента в соответствии с «Соглашением о форматах Сбербанк Интеграция (API)».

«Соглашение о форматах Сбербанк Интеграция (API)» – описание набора сервисов и форматов их вызова, размещенные на официальном сайте Банка.

Сертификаты ключей – Сертификат ключа проверки ЭП и Сертификат ключа шифрования

Сертификат ключа шифрования – документ на бумажном носителе, который содержит открытую компоненту ключа шифрования, и который выдается УЦ участнику Системы для идентификации Владельца сертификата ключа шифрования.

Сервис «Отчетность» - сервис обмена ЮЗЭД с налоговыми органами.

Система – совокупность систем дистанционного банковского обслуживания, «Сбербанк Бизнес Онлайн» или «Сбербанк Бизнес», «Сбербанк Интеграция». Системы электронного документооборота (прием/передача электронных документов) между Банком и Клиентами, предоставляющие Клиентам возможность по удаленному управлению банковскими счетами, а также получения банковских услуг через сеть Интернет.

Стороны – стороны по договору присоединения: Банк - с одной стороны, Клиент – с другой стороны.

Сомнительная операция – операция, имеющая признаки, свидетельствующие о возможном осуществлении легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

Тарифный план – набор банковских услуг, предоставляемых Клиенту в течение календарного месяца в пределах установленного лимита за определенную плату.

Тарифы – установленная Банком цена банковской услуги для Клиентов.

Уполномоченное лицо Клиента – работник Клиента, уполномоченный распоряжаться денежными средствами, находящимися на счете, и совершать иные действия, предусмотренные разделом 3 Условий, используя АСП/ЭП, а также работник Клиента, наделенный полномочиями по подготовке документов в Системе.

Услуга «E-invoicing» – сервис межкорпоративного электронного документооборота (прием/передача электронных документов), предоставляющий Клиентам Банка возможность обмениваться ЮЗЭД с третьими лицами.

Условия – Условия предоставления услуг с использованием системы дистанционного банковского обслуживания ОАО «Сбербанк России» юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся частной практикой в порядке, установленном законодательством Российской Федерации.

Участник Системы – Представитель Клиента, использующий ЭП.

Хэш-функция – однонаправленное отображение (свертка) содержимого файла или блока данных произвольного размера в блок данных фиксированного размера, обладающее заданными математическими свойствами; используется при формировании ЭП и аналога собственноручной подписи.

Электронный документ (ЭД) – электронный образ документа (платежного или иного), представленный в согласованном Сторонами формате, определяемом программными средствами создания документа.

Электронный документ валютного контроля (ЭД ВК) – документ, используемый для целей валютного контроля и:

- представляемый Клиентом в Банк
 - в виде заполненной формы, предоставляемой системой (ПС, СВО, СПД, Заявление о переоформлении паспорта сделки, Заявление о закрытии паспорта сделки);
 - в виде полученного с использованием сканирующих устройств изображений документа, оформленного первоначально на бумажном носителе (документы, необходимые для оформления/переоформления/закрытия/перевода на обслуживание ПС; документы, связанные с проведением валютных операций; подтверждающие документы; ПС и ВБК другого банка, необходимые для перевода ПС на обслуживание из другого банка; иные документы, установленные НПА ВЗ);

- в электронном виде в формате XML (XML-файлы ПС и ВБК другого банка, необходимые для перевода ПС на обслуживание из другого банка);
- в виде документа, сформированного в электронном виде (информация, связанная с проведением валютных операций и с представляемыми в Банк ЭД ВК);
- направляемый Банком Клиенту
 - в виде реквизитов, проставляемых в ЭД ВК, аналогичных реквизитам, проставляемым Банком на бумажном носителе;
 - в электронном виде в графическом формате;
 - в электронном виде в формате XML (XML-файлы ПС и ВБК, необходимые для перевода ПС на обслуживание в другой банк).

Электронный ключ – программно-аппаратное средство Электронный идентификатор Клиента на базе «VPN-key-TLS», используемое в Системе для генерации ключей ЭП, ключей шифрования, формирования и проверки ЭП, шифрования и подключения к защищенной корпоративной VPN-сети ОАО «Сбербанк России». Используется в вариантах стандартном, с сенсором и с экраном. Вариант с сенсором предусматривает использование сенсорной площадки для подтверждения факта подписания ЭП электронных документов. Вариант с экраном предусматривает использование сенсорного экрана для отображения подписываемых электронных документов и подтверждения подписания ЭП электронных документов¹. Электронный ключ реализует алгоритмы в соответствии с ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи", ГОСТ Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хэширования" и ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Электронный платежный документ (ЭПД) – электронный документ (платежное поручение Клиента в электронном виде), являющийся основанием для совершения Банком операций по банковскому счету Клиента. ЭПД, защищенные корректным АСП/ЭП, в соответствии с законодательством Российской Федерации имеют равную юридическую силу с расчетными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

Электронный реестр – список физических лиц в виде электронного файла, внутренний формат (содержание) которого соответствует требованиям, определенным специальным(ыми) договором(ами), заключенным(ыми) Сторонами. Электронный реестр является специальным типом документа в Системе и подписывается АСП/ЭП средствами Системы.

Юридически значимый ЭД (ЮЗЭД) – ЭД, защищенный корректным АСП/ЭП, в соответствии с законодательством Российской Федерации и положениями настоящих условий имеют равную юридическую силу с документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

IMSI (International Mobile Subscriber Identity) – международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи GSM, UMTS или CDMA. При регистрации в сети аппарат абонента передает IMSI, по которому происходит его идентификация.

Fraud-операция – вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомерное использование ресурсами и услугами.

PIN-код – пароль, необходимый для получения доступа к функциям Электронного ключа.

2. ОБЩИЕ ПОЛОЖЕНИЯ

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

2.2. Заключение Договора между Банком и Клиентом 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.

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

2.4. Фактом заключения Договора является подача Клиентом в Банк Заявления на заключение договора.

2.5. Клиент может начать работу в Системе с момента передачи Банком (посредством SMS-сообщений) Уполномоченным лицам Клиента на телефонные номера, указанные в Заявлении на заключение договора, уведомления, содержащего первоначальный пароль.

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

2.7. Банк предоставляет Клиенту следующие услуги с использованием Системы, в том числе услуги на платной основе, предусмотренные Тарифами:

- прием от Клиента ЭПД, на выполнение операций по счетам Клиента;
- предоставление Клиенту в ЭД информации об операциях, совершенных по счетам Клиента;
- прием от Клиента и предоставление Клиенту ЭД в соответствии с условиями отдельных заключенных Сторонами договоров, которые предусматривают электронный документооборот с использованием Системы;
- обмен между Клиентом и Банком в электронном виде документами и информацией, связанными с проведением валютных операций, требование о представлении (направлении) которых предусмотрено действующими НПА ВЗ);

¹ Вариант VPNKey-TLS с экраном доступен и предлагается клиентам после соответствующей доработки Системы.

- прием от Клиента и предоставление Клиенту информации свободного формата в виде ЭД;
- прием от Клиента информации для формирования ЭД по заданным Клиентом шаблонам (при этом для снижения рисков Банк имеет право по своему усмотрению устанавливать ограничения на ЭД, формируемые таким образом, например, на сумму) и предоставление Клиенту информации посредством SMS-сообщений (SMS-банкинг);
- заключение Договоров/Соглашений средствами Системы в рамках реализованных электронных форм заявлений, прием Банком в обработку подписанных АСП/ЭП заявлений от Клиента;
- осуществление обмена (отправки/получения) ЮЗЭД с третьими лицами и непосредственно с Банком и использование сервиса «Отчетность».

