

СОГЛАШЕНИЕ

о предоставлении услуги стандартного электронного документооборота Система «Клиент-Банк.WEB»

Настоящее Соглашение о предоставлении услуги стандартного электронного документооборота Система «Клиент-Банк.WEB»¹ (далее – Соглашение) является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

Размещение Соглашения, в том числе опубликование его в информационно-телекоммуникационной сети Интернет, на официальном сайте Банка (www.gazprombank.ru) должно рассматриваться всеми заинтересованными лицами как публичное предложение (оферта) Банка, адресованное юридическим лицам (некредитным организациям) и индивидуальным предпринимателям, зарегистрированным в установленном законодательством Российской Федерации порядке, а также физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, о заключении с Банком Соглашения в пределах таможенной границы Российской Федерации на условиях, установленных Соглашением и Тарифами.

Присоединение к Соглашению осуществляется заинтересованными лицами путем его акцепта без каких-либо изъятий и оговорок в порядке, установленном Соглашением.

1. ПЕРЕЧЕНЬ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Банк – «Газпромбанк» (Акционерное общество), ИНН 7744001497, ОГРН 1027700167110.

Доверенный УЦ – удостоверяющий центр, аккредитованный в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», либо федеральный орган исполнительной власти, уполномоченным в сфере использования электронной подписи.

Договоры – договоры банковского счета, иные договоры, соглашения, в том числе соглашения о порядке заключения и исполнения сделок и соглашения, определяющие общие условия обязательственных взаимоотношений сторон, которые заключены или которые будут заключены в будущем между Банком и Клиентом.

Документ свободного формата (ДСФ) – электронный документ, не имеющий регламентированной структуры, подписываемый Банком или Клиентом посредством электронной подписи, обмен, направление которого осуществляется в целях заключения и исполнения Договоров, осуществления прав и обязанностей по Договорам.

Заявление на заключение ДБС – заявление на заключение договора банковского счета с возможностью открытия необходимого количества банковских счетов, открытие банковских счетов и подключение Системы «Клиент-Банк.WEB», форма которого размещена на официальном сайте Банка www.gazprombank.ru.

Заявление на комплексное банковское обслуживание² – заявление Клиента о присоединении к договорам о предоставлении продуктов/услуг Банка, составленное по форме Банка.

Клиент – юридическое лицо (некредитная организация) или индивидуальный предприниматель, зарегистрированные в установленном законодательством Российской Федерации

¹ Применяется в случае направления клиентом в Банк ГПБ (АО) посредством системы «Клиент-Банк.WEB» уведомления о начале работы в системе «Клиент-Банк.WEB».

² Типовая форма применима с момента технической реализации.

Федерации порядке, а также физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее(-ий) с Банком Соглашение.

Ключ доступа MyDSS – конфиденциальный код, устанавливаемый Клиентом (уполномоченным представителем Клиента) для доступа к хранилищу ключа УНЭП (MyDSS).

Компрометация доступа к Мобильному приложению (Компрометация) – факт несанкционированного использования Мобильного приложения или обнаружение вероятности такого использования в результате передачи пароля для входа в Мобильное приложение сторонними лицами, а также обнаружение факта установки Мобильного приложения на стороннее Мобильное устройство для последующего использования в мошеннических целях.

Компрометация ключа – утрата Стороной – владельцем ключа электронной подписи доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам. К событиям, связанным с компрометацией ключей, относятся следующие:

- утрата носителей ключевой информации;
- увольнение работников, имевших доступ к ключевой информации;
- временный доступ посторонних лиц к ключевой информации;
- воздействие вредоносного программного обеспечения на компьютер, предназначенный для работы с ключевой информацией Системы «Клиент-Банк.WEB»;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к ключу электронной подписи со стороны неуполномоченных лиц.

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Мобильное приложение (Мобильное приложение) – приложение для Мобильных устройств, являющееся одним из каналов доступа к Системе «Клиент-Банк.WEB» с использованием Мобильного устройства, имеющего доступ в Интернет.

Мобильное устройство – устройство Клиента в виде смартфона или планшета (планшетного компьютера), функционирующего на базе операционных систем iOS и Android или их аналога, которые используются Клиентом для доступа в Мобильное приложение и/или Приложение MyDSS.

Несанкционированный доступ к информации – доступ к информации неуполномоченных лиц.

Номер телефона Клиента – номер(-а) мобильного телефона Клиента или уполномоченного представителя (уполномоченных представителей) Клиента, предоставленный(-ые) Клиенту оператором сотовой связи, зарегистрированным и действующим на территории Российской Федерации в порядке, предусмотренном законодательством Российской Федерации, и указанный(-ые) Клиентом в соответствии с Соглашением для использования в Мобильном приложении.

Приложение MyDSS – приложение для Мобильных устройств, с помощью которого организован доступ уполномоченных представителей Клиента к сервису ЭП для удаленной реализации функций централизованного хранения ключей УНЭП (MyDSS) (хранение ключей УНЭП (MyDSS) осуществляется Банком с использованием СЭП MyDSS.), создания и проверки УНЭП (MyDSS), аутентификации владельцев сертификатов ключей проверки УНЭП (MyDSS) при осуществлении доступа к СЭП MyDSS и выполнение операций с использованием принадлежащих им ключей УНЭП (MyDSS).

Приложение MyDSS для мобильных платформ iOS и Android размещается в интернет-магазинах Apple AppStore и GooglePlay Market.

Регламент – «Регламент удостоверяющего центра Банка ГПБ (АО)», опубликованный на официальном сайте Банка www.gazprombank.ru.

Регламент Доверенного УЦ – документ, определяющий условия предоставления и правила пользования услугами Доверенного УЦ, включая права, обязанности, ответственность Доверенного УЦ и пользователей Доверенного УЦ, которые определяются Доверенным УЦ и, как правило, размещаются им в сети Интернет на сайте Доверенного УЦ.

Сертификат ключа проверки электронной подписи (Сертификат ключа проверки ЭП) – Электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром, либо доверенным лицом Удостоверяющего центра, либо Доверенным УЦ и подтверждающий принадлежность Ключа проверки электронной подписи Владельцу сертификата ключа проверки электронной подписи.

Система «ГПБ Бизнес-Онлайн» – корпоративная информационная система, владельцем и оператором которой является Банк, обеспечивающая электронный документооборот между Клиентом и Банком, доступ к которой осуществляется по адресу <https://gbo.gazprombank.ru>. Порядок и условия использования Системы «ГПБ Бизнес-Онлайн», в том числе порядок подписания и направления документов, определяются соглашением об использовании системы электронного документооборота «ГПБ Бизнес-Онлайн», заключенным между Клиентом и Банком.

Система «Клиент-Банк» – корпоративная информационная система, владельцем и оператором которой является Банк, предназначенная для обмена электронными документами между Клиентом и Банком.

Система «Клиент-Банк.WEB» – Система «Клиент-Банк», предоставляющая Клиенту возможность обмениваться электронными документами с Банком через сеть Интернет и Web-интерфейс.

Средство электронной подписи MyDSS (СЭП MyDSS) – шифровальные (криптографические) средства, используемые Банком для реализации хотя бы одной из следующих функций – создание УНЭП (MyDSS), проверка УНЭП (MyDSS), создание ключа УНЭП (MyDSS) и ключа проверки УНЭП (MyDSS), хранения ключей УНЭП (MyDSS).

Стандартный электронный документооборот – обмен электронными документами между Клиентом и Банком с использованием Системы «Клиент-Банк.WEB».

Статус – информация в электронно-цифровой форме, отражающая текущее состояние электронного документа в результате смены его состояния в Системе «Клиент-Банк.WEB».

Сторона (Стороны) – Банк и/или Клиент.

Тарифы – установленные Банком размеры, порядок начисления и взимания комиссий, платежей, иных вознаграждений Банка, уплачиваемых Клиентом Банку за предоставление Услуги, размещенные на официальном сайте Банка www.gazprombank.ru.

УКЭП – усиленная квалифицированная Электронная подпись в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», сертификат ключа проверки которой выдан Доверенным УЦ.

УНЭП – усиленная неквалифицированная Электронная подпись в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», сертификат ключа проверки которой выдан УЦ.

УНЭП (MyDSS) – усиленная неквалифицированная электронная подпись в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», сформированная по технологии MyDSS и сертификат ключа проверки, которой выдан УЦ.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, которая используется для определения лица, подписывающего

информацию. В качестве ЭП в Системе «Клиент-Банк.WEB» используются УНЭП и УКЭП Стороны.

Электронный документ (ЭД) – информация, подписанная Электронной подписью, представленная в электронной форме в формате, определенном Банком, предназначенная для передачи посредством Системы «Клиент-Банк.WEB».

Face ID – система аутентификации, основанная на распознавании контуров лица владельца Мобильного устройства. Используется в устройствах для их разблокировки и входа в электронные приложения (при наличии технической возможности на Мобильном устройстве).

MyDSS – технология, обеспечивающая строгую криптографическую аутентификацию Клиента (уполномоченного представителя Клиента), безопасное онлайн-взаимодействие, отображение проекта Электронного документа и визуализацию Электронного документа, подтверждение операций, которая позволяет контролировать действия пользователя в системах дистанционного банковского обслуживания с технологией аутентификации и подтверждением операций формирования Электронной подписи с помощью мобильных приложений для iOS и Android).

Push-уведомление Приложения MyDSS – короткое текстовое сообщение, информирующее о необходимости подписания Электронного документа, направляемое Банком Клиенту (уполномоченному представителю Клиента) на Мобильное устройство, на котором установлено Приложение MyDSS и проведена авторизация Клиента (уполномоченного представителя Клиента) для использования УНЭП (MyDSS), и появляющееся на экране данного устройства (при наличии технической возможности Мобильного устройства).

Touch ID – система аутентификации, основанная на использовании датчика, распознающего индивидуальный рисунок отпечатка пальца владельца Мобильного устройства (сканер отпечатков пальцев) (при наличии технической возможности на Мобильном устройстве).

Следующие термины употребляются по тексту Соглашения в значении, установленном Регламентом: «Владелец сертификата ключа проверки ЭП», «Ключ проверки электронной подписи (Ключ проверки ЭП)», «Ключ электронной подписи (Ключ ЭП)», «Подтверждение подлинности ЭП в электронном документе», «Средства электронной подписи (Средства ЭП)», «Средства криптографической защиты информации (СКЗИ)», «Удостоверяющий центр (УЦ)».

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. Банк предоставляет Клиенту услугу Стандартного электронного документооборота Система «Клиент-Банк.Web» (далее – Услуга) для обмена между Банком и Клиентом Электронными документами в целях исполнения договора банковского счета, а также в целях заключения Договоров, направления документов, необходимых для заключения и исполнения Договоров, заключения, исполнения и расторжения сделок, заключенных в рамках Договоров, а также обмена любыми иными документами, предусмотренными Договорами.

Банк предоставляет Клиенту Услугу при осуществлении операций по всем счетам Клиента в рублях и иностранной валюте вне зависимости от места открытия/обслуживания счета(-ов).

Банк предоставляет Клиенту Услугу в целях заключения Договоров в случаях, когда такая возможность предусмотрена в соответствующих оферте, направленной Банком Клиенту, и/или порядке заключения Договора, доведенном до сведения Клиента, в том числе предусмотренном в соответствующей форме Договора и/или размещенном на официальном сайте Банка www.gazprombank.ru и/или предусмотренном в соглашении между Банком и Клиентом, за исключением случаев, предусмотренных Соглашением.

Банк предоставляет Клиенту Услугу в целях направления документов, необходимых для исполнения Договоров, заключения, исполнения и расторжения сделок в рамках Договоров, а также обмена любыми иными документами, предусмотренными Договорами, в случаях, когда

такая возможность предусмотрена в соответствующих Договорах, документах, направляемых Банком в соответствии с Договорами.

Клиент вправе предоставить в Банк посредством Системы документы (копии документов), подписанные (заверенные) ЭП для целей идентификации и обновления сведений, проверки правоспособности Клиента и полномочий лиц, действующих от имени Клиента, в том числе при заключении/исполнении/прекращении Договора, а также иные документы, необходимые в целях принятия решения Банком о заключении Договора.

Клиент вправе предоставить в Банк посредством Системы документы, предусмотренные законодательством о кредитных историях, включая заявления и согласия, а также иные согласия, предусмотренные законодательством Российской Федерации и/или Договором.