2.8. ЭД передаются и принимаются Сторонами с использованием Системы без их последующего представления на бумажном носителе.

ЭД ВК представляются Клиентом в Банк с использованием Системы без их последующего представления на бумажном носителе. ЭД ВК направляются Банком Клиенту с использованием Системы без последующего направления документов на бумажном носителе.

2.9. Совокупный размер вложенных файлов, направляемых по Системе, в т.ч. архивных, не должен превышать размера, установленного в Системе.

2.10. С использованием электронного документооборота в рамках настоящих Условий существующий между Сторонами документооборот с использованием бумажных носителей не утрачивает силу.

2.11. Для снижения рисков, связанных с работой в сети Интернет, Банк может:

2.11.1. установить Уполномоченным лицам Клиента признак, обеспечивающий их вход в Систему после ввода дополнительного одноразового пароля, направляемого Банком на мобильные телефоны Уполномоченных лиц Клиента.

2.11.2. при использовании электронного ключа запрашивать подтверждение авторства некоторых электронных документов по альтернативному каналу (с использованием одноразовых паролей, передаваемых посредством SMS-сообщений, и/или звонка из Банка по телефонному номеру Уполномоченного лица клиента).

2.11.3. при использовании электронного ключа, включить режим работы системы с одноразовым подтверждением контрагентов по альтернативному каналу связи. Записи в справочнике контрагентов подтверждаются с использованием одноразовых паролей, передаваемых посредством SMS-сообщений, содержащих основные банковские реквизиты контрагентов.

2.11.4. включить контроль изменения индивидуального номера абонента сим-карты (IMSI) Клиента, в случае если телефонный провайдер поддерживает контроль IMSI сим-карты абонента. При включенном режиме проверки, в случае замены сим-карты Клиента, необходимо информировать банк установленным порядком, путем подачи соответствующего заявления.

2.12. При подаче Заявления на заключение договора и выборе системы «Сбербанк Бизнес Онлайн», Клиент может выбрать для каждого из своих Уполномоченных лиц один из следующих вариантов защиты данных:

2.12.1. с использованием одноразовых паролей, передаваемых посредством SMS-сообщений. При каждом подписании документа в Системе, Система запрашивает одноразовый пароль, который Уполномоченное лицо Клиента получает на мобильный телефон посредством SMS-сообщения.

2.12.2. с использованием ЭП, формируемой Электронным ключом. Клиент имеет возможность изменить для Уполномоченного лица вариант защиты путем подачи соответствующим образом заполненного Заявления.

2.13. При подаче Заявления на заключение договора и выборе системы «Сбербанк Бизнес», для каждого из своих Уполномоченных лиц Клиент использует вариант защиты данных с ЭП, формируемой Электронным ключом.

2.14. Клиент самостоятельно подключает и отключает возможность использования мобильного приложения в системе Сбербанк Бизнес Онлайн. Подтверждение операций в мобильном приложении осуществляется с использованием АСП.

2.15. Клиент самостоятельно подключает и отключает в системе Сбербанк Бизнес Онлайн услугу по предоставлению сервиса e-invoicing, включая направление электронных документов в адрес третьих лиц и использование сервиса «Отчетность».

2.16. В целях обеспечения значимости ЮЗЭД для налоговых и иных государственных органов, для выполнения функций организации обмена ЮЗЭД между Клиентами, хранения ЮЗЭД, передачи отчетности в государственные органы привлекается дочерняя компания ОАО «Сбербанк России» ООО «КОРУС Консалтинг СНГ», являющаяся специализированным оператором связи на основании «Паспорта о присоединении к сети доверенных операторов электронного документооборота счетов-фактур» № 0060 от 05.08.2014 зарегистрированного МИ ФНС России №17 по г.Санкт-Петербургу.

2.17. При осуществлении Головной компанией функций контроля движения денежных средств по счетам Клиента с использованием бюджета:

2.17.1. Лимиты по строкам бюджета, установленные Головной компанией, отражаются в Системе.

2.17.2. Клиент считается уведомленным об установленных лимитах с момента их отражения в Системе.

2.17.3. Клиенту предоставляется возможность формирования ЭПД с использованием Системы в соответствии со строками бюджета.

2.18. Получение дополнительных услуг, неоговоренных в рамках настоящих Условий, оформляется путем заключения отдельных договоров (соглашений).

3. УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ И ОПЛАТЫ УСЛУГ

3.1. Система состоит из:

- программных и аппаратных средств Банка, эксплуатируемых Банком за свой счет;
- программных и аппаратных средств, комплектуемых и эксплуатируемых Клиентом за свой счет;
- программных и аппаратных средств связи, обеспечивающих обмен ЭД между Сторонами;

- программных средств Системы, устанавливаемых на аппаратных средствах Клиента, и самостоятельно эксплуатируемых Клиентом (для «Сбербанк Бизнес»);
- программных средств Системы, устанавливаемых на аппаратных средствах Клиента, и самостоятельно разработанных и эксплуатируемых Клиентом (для «Сбербанк Интеграция»).

3.2. Количество Уполномоченных лиц Клиента и их полномочия, количество АСП/ЭП, используемых Клиентом для подписания передаваемых Банку ЭПД, определяются действующим законодательством Российской Федерации, требованиями Банка России и указывается Клиентом в Заявлении на заключение договора, в т.ч. использование Уполномоченными лицами АСП или ЭП. При использовании двух и более АСП и/или ЭП, ЭД признается корректным, если корректны и принадлежат разным лицам, имеющим право первой и второй подписи, все АСП и ЭП, которыми он подписан.

3.3. Доступ Клиента к Системе предоставляется в сети Интернет следующими способами:

- через браузер и мобильное приложение, в случае выбора системы «Сбербанк Бизнес Онлайн»;
- посредством установки специализированного программного обеспечения, на рабочее место Клиента, в случае выбора системы «Сбербанк Бизнес»;
- посредством передачи в Банк и приема из Банка информации с использованием специализированного программного обеспечения, разработанного в соответствии с форматами и средствами защиты информации, изложенных в «Соглашении о форматах Сбербанк Интеграция (API)».

3.4. Операции в системе «Сбербанк Бизнес Онлайн» Уполномоченное лицо Клиента подтверждает постоянным паролем (вводится при входе в Систему) и одноразовыми паролями (вводятся при совершении каждой операции в Системе) или ЭП. Операции в системе «Сбербанк Бизнес» Уполномоченное лицо Клиента подтверждает постоянным паролем (вводится при входе в Систему) и ЭП. Операции в системе «Сбербанк Интеграция» подтверждает с использованием ЭП.

3.5. Клиент соглашается с тем, что подтверждение Уполномоченными лицами Клиента операций (электронных документов/поручений) в Системе постоянным и одноразовым паролем является АСП (или ЭП) Уполномоченных лиц Клиента являются равнозначными бумажным документам/договорам с Банком.

3.6. Электронные документы Клиента без АСП/ЭП Клиента не имеют юридической силы и в обработку Банком не принимаются.

3.7. Клиент дает свое безусловное согласие на право Банка отнесения принадлежности ЭПД к fraud-операции.

3.8. Клиент признает все ЮЗЭД, направленные им или полученные посредством Системы от Банка или третьих лиц с использованием услуги e-invoicing, равнозначными документам на бумажном носителе, подписанным собственноручными подписями уполномоченных должностных лиц и заверенным печатями Сторон.