При наличии технической возможности у Банка заявление (оферта Клиента/акцепт оферты Банка) на заключение соглашения об использовании системы электронного документооборота «ГПБ Бизнес-Онлайн» и заявления о регистрации/блокировке уполномоченного лица Клиента могут быть направлены Клиентом в Банк с использованием Системы «ГПБ Бизнес-Онлайн». В этом случае заявление (оферта Клиента/акцепт оферты Банка) на заключение соглашения об использовании системы электронного документооборота «ГПБ Бизнес-Онлайн» и заявления о регистрации/блокировке уполномоченного лица Клиента должны быть подписаны Электронной подписью уполномоченного лица Клиента, полученной в соответствии с Регламентом, либо Регламентом Доверенного УЦ. Порядок использования Электронной подписи в Системе «ГПБ Бизнес-Онлайн» и осуществления всех иных действий Сторон в указанном в настоящем абзаце случае аналогичны порядку, установленному условиями Соглашения.

2.2. Для реализации Услуги, предусмотренной пунктом 2.1 Соглашения, Банк предоставляет Клиенту логин и пароль для входа в Систему «Клиент-Банк.WEB»³.

2.3. Стороны договорились о том, что используемые во взаимоотношениях между Банком и Клиентом ЭД, подписанные посредством ЭП, признаются Сторонами равнозначными документам, подписанным собственноручными подписями на бумажных носителях, и порождают аналогичные им права и обязанности Сторон.

2.4. ЭД порождает обязательства Сторон, если он оформлен передающей Стороной, подписан ЭП, зашифрован и направлен принимающей Стороне, а принимающей Стороной – принят, расшифрован и подтверждена подлинность ЭП данного ЭД. Свидетельством того, что подтверждена подлинность ЭП данного ЭД, являются Статусы «Распечатан» – для ЭД валютного контроля, «Принят» – для остальных ЭД в Системе «Клиент-Банк.WEB».

2.5. Стороны признают используемые ими в соответствии с Соглашением Средства ЭП достаточными для установления лица, подписавшего ЭД (авторство ЭД), и невозможность внесения в него изменений (неизменность содержания ЭД).

2.6. Обмен ЭД осуществляется по открытым каналам связи с использованием СКЗИ.

3. ПОРЯДОК ЗАКЛЮЧЕНИЯ СОГЛАШЕНИЯ

3.1. Для заключения Соглашения Клиент предоставляет в Банк Заявление об акцепте Условий соглашения о предоставлении услуги стандартного электронного документооборота по форме приложения № 1 к Соглашению (далее – Заявление об акцепте) либо Заявление на

³ В случае если ранее Клиенту были предоставлены пароль и логин для входа в Систему «Клиент-Банк.WEB» на основании соглашения об электронном документообороте с использованием отдельных модулей Системы «Клиент-Банк.WEB» и при наличии у Банка технической возможности, после присоединения Клиента к настоящему Соглашению могут использоваться ранее предоставленные пароль и логин. В случае использования ранее предоставленных логина и пароля повторно пароль и логин не предоставляются. Указанный порядок не действует, если соглашения об электронном документообороте с использованием отдельных модулей Системы «Клиент-Банк.WEB» прекратило действие до момента присоединения Клиента к настоящему Соглашению.

заключение ДБС / Заявления на комплексное банковское обслуживание (при условии заключения договора банковского счета на основании такого заявления):

3.1.1. Заявление об акцепте заполняется на бумажном носителе, подписывается собственноручной подписью уполномоченного лица Клиента и подается им в офис Банка по обслуживанию Клиентов в двух экземплярах (пункт 2.1 Заявления об акцепте). Акцепт считается полученным Банком с даты регистрации Заявления об акцепте в Банке. Регистрация Банком Заявления об акцепте проводится путем проставления на нем отметки Банка с указанием номера и даты заключенного с Клиентом Соглашения. Банк передает Клиенту второй экземпляр Заявления, содержащего номер и дату зарегистрированного Заявления.

3.1.2. Заявление об акцепте может быть подано в Банк в электронной форме. В таком случае Заявление об акцепте заполняется уполномоченным лицом Клиента в электронной форме, подписывается ЭП уполномоченного лица Клиента в порядке, предусмотренном Соглашением о предоставлении услуг стандартного электронного документооборота с использованием Системы «Клиент-Банк», ранее заключенному между Банком и Клиентом, и направляется в Банк. Заявление об акцепте, поданное в порядке, предусмотренном настоящим пунктом, считается равнозначным Заявлению об акцепте, поданном на бумажном носителе.

3.1.3. Для заключения Соглашения на основании:

3.1.3.1. Заявления на заключение ДБС в таком заявлении должен быть заполнен раздел «Подключение к системе «Клиент-Банк.WEB»; Заявление на заключение ДБС заполняется на бумажном носителе, подписывается собственноручной подписью уполномоченного лица Клиента и подается уполномоченным лицом Клиента в офис Банка по обслуживанию Клиентов в одном экземпляре. Акцепт Клиента на заключение Соглашения, выраженный в указанном заявлении, считается полученным Банком с даты регистрации в Банке заключенного с Клиентом Соглашения;

3.1.3.2. Заявления на комплексное банковское обслуживание в таком заявлении должен быть заполнен раздел «Предоставление услуг стандартного электронного документооборота Система «Клиент-Банк.WEB». Заявление на комплексное банковское обслуживание заполняется на бумажном носителе, подписывается собственноручной подписью уполномоченного лица Клиента и подается в офис Банка по обслуживанию Клиентов. Акцепт Клиента на заключение Соглашения, выраженный в указанном заявлении, считается полученным Банком с даты регистрации в Банке заключенного с Клиентом Соглашения.

3.2. «Условия предоставления Банком ГПБ (АО) услуги стандартного электронного документооборота Система «Клиент-Банк.WEB» указаны в приложении № 2 к Соглашению (далее – Условия) и определяют условия предоставления услуг, связанных с использованием Системы «Клиент-Банк.WEB» и Мобильного приложения.

3.3. Подписание и предоставление Клиентом в Банк Заявления об акцепте, либо Заявления на заключение ДБС / Заявления на комплексное банковское обслуживание означает согласие Клиента присоединиться к Соглашению в целях получения от Банка Услуги на Условиях, предусмотренных Соглашением.

3.4. Клиент подтверждает Банку, что в течение срока действия Соглашения у Владельцев сертификата ключа проверки ЭП имеются полномочия на подписание от имени Клиента соответствующих ЭД, предусмотренных Соглашением и/или Договорами, в том числе Заявления об акцепте, предусмотренного подпунктом 3.1.2 Соглашения, акцепта оферты Банка, предусмотренного абзацем шестым пункта 2.1 Соглашения.

4. ОСНОВНЫЕ УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ

4.1. При использовании Клиентом УНЭП необходимым условием предоставления Клиенту Услуги является присоединение Клиента к Регламенту. Клиент подтверждает факт

присоединения к Регламенту в заявлении на изготовление Сертификата ключа проверки ЭП. При обмене ЭД в соответствии с Соглашением Стороны руководствуются положениями Регламента.

4.2. Для подключения к Системе «Клиент-Банк.WEB» Клиент предоставляет в Банк Заявку по форме приложения № 3 к Соглашению в одном экземпляре и документы, подтверждающих полномочия на подписание Соглашения, если указанные документы ранее не предоставлялись в Банк. Если Соглашение заключается на основании Заявления на заключение ДБС / Заявления на комплексное банковское обслуживание, то предоставление в Банк Заявки по форме приложения № 3 к Соглашению не требуется.

4.3. Клиент самостоятельно и за свой счет обеспечивает наличие программно-аппаратных средств согласно Условиям.

4.4. Клиент самостоятельно и за свой счет обеспечивает получение услуг связи, необходимых для обмена ЭД с использованием Системы «Клиент-Банк.WEB».

4.5. Клиент за свой счет поддерживает в рабочем состоянии программно-аппаратные средства, обеспечивающие доступ Клиента к Системе «Клиент-Банк.WEB», восстанавливает доступ к Системе «Клиент-Банк.WEB», нарушенный по его вине.

4.6. Банк осуществляет прием ЭД от Клиента круглосуточно, за исключением, случаев приостановления, установленных Соглашением. Банк может приостановить прием ЭД для проведения профилактических работ без предварительного уведомления Клиента.

4.7. Стороны определили, что Доверенными УЦ, выдающими сертификаты ключей проверки УКЭП, в целях использования в Системе «Клиент-Банк.WEB» являются удостоверяющие центры, перечисленные в приложении № 6 к Соглашению (далее – Перечень Доверенных УЦ).

4.8. Наименование Мобильного приложения может отличаться в зависимости от Мобильного устройства Клиента и доводится до его сведения Банком посредством Системы «Клиент-Банк.WEB» и/или в Тарифах Банка и/или посредством СМС-сообщения Клиенту на Номер телефона Клиента и/или иным доступным Банку способом. В случае одновременного использования Клиентом Мобильных приложений с разными наименованиями, установленных на одно или несколько Мобильных устройств, Клиент признает действительность всех совершенных им действий с использованием каждого Мобильного приложения.

5. ОБЯЗАННОСТИ СТОРОН

5.1. Стороны обязуются:

5.1.1. При исполнении условий Соглашения руководствоваться действующим законодательством Российской Федерации и нормативными актами Банка России, а также условиями заключенных Договоров.

5.1.2. Принимать к исполнению полученные ЭД, если получатель успешно расшифровал полученные ЭД, а ЭП документов соответствуют ЭП зарегистрированных Владельцев сертификатов ключей проверки ЭП.

5.1.3. Не разглашать третьей стороне (за исключением случаев, предусмотренных законодательством Российской Федерации или соглашениями Сторон) способы защиты информации, реализованные в используемой Системе «Клиент-Банк.WEB».

5.1.4. Обеспечивать конфиденциальность действующей парольной и ключевой информации, используемой для разграничения доступа в Систему «Клиент-Банк.WEB», шифрования данных и подтверждения авторства ЭД.

5.1.5. Организовать внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность доступа к программно-аппаратным средствам Системы «Клиент-Банк.WEB» лицам, не имеющим допуска к работе с ней, и использования паролей доступа и ключей системы защиты информации не уполномоченными на то лицами.

5.1.6. Выполнять технические требования к Системе «Клиент-Банк.WEB» согласно разделу 3 «Требования к программно-техническим средствам Клиента» Условий.

5.1.7. Предоставлять другой Стороне по ее требованию надлежащим образом оформленные и удостоверенные уполномоченным лицом ЭД на бумажном носителе.

5.2. Банк обязуется:

5.2.1. Зарегистрировать Клиента в Системе «Клиент-Банк.WEB» в порядке и на условиях, предусмотренных Соглашением.

5.2.2. Ежедневно осуществлять прием от Клиента и передачу Клиенту ЭД в Системе «Клиент-Банк.WEB».

5.2.3. Устанавливать Статусы о приеме от Клиента ЭД в Системе «Клиент-Банк.WEB». При наличии ошибок ЭД не принимается, а для Клиента устанавливается Статус с отказом.

5.2.4. Предоставлять Клиенту информацию о размещении Мобильного приложения одним из способов, указанных в п. 4.8 Соглашения.

5.2.5. Принять все необходимые меры для предотвращения несанкционированного/неправомерного доступа третьих лиц к Мобильному устройству, а также к конфиденциальной информации, связанной с использованием Клиентом Мобильного приложения.

5.2.6. Не разглашать и не передавать третьим лицам информацию, переданную (полученную) Клиентом с использованием Системы «Клиент-Банк.WEB», Мобильного приложения, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.2.7. Не направлять через Мобильное приложение ЭД, содержащие компьютерные вирусы и вредоносные программы.

5.2.8. Информировать Клиента о приеме, исполнении или отказе в приеме ЭД, в том числе об исполнении ЭД, предусматривающих совершение операций по счету(-ам), путем присвоения соответствующего статуса ЭД в Системе «Клиент-Банк.WEB» и Мобильном приложении, а также информировать Клиента о приостановлении приема/отправки ЭД в Системе «Клиент-Банк.WEB» и Мобильном приложении по основаниям, предусмотренным Соглашением, путем направления соответствующего уведомления (с указанием причины) в Системе «Клиент-Банк.WEB».

5.3. Клиент обязуется:

5.3.1. Ознакомиться с «Рекомендациями по обеспечению информационной безопасности в Системе «Клиент-Банк.WEB», приведенными в приложении № 4 к Соглашению (далее – Рекомендации). При этом Клиент понимает и, безусловно, принимает на себя риски, связанные с использованием Системы «Клиент-Банк.WEB» без соблюдения мер, указанных в Рекомендациях и несет ответственность за несоблюдение требований, указанных в Рекомендациях.

5.3.2. Производить выплату Банку комиссионного вознаграждения за предоставление услуги в соответствии с Тарифами, с которыми Клиент ознакомлен и согласен.

5.3.3. В течение 3 (Трех) рабочих дней с даты направления Клиентом в Банк посредством Системы «Клиент-Банк.WEB» уведомления о начале работы в Системе «Клиент-Банк.WEB» оплатить стоимость предоставления Банком Клиенту программного обеспечения Системы «Клиент-Банк.WEB».

5.3.4. Использовать Систему «Клиент-Банк.WEB» только на исправном и проверенном на отсутствие компьютерных вирусов оборудовании.

5.3.5. Не передавать третьим лицам логин и пароль для входа в Систему «Клиент-Банк.WEB» и используемые СКЗИ.

5.3.6. Ежедневно осуществлять прием от Банка ЭД и информационных сообщений, а также знакомиться с поступившим от Банка ЭД, иными уведомлениями, а также со статусами ЭД

в Системе «Клиент-Банк.WEB» и Мобильном приложении не позднее дня их получения или обновления в Системе «Клиент-Банк.WEB» и Мобильном приложении.

5.3.7. За собственный счет поддерживать в рабочем состоянии программно-технические средства Клиента, обеспечивающие функционирование Системы «Клиент-Банк.WEB».

5.3.8. При смене Владельцев сертификатов ключей проверки ЭП, прекращении полномочий у Владельцев сертификатов ключей проверки ЭП, а также изменении местонахождения организации, правового статуса, номеров телефонов (включая мобильные телефоны), внесения изменений и дополнений в учредительные документы письменно сообщать Банку об этом одним из способов, указанным в пункте 11.1 Соглашения в течение 3 (Трех) рабочих дней. При смене Владельцев сертификатов ключей проверки ЭП, прекращении полномочий, инициировать формирование новых Ключей ЭП и Сертификатов ключей проверки ЭП в соответствии с Регламентом (для УНЭП) или Регламентом Доверенного УЦ (для УКЭП) или Соглашением (для УНЭП (MyDSS)).

До поступления сообщения об указанных изменениях все действия, совершенные по ранее указанным Клиентом реквизитам, считаются совершенными законно и засчитываются как выполнение Сторонами своих обязательств.

5.3.9. Контролировать срок действия Ключей ЭП и Сертификатов ключей проверки ЭП и заблаговременно инициировать их замену.

5.3.10. Незамедлительно информировать Банк о прекращении (изменении) полномочий у Владельцев сертификатов ключей проверки ЭП. Предоставлять в Банк до окончания срока полномочий Владельцев сертификатов ключей проверки ЭП документы, подтверждающие продление соответствующих полномочий. До предоставления документов, подтверждающих наличие полномочий у Владельцев сертификатов ключей проверки ЭП, не направлять в Банк ЭД, подписанные их ЭП.

5.3.11. В случае прекращения действия Соглашения уничтожить ключи ЭП, относящиеся к Соглашению за исключением случаев, когда:

- между Клиентом и Банком заключено соглашение об использовании системы электронного документооборота «ГПБ Бизнес-Онлайн»;
- пользователи, зарегистрированные в Системе «Клиент-Банк.WEB», могут выполнять вход в Систему «ГПБ Бизнес-Онлайн» по логину/паролю для входа в Систему «Клиент-Банк.WEB» и с использованием сертификата ключа проверки электронной подписи, используемой ими в Системе «Клиент-Банк.WEB».

5.3.12. Клиент обязуется не использовать Систему «Клиент-Банк.WEB» за пределами таможенной границы Российской Федерации.

5.3.13. Клиент обязан предоставить сведения и документы, необходимые для идентификации уполномоченных Клиентом лиц (включая Владельцев сертификатов ключей проверки ЭП), в том числе при смене Владельцев сертификатов ключей проверки ЭП, в случае, если ранее такие сведения и документы в Банк не предоставлялись.

5.3.14. Клиент обязан предоставлять информацию и документы, запрашиваемые Банком в соответствии с требованиями законодательства Российской Федерации в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

5.3.15. В случае наступления или возникновения угрозы наступления любого из событий, создающих Компрометацию ключей Клиента, уведомить Банк в день возникновения такого события или его угрозы одним из предусмотренных в подпункте 11.1.1 Соглашения способов.

5.3.16. Подтверждать актуальность предоставленных Банку контактных телефонов и адресов электронной почты для экстренной связи не реже, чем один раз в три месяца одним из способов, предусмотренных в подпункте 11.1.1 Соглашения, либо при смене контактного лица.

5.3.17. Хранить и использовать логин и пароль для входа в Мобильное приложение, а также в Мобильное устройство таким образом, чтобы исключить к ним доступ любых третьих лиц. В случае если третьи лица получили доступ к Мобильному устройству или Мобильному приложению или Клиент предполагает, что третьи лица получили доступ к Мобильному устройству или Мобильному приложению, Клиент обязуется незамедлительно уведомить Банк посредством Системы «Клиент-Банк.WEB» или путем обращения в офис, в котором Клиент находится на обслуживании.

5.3.18. В случае утраты Мобильного устройства, а также в случае появления у Клиента подозрений в его Компрометации немедленно информировать об этом Банк.

5.3.19. Не раскрывать третьим лицам информацию, которая может быть использована для доступа к Мобильному приложению и совершения с его использованием операций. Немедленно уведомить Банк обо всех случаях доступа или предполагаемой возможности доступа третьих лиц к указанной информации.

5.3.20. Соблюдать меры безопасности при использовании Мобильного приложения, указанные в приложении № 5 к Соглашению.

5.3.21. Предпринимать все необходимые действия для исключения возможности присутствия на Мобильном устройстве с установленным Мобильным приложением вредоносного программного обеспечения. Клиент несет полную ответственность за операции, проведенные с его Мобильного устройства в результате компрометации критичных платежных данных вредоносным программным обеспечением, установленным на Мобильное устройство с санкции или без таковой со стороны Клиента.

6. ПРАВА СТОРОН

6.1. Банк имеет право:

6.1.1. Ежемесячно взимать со счетов Клиента без его дополнительного распоряжения комиссионное вознаграждение за предоставление Услуги в соответствии с Тарифами, с которыми Клиент ознакомлен и согласен. Комиссионное вознаграждение взимается Банком за каждый полный и неполный месяц предоставления услуги.

6.1.2. Производить замену требований к аппаратно-программным средствам Клиента, форматов и списка ЭД, а также Перечня Доверенных УЦ. В случае замены требований к аппаратно-программным средствам Клиента, форматов и списка ЭД Банк обязан сообщением по Системе «Клиент-Банк.WEB» или иным способом, определенным Соглашением, известить Клиента о предстоящих изменениях не менее чем за 10 (Десять) календарных дней. Банк вправе в одностороннем порядке вносить изменения в Перечень Доверенных УЦ, отвечающих требованиям Банка, о чем Банк уведомляет Клиента одним из способов, указанных в пункте 10.2 или 11.1.2 Соглашения.

6.1.3. Изменять, отменять, дополнять в одностороннем порядке Тарифы с предварительным уведомлением Клиента за 10 (Десять) календарных дней путем направления сообщения по Системе «Клиент-Банк.WEB» или иным способом, определенным в подпункте 11.1.2 Соглашения (по выбору Банка).

6.1.4. Приостанавливать прием и отправку любого ЭД по Системе «Клиент-Банк.WEB» и Мобильному приложению (использование Системы «Клиент-Банк.WEB») в случае неисполнения Клиентом обязательств по уплате Банку комиссионного вознаграждения за предоставление Услуги, о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины).

При этом Клиент не освобождается от обязанности уплачивать Банку комиссионное вознаграждение за предоставление Услуги в соответствии с Тарифами, когда такое приостановление произошло в соответствии с условиями Соглашения.

6.1.5. Возобновить прием и отправку ЭД по Системе «Клиент-Банк.WEB» (использование Системы «Клиент-Банк.WEB») не позднее рабочего дня, следующего после дня уплаты Клиентом Банку комиссионного вознаграждения за предоставление Услуги.

6.1.6. Приостанавливать прием и отправку ЭД Клиента по Системе «Клиент-Банк.WEB» и Мобильному приложению (использование Системы «Клиент-Банк.WEB» (в том числе с использованием Мобильного приложения)), о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины):

- до предоставления в Банк надлежаще оформленных документов, подтверждающих наличие полномочий у Владельцев сертификатов ключей проверки ЭП;
- до момента регистрации новых Владельцев сертификатов ключей проверки ЭП в случае смены уполномоченных лиц Клиента;
- в случаях, указанных в подпункте 6.1.8 Соглашения.

6.1.7. Расторгнуть Соглашение в одностороннем порядке, предупредив об этом Клиента одним из способов, указанных в подпункте 11.1.2 Соглашения, не менее чем за 3 (Три) календарных дня до даты расторжения.

6.1.8. Отказать в приеме и отправке ЭД по Системе «Клиент-Банк.WEB» и Мобильному приложению:

- в случае непредоставления Клиентом по запросу Банка документов, необходимых Банку для исполнения требований законодательства Российской Федерации в сфере противодействия легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма,
- в случае непредоставления Клиентом по запросу Банка документов, необходимых Банку для исполнения требований законодательства Российской Федерации в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- в случае, если у Банка возникают подозрения, что операции осуществляются Клиентом с целью легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения, а также в иных случаях, предусмотренных законодательством Российской Федерации".

6.1.9. Возобновить использование Системы «Клиент-Банк.WEB» / прием и отправку ЭД по Системе «Клиент-Банк.WEB» и Мобильному приложению, приостановленных в соответствии с подпунктом 6.1.6 Соглашения, в случае получения Банком от Клиента документов, надлежащим образом подтверждающих полномочия Владельцев сертификатов ключей проверки ЭП (уполномоченных лиц Клиента).

6.1.10. Приостановить использование Клиентом Системы «Клиент-Банк.WEB» в день получения от Клиента уведомления о Компрометации ключей Клиента, предусмотренного подпунктом 5.3.15 Соглашения, о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины).

6.1.11. Возобновить доступ Клиента к Системе «Клиент-Банк.WEB», приостановленный согласно подпункту 6.1.10 Соглашения, не позднее следующего рабочего дня после проведения Клиентом процедуры внеплановой смены Ключей ЭП.

6.1.12. Запрашивать и получать от Клиента и получать копии ЭД на бумажном носителе, оформленные надлежащим образом и удостоверенные уполномоченным лицом Клиента.

6.1.13. Определять перечень сервисов/услуг, доступных Клиенту для использования в Системе «Клиент-Банк.WEB» и Мобильном приложении, а также условия их использования.

6.1.14. Проводить обновление Системы «Клиент-Банк.WEB» и Мобильного приложения.

6.1.15. Не осуществлять техническую поддержку Мобильного приложения, версия которого ниже версии предыдущего Мобильного приложения, выпущенного Банком.

6.1.16. Отказывать в установке, обновлении и работоспособности Мобильного приложения на Мобильном устройства, версия операционной системы которого устарела.

6.1.17. Устанавливать лимиты в отношении размера, количества и периодичности совершения операций по Счету, распоряжения на совершение которых подписываются УНЭП MyDSS Клиента (уполномоченного представителя Клиента), путем опубликования таких лимитов на сайте Банка, или в Системе «Клиент-Банк.WEB», или путем уведомления Клиента иным способом, предусмотренным Соглашением. В случае превышения Клиентом установленных Банком лимитов, Банк вправе отказать в приеме к исполнению распоряжений, подписанных УНЭП MyDSS Клиента (уполномоченного представителя Клиента). При этом Клиент (уполномоченный представитель Клиента) в таком случае вправе подать в Банк через Систему «Клиент-Банк.WEB» распоряжение о совершении операции по Счету, подписанное УКЭП или УНЭП Клиента (уполномоченного представителя Клиента).