3.9. Проверка индивидуального номера абонента (IMSI) совершается в момент инициации процесса подписания Электронного документа в Системе. Электронный документ не проходит процедуру подписания с незарегистрированным уникальным номером сим-карты (IMSI) в Системе, соответственно в обработку Банком не принимается.

3.10. Клиент уведомлен, что в случае использования оператора сотовой, который не поддерживает использование дополнительного механизма защиты систем дистанционного банковского обслуживания, международного идентификатора мобильного абонента (IMSI) увеличивается риск мошеннических действий третьих лиц, которые могли быть предотвращены с помощью указанного механизма защиты. Все риски связанные с использованием системы дистанционного банковского обслуживания без использования дополнительного механизма защиты Клиент принимает на себя.

3.11. Клиент соглашается с получением услуг Системы через сеть Интернет, осознавая, что сеть Интернет не является безопасным каналом связи, и соглашается нести все риски, связанные с подключением его вычислительных средств и мобильных устройств к сети Интернет, возможным нарушением конфиденциальности и целостности информации при работе через сеть Интернет. Стороны также признают, что выход из строя рабочего места Системы, установленного у Клиента, мобильных устройств Клиента в результате вмешательства третьих лиц через сеть Интернет рассматривается как выход из строя по вине Клиента.

3.12. Клиент соглашается на получение доступа ЗАО «Астерос» (ОГРН 1027739254025) и ЗАО «Ай-теко» (ОГРН 1027700031061) к информации об операциях по счетам Клиента, в процессе осуществления технической поддержки Системы и смежного программного обеспечения указанными организациями, с учетом обязательств последних по обеспечению конфиденциальности и нераспространению ставшей им доступной информации.

3.13. «Клиент соглашается на получение доступа ООО «КОРУС Консалтинг СНГ» (ОГРН 1057812752502) к информации об операциях Клиента в процессе технического обеспечения ООО «КОРУС Консалтинг СНГ» функций по организации обмена ЮЗЭД между Клиентами, хранения ЮЗЭД, передачи отчетности в государственные органы, с учетом обязательств ООО «КОРУС Консалтинг СНГ» по обеспечению конфиденциальности и нераспространению ставшей доступной информации об операциях Клиента».

3.14. Клиент обязуется обеспечить предоставление физическими лицами, чьи персональные данные содержатся в представляемых на основании настоящего Договора Клиентом Банку документах, согласия на обработку (включая автоматизированную обработку) этих данных ООО «КОРУС Консалтинг СНГ» (ОГРН 1057812752502), в соответствии с требованиями действующего законодательства Российской Федерации, в том числе Федерального закона от 27.07.2006 № 152 – ФЗ «О персональных данных», Рекомендуемая форма заявления о согласии размещается на web-сайте Банка.

Обработка персональных данных ООО «КОРУС Консалтинг СНГ» (ОГРН 1057812752502) осуществляется в целях выпуска сертификатов ключей проверки ЭП для осуществления посредством Системы обмена ЮЗЭД и/или информацией свободного формата между Клиентами и/или между Клиентом и третьим лицом, выбравшим Клиента для участия в ЮЗЭД, для хранения ЮЗЭД, а также передачи отчетности в государственные органы.

3.15. При обмене ЭД между Клиентами, датой получения ЭД является дата доставки ЭД Системой, Датой отправки - Дата передачи документа в Систему.

3.16. Клиент самостоятельно и за свой счет обеспечивает подключение своих вычислительных средств и мобильных устройств к сети Интернет, доступ к сети Интернет, а также обеспечивает защиту собственных вычислительных средств, мобильных устройств и криптографических ключей от несанкционированного доступа и вредоносного программного обеспечения.

3.17. Стороны признают в качестве единой шкалы времени при работе в Системе местное время по месту расположения подразделения Банка, оказывающего услуги по Договору. Контрольным является время системных часов аппаратных средств подразделения Банка, оказывающего услуги по Договору.

3.18. Банк исполняет поступившие от Клиента ЭПД согласно условиям соответствующего Договора банковского счета.

3.19. Плата за услуги Банка по Договору списывается Банком в соответствии с Тарифами Банка со счета Клиента, указанного в Заявлении на заключение договора, без распоряжения клиента (на основании заранее данного акцепта) или в случае отсутствия у Клиента счетов открытых в ОАО «Сбербанк России», оплачиваются Клиентом самостоятельно или по выставленным Банком счетам:

- плата за организацию обслуживания с использованием Системы причитается Банку в день приема Заявления на заключение договора;
- ежемесячная плата за предоставление услуг с использованием Системы (за исключением предоставления сервиса e-invoicing) причитается Банку, начиная с месяца, следующего за месяцем заключения Договора, в последний рабочий день месяца, в котором услуга была предоставлена;
- ежемесячная плата за предоставление сервиса e-invoicing причитается Банку, начиная с месяца отправки электронного Заявления на подключение к услуге E-invoicing, взимается в первый рабочий день месяца, следующего за месяцем, в котором услуга была предоставлена.
- ежемесячная плата за использование мобильного приложения;
- плата за предоставление услуг по Договору, кроме указанных в настоящем пункте, причитается Банку в день, в котором услуга была предоставлена.
- при обслуживании Клиента на условиях тарифного плана, плата за предоставление услуг по Договору взимается в соответствии с выбранным тарифным планом.

3.20. Предоставление услуг по Договору может быть приостановлено по письменному заявлению Клиента. На время приостановления предоставления услуг по Договору ежемесячная плата за предоставление услуг с использованием Системы Банком не взимается. В случае возобновления предоставления услуги плата за ежемесячное обслуживание начисляется с месяца, в котором предоставление услуги было возобновлено.

3.21. Стороны признают, что:

- в соответствии с настоящими Условиями Сторонами используется усиленная неквалифицированная электронная подпись в терминах Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи».
- после подписания ЭД ЭП любое изменение, добавление или удаление символов документа делает ЭП некорректной, т.е. проверка подписи по ключу проверки ЭП Клиента дает отрицательный результат;
- создание Корректной ЭП ЭД возможно исключительно с использованием ключа ЭП;
- по содержанию ЭД, подписанных ЭП, и ключей проверки ЭП невозможно определить ключи ЭП;
- Клиент несет полную ответственность за обеспечение конфиденциальности и сохранность своих ключей ЭП, а также за действия своего персонала;
- Клиент может иметь несколько ключей ЭП, каждому ключу ЭП соответствует собственный ключ проверки ЭП;
- Клиент самостоятельно формирует свои ключи ЭП;
- ЭД, подписанные Корректной ЭП Клиента, а также журналы учета ЭД, ведущиеся в Системе, могут быть представлены Банком в качестве доказательств в случае рассмотрения спора, возникшего в результате применения Системы.
- Клиент самостоятельно формирует свои ключи шифрования.
- Клиент формирует ключи ЭП/шифрования в сеансе работы с Системой или с использованием встроенных средств Электронного ключа при отсутствии такой возможности.