6.1.18. Отказать в приеме и отправке ЭД по Мобильному приложению в связи с прекращением доступа к Системе «Клиент-Банк.WEB» посредством Мобильного приложения по инициативе Банка, о чем Банк направляет Клиенту соответствующее уведомление (с указанием причины и даты прекращения доступа к Системе «Клиент-Банк.WEB» посредством Мобильного приложения).

Прекращение доступа к Системе «Клиент-Банк.WEB» посредством Мобильного приложения не прекращает доступ к Системе «Клиент-Банк.WEB».

6.2. Клиент имеет право:

6.2.1. Запрашивать и получать от Банка разъяснения по вопросам использования Системы «Клиент-Банк.WEB» и Мобильного приложения.

6.2.2. Запрашивать и получать от Банка копии ЭД на бумажном носителе.

6.3. Клиент на весь период действия Соглашения дает согласие (заранее данный акцепт) и предоставляет безусловное и безотзывное право Банку списывать со счетов Клиента, открытых в Банке, суммы комиссионного вознаграждения за предоставление Услуги в соответствии с Тарифами на основании расчетных документов, предусмотренных законодательством Российской Федерации (в том числе на основании банковского ордера), без дополнительных распоряжений Клиента. Заранее данный акцепт дается без ограничения по сумме с возможностью частичного исполнения распоряжений.

6.4. Банк, имеющий право на использование СКЗИ и имеющий право предоставлять третьим лицам право на использование СКЗИ на основании лицензионного соглашения, заключенного Банком с правообладателями СКЗИ, предоставляет Клиенту с даты заключения Соглашения право использования СКЗИ на следующих условиях:

6.4.1. Право использования СКЗИ предоставляется Клиенту без взимания дополнительного вознаграждения (комиссии) с даты заключения Соглашения и действует в течение срока действия Соглашения.

6.4.2. Право использования СКЗИ предоставляется Клиенту на условиях простой (неисключительной) лицензии только для целей создания ЭП, проверки ЭП и отсутствия искажений в ЭД, создания ключа ЭП и ключа проверки ЭП, а также для целей шифрования и расшифрования ЭД, передаваемых в рамках Системы ЭДО.

6.4.3. Право использования СКЗИ, предоставляемое Клиенту по Соглашению, предусматривает возможность использовать СКЗИ по функциональному назначению, за исключением действий, указанных в подпункте 6.4.5 Соглашения.

6.4.4. Копирование СКЗИ допускается при условии, что копия предназначается только для архивных целей и при необходимости (в случае, когда оригинал утерян, уничтожен или стал непригодным для использования) для замены правомерно полученного экземпляра СКЗИ с обязательным сохранением в каждой воспроизведенной копии СКЗИ наименования правообладателя.

6.4.5. Полученное Клиентом право использования СКЗИ не включает права на:

- передачу СКЗИ третьим лицам;
- распространение СКЗИ;
- модифицирование и декомпилирование программных компонентов СКЗИ;
- иное использование СКЗИ, прямо не предусмотренное Соглашением.

6.4.6. Банк предоставляет Клиенту информацию о лицензии программного обеспечения СКЗИ «Крипто-ПРО CSP» посредством СМС-сообщения (на номер сотовой связи, указанный Клиентом в Заявке или Заявлении на заключение ДБС / Заявлении на комплексное банковское обслуживание), а Клиент подтверждает получение указанной информации направлением в Банк посредством Системы «Клиент-Банк.WEB» уведомления о начале работы в Системе «Клиент-Банк.WEB», составленного по форме Банка (в электронной форме) и подписанного ЭП. Клиент заявляет и гарантирует, что Владелец сертификата ключа проверки ЭП подписавший и направивший в Банк указанное уведомление надлежащим образом уполномочено на это Клиентом.

6.5. Клиент самостоятельно выбирает организацию провайдера, обеспечивающую доступ к сети Интернет. Все расходы, связанные с подключением к сети Интернет, эксплуатацией и обменом данными с Банком через сеть Интернет, осуществляются Клиентом за счет собственных средств и не входят в стоимость услуг Банка.

6.6. Клиент соглашается, что сеть Интернет не является безопасной средой, и соглашается нести все риски, связанные с подключением его оборудования (в том числе компьютерного, Мобильных устройств) к сети Интернет. Клиент обязан самостоятельно обеспечивать защиту данного оборудования от вредоносного кода, несанкционированного доступа к нему третьих лиц, вирусных атак из сети Интернет и локальных вычислительных сетей.

6.7. Стороны признают, что Мобильное приложение обеспечивает достаточный уровень защиты информации от несанкционированного доступа при приеме, передаче, обработке и хранении ЭД и иных сведений, а также является каналом связи, однозначно подтверждающим авторство, направленных с его использованием ЭД и иных сведений.

6.8. Клиент (уполномоченный представитель Клиента) в целях регулирования взаимоотношений, возникающих при использовании Системы «Клиент-Банк.WEB» и Мобильного приложения, поручает Банку:

- создать и хранить Ключ УНЭП (MyDSS) с обеспечением его защиты от компрометации и/или несанкционированного использования;
- сформировать УНЭП (MyDSS) при помощи указанного Ключа УНЭП (MyDSS) по настоящему поручению Клиента;
- информировать Клиента (уполномоченного представителя Клиента) об использовании Ключа УНЭП (MyDSS).

6.9. Отказаться от обслуживания с использованием Мобильного приложения.

Банк прекращает предоставление Услуги при использовании Мобильного приложения при отказе Клиента от использования Мобильного приложения путем его удаления со всех Мобильных устройств и блокировки Банком доступа в Мобильное приложение на основании письменного заявления Клиента (в свободной форме).

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по Соглашению в соответствии с законодательством Российской Федерации и настоящим Соглашением.

7.2. Банк не несет ответственность за убытки, причиненные Клиенту в случаях, предусмотренных Соглашением, в том числе:

7.2.1. В связи с Компрометации ключей Клиента.

7.2.2. Исполнения ЭД Клиента, подписанного ЭП в случае использования Системы «Клиент-Банк.WEB» и Ключей ЭП неуполномоченными лицами Клиента.

7.2.3. Реализации на стороне Клиента угроз несанкционированного доступа к Системе «Клиент-Банк.WEB», включая угрозы воздействия вредоносного программного обеспечения из сетевого окружения компьютера(-ов) Клиента.

7.2.4. Действий третьих лиц, предоставляющих услуги связи.

7.2.5. Приостановления Банком оказания Услуги в случаях, предусмотренных подпунктами 6.1.4, 6.1.6 и 6.1.8 Соглашения.

7.2.6. За ущерб перед Клиентом, возникший вследствие нарушения системы защиты информации не по вине Банка, в том числе в результате вирусного заражения используемых Клиентом в дистанционном банковском обслуживании электронных устройств (персонального компьютера, смартфона, планшета и т.п.) вредоносным кодом или несанкционированного доступа к нему третьих лиц.

7.2.7. За сбои работы Системы «Клиент-Банк.WEB» и/или Мобильного приложения, связанные с неработоспособностью оборудования Клиента по любым причинам, в том числе при проведении Банком профилактических работ по модернизации Системы «Клиент-Банк.WEB» и/или Мобильного приложения.

7.2.8. За последствия исполнения ЭД Клиента, переданного в Банк в случае использования Мобильного устройства Клиента неуполномоченным лицом.

7.2.9. За неработоспособность оборудования (в том числе компьютерного) и программных средств Клиента и третьих лиц, повлекшую за собой невозможность доступа Клиента к Системе «Клиент-Банк.WEB» и/или Мобильному приложению, и возникшие в результате задержки в осуществлении операций в Системе «Клиент-Банк.WEB» и/или Мобильном приложении.

7.2.10. За ущерб, возникший вследствие нарушения системы защиты информации не по вине Банка, в том числе в результате вирусного заражения Мобильного устройства.

7.2.11. В случае утери/передачи третьим лицам (в том числе на обозрение) Клиентом Мобильного устройства и/или средств доступа к Мобильному приложению.

7.2.12. Действия или бездействия оператора сотовой связи и/или интернет провайдера, либо иного третьего лица, при осуществлении Клиентом доступа к Системе «Клиент-Банк.WEB» при помощи Мобильного устройства и Мобильного приложения.

7.3. Клиент несет ответственность:

7.3.1. За исполнение своих обязательств, предусмотренных Соглашением

7.3.2. За убытки, возникшие вследствие разглашения или передачи третьей стороне Ключей ЭП.

7.3.3. За своевременность, достоверность и действительность предоставляемых сведений и информации.

7.3.4. За все действия и операции, проводимые Клиентом с использованием Системы «Клиент-Банк.WEB» и Мобильного приложения.

7.3.5. До получения Банком уведомления Клиента об утрате Мобильного устройства или компрометации средств доступа к Мобильному приложению Клиент несет ответственность за все операции, совершенные третьими лицами через Мобильное приложение, а также за убытки, которые могут возникнуть в результате его использования.

7.4. Любая просрочка в выполнении Банком своих обязательств по Соглашению, которая произошла вследствие невыполнения Клиентом его обязательств по Соглашению, сбой программных и аппаратных средств Клиента, исключает ответственность Банка.

7.5. Клиент несет всю ответственность за использование Системы «Клиент-Банк.WEB» при изменении Владельцев сертификатов ключей проверки ЭП, назначенных Клиентом, до момента уведомления Клиентом Банка о произошедших изменениях.

Стороны признают, что до поступления от Клиента информации об указанных изменениях в соответствии с подпунктами 5.3.8–5.3.10 Соглашения, все действия, совершенные в соответствии с Соглашением в отношении ЭД, подписанных ЭП Владельцев сертификатов ключей, направленных Клиентом в Банк по Системе «Клиент-Банк.WEB», успешно принятые и расшифрованные Банком, считаются совершенными законно и поданными уполномоченными лицами Клиента.

7.6. Стороны не несут ответственность за какие-либо задержки, невозможность оказания Услуги, недостатки в процессе выполнения работ и исполнения обязательств по Соглашению, если такое неисполнение обусловлено обстоятельствами непреодолимой силы, в числе которых стихийные бедствия, забастовки, отказ оборудования систем связи, военные действия, решения федеральных, государственных, муниципальных органов, запрещения, а также любые иные обстоятельства, находящиеся вне разумного контроля Сторон, при условии незамедлительного уведомления.

8. ОСНОВНОЙ ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ И КОНФЛИКТОВ

8.1. Все разногласия, споры и конфликтные ситуации, возникающие между Сторонами вследствие неисполнения или ненадлежащего исполнения Соглашения, а также его заключения, изменения и расторжения разрешаются с учетом взаимных интересов Сторон путем переговоров. На время разрешения спорной ситуации Банк имеет право немедленно приостановить прием/отправку ЭД в одностороннем порядке, уведомив об этом Клиента по Системе «Клиент-Банк.WEB» или иным способом, определенным пунктом 11.1 Соглашения.

8.2. Спорные ситуации между Банком и Клиентом, связанные с использованием УНЭП в Системе «Клиент-Банк.WEB» и в Мобильном приложении разрешаются в порядке, определенном разделами 7 Условий.

9. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ И ПОРЯДОК ЕГО РАСТОРЖЕНИЯ

9.1. Соглашение считается заключенным с даты получения Банком акцепта Клиента согласно порядку, установленному разделом 3 Соглашения.

9.2. Обмен ЭД в Системе «Клиент-Банк.WEB» начинается с даты получения Банком посредством Системы «Клиент-Банк.WEB» уведомления Клиента о начале работы в Системе «Клиент-Банк.WEB».

ЭД, направленные ранее этой даты, не создают прав и обязанностей для Сторон, если иное не предусмотрено иным заключенным между Сторонами соглашением.

9.3. Соглашение действует с даты его заключения до 31 декабря текущего года включительно. В случае если ни одна из Сторон не заявит о желании расторгнуть Соглашение не менее чем за 3 (Три) календарных дня до даты окончания срока его действия, Соглашение считается пролонгированным до 31 декабря включительно следующего календарного года. Пролонгация Соглашения в порядке, установленном настоящим пунктом, осуществляется неограниченное количество раз.