3.22. Порядок выпуска Сертификатов ключей Клиента предусматривает что:

- Функцию УЦ по Договору выполняет Банк и ООО «КОРУС Консалтинг СНГ».
- Клиент предоставляет в Банк проекты Сертификатов ключей проверки ЭП и шифрования на бумажном носителе, сформированных Клиентом и заверенных собственноручной подписью Владельца Сертификатов, руководителя или лица, наделенного правом подписывать Договор(-ы) финансово-банковских услуг, и оттиском печати Клиента, а также ключей проверки ЭП/ключей шифрования в виде электронных файлов запросов на сертификаты, что эквивалентно подаче в УЦ заявления на выдачу Сертификатов ключей проверки ЭП/шифрования Уполномоченного лица Клиента. В случае, когда Уполномоченное лицо Клиента является руководителем или лицом, наделенным правом подписывать Договор(-ы) финансово-банковских услуг, данные проекты Сертификатов ключей на бумажном носителе заверяются одной подписью Уполномоченного лица Клиента и оттиском печати Клиента.
- УЦ не позднее 3 (Трех) рабочих дней со дня предоставления Клиентом в Банк распечаток проектов Сертификатов ключей проверки ЭП/шифрования на бумажном носителе осуществляет контроль корректности и соответствия ключей проверки ЭП/шифрования в распечатках электронным файлам.
- УЦ выпускает Сертификат ключа проверки ЭП/шифрования в электронном виде. По отдельному запросу Клиента Банк оформляет и передает Клиенту копии Сертификатов ключей проверки ЭП/шифрования на бумажном носителе с указанием сроков их действия.
- Предоставленные Клиентом ключи проверки ЭП/шифрования вводятся в действие с даты, указанной в их Сертификатах.

- Клиент предоставляет Банку документы, подтверждающие права Уполномоченных лиц на совершение операций с использованием ЭП. 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.
- В случае окончания или прекращения полномочий Уполномоченного лица в период действия Сертификата ключа проверки ЭП УЦ блокирует его использование. Для разблокировки необходимо предоставить в Банк новые документы, подтверждающие полномочия.
- После проведения процедуры генерации новых ключей ЭП/шифрования Клиента услуга обмена ЮЗЭД с третьими лицами и услуга по передаче отчетности в налоговые и иные государственные органы становится недоступна до выпуска сертификата ключа проверки ЭП/шифрования в УЦ Банка, его ввода в действие, а также выпуска сертификата ключа проверки ЭП в УЦ ООО «Корус-Консалтинг СНГ».

3.23. При компрометации или подозрении на компрометацию ключа ЭП/шифрования Клиентом (т.е. при несанкционированном использовании или подозрении на несанкционированное использование Электронного ключа) Банк извещается о прекращении действия факте компрометации ключа ЭП/шифрования, путем передачи соответствующего ЭД по Системе или иным доступным способом. Одновременно Клиент прекращает передачу ЭД с использованием указанного ключа ЭП/шифрования и выводит из действия соответствующие ключи. Банк, получивший сообщение о компрометации и/или замене ключа ЭП, выводит соответствующий сертификат ключа проверки ЭП из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о компрометации. Скомпрометированные ключи уничтожаются Сторонами самостоятельно.

3.24. Обмен электронными документами между Клиентом и Банком является односторонним - Клиент направляет в Банк на исполнение электронные платежные документы по счетам Клиента. Непосредственно в том же сеансе связи Клиенту сообщается о результате приема поручения в работу. Данные сообщения носят информационный характер и не являются электронными документами. Контроль за исполнением Банком электронных расчетных документов по счетам Клиента осуществляется Клиентом самостоятельно путем просмотра в Системе состояния этих счетов.

3.25. Клиент соглашается на получение информации-приглашения свободного формата посредством электронной почты или SMS-сообщений от третьих лиц, выбравших Клиента для участия в ЮЗЭД.

3.26. Создание чрезмерной нагрузки на оборудование Банка (посредством генерации чрезмерно интенсивных запросов к интерфейсу или любым иным образом) является основанием для прекращения предоставления доступа к системе «Сбербанк Интеграция».

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Клиент имеет право:

4.1.1. Отозвать ранее переданный ЭД, имеющий корректный АСП и/или корректную ЭП Клиента, путем направления в Банк по Системе соответствующего уведомления в виде ЭД, защищенного АСП и/или ЭП, при условии, что Банк к моменту получения уведомления Клиента не произвел операции во исполнение ранее полученного от Клиента ЭД.

4.1.2. Приостановить предоставление услуг Банком без расторжения Договора на срок до 3 (Трех) месяцев путем подачи письменного Заявления на приостановление/возобновление обслуживания по системе дистанционного банковского обслуживания, не менее чем за 10 (Десять) рабочих дней в подразделение Банка, обслуживающее Договор. Возобновление обслуживания производится с даты указанной в данном заявлении, без дополнительного уведомления, комиссия за ежемесячное обслуживание начисляется с месяца возобновления обслуживания по системе.

4.1.3. Обратиться в Банк за возобновлением предоставления услуг путем подачи письменного Заявления на приостановление/возобновление обслуживания по системе дистанционного банковского обслуживания, в срок, не превышающий 3 (Трех) месяцев со дня приостановления предоставления услуг Банком в соответствии с п. 4.1.2.

4.1.4. Изменить перечень банковских счетов, по которым необходимо оказание расчетно-кассового обслуживания с использованием Системы, путем подачи соответствующих письменных заявлений не менее, чем за 15 (Пятнадцать) рабочих дней до предполагаемой даты изменений.

4.1.5. В случае возникновения у Клиента претензий, связанных с предоставлением услуг с использованием Системы, представить в Банк заявление на бумажном носителе или через официальный сайт Банка (sberbank.ru).

4.1.6. В любое время производить замену ключей ЭП/шифрования. При этом производится одновременная смена ключей ЭП/шифрования.

4.1.7. Обратиться в Банк для замены вышедшего из строя Электронного ключа на новый, в случае если поломка произошла не по вине Клиента.

4.1.8. В случае заключения специального(ых) договора(ов) в установленном Банком порядке осуществлять передачу ЭД, в т.ч. Электронных реестров, защищенных ЭП/АСП, на перечисление денежных средств со счета(ов) Клиента на счета физических лиц.

4.1.9. Путем подачи соответствующего заявления отключить контроль проверки индивидуального номера абонента (IMSI). В данном случае Клиент принимает все риски связанные с совершением fraud-операции на себя. Претензии Клиента по Электронным документам/поручениям попадающим в число fraud-операций Банком не принимаются и не рассматриваются.

4.2. Клиент обязуется:

4.2.1. Оплачивать услуги Банка в соответствии с Тарифами Банка в порядке и сроки, предусмотренные п.3.19 настоящих Условий.

4.2.2. По требованию Банка предоставлять документ, удостоверяющий личность Уполномоченного лица Клиента, а также передать в Банк документы, подтверждающие полномочия Уполномоченного лица Клиента по распоряжению

денежными средствами, находящимися на счете, используя АСП и/или ЭП, или копии указанных документов, заверенные установленным порядком.

4.2.3. Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и настоящими Условиями.

4.2.4. При выявлении фактов или признаков нарушения безопасности Системы немедленно приостановить использование Системы и оповестить об этом Банк любым доступным образом.

4.2.5. Подписывать ЭПД АСП и/или ЭП Уполномоченных лиц в соответствии с требованиями действующего законодательства Российской Федерации и Банка России.

4.2.6. Обеспечить, при установке и обновлении собственными силами рабочего места «Клиент» системы «Сбербанк-Бизнес», установку и настройку программного обеспечения, а также готовность к вводу Системы в действие.

4.2.7. 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.

4.2.8. Организовывать внутренний режим функционирования рабочих мест Уполномоченных лиц таким образом, чтобы исключить возможность использования Системы, мобильных телефонов и/или Электронных ключей и PIN-кодов Уполномоченных лиц лицами, не имеющими допуска к работе с Системой.

4.2.9. При использовании Электронных ключей соблюдать Требования по обеспечению безопасности в процессе эксплуатации рабочего места Системы, размещенные в Системе и на web-сайте банка.

4.2.10. По первому требованию Банка в течение 2 (Двух) рабочих дней заверить печатями и подписями Уполномоченных лиц распечатанные Банком принятые и проведенные по счету Клиента платежные документы.

4.2.11. По требованию Банка обеспечить предоставление согласия на обработку персональных данных Банком от физических лиц Клиента уполномоченных работать в системе, распоряжаться счетом и/или получать от Банка информацию о состоянии счета или иную информацию в связи с наличием счета, в том числе автоматизированную в соответствии с Федеральным законом от 27 июля 2006 года № 152 – ФЗ «О персональных данных», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение. Рекомендуемая форма заявления о согласии размещается на web-сайте Банка.

4.2.12. Производить замену ключей ЭП Уполномоченных лиц в случаях, предусмотренных п.4.4.3 настоящих Условий.

4.2.13. Предоставлять Банку Электронные ключи в случае необходимости их обновления.

4.2.14. Для обеспечения безопасности не использовать одно и то же устройство для работы в Системе и приема/передачи SMS-сообщений с одноразовыми паролями.

4.2.15. Обеспечить сохранность мобильных устройств с установленным мобильным приложением. В случае утери мобильного устройства с установленным мобильным приложением, незамедлительно информировать Банк.

4.2.16. Обеспечить использование Уполномоченными лицами Клиента персональных мобильных телефонов для получения SMS-сообщений с одноразовыми паролями, указав их в Заявлении на заключение договора/на дополнение перечня банковских счетов.

4.2.17. Информировать Уполномоченных лиц Клиента о недопущении ситуаций переполнения памяти мобильных телефонов, что может являться препятствием для приема SMS-сообщений с одноразовыми паролями.

4.2.18. Информировать банк, в случае замены зарегистрированной в Системе сим-карты Клиента, путем подачи Заявления об использовании дополнительного механизма защиты системы в рамках использования международного идентификатора мобильного абонента, при включенном режиме защиты.

4.2.19. 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.

4.2.20. При осуществлении Головной компанией функций контроля движения денежных средств по счетам Клиента с использованием бюджета, указывать код строки бюджета при формировании ЭПД в Системе.

4.2.21. В случае использования «Сбербанк Интеграции»:

4.2.21.1. производить разработку, доработку и тестирование специализированного программного обеспечения в соответствии с форматами и средствами защиты информации, изложенных в «Соглашении о форматах Сбербанк Интеграция (API)» за счет собственных средств.

4.2.21.2. самостоятельно отслеживать информацию об изменении форматов «Соглашения о форматах Сбербанк Интеграция (API)» на корпоративном сайте Банка.

4.2.21.3. самостоятельно устанавливать и использовать версии специализированного программного обеспечения, строго соответствующие в части интеграции с Банком требованиям изложенным «Соглашении о форматах Сбербанк Интеграция (API)»;

4.2.21.4. не изменять алгоритмы передачи данных API в одностороннем порядке, если иное не предусмотрено отдельными соглашениями.

4.3. Банк обязуется:

4.3.1. Принимать к исполнению поступившие от Клиента подписанные корректными АСП и/или ЭП Клиента ЭД, оформленные и переданные в Банк в соответствии с настоящими Условиями.

4.3.2. Не исполнять поступившие от Клиента ЭПД, оформленные с нарушением требований действующего законодательства Российской Федерации, нормативных документов Банка России и настоящих Условий, а также при отсутствии или некорректности АСП и/или ЭП Клиента.

4.3.3. Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и настоящими Условиями.

4.3.4. Поддерживать до помещения в электронные архивы системные журналы и текущие базы переданных и принятых файлов с ЭД, АСП и/или ЭП на аппаратных средствах Системы в течение не менее 30 (Тридцати) календарных дней после их получения, а в случае возникновения споров – до их разрешения. Обеспечить сохранность архивов переданных и принятых файлов, подписанных АСП и/или ЭП Клиента, ключей проверки ЭП Клиента, а также системных журналов в течение срока, установленного действующим законодательством Российской Федерации.

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

4.3.6. Выдать Клиенту новый Электронный ключ взамен вышедшего из строя, в случае если на корпусе вышедшего из строя Электронного ключа, отсутствуют механические повреждения.

4.3.7. Консультировать Клиента по вопросам эксплуатации Системы.

4.3.8. При осуществлении Головной компанией функций контроля движения денежных средств по счетам Клиента с использованием бюджета обеспечить техническую возможность доступа Клиента к строкам бюджета.

4.3.9. Размещать не менее чем за 30 календарных дней информацию на официальном сайте Банка об изменении «Соглашения о форматах Сбербанк Интеграция (API)», за исключением изменений, которые носят характер расширения форматов и не затрагивают опубликованные ранее части документа, либо которые являются полностью совместимыми и не противоречащими опубликованной ранее версии.

4.4. Банк имеет право:

4.4.1. При выявлении фактов или признаков нарушения безопасности Системы немедленно приостановить использование Системы и оповестить об этом Клиента любым доступным образом.

4.4.2. При выявлении или подозрении на осуществление fraud-операции осуществить приостановку ЭПД до подтверждения его Клиентом. В случае если клиент не подтвердил ЭПД в срок, установленный договором банковского счета по исполнению ЭПД Банком, отказать в исполнении ЭПД. Банк направляет соответствующее уведомление о приостановке ЭПД Клиенту по Системе, а так же в виде SMS-сообщения на телефонные номера указанные в договоре банковского счета.

4.4.3. Требовать от Клиента замены (формирования новых) ключей ЭП/шифрования Клиента в срок не позднее 10 (Десяти) рабочих дней с даты соответствующего уведомления при проведении периодической плановой замены ключей ЭП/шифрования, смене лиц, уполномоченных распоряжаться счетами, компрометации или подозрении на компрометацию ключей ЭП или шифрования, а также в случае необходимости замены программного обеспечения, предназначенного для вычисления значения Хэш-функции, подтверждения авторства, целостности и обеспечения конфиденциальности ЭД.

4.4.4. В случае непредставления в течение тридцати дней проектов Сертификатов ключей Клиентом, удалять запросы на сертификаты в Системе.

4.4.5. Блокировать использование ключей ЭП/шифрования Клиента после окончания срока их действия или по истечении срока действия полномочий Владельца Сертификатов ключей.

4.4.6. Требовать от Клиента предоставления Электронных ключей при необходимости их обновления.

4.4.7. В одностороннем порядке:

- вводить новые, изменять и дополнять действующие Тарифы на услуги Банка,
- изменять порядок и сроки взимания платы,
- вносить изменения в настоящие Условия, включая Порядок использования средств криптографической защиты информации и порядок работы Удостоверяющего центра

Изменения вносятся, уведомив об этом Клиента не позднее 15 (Пятнадцати) календарных дней до даты вступления в силу соответствующих изменений. Информация об изменении и дополнении действующих Тарифов на услуги Банка, об изменении порядка и сроков взимания платы, об изменении настоящих Условий и Порядка использования средств криптографической защиты информации и порядка работы Удостоверяющего центра размещается в соответствующих разделах о Системе на официальном сайте ОАО «Сбербанк России». Датой извещения Клиента считается дата размещения Банком вышеуказанной информации.