9.4. Любая из Сторон вправе расторгнуть Соглашение в любое время, предупредив об этом другую Сторону письменно одним из способов, указанным в пункте 11.1 Соглашения, не менее чем за 3 календарных дня до предполагаемой даты расторжения Соглашения. До даты расторжения Соглашения Клиент обязан оплатить задолженность за оказанные Банком услуги.

Настоящим Стороны пришли к соглашению, что в случае закрытия последнего банковского счета Клиента, открытого в Банке, Соглашение считается расторгнутым в дату закрытия последнего банковского счета без уведомления Клиента. В случае невозможности списания задолженности за оказанные Банком услуги, Банк вправе направить Клиенту информацию о задолженности (с целью самостоятельного погашения Клиентом) одним из способов, указанных в подпункте 11.1.2 Соглашения.

9.5. Соглашение может быть расторгнуто по инициативе Банка, если в течение трех месяцев после его подписания Клиент не направил в Банк посредством Системы «Клиент-Банк.WEB» уведомление о начале работы в Системе «Клиент-Банк.WEB».

9.6. В случае если на момент присоединения Клиента к Соглашению между Сторонами действует соглашение о предоставлении услуг стандартного электронного документооборота с использованием Системы «Клиент-Банк», с даты заключения Соглашения соглашение о предоставлении услуг стандартного электронного документооборота с использованием Системы «Клиент-Банк» считается измененным и изложенным в редакции Соглашения.

10. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В СОГЛАШЕНИЕ

10.1. Банк вправе в одностороннем порядке вносить изменения в Соглашение и Условия, уведомив об этом всех лиц, присоединившихся к Соглашению, не позднее чем за 5 (Пять) календарных дней до вступления в силу указанных изменений. Указанный в настоящем пункте срок уведомления может быть уменьшен Банком в случае внесения изменений в Соглашение в связи с изменением законодательства Российской Федерации, а также в связи с введением дополнительных услуг для Клиента, о чем Банк уведомляет Клиента одним из способов, указанных в подпункте 11.1.2 Соглашения.

10.2. Банк уведомляет всех Клиентов, присоединившихся к Соглашению, о внесении в него изменений путем публикации информационного письма, а также полного текста изменений на информационных стендах во всех офисах Банка по обслуживанию клиентов – юридических лиц, а также на официальном сайте Банка www.gazprombank.ru. Дополнительно к указанному способу уведомления Банк по своему усмотрению может использовать иные способы информирования Клиента.

10.3. Действие изменений, внесенных в Соглашение, вступивших в силу, распространяется на всех Клиентов, присоединившихся к Соглашению, независимо от даты присоединения к Соглашению (даты заключения Соглашения). В случае несогласия с изменениями, вносимыми в Соглашение, Клиент вправе расторгнуть Соглашение до вступления таких изменений в силу в порядке, установленном в пункте 9.4 Соглашения.

10.4. В целях своевременного получения информации о внесении изменений в Соглашение Клиент обязан не реже одного раза в 5 (Пять) дней обращаться в Банк за получением указанной информации.

11. ПРОЧИЕ УСЛОВИЯ

11.1. Уведомления в рамках Соглашения могут быть направлены одним или несколькими из способов:

11.1.1. Клиентом Банку:

- по Системе «Клиент-Банк.WEB»;
- посредством Мобильного приложения;
- курьером под расписку ответственному представителю Банка;
- путем направления копии с использованием факсимильной связи или электронной почты с последующим представлением оригинала не позднее следующего рабочего дня;
- по почте заказным письмом.

11.1.2. Банком Клиенту:

- по Системе «Клиент-Банк.WEB»;
- посредством Мобильного приложения;
- под расписку уполномоченному представителю Клиента;
- путем помещения в абонентский ящик Клиента;
- по почте заказным письмом.

11.2. Для целей соблюдения досудебного порядка урегулирования спора, за исключением порядка урегулирования разногласий, предусмотренного разделами 7, 8 Условий и раздела 11 Регламента, Стороны определили:

11.2.1. Срок для рассмотрения Клиентом претензии Банка и для принятия мер по досудебному урегулированию такой претензии (в совокупности) составляет 20 (Двадцать) календарных дней от даты направления претензии Банком.

11.2.2. Срок для рассмотрения Банком претензии Клиента и для принятия мер по досудебному урегулированию такой претензии (в совокупности) составляет 20 (Двадцать) календарных дней от даты получения претензии.

11.2.3. Разногласия, по которым Стороны не достигли соглашения путем переговоров, подлежат разрешению в арбитражном суде в соответствии с действующим процессуальным законодательством Российской Федерации.

11.3. Все приложения к Соглашению являются его неотъемлемой частью.

Приложение № 1
к Соглашению о предоставлении услуги
стандартного электронного
документооборота Система «Клиент-
Банк.WEB»

Отметка о регистрации Заявления:

Соглашение о предоставлении услуги стандартного электронного
документооборота Система «Клиент-Банк.WEB»

№ _____ от «___» _____ 20__ г.

Работник Банка _____ / _____ /
Подпись Фамилия, инициалы

ЗАЯВЛЕНИЕ

**об акцепте условий соглашения о предоставлении услуги стандартного электронного
документооборота Система «Клиент-Банк.WEB»**

Наименование Клиента _____

В лице _____

действующего на
основании _____

Адрес местонахождения _____

ОГРН _____

ИНН _____

Почтовый адрес _____

Телефон / Факс _____

Адрес электронной почты _____

Контактное лицо _____

Настоящим:

1. Подтверждаю свои полномочия подписывать настоящее Заявление.

2. Заявляю:

- Отметьте один из вариантов
- 2.1. О своем присоединении к «Соглашению о предоставлении услуг стандартного электронного документооборота Система «Клиент-Банк.WEB» (далее – Соглашение) в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации и на Условиях предоставления Банком ГПБ (АО) услуги стандартного электронного документооборота с использованием системы «Клиент-Банк.WEB» фирмы – разработчика Общество с ограниченной ответственностью «Бэнкс Софт Системс».
- 2.2. О своей согласии с тем, что ранее заключенное соглашение о предоставлении услуг стандартного электронного документооборота с использованием Системы «Клиент-Банк» с даты подписания настоящего Заявления об акцепте и его регистрации Банком применяется Сторонами для использования системы «Клиент-Банк.WEB» фирмы – разработчика Общество с ограниченной ответственностью «Бэнкс Софт Системс» в редакции «Соглашения о предоставлении услуг стандартного электронного документооборота Система «Клиент-Банк.WEB» (далее – Соглашение).

Все положения Соглашения, включая взаимные права и обязанности сторон, а также порядок внесения изменений в Соглашение, мне понятны.

Все положения Условий предоставления Банком ГПБ (АО) услуги стандартного электронного документооборота, заявленных мною, включая требования к программно-техническим средствам, порядок подключения услуги и разрешения спорных ситуаций мне понятны.

С Рекомендациями по обеспечению информационной безопасности в Системе «Клиент-Банк.WEB» ознакомлен.

Настоящим заявляю о своей согласии с тем, что электронный документ, сформированный и подписанный электронной подписью с соблюдением требований Соглашения, имеет силу документа, составленного на бумажном носителе и подписанного собственноручной подписью.

От имени Клиента:

(Подпись)

_____ (Фамилия, инициалы руководителя Клиента)

М.П.

**УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ БАНКОМ ГПБ (АО)
УСЛУГИ СТАНДАРТНОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
СИСТЕМА «КЛИЕНТ-БАНК.WEB»**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Условия (далее – Условия) являются типовым формуляром Банка, являющимся неотъемлемой частью Соглашения о предоставлении услуг стандартного электронного документооборота Система «Клиент-Банк.WEB», и определяют условия предоставления Клиенту услуги стандартного электронного документооборота Система «Клиент-Банк.WEB» и Мобильного приложения фирмы-разработчика Общество с ограниченной ответственностью «Бэнкс Софт Системс» (далее – Услуга), а именно:

- ЭД, оборот которых предусмотрен Услугой;
- требования к программно-техническим средствам Клиента;
- обязанности Сторон при подключении к Системе «Клиент-Банк.WEB»;
- ЭД, оборот которых предусмотрен Мобильным приложением;
- организация работы с Мобильным приложением;
- порядок разрешения спорных ситуаций.

1.2. Условия являются публичными и распространяются Банком в открытых источниках, в том числе в сети Интернет.

2. СПИСОК ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В СИСТЕМЕ «КЛИЕНТ-БАНК.WEB»

В рамках Условий у Сторон возникают обязательства по приему/передаче в Системе «Клиент-Банк.WEB» ЭД (при условии, что прием и передача таких ЭД реализованы Банком):

№ п/п	Наименование ЭД
1	Поручения/требования о платежах в рублях
2	Поручения о переводах в валюте
3	Поручения о конвертации валют
4	Поручения/уведомления о списании/зачислении средств с/на транзитный валютный счет
5	Выписки по счетам в рублях и валюте и приложения к ним, запросы в Банк на получение выписки
6	Документы валютного контроля
7	Подтверждения по сделкам
8	Заявления о платежах (отзыв, акцепт, отказ от акцепта)
9	Документы свободного формата от Клиента в Банк и из Банка Клиенту
10	Запросы в Банк об изготовлении сертификатов ключей проверки ЭП
11	Заявление об акцепте Соглашения
12	Иные документы, предусмотренные Договорами
13	Договоры, заявления на заключение Договоров (оферты), заявления об акцепте Договоров, направляемые с использованием Документов свободного формата

Банк осуществляет информирование Клиента о совершаемых/совершенных операциях по банковским счетам посредством Системы (путем изменения статуса обработки ЭД, указанных в настоящем разделе).

3. ТРЕБОВАНИЯ К ПРОГРАММНО-ТЕХНИЧЕСКИМ СРЕДСТВАМ КЛИЕНТА

3.1. При использовании Системы «Клиент-Банк.WEB» и Мобильного приложения к аппаратному обеспечению Клиента предъявляются следующие требования:

Содержание требования
к Компьютеру
Процессор не ниже Pentium 166
Объем оперативной памяти от 32 Мб
Объем свободного места на жестком диске на менее 50 Мб
Прямой доступ в интернет с шириной канала 512 кб/с и выше
Видеосистема, обеспечивающая область экрана не менее 1024x768 пикселей
к Мобильному устройству
Смартфон с предустановленной производителем устройства операционной системой IOS или Android

3.2. При использовании Системы «Клиент-Банк.WEB» и Мобильного приложения к стороннему программному обеспечению (ПО) Клиента предъявляются следующие требования:

Вид ПО	Наименование ПО	Версии ПО		Примечания
		Рекомендовано	Поддерживается	
ОС	Windows		Windows 8 x86 и x64 (Windows 8, Windows 8 Pro, Windows 8 Enterprise)	
Веб-браузер	Microsoft Internet Explorer	9.0, 10.0, 11.0		
	Mozilla Firefox	3.0.x, 3.5.x, 3.6.x, 24.0		
	Opera	9.50, 10, 10.10, 10.53, Next 17.x		
	Google Chrome	29.x		
Текстовый процессор	Microsoft Word	2003, 2007, 2010		Не обязательно. Для чтения RTF- файлов документов, сформированных с помощью подсистемы
	OpenOffice		2.3.0, 3.0, 3.3	
Редактор электронных таблиц	Microsoft Excel	2003, 2007, 2010		
ПО для работы с документацией	Adobe Reader, Adobe Acrobat Standart, Adobe	5.0 и выше		Необходимо для чтения документации подсистемы

Вид ПО	Наименование ПО	Версии ПО		Примечания
		Рекомендовано	Поддерживается	
	Acrobat Professional			
ПО для Мобильного устройства	Android	5.x и выше		
	iOS	iOS 11 и выше		
	1. На Мобильном устройстве установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение 2. Мобильное устройство не подвергнуто операциям повышения привилегий/взлома операционной системы устройства (jail-break, rooting) 3. Не допускается использование устройств Android с разблокированным загрузчиком (unlocked bootloader) (при наличии технической возможности)			

4. ОБЯЗАННОСТИ СТОРОН ПРИ ПОДКЛЮЧЕНИИ К СИСТЕМЕ «КЛИЕНТ-БАНК.WEB»

4.1. Для подключения к Системе «Клиент-Банк.WEB» Клиенту необходимо предоставить в Банк (в любой офис Банка по обслуживанию клиентов-юридических лиц) Заявку на подключение к системе «Клиент-Банк.WEB» по форме приложения № 3 к Соглашению (далее – Заявка) в бумажном виде в 1 (Одном) экземпляре. Предоставление Заявки не требуется, если Соглашение заключено на основании Заявления на заключение ДБС / Заявления на комплексное банковское обслуживание.