4.4.8. Отказать Клиенту в исполнении платежного документа, принятого Банком по Системе и подписанного корректным АСП и/или корректной ЭП на проведение операции по счету, а также полностью прекратить предоставление услуг по Договору, в случае осуществления Клиентом Сомнительной операции или в случае отсутствия Клиента, его постоянно действующего органа управления, иного органа или лица, которые имеют право действовать от имени Клиента без доверенности по адресу (месту нахождения), внесенному в Единый государственный реестр юридических лиц. При этом право отнесения операций к числу Сомнительных принадлежит Банку, на что Клиент дает свое безусловное согласие. Банк направляет Клиенту по Системе соответствующее уведомление об отказе в исполнении платежного документа Клиента, принятого по Системе.

После получения такого уведомления Клиент для осуществления расчетной операции, в проведении которой ему отказано по Системе, вправе представить в Банк надлежащим образом оформленный расчетный документ на бумажном носителе, который исполняется Банком в соответствии с действующим законодательством и договором банковского счета.

4.4.9. Оставить ЭД, содержащий Электронные реестры, без исполнения, уведомив об этом Клиента путем направления соответствующего электронного сообщения с использованием Системы, в случаях:

- невозможности прочтения Электронных реестров соответствующими программными средствами;
- не поступления и/или несвоевременного поступления в Банк Электронных реестров;
- отсутствия или некорректности ЭП, удостоверяющей Электронные реестры;

- не поступления или поступления не в полной сумме от Клиента на счет Банка (филиала Банка) денежных средств, предназначенных для зачисления на счета физических лиц и/или платы за услуги Банка;
- несоответствия внутреннего формата файлов Электронных реестров формату, установленному специальным(ыми) договором(ами).

4.4.10. Вводить ограничения или полностью прекратить предоставление Клиенту услуг по Договору в случае выявления попыток сканирования, атак информационных ресурсов Банка, а также иных признаков нарушения безопасности с использованием программно-аппаратных средств Клиента.

4.4.11. Списывать с расчетного счета Клиента, указанного в Заявлении на заключение договора комиссию за оказываемые Банком по Договору услуги в соответствии с Тарифами в порядке и сроки, предусмотренные п.3.19 настоящих Условий, без распоряжения клиента (на основании заранее данного акцепта).

4.4.12. При неоплате/задержке оплаты услуг Клиентом Банк имеет право в одностороннем порядке расторгнуть Договор в порядке, предусмотренном п.8.4 настоящих Условий.

4.4.13. Уведомить Клиента о необходимости подачи корректирующего Заявления на заключение договора, в т.ч. посредством Системы, в срок, предусмотренный п.4.2.19 настоящих Условий. Если корректирующее Заявление не будет подано Клиентом Банк имеет право приостановить оказание услуги.

4.4.14. По своему усмотрению предоставлять полный или ограниченный набор услуг с использованием Системы в каждом из своих подразделений в конкретный период времени, а также расширять перечень предоставляемых услуг.

4.4.15. В рамках требований по безопасности, предложить клиенту замену постоянного пароля Клиента в системе на новый.

4.4.16. 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 (для системы «Сбербанк Бизнес»).

4.4.17. Не осуществлять техническую поддержку рабочего места «Клиент» системы «Сбербанк Бизнес», версия которого ниже двух последних, выпущенных Банком.

4.4.18. Изменять «Соглашения о форматах Сбербанк Интеграция (API)» в одностороннем порядке без дополнительных согласований со стороны Клиента в порядке, описанном в п.4.3.9.

4.4.19. Не осуществлять техническую поддержку мобильного приложения, версия которого ниже двух последних, выпущенных Банком.

4.4.20. Привлекать сторонние организации/аутсорсинговые компании для оказания Клиенту услуг, связанных с установкой и эксплуатацией систем дистанционного банковского обслуживания.

4.4.21. Осуществлять иные права, предусмотренные действующим законодательством Российской Федерации, нормативными актами Банка России и настоящими Условиями.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За невыполнение или ненадлежащее выполнение обязательств, вытекающих из настоящих Условий, виновная Сторона несет ответственность в соответствии с действующим законодательством Российской Федерации.

5.2. 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 освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств. Факт наступления обстоятельств непреодолимой силы подтверждается Сторонами путем предоставления соответствующих документов.

5.3. Стороны не отвечают за правильность заполнения и оформления электронных документов другой Стороной.

5.4. Банк не несет ответственности за последствия компрометации идентификатора, PIN-кода, постоянного и одноразовых паролей Уполномоченных лиц Клиента, а также за убытки, понесенные Клиентом в связи с неправомерными действиями третьих лиц.

5.5. Банк не несет ответственности за последствия исполнения электронного документа, защищенного корректными АСП и/или ЭП Клиента, в т.ч. в случае использования мобильных телефонов и/или Электронных ключей, программно-аппаратных средств клиентской части Системы неуполномоченным лицом.

5.6. Банк не несет ответственности за ущерб, возникший вследствие разглашения Уполномоченными лицами Клиента собственных ключей ЭП/шифрования, их утраты или передачи, вне зависимости от причин, неуполномоченным лицам.

5.7. Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к рабочему месту Системы, установленному у Клиента (включая удаленный сетевой доступ), и ключам ЭП/шифрования Клиента, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

5.8. 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 этого задержки в осуществлении операций 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 настоящему Договору.

5.9. Банк не несет ответственности за неработоспособность оборудования и программных средств Клиента, за несоответствие реализованного клиентом в его программном обеспечении формата обмена к актуальному формату «Соглашения-оферты о форматах Сбербанк Интеграция (API)» заявленному на сайте Банка в случае использования системы «Сбербанк Интеграция», повлекшую за собой невозможность доступа Клиента к счетам, и возникшие в результате этого задержки в осуществлении операций 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 настоящему Договору.

5.10. Банк не несет ответственности в случае утери мобильного устройства Клиента.

5.11. Ответственность банка по исполнению ЭД наступает, после перехода ЭД в статус «принят».

6. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

6.1. При возникновении разногласий и споров в связи с обменом электронными документами с ЭП 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 разделом 7 настоящих Условий. 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.

6.2. При возникновении претензий Клиента в связи с обменом электронных документами с АСП они рассматриваются после подачи Клиентом соответствующего заявления в подразделение Банка с указанием сути претензии. Результаты рассмотрения заявления доводятся до Клиента.

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

7.1. При возникновении разногласий Сторон в связи с обменом документами в электронном виде с помощью Системы, а также в иных случаях возникновения спорных ситуаций в связи с эксплуатацией системы, обмен документами в электронном виде с использованием Системы между Сторонами немедленно прекращается.

7.2. Клиент обязан направить в Банк заявление о разногласиях, подписанное руководителем или лицом Клиента, наделенного 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 Клиента, которые будут участвовать в работе комиссии, место, время и дату сбора комиссии. Дата сбора комиссии должна быть не позднее 10 (десяти) рабочих дней со дня получения Банком заявления.

7.3. 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 5 (пяти) рабочих дней. В исключительных ситуациях этот срок может быть увеличен по взаимной договоренности Сторон.

7.4. 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.

7.5. При возникновении у Клиента претензий к Банку по поводу корректности действий, совершенных в рамках выполнения обязательств по п.п. 4.3.1, 4.3.2 Условий, комиссия должна:

7.5.1. проверить авторство предъявляемого Банком полученного им от Клиента электронного документа, в соответствии с которым совершены действия;

7.5.2. проверить, что совершенные Банком действия соответствуют содержанию электронного документа.

7.6. Для проверки авторства электронного документа выполняются следующие действия:

7.6.1. Определяется сообщение, содержащее ЭД, авторство которого должно быть проверено в связи со спорной ситуацией на основе проверки корректности ЭП сообщения, содержащего оспариваемый документ.

7.6.2. Из электронного архива Банка комиссии предъявляется сообщение с ЭП, содержащее оспариваемый электронный документ Клиента.

7.6.3. Банк предъявляет комиссии действовавший на момент подписания Сертификат проверки ЭП подписи Клиента, предназначенный для проверки корректности ЭП сообщения, содержащего оспариваемый документ.

7.6.4. Проверяется целостность программного модуля, предъявляемого любой из Сторон, путем вычисления значения Хэш-функции в соответствии с Порядком вычисления значений Хэш-функции для файлов с помощью программного модуля Hashctrl.exe и сравнения его со значением, указанным на web-сайте Банка.

7.6.5. Проверяется корректность ЭП сообщения, содержащего оспариваемый ЭД, с помощью указанного программного модуля.

7.6.6. По требованию Клиента может быть проверена принадлежность предъявленного электронного Сертификата ключа проверки ЭП Клиенту. Электронный Сертификат ключа проверки ЭП признается принадлежащим Клиенту, если содержащийся в нём ключ проверки ЭП, соответствует ключу проверки ЭП, содержащемуся в проекте Сертификата ключа проверки ЭП.

7.6.7. Если предъявленный в виде файла сертификат не соответствует ключу проверки ЭП, содержащемуся в проекте Сертификата ключа проверки ЭП, либо период действия предъявленного ключа не соответствует времени получения оспариваемого документа, то комиссия признает, Электронный Сертификат ключа проверки ЭП не был представлен Банком.

7.7. Если в результате проведенной проверки корректности ЭП сообщения, содержащего оспариваемый документ, с Сертификатом ключа проверки ЭП, предъявленным Банком, ЭП признана корректной, то авторство оспариваемого ЭД признается комиссией установленным.

Если авторство оспариваемого ЭД признано комиссией установленным и действия Банка соответствуют содержанию оспариваемого документа, то претензии Клиента признаются необоснованными.

Если авторство оспариваемого ЭД признано комиссией установленным и действия Банка не соответствуют содержанию оспариваемого документа, то претензии Клиента признаются обоснованными.

7.8. Если в результате проведенной проверки корректности ЭП сообщения, содержащего оспариваемый документ, с Сертификатом ключа проверки ЭП, предъявленным Банком, ЭП признана некорректной, то предъявленный для проверки авторства ЭД признается комиссией ложным.

Если Банк исполнил оспариваемый документ, признанный комиссией ложным, то претензии Клиента к Банку признаются обоснованными.

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

7.10. Отсутствие на клиентском рабочем месте Системы признаков отправки электронного документа, принятого Банком с корректной ЭП данного Клиента, не является основанием для отказа Клиента от авторства данного документа, в том числе при использовании системы «Сбербанк Интеграция».

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

7.11.1. состав комиссии;

7.11.2. действия членов комиссии;

7.11.3. установленные обстоятельства;

7.11.4. основания, которые послужили для формирования выводов;

7.11.5. выводы, влияющие на возможность установления подлинности оспариваемого документа.

В этом случае акт признается Сторонами надлежащим.

7.12. 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 ЭД 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.

Составленный комиссией акт является основанием для выработки Сторонами окончательного решения комиссии. Данное решение должно быть подписано Сторонами не позднее 10 (десяти) календарных 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

8. СРОК ДЕЙСТВИЯ ДОГОВОРА

8.1. Договор вступает в силу с даты подачи Клиентом в Банк Заявления на заключение договора и действует в течение 1 (Одного) года.

8.2. 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 (Тридцать) календарных дней до даты окончания срока действия Договора.

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

8.4. Банк имеет право в одностороннем порядке расторгнуть настоящий Договор в следующих случаях:

8.4.1. В случае неоплаты Клиентом предоставленных Банком услуг, в том числе по следующим причинам:

- отсутствие достаточной суммы средств на счете Клиента, указанном в Заявлении на заключение договора,
- невозможно списание средств в связи с приостановлением расходных операций по счету,
- наложение ареста на денежные средства, находящиеся на счете,
- закрытие счета(ов) для оплаты услуг с использованием системы, указанного(ых) в Заявлении на заключение договора.

Банк имеет право приостановить на срок до 3 (Трех) месяцев предоставление услуг по Договору, а в случае неоплаты по истечении указанного срока – расторгнуть Договор в одностороннем порядке без соблюдения срока, установленного п.8.3 настоящих Условий. При этом Клиенту направляется уведомление о расторжении Договора.

8.4.2. В случае возврата указанного выше уведомления, направленного Банком по последнему известному адресу Клиента, уведомление о прекращении настоящего Договора считается врученным Клиенту, что влечет прекращение прав и обязанностей Сторон и является основанием для расторжения Договора.

8.4.3. При проведении Клиентом Сомнительных операций или в случае отсутствия Клиента, его постоянно действующего органа управления, иного органа или лица, которые имеют право действовать от имени Клиента без доверенности по адресу (месту нахождения), внесенному в Единый государственный реестр юридических лиц, письменно уведомив Клиента о расторжении Договора в порядке, аналогичном указанному в п. 8.4.1 настоящих Условий.

8.4.4. При непредставлении Клиентом Заявления на приостановление/возобновление обслуживания по системе дистанционного банковского обслуживания для возобновления предоставления услуг по Договору по истечении 6 (Шести) месяцев со дня приостановления предоставления услуг Банком и в случае не указания Клиентом в Заявлении даты возобновления при приостановлении услуг, Банк имеет право расторгнуть Договор, письменно уведомив Клиента в порядке, аналогичном указанному в п. 8.4.1.

Порядок обмена между банком и Клиентом в электронном виде документами и информацией, связанными с проведением валютных операций, требование о представлении (направлении) которых предусмотрено НПА ВЗ.

1. Документы валютного контроля, документы и информация, связанные с проведением валютных операций, подтверждающие документы представляются Клиентом в Банк в электронном виде в следующем порядке.

Формализованные и структурированные документы валютного контроля:

- ПС по контракту,
- ПС по кредитному договору,
- СВО (корректирующая СВО),
- СПД (корректирующая СПД),
- заявление о переоформлении паспорта сделки,
- заявление о закрытии паспорта сделки,

- представляются в виде заполненных форм, предоставляемых системой.

Документы, связанные с проведением валютных операций, представляются в виде полученных с использованием сканирующих устройств изображений документов, оформленных первоначально на бумажном носителе, вложениями в электронные формы формализованных/структурированных документов.

Информация, связанная с проведением валютных операций, может представляться в виде документа, сформированного в электронном виде, вложением в электронную форму формализованного/структурированного документа.

Документы и информация, необходимые для оформления паспорта сделки, представляются вложением в электронную форму ПС.

В случае необходимости представления в банк для оформления ПС ведомости банковского контроля (далее – ВБК) по закрытому в другом банке ПС в электронном виде в формате XML она представляется вложением в электронную форму ПС.