4.2. Банк проверяет правильность заполнения Заявки, Заявления об акцепте условий соглашения о предоставлении услуг стандартного электронного документооборота/Заявления на заключение ДБС/Заявления на комплексное банковское обслуживание, полноту содержащейся информации, полномочия подписанта. В случае отрицательного результата проверки Банк возвращает документы Клиенту.

4.3. Банк формирует логин и пароль для входа в Систему «Клиент-Банк.WEB» и предоставляет их Клиенту⁴. Стандартным способом предоставления логина является его сообщение Клиенту по телефону в ответ на звонок Клиента в службу поддержки Системы «Клиент-Банк.WEB». Стандартным способом предоставления пароля является его направление Клиенту СМС сообщением на номер сотовой связи, указанный Клиентом в Заявке или Заявлении на заключение ДБС/ Заявлении на комплексное банковское обслуживание.

4.4. Клиент выполняет подключение к Системе «Клиент-Банк.WEB» с использованием собственных программно-технических средствах.

4.5. В случае использования УНЭП Клиент обращается в Банк для изготовления Сертификатов ключей проверки ЭП в порядке, предусмотренном Регламентом.

4.6. Для использования УКЭП Владелец сертификата ключа проверки УКЭП выполняет регистрацию имеющегося сертификата ключа проверки УКЭП через Систему «Клиент-Банк.WEB».

⁴ В случае если ранее Клиенту были предоставлены пароль и логин для входа в Систему «Клиент-Банк.WEB» на основании соглашения об электронном документообороте с использованием отдельных модулей Системы «Клиент-Банк.WEB» и при наличии у Банка технической возможности, после присоединения Клиента к настоящему Соглашению могут использоваться ранее предоставленные пароль и логин. В случае использования ранее предоставленных логина и пароля повторно пароль и логин не предоставляются. Указанный порядок не действует, если соглашения об электронном документообороте с использованием отдельных модулей Системы «Клиент-Банк.WEB» прекратило действие до момента присоединения Клиента к настоящему Соглашению.

После выполнения проверки сертификата ключа проверки УКЭП и его успешной регистрации предоставляется возможность подписывать ЭД в Системе «Клиент-Банк.WEB» ключом УКЭП.

4.7. Обмен ЭД в Системе «Клиент-Банк.WEB» начинается с даты получения Банком посредством Системы «Клиент-Банк.WEB» уведомления Клиента о начале работы в Системе «Клиент-Банк.WEB».

5. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

5.1. Доступ к Системе «Клиент-Банк.WEB»/отдельным сервисам/функциям Системы «Клиент-Банк.WEB» посредством Мобильного приложения предоставляется Клиенту, уполномоченным представителям Клиента при одновременном соблюдении следующих условий:

- между Банком и Клиентом заключено Соглашение;
- на Мобильном устройстве уполномоченного представителя Клиента установлено Мобильное приложение;
- произведена аутентификация уполномоченного представителя Клиента в Мобильном приложении (далее – Аутентификация) одним из способов, указанных в пункте 5.2 Условий;
- уполномоченным представителем Клиента получены Сертификаты ключей проверки УНЭП для использования в Мобильном приложении (для создания и подписания ЭД) в соответствии с Соглашением и Регламентом (если применимо);
- на Мобильном устройстве Клиента / уполномоченного представителя Клиента установлено Приложение MyDSS;

5.2. Аутентификация уполномоченного представителя Клиента в Мобильном приложении проводится в следующем порядке:

5.2.1. Проводится двухфакторная аутентификация, которая предполагает при входе в Мобильное приложение совместно с парой логин / пароль, ранее предоставленных уполномоченному представителю Клиента для входа в Систему «Клиент-Банк.WEB», указывать также специальный одноразовый код (технический (временный) пароль, необходимый для первого входа в Мобильное приложение.

Одноразовый код (технический (временный) пароль) высылается посредством SMS-сообщения на Номер телефона Клиента, после проверки со стороны Банка логина и пароля для входа в Систему «Клиент-Банк.WEB».

5.2.2. Номер телефона Клиента предоставляется Банку уполномоченным представителем Клиента посредством Системы «Клиент-Банк.WEB» в специальной форме (привязка Номера Клиента).

5.2.3. В дальнейшем Клиент в зависимости от технических возможностей Мобильного устройства может выбрать упрощенный порядок аутентификации в Мобильном приложении: путем подтверждения отпечатка пальца/распознавании контура лица (при наличии технологии Touch ID/Face ID на используемом Мобильном устройстве) или специального кода (ПИН-код), который самостоятельно задается уполномоченным представителем Клиента в специальной форме Мобильного приложения (формирование ПИН-кода).

Авторизация уполномоченного представителя Клиента с использованием Touch ID и Face ID доступна, если такая функциональность предусмотрена и настроена на Мобильном устройстве, а также их применение реализовано Банком в Мобильном приложении.

5.3. Если между Банком и Клиентом заключено Соглашение, лицам, уполномоченным распоряжаться денежными средствами, находящимися на счете(-ах) Клиента в электронном

виде, имеющим сертификат ключа проверки УНЭП (MyDSS), выпущенный для работы в Мобильном приложении, предоставляется возможность обмена ЭД в Мобильном приложении в следующем объеме: формирование, подписание и отправка в Банк платежных документов, осуществление иных функций, указанных в пункте 5.5 настоящего раздела.

5.4. Уполномоченный представитель Клиента после аутентификации в Системе «Клиент-Банк.WEB» для выпуска УНЭП (MyDSS) формирует запрос на создание Сертификата ключа проверки УНЭП (MyDSS) посредством интерфейса Системы «Клиент-Банк.WEB», проверяет заполненные параметры (в том числе Номер телефона Клиента) и подписывает запрос на создание Сертификата ключа проверки УНЭП (MyDSS), который направляется на рассмотрение в УЦ в порядке, предусмотренном Регламентом. При наличии действующего Сертификата ключа проверки УНЭП уполномоченный представитель Клиента вправе подписать указанный в настоящем пункте запрос с использованием соответствующего Ключа УНЭП.

После отправки запроса на создание Сертификата ключа проверки УНЭП (MyDSS) Клиенту (уполномоченному представителю Клиента) в интерфейсе Системы «Клиент-Банк.WEB» отображается QR-код и служебные данные, необходимые для активации СЭП MyDSS. Перенос необходимых для активации СЭП MyDSS служебных данных на Мобильное приложение MyDSS Клиента (уполномоченного представителя Клиента) выполняется путем сканирования (считывания) QR-кода в Приложении MyDSS, ввода в специальной форме кода активации, который направляется Банком в виде СМС-сообщения на Номер телефона Клиента и установления нового Ключа доступа MyDSS, используемого в дальнейшем Клиентом (уполномоченным представителем Клиента) для использования Ключа УНЭП (MyDSS) при подписании ЭД в Мобильном приложении. При этом Клиент (уполномоченный представитель Клиента) вправе установить дополнительные факторы аутентификации в Приложении MyDSS в соответствии с его функционалом.

После положительного рассмотрения запроса на создание Сертификата ключа проверки УНЭП (MyDSS) при входе в Систему «Клиент-Банк.WEB» уполномоченному представителю Клиента визуализируется сообщение о выпуске Сертификата ключа проверки УНЭП (MyDSS). После нажатия соответствующей кнопки в Системе «Клиент-Банк.WEB» («получить сертификат (ключ)») уполномоченный представитель Клиента (Владелец сертификата ключа проверки УНЭП (MyDSS)) может использовать выпущенный Ключ УНЭП (MyDSS) посредством Мобильного приложения в соответствии с Соглашением.

После выпуска Сертификата ключа проверки УНЭП (MyDSS) соответствующий Ключ УНЭП будет доступен Владельцу сертификата ключа проверки УНЭП (MyDSS) для использования в соответствии с Соглашением.

5.5. С использованием Мобильного приложения Клиенту доступно совершение следующих действий (при условии их технической реализации Банком в Мобильном приложении):

- обмен ЭД для осуществления расчетных и иных операций по счету(-ам) Клиента, открытому(-ым) в Банке (в том числе формирование, подписание и отправка в Банк платежных документов);
- получение Клиентом информации в электронной форме о счете(-ах) (выписки по счетам в рублях РФ и иностранной валюте и приложения к ним);
- получение иных документов, сообщений и информации, обмен которыми предусмотрен Соглашением и Договорами (в том числе документы свободного формата от Клиента в Банк и из Банка Клиенту);

- осуществления перевода денежных средств в российских рублях в рамках использования сервиса платежной системы Банка России (сервис системы быстрых платежей)⁵.

5.6. Банк осуществляет распространение Мобильного приложения путем размещения файлов для его загрузки соответствующих операционных систем Мобильных устройств⁶ в официальных магазинах приложений, а также на интернет-ресурсах или официальном сайте Банка.

6. ПОРЯДОК ПОДПИСАНИЯ И НАПРАВЛЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

6.1. В целях подписания ЭД Электронной подписью Клиент в Системе «Клиент-Банк.WEB» или Мобильном приложении инициирует процедуру его подписания путем нажатия соответствующей кнопки в интерфейсе Системы «Клиент-Банк.WEB» или Мобильном приложении. При этом Клиент (уполномоченный представитель Клиента) обязуется ознакомиться с содержанием проекта ЭД до его подписания ЭП.

6.2. Клиент выбирает в форме, вызванной Системой «Клиент-Банк.WEB» или Мобильным приложением, один из доступных ему видов ЭП для использования в Системе «Клиент-Банк.WEB» (УКЭП, УНЭП или УНЭП (MyDSS)). В Мобильном приложении Клиент может подписать ЭД только с использованием УНЭП (MyDSS).

6.3.1. Для использования зарегистрированного УКЭП для подписания ЭД в Системе «Клиент-Банк.WEB» Клиент (уполномоченный представитель Клиента) использует принадлежащий ему Ключ УКЭП, выданный Доверенным УЦ.

6.3.2. Для использования УНЭП для подписания ЭД документооборота Клиент (уполномоченный представитель Клиента) должен присоединиться к Регламенту и быть Владельцем Сертификата ключа проверки УНЭП.

6.3.3. Для использования УНЭП (MyDSS) для подписания ЭД в Системе «Клиент-Банк.WEB» и Мобильном приложении Клиент (уполномоченный представитель Клиента) в дополнении к требованиям п. 6.3.2. должен установить на Мобильное устройство Приложение MyDSS.

После того, как Клиент (уполномоченный представитель Клиента) в Системе выбрал УНЭП (MyDSS) для подписания ЭД, в Приложение MyDSS Клиента (уполномоченного представителя Клиента) поступает Push-уведомление Приложения MyDSS (или СМС-сообщение на Номер телефона Клиента (при технической реализации Банком)).

Клиент авторизуется в Приложении MyDSS (в том числе путем ввода установленного Клиентом пароля доступа к Приложению MyDSS), выбирает соответствующий ЭД в интерфейсе Приложения MyDSS и получает возможность ознакомиться с ЭД и подписать его путем нажатия соответствующей кнопки в интерфейсе Приложения MyDSS или отказаться его подписания. Клиент (уполномоченный представитель Клиента) обязуется ознакомиться с содержанием ЭД в Приложении MyDSS до его подписания УНЭП (MyDSS).

После ознакомления с ЭД Клиент (уполномоченный представитель Клиента) вызывает функцию подписания ЭД путем нажатия соответствующей кнопки в интерфейсе Приложения MyDSS.

Волеизъявлением Клиента (уполномоченного представителя Клиента) на подписание Электронного документа УНЭП (MyDSS) считается полученным Банком при соответствии

⁵ Сервис предоставляется при наличии технической возможности и соответствующего заключенного договора о предоставлении сервиса. Наименование формы ЭД в Системе «Клиент-Банк.WEB», используемой для осуществления таких переводов, – «b2c перевод СБП» (business-to-consumer, «бизнес для потребителя» – коммерческое взаимодействие юридических и физических лиц).

⁶ При наличии возможности размещение Мобильного приложения осуществляется в официальных магазинах приложений App Store (itunes.apple.com), Play Market (play.google.com) и иных источниках приложений.

Ключа доступа MyDSS, введенного Клиентом (уполномоченным представителем Клиента) при подписании ЭД, Ключу доступа MyDSS, установленному Клиентом (уполномоченным представителем Клиента) в соответствии с п. 5.4 настоящего приложения (или Ключа доступа MyDSS, который был установлен Клиентом (уполномоченным представителем Клиента) в результате изменения Ключа доступа MyDSS в последующем при использовании Приложения MyDSS).

6.4. После подписания Электронной подписью ЭД автоматически направляется Системой «Клиент-Банк.WEB» или Мобильным приложением в адрес Банка, дополнительных действий для направления ЭД в адрес Банка после его подписания со стороны Клиента не требуется. В случае, если соглашением между Банком и Клиентом предусмотрено подписания документов несколькими подписями в Системе «Клиент-Банк.WEB» или Мобильным приложением реализована такая возможность подписание ЭД и его направление в Банк осуществляется после подписания ЭД всеми необходимыми ЭП.

6.5. Банк обеспечивает доступ Клиента к визуализации подписанных ЭД в Системе «Клиент-Банк.WEB» и Мобильном приложении (по мере технической реализации). При технической реализации визуализация ЭД, подписанных Клиентом, также доступна в Приложении MyDSS, ответственность за доступность указанного функционала несет поставщик Приложения MyDSS.

6.6. Банк обеспечивает хранение ЭД, подписанных Клиентом в Системе «Клиент-Банк.WEB» и Мобильном приложении, в соответствии с требованиями законодательства и условиями Соглашения.

6.7. Стороны признают, что при отсутствии между Сторонами спора относительно использования ЭП при подписании ЭД, наличие в электронном журнале Системы Клиент-Банк.WEB» записи о заключении Клиентом договора или совершения им иного юридически значимого действия, являются достаточным доказательством факта их совершения. Базы данных Системы, электронные журналы Системы «Клиент-Банк.WEB», выписки из журналов Системы «Клиент-Банк.WEB», распечатанные на бумажном носителе или представленные в электронном виде и заверенные уполномоченным представителем Банка, могут быть использованы в качестве доказательств в случае рассмотрения спора в суде.

7. ПОРЯДОК РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ ПРИ ИСПОЛЬЗОВАНИИ УНЭП В СИСТЕМЕ «КЛИЕНТ-БАНК.WEB»

7.1. Общие положения.

7.1.1. При возникновении разногласий между Клиентом и Банком по поводу корректности действий, совершенных в рамках заключенного Соглашения между Сторонами, Сторона-инициатор спора в течение 3 (Трех) рабочих дней с даты, когда ей стало известно о предполагаемом нарушении ее прав, обязана подготовить и направить Стороне-ответчику документ, подписанный должностным лицом, с подробным изложением обстоятельств происшедшего и предложением создать комиссию. В предложении о создании комиссии указывается место сбора комиссии (адрес), время и дата. Дата сбора комиссии устанавливается не позднее чем на 7-й календарный день с даты доставки получателю предложения о создании комиссии.

7.1.2. В состав комиссии должны входить не более четырех представителей от каждой из Сторон. При необходимости, с письменного согласия обеих Сторон, в состав комиссии могут быть дополнительно включены независимые эксперты и специалисты организаций - изготовителей программного обеспечения Системы «Клиент-Банк.WEB». Состав комиссии согласовывается Сторонами и утверждается двусторонним актом.

7.1.3. Комиссия в двухнедельный срок проводит разбор конфликтной ситуации и по итогам работы составляет акт, в котором в обязательном порядке указываются: суть конфликта, виновная Сторона, сроки устранения причин возникновения конфликтной ситуации.

В случае привлечения независимых экспертов, их услуги оплачивает Сторона, признанная виновной.

Проверка достоверности документа производится с использованием программного комплекса «АРМ разбора конфликтных ситуаций» производства ООО «Крипто-ПРО» (<http://www.cryptopro.ru/products/ca/arm-rks>).

Соответствующие протоколы проверки подписи, полученные с использованием указанного программного комплекса, приобщаются к результатам работы комиссии.

7.1.4. Стороны обязаны предоставить комиссии следующие документы и материалы:

- акт готовности Клиента к работе в Системе «Клиент-Банк.WEB» (если в рамках заключения Соглашения оформлялся акт готовности);

- сертификаты ключей проверки электронной подписи электронного документа (далее – ЭД) по спорной сделке, а также соответствующие им заявления и запросы на изготовление сертификатов ключей проверки электронной подписи (предоставляет Банк);

- список отозванных сертификатов (CRL), действующий на момент отправки/получения ЭД (предоставляет Банк);

- файл, содержащий ЭД, по исполнению которого предъявляются претензии и файлы всех проставленных под ним электронных подписей ответчика (далее – ЭП);

- журналы работы Системы «Клиент-Банк.WEB» (предоставляет Банк).

7.1.5. Стороны должны способствовать работе комиссии и предоставлять в кратчайший срок необходимые сведения и документы.

7.1.6. Для получения файлов ЭД и проставленных под ним ЭП, указанных в подпунктах 7.2.2, 7.3.2 и 7.4.2 настоящего раздела приложения № 2 к Соглашению, Банк и Клиент используют руководство «Система ДБО BS-Client x64. Версия 020.1.200. Централизованная и распределенная схемы. Документация банка. Комплект администратора ДБО. Защита информации в системе «ДБО BS-Client».

7.2. Порядок разрешения конфликта отказа Клиента от документа.

7.2.1. В данном разделе описана процедура разрешения конфликта отказа Клиента от ЭД: Клиент утверждает, что исполненный Банком документ не передавался, Банк отрицает это.

7.2.2. Банк предъявляет выгруженные из Системы «Клиент-Банк.WEB» файлы, содержащие спорный ЭД Клиента и все проставленные под ним ЭП. В случае отказа Банка предоставить указанные файлы конфликт решается в пользу Клиента.

7.2.3. Если проверка ЭП оспариваемого ЭД дает положительный результат с применением действующих на момент отправки/получения ЭД Клиента ключей проверки ЭП, и ЭП под ЭД Клиента соответствуют ЭП Владельцев сертификатов ключей проверки ЭП, то конфликт решается в пользу Банка.

7.3. Порядок разрешения конфликта, связанного с достоверностью принятого к исполнению ЭД.

7.3.1. В данном разделе описана процедура разрешения конфликта, связанного с достоверностью принятого к исполнению ЭД: Клиент утверждает, что исполненный Банком ЭД не соответствует переданному, Банк отрицает это.

7.3.2. Банк предъявляет выгруженные из Системы «Клиент-Банк.WEB» файлы, содержащие спорный ЭД Клиента и все проставленные под ним ЭП. В случае отказа Банка предоставить указанные файлы конфликт разрешается в пользу Клиента.

7.3.3. Производится проверка ЭП предъявленного ЭД с применением действующих на момент отправки/получения ключей проверки ЭП. Если проверка дает положительный результат, ЭП под ЭД соответствуют ЭП Владельцев сертификатов ключей проверки ЭП и содержимое файла соответствует содержанию оспариваемого документа, то конфликт решается в пользу Банка. В противном случае конфликт разрешается в пользу Клиента.

7.4. Порядок разрешения конфликта отказа Банка от документа.

7.4.1. В данном разделе описана процедура разрешения конфликта отказа Банка от ЭД: Банк утверждает, что документ не передавался, Клиент отрицает это.

7.4.2. Клиент предъявляет выгруженные из Системы «Клиент-Банк.WEB» файлы, содержащие спорный ЭД Банка и файл ЭП банка под ним. В случае отказа Клиента предоставить указанные файлы конфликт решается в пользу Банка.

7.4.3. Если проверка ЭП оспариваемого ЭД дает положительный результат с применением действующих на момент отправки/получения ЭД Банка ключей проверки ЭП, и ЭП под ЭД Банка соответствуют ЭП Владельцев сертификатов ключей проверки ЭП, то конфликт решается в пользу Клиента.

7.5. При возникновении разногласий между Сторонами по поводу подписания ЭД УНЭП (MyDSS) Стороны руководствуются порядком разрешения спорных ситуаций, описанных в настоящем разделе Приложения №2 к Соглашению.

При этом проверка наличия волеизъявления Клиента на подписание ЭД УНЭП (MyDSS), подлинности ЭД, авторства и неизменности ЭД производится с использованием программного комплекса «АРМ разбора конфликтных ситуаций» производства ООО «Крипто-ПРО» (компонент, обеспечивающий выполнение процедур по подтверждению подлинности электронной цифровой подписи (электронной подписи) в электронных документах и установлению статуса сертификата открытого ключа на определенный момент времени. Итогом работы АРМ разбора конфликтных ситуаций является протокол, содержащий результаты выполненных проверок. <http://www.cryptopro.ru/products/ca/arm-rks>).

8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ ПРИ ИСПОЛЬЗОВАНИИ УКЭП

8.1. При возникновении разногласий между Сторонами по поводу корректности действий, совершенных в рамках заключенного Соглашения между Сторонами с использованием УКЭП, Стороны руководствуются порядком разрешения спорных ситуаций, указанным в разделе 6 настоящего Приложения с учетом следующих особенностей:

8.1.1. Любая из Сторон Соглашения вправе потребовать привлечения в состав Комиссии представителя Доверенного УЦ. При этом соответствующие расходы оплачивает Сторона, которая заявила данное требование. В случае, если по итогам рассмотрения спора будет принято решение в пользу Стороны, заявившей о привлечении представителя, Доверенного УЦ для работы в составе Комиссии, данные расходы подлежат возмещению другой Стороной. Полномочия членов Комиссии подтверждаются доверенностями, выданными в установленном порядке.

8.1.2. Стороны обязаны предоставить комиссии документы и материалы, указанные в подпункте 7.1.4 приложения № 2 к Соглашению, за исключением заявлений и запросов на изготовление сертификатов ключей проверки электронной подписи, списка отозванных сертификатов (CRL), действующий на момент отправки/получения ЭД.

8.1.3. В случае неподтверждения Электронной подписи Доверенного УЦ в Сертификате ключа проверки электронной подписи, нарушения сроков действия или нарушения области использования Электронной подписи, которые указаны в Сертификате ключа проверки электронной подписи в соответствии с Регламентом Доверенного УЦ, подлинность и правомерность использования Электронной подписи оспариваемого Электронного документа признается неподтвержденной.

8.2. При возникновении между Сторонами споров и разногласий, связанных с проверкой подлинности УКЭП Электронного документа, Сторона, которая инициировала данный спор, вправе обратиться в Доверенный УЦ для разрешения спорной ситуации. Оплата услуг Доверенного УЦ, иные расходы, связанные с разрешением спорной ситуации, осуществляются Клиентом.

Проверка подлинности УКЭП осуществляется в порядке, предусмотренном Регламентом Доверенного УЦ.

ЗАЯВКА на подключение Клиента к Системе «Клиент-Банк.WEB»

Наименование организации (Клиента)

ИНН _____

ОГРН _____

КПП _____

1. Прошу оказывать услуги с использованием Системы «Клиент-Банк.WEB» при осуществлении операций по всем договорам банковского счета в соответствии с п. 2.1 Соглашения, в том числе заключенным после предоставления настоящей заявки.

2. Прошу обеспечить установку дополнительного программного обеспечения для взаимодействия с другими участниками Системы «Клиент-Банк.WEB»*.

(поставить отметку при необходимости)

Контакты Клиента (обязательны к заполнению)

Адрес установки системы _____

Обязанности Администратора безопасности согласно определению «Регламента удостоверяющего центра Банка ГПБ (АО)» в действующей редакции возложены на

Адрес электронной почты _____

(должность, подразделение, фамилия, имя, отчество полностью)

Телефон (в т.ч. код) _____

Моб. телефон (в т.ч. код) _____

Контакты для оперативной связи, чтобы Банк мог связаться с Вами в любое время в случае экстренной ситуации

Адрес электронной почты _____

(должность, подразделение, фамилия, имя, отчество полностью)

Телефон (в т.ч. код) _____

Моб. телефон (в т.ч. код) _____

Адрес электронной почты _____

(должность, подразделение, фамилия, имя, отчество полностью)

Телефон (в т.ч. код) _____

Моб. телефон (в т.ч. код) _____

Адрес электронной почты _____

(должность, подразделение, фамилия, имя, отчество полностью)

Телефон (в т.ч. код) _____

Моб. телефон (в т.ч. код) _____

Руководитель Клиента

М.П.