Документы и информация, в т.ч. ПС и ВБК другого банка и ПС и ВБК другого банка в электронном виде в формате XML, необходимые для перевода ПС на обслуживание из другого банка, представляются вложением в предназначенный для этих целей тип документа «Паспорта сделок, переводимые из других банков».

При осуществлении операций, связанных с зачислением иностранной валюты на транзитный валютный счет и со списанием иностранной валюты с расчетного счета в иностранной валюте, документы и информация, связанные с проведением валютной операции (документы, являющиеся основанием для проведения валютных операций), представляются только вложением в электронную форму СВО.

При осуществлении валютной операции, связанной со списанием валюты РФ с расчетного счета в валюте РФ, документы и информация, связанные с проведением валютной операции, представляются вложением в электронную форму расчетного документа. В случае осуществления валютной операции, связанной со списанием с расчетного счета в валюте РФ валюты РФ в пользу нерезидента, по контракту (кредитному договору), по которому оформлен ПС, документы и информация, связанные с проведением валютной операции, представляются только вложением в форму СВО.

При осуществлении валютных операций, связанных с расчетами по контракту (кредитному договору), по которому оформлен паспорт сделки: третьим лицом - резидентом (другим лицом - резидентом, резидентом, который не оформляет паспорта сделки); с проведением расчетов по аккредитиву; с использованием банковской карты; через счета, открытые в банке-нерезиденте, – документы, связанные с проведением указанных валютных операций, представляются вложением в форму СВО.

При представлении в банк подтверждающих документов, связанных с осуществлением валютных операций по договорам (контрактам), на которые установлено требование об оформлении ПС, а также документов, подтверждающих исполнение (прекращение) обязательств по контракту (кредитному договору), по которому оформлен ПС, они представляются вложением в СПД.

Документы и информация, необходимые для переоформления ПС, представляются вложением в форму заявления о переоформлении ПС.

Документы и информация, подтверждающие основание закрытия ПС, представляются вложением в электронную форму заявления о закрытии ПС.

2. Заявления по тематике валютного контроля и иные документы, используемые для целей валютного контроля, передаются в Банк сообщениями почты Системы. Клиент обязуется начинать текст поля «Тема» сообщения с латинской аббревиатуры «VO», означающей «валютная операция». В тексте поля «Тема» может указываться краткая информация, которая позволит соотнести пересылаемые электронные документы с номером электронного платежного документа, номером ПС или иным документом. При этом сообщения с Заявлениями по тематике валютного контроля должны быть подписаны в соответствии с требованиями нормативных актов Банка России в области валютного контроля.

3. Формализованные/структурированные документы, направляемые Клиентом в банк, подписываются электронной подписью Клиента.

Документы и информация, вложенные в электронную форму формализованного/структурированного документа (пакет электронных документов), автоматически подписываются одновременно с формализованным/структурированным документом.

4. Представляемые Клиентом копии документов, полученные с использованием сканирующих устройств, формируются Клиентом в одном из следующих графических форматов хранения изображений – PDF, TIF или JPEG / JPG и должны быть надлежащего качества (с отражением без искажений всех элементов документа) и доступны для чтения без использования специальных устройств. Банк вправе отказать в принятии документов в случае представления сканированных копий документов ненадлежащего качества.

5. Допускается вложение в ЭД ВК архивных файлов в формате ZIP, RAR или ARJ, содержащих один или несколько файлов ЭД ВК. Если форма ЭД ВК с вложенным в нее архивным файлом имеет корректную ЭП, то каждый ЭД ВК, входящий в архивный файл, считается подписанным корректной ЭП.

6. Совокупный размер вложенных в форму ЭД ВК файлов, в т.ч. архивных, не должен превышать размера, установленного в Системе.

7. Ответственное лицо, направляя Клиенту оформленный/принятый на обслуживание/переоформленный/закрытый ПС, приняую СВО/СПД:

- проставляет в форме ПС номер и дату оформления ПС, регистрационный номер банка ПС, способ и дату представления Клиентом документов, способ и дату направления Клиенту ПС (в отдельных случаях (в случаях выявления ошибок в заполнении ПС, вызванных ошибками/сбоями системы) вкладывает в электронную форму ПС файл с оформленным ПС, не внося в форму ПС присвоенные банком ПС реквизиты и подпись Ответственного лица);

- вкладывает в электронное сообщение с переведенным на обслуживание ПС файл с принятым на обслуживание ПС;

- вкладывает в электронную форму заявления о переоформлении ПС файл с переоформленным ПС;

- вкладывает в электронную форму заявления о закрытии ПС файлы с закрытым ПС и ВБК, сформированной на дату закрытия ПС, а также в случаях, установленных НПА ВЗ, ПС и ВБК в электронном виде в формате XML;

- проставляет в форме СВО/СПД дату представления и дату принятия (в отдельных случаях (в случаях выявления ошибок в заполнении ПС, вызванных ошибками/сбоями системы, вкладывает в электронную форму СВО/СПД файл с принятой СВО/СПД, не внося в форму СВО/СПД дату принятия и подпись Ответственного лица);

- проставляет подпись Ответственного лица;

- присваивает документу в системе статус «Принят ВК».

8. В случае отказа в оформлении/принятии на обслуживание/переоформлении/закрытии ПС, принятии СВО/СПД Ответственное лицо проставляет в системе дату возврата документов и указывает причины отказа в оформлении/принятии на обслуживание/переоформлении/закрытии ПС, принятии СВО/СПД, а также в виде ссылки на соответствующий(е) пункт(ы) НПА ВЗ - причины возврата СВО/СПД. При этом дата возврата и причины возврата СВО/СПД фиксируются в разделе «Информация уполномоченного банка»/«Информация банка ПС» печатной формы СВО/СПД.

Присвоение документу в системе Ответственным лицом статуса «Отказан ВК» означает возврат Клиенту представленных документов с указанием даты возврата и причин отказа.

В случае непредставления Клиентом в банк при осуществлении валютной операции, связанной со списанием денежных средств с расчетного счета Клиента, СВО и (или) документов, связанных с проведением валютной операции, либо при отказе в их принятии Ответственное лицо отказывает в списании иностранной валюты со счета Клиента в иностранной валюте либо в списании валюты РФ с его расчетного счета в валюте РФ (отказывает в акцепте валютного контроля).

При отрицательном результате проверки расчетного документа по валютной операции в валюте РФ, не требующей оформления ПС, и документов, связанных с проведением валютной операции, Ответственное лицо отказывает в акцепте валютного контроля с указанием причин отказа.

По запросу Клиента в подразделении Банка по месту обслуживания Клиента может быть получен отказ в принятии документов валютного контроля на бумажном носителе, заверенный подписью Ответственного лица.

9. Дата представления документов валютного контроля в банк соответствует дате поступления документа валютного контроля на банковскую часть системы в установленное операционное время.

Документ валютного контроля, направленный или возвращенный банком, считается полученным Клиентом в момент изменения статуса документа на «Принят ВК» или «Отказан ВК».

10. Банк имеет право запросить у Клиента представление оригинала или надлежащим образом заверенной копии обосновывающего и/или подтверждающего документа на бумажном носителе и отказать Клиенту в приеме ЭД ВК до представления документов на бумажном носителе.

11. Банк отказывает Клиенту в приеме ЭД ВК в случае невыполнения Клиентом требований пунктов 1 – 3 настоящего порядка обмена.

12. Банк имеет право отказать Клиенту в приеме ЭД ВК в случае невыполнения Клиентом требований пунктов 4 или 6 настоящего порядка обмена.