(должность)

(фамилия, инициалы)

(подпись)

« ____ » _____ 20__ г.

* После предварительной консультации со специалистами Банка.

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ «КЛИЕНТ-БАНК.WEB»

1. При первом входе в Систему «Клиент-Банк.WEB» необходимо изменить выданный Банком пароль согласно инструкции, прилагаемой к дистрибутиву Системы «Клиент-Банк.WEB».

2. Пароль необходимо регулярно изменять (не реже 1 (Одного) раза в 50 (Пятьдесят) календарных дней). Длина пароля должна быть не менее 8 (Восьми) символов. Пароль должен состоять из цифр, больших и маленьких букв английского алфавита. Использование простых и легко угадываемых паролей (например, имена, фамилии, номера телефонов, даты рождения и т.д.) должно быть исключено.

3. Разглашение пароля Системы «Клиент-Банк.WEB» запрещается (если к Вам обратятся лица, представившиеся работниками Банка, и запросят пароль, помните, что работники Банка никогда не запрашивают такую информацию). В случае возникновения подозрений компрометации пароля его необходимо изменить.

4. Ключевая информация (ключ электронной подписи для работы в Системе «Клиент-Банк.WEB») должна размещаться на сменном носителе информации (floppy-дискета, USB-flash накопитель, рекомендуется использовать USB-ключи e-Token). Размещение ключевой информации на жестком диске компьютера, на котором установлена Система «Клиент-Банк.WEB», запрещается.

5. Сменный носитель с ключевой информацией должен использоваться только владельцем сертификата ключа проверки электронной подписи либо лицом, уполномоченным на использование такого сменного носителя, и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик).

6. Сменный носитель с ключевой информацией должен быть вставлен в считывающее устройство только во время работы в Системе «Клиент-Банк.WEB». Размещение сменного носителя в считывающем устройстве вне сеансов работы в Системе «Клиент-Банк.WEB» должно быть исключено.

7. На сменном носителе, используемом для хранения ключевой информации, запрещается хранить иную информацию.

8. С целью контроля исходящего и входящего подозрительного трафика компьютер с подключением к Системе «Клиент-Банк.WEB» должен быть защищен от внешнего доступа программным или аппаратным средством межсетевого экранирования. Программные межсетевые экраны должны пресекать отправку в Интернет информации, инициированной программами, не имеющими соответствующих полномочий.

9. На компьютере с подключением к Системе «Клиент-Банк.WEB»:

- работа в Системе «Клиент-Банк.WEB» осуществляется под учетной записью с максимально ограниченными правами, запрещается работать с правами Администратора;

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие п. 2 настоящих Требований;

- должно быть установлено только лицензионное программное обеспечение;

- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

- должны быть отключены все неиспользуемые для связи с Банком службы и процессы операционной системы Windows (в том числе службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

- должна быть запрещена работа с ресурсами и сайтами сети Интернет (в том числе с сайтами налоговых служб, с бесплатной электронной почтой, с социальными сетями, развлекательными сайтами, сайтами файловыми обменниками, интернет-мессенджерами и пр.), за исключением указанных в договоре ресурсов нашего Банка (или сторонних банков);

- необходимо установить средства проактивной защиты либо активировать данный функционал средствами антивирусной защиты (если поддерживается) и включить режим «белого списка»: разрешена работа только строго определенных процессов (программ), все остальное запрещено;

- должны регулярно устанавливаться обновления операционной системы и установленного программного обеспечения;

- должен быть исключен доступ (физический и/или удаленный) к компьютеру третьих лиц, не имеющих полномочий для работы в Системе «Клиент-Банк.WEB»;

- должна быть активирована подсистема регистрации событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после ухода ответственного работника с рабочего места.

10. Если работа с системой «Клиент-Банк.WEB» осуществляется с одного компьютера, то рекомендуется предоставить в Банк IP адрес (диапазон IP-адресов) Интернет, выделяемых Интернет-провайдером для Клиента.

11. Рекомендуется ежедневно, до 16:30, входить в Систему «Клиент-Банк.WEB» и контролировать платежи, отосланные в Банк.

12. В случае, если не удается в штатном режиме войти в систему «Клиент-Банк.WEB», или по невыясненным причинам компьютер, с которого осуществляется работа в системе «Клиент-Банк.WEB», перестал загружаться, некорректно реагирует на команды в обычном рабочем режиме (самопроизвольное перемещение курсора, открытие и закрытие окон, набор текста), внезапно прекратил работать – рекомендуется **НЕЗАМЕДЛИТЕЛЬНО** связаться со службой технической поддержки Банка, проинформировать Банк о сложившейся ситуации, выяснить не было ли в последнее время несанкционированных операций и, возможно, временно заблокировать вход клиента в систему до выяснения причин, вызвавших сбой.

13. Если в качестве аппаратного средства для работы в Системе «Клиент-Банк.WEB» выбран переносной компьютер (ноутбук), его подключение к сетям общего доступа в местах свободного доступа в Интернет (интернет-кафе, гостиницы, офисные центры и т.д.) должно быть исключено.

14. Если Вы получили письмо от имени Банка, содержание которого вызывает подозрение, либо с Вами связались по телефону от имени Банка, с просьбой установить какое-либо программное обеспечение, просьба связаться со службой технической поддержки Банка и уточнить ситуацию. Всегда используйте контактную информацию служб поддержки Банка, указанную в официальных источниках информации, и не используйте контактную информацию, указанную в письме или полученную в ходе телефонного разговора.

15. В случае передачи (списания, утилизации и т.п.) сторонним лицам стационарного компьютера (или ноутбука), на котором ранее была установлена Система «Клиент-Банк.WEB», необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Вашей организации, в том числе следы работы в Системе «Клиент-Банк.WEB».

МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

1. На Мобильном устройстве не должно устанавливаться нелицензионное программное обеспечение.

2. При использовании Мобильного приложения, Приложения MyDSS необходимо применять регулярно обновляемое антивирусное программное обеспечение и осуществлять установку последних обновлений (в том числе обновлений по безопасности), выпускаемых разработчиками приложений, операционных систем, web-браузеров.

3. Запрещается использовать Мобильное приложение, Приложения MyDSS на Мобильном устройстве, в отношении которого установлены права суперпользователя операционной системы Мобильного устройства (jailbreak, root).

4. В случаях утраты Мобильного устройства необходимо немедленно обратиться в любой офис Банка или в Банк по номерам телефонов, указанным на сайте Банка для блокировки Мобильного приложения.

5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия соответствующего сертификата ключа проверки УНЭП (MyDSS) и не применять Ключ УНЭП (MyDSS) в любом из следующих случаев:

- при наличии оснований полагать, что конфиденциальность Ключа УНЭП (MyDSS) нарушена;

- компрометации аутентификационной информации и утраты Мобильных устройств, на которых установлено Приложение MyDSS;

- если стало известно, что Ключ УНЭП (MyDSS) используется или использовался ранее другими лицами, в том числе если уполномоченный представитель Клиента получил сообщение от СЭП MyDSS о выполнении каких-либо операций от его имени, если он их не выполнял.

6. Запрещается передача Мобильного устройства третьим лицам, предоставление доступа третьих лиц к Мобильному приложению, Приложению MyDSS, установленному на Мобильном устройстве.

7. Запрещается хранение Мобильного устройства таким образом, когда оно может быть доступным третьим лицам;

8. Запрещается передача логина и пароля от Мобильного приложения, паролей доступа к Приложению MyDSS, Ключа доступа MyDSS третьим лицам.

9. Запрещается хранение логина и пароля к Мобильному приложению, паролей доступа к Приложению MyDSS, Ключа доступа MyDSS таким образом, когда они могут быть доступным третьим лицам.

10. Рекомендуется исключить ситуации установки вредоносного ПО, а также использования Мобильного приложения, Приложения MyDSS с программным обеспечением, осуществляющим захват экрана или удаленный доступ к Мобильному устройству.

Дополнительные рекомендации для Мобильных устройств с операционной системой Android:

1. Используйте операционную систему Android последней поддерживаемой производителем устройства версии.

2. Отключите «Режим разработчика». Если был активирован режим разработчика и после этого включен режим отладки по USB, отключите его.
3. Отключите «Специальные возможности».
4. Приложения должны функционировать на Мобильном устройстве только совместно с приложением, в составе которого реализована защита с помощью «Kaspersky Fraud Prevention SDK».
5. Отключите возможность установки любого программного обеспечения на Мобильное устройство из неизвестных источников.

Дополнительные рекомендации для мобильных устройств с операционной системой iOS:

Используйте операционную систему iOS последней поддерживаемой производителем устройства версии.

ПЕРЕЧЕНЬ ДОВЕРЕННЫХ УЦ

1. Центральный банк Российской Федерации (ИНН 7702235133).
2. Федеральная налоговая служба России (ИНН 7707329152).
3. Федеральное казначейство (ИНН 7710568760).
4. Федеральное государственное бюджетное учреждение «Федеральная кадастровая палата Федеральной службы государственной регистрации, кадастра и картографии» (ИНН 7705401340).
5. Акционерное общество «Производственная фирма «СКБ Контур», г. Екатеринбург (ИНН 6663003127).
6. Акционерное общество «Гринатом» (ИНН 7706729736).
7. Общество с ограниченной ответственностью «КОРУС Консалтинг СНГ», г. Санкт-Петербург (ИНН 7801392271).
8. Общество с ограниченной ответственностью «ЭТП ГПБ Консалтинг» (ИНН 7728356929).
9. Акционерное общество «Единая электронная торговая площадка» (ИНН 7707704692).
10. Общество с ограниченной ответственностью «Такском» (ИНН 7704211201).
11. Публичное акционерное общество «Мобильные ТелеСистемы» (ИНН 7740000076).
12. Общество с ограниченной ответственностью «Сертум-Про», г. Екатеринбург (ИНН 6673240328).
13. Общество с ограниченной ответственностью «Научно-производственный центр «1С» (ИНН 7729510210).
14. Общество с ограниченной ответственностью «ГАЗИНФОРМСЕРВИС» (ИНН 7838017968).
15. ООО «Компания «Тензор» (ИНН 7605016030).
16. АО «Электронная Москва» (ИНН 7707314029).
17. Акционерное общество «Энергоцентр» (ИНН 5036072424).

18. Общество с ограниченной ответственностью «Центр Бухгалтерских услуг» (ИНН 2315096691).
19. Общество с ограниченной ответственностью «Модум» (ИНН 7716866347).
20. Акционерное общество «Информационные технологии и коммуникационные системы» (АО «ИнфоТеКС») (ИНН 7710013769).
21. Публичное акционерное общество «МегаФон» (ИНН 7812014560).
22. Акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (ИНН 7709752846).
23. Публичное акционерное общество «Сбербанк России» (ИНН 7707083893).
24. Открытое акционерное общество «Российские железные дороги» (ИНН 7708503727).
25. Акционерное общество «Почта России» (ИНН 7724490000).
26. Банк ВТБ (публичное акционерное общество) (ИНН 7702070139).
27. Акционерное общество «Тандер» (ИНН 2310031475).
28. Акционерное общество «Тинькофф Банк» (ИНН 7710140679).
29. Акционерное общество «Торговый дом «ПЕРЕКРЕСТОК» (ИНН 7728029110).
30. Коммерческий банк «Кубань кредит» Общество с ограниченной ответственностью (ИНН 2312016641).
31. Российский национальный коммерческий банк (Публичное акционерное общество) (ИНН 7701105460).
32. Публичное акционерное общество «Совкомбанк» (ИНН 4401116480).
33. Публичное акционерное общество «Промсвязьбанк» (ИНН 7744000912).
34. Акционерное общество «Сбербанк – Автоматизированная система торгов» (ИНН 7707308480.)
35. Публичное акционерное общество «Вымпел-Коммуникации» (ИНН 7713076301).
36. Акционерное общество «ИнфоТеКС Интернет Траст» (ИНН 7743020560).
37. Общество с ограниченной ответственностью «АйТи Мониторинг» (ИНН 2311187588).
38. Акционерное общество «Аналитический центр» (ИНН 5260270696).