АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «ЕВРОФИНАНС МОСНАРБАНК» (акционерное общество) (АО АКБ «ЕВРОФИНАНС МОСНАРБАНК»)

Evrofinance Mosnarbank

УТВЕРЖДЕНО
Протокол заседания Правления Банка
от 19.12.2024 г. № 75
Действует с 09.01.2025 г.

APPROVED
Board Meeting Protocol
dated 19.12.2024 № 75
Effected from 09.01.2025

УСЛОВИЯ
использования электронной системы дистанционного банковского обслуживания

TERMS
of Use of the Electronic System for Remote Banking Services

Москва
2024 г.

Moscow
2024

Термины и определения	**Terms and definitions**
Акт признания Сертификата ключа проверки ЭП для обмена сообщениями (Акт признания) – документ на бумажном носителе, подписываемый Сторонами и удостоверяющий принадлежность приведенного в нем Ключа проверки ЭП и соответствующего ему Ключа ЭП Уполномоченному представителю Клиента (по форме Банка).	**Act of acknowledgement of the ES verification key Certificate for message exchange (Act of acknowledgement)** – a paper document signed by the Parties, certifying the ownership of the ES verification Key and the corresponding ES Key by the Authorized Representative of the Client (in the Bank's form).
Аутентификация – процедура проверки подлинности Клиента/Уполномоченного представителя Клиента с помощью Логина, Пароля, Кодового слова или иным способом, предусмотренным Условиями. Положительный результат Аутентификации подтверждает, что формирование и передача в Банк Электронных документов, а также подтверждение исполнения Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без добровольного согласия Клиента, производится самим Клиентом/ Уполномоченным представителем Клиента.	**Authentication** – a procedure for verifying the authenticity of the Client/Authorized Representative of the Client using a Login, Password, Code Word, or any other method stipulated by the Terms. A Positive Authentication Result confirms that the formation and transmission of Electronic Documents to the Bank, as well as the confirmation of execution of an order suspended due to signs of money transfer without the voluntary consent of the Client, is carried out by the Client/Authorized Representative of the Client.
База данных – база данных Банка России о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к Клиенту и/или его электронному средству платежа, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемые в соответствии с законодательством Российской Федерации.	**Database** – database of the Bank of Russia with cases and attempts of money transfers without the voluntary consent of the Client which contains the data related to the Client and/or their electronic payment instrument, including data of the federal executive body in the area of internal affairs on commited unlawful actions obtained in accordance with the legislation of the Russian Federation.
Банк – АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «ЕВРОФИНАНС МОСНАРБАНК» (акционерное общество) (полное наименование), АО АКБ «ЕВРОФИНАНС МОСНАРБАНК» (сокращенное наименование), адрес: 121099, г. Москва, ул. Новый Арбат, д.29, официальный сайт в сети «Интернет»: www.evrofinance.ru, генеральная лицензия на проведение банковских операций №2402, выданная Банком России 23.07.2015.	**Bank** – Evrofinance Mosnarbank, address: 29 Novy Arbat Street, Moscow, 121099, official website in the Internet: www.evrofinance.ru, general license for banking transactions No. 2402 issued by the Bank of Russia on 23.07.2015.
Владелец сертификата ключа проверки ЭП – Клиент, которому в установленном	**ES verification key certificate Holder** – a Client to whom has been issued an ES

Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Закон № 63-ФЗ) порядке выдан Сертификат ключа проверки ЭП.	verification key Certificate in accordance with the procedure established by Federal Law No. 63-FZ dated 06.04.2011 "On Electronic Signature" (hereinafter referred to as Law No. 63-FZ).
Временный Пароль – уникальная последовательность символов, передаваемая Клиенту Банком в соответствии с Заявлением на доступ/Заявлением об изменении сведений/Заявлением о Компрометации.	**Temporary Password** – a unique sequence of characters provided to the Client by the Bank in accordance with the Access Application/Application for change of information/Compromise Statement.
Дистанционное банковское обслуживание (ДБО) – комплекс услуг, предоставляемых Банком Клиенту, предназначенный для осуществления обмена Электронными документами между Клиентом и Банком с использованием Системы в целях проведения на основании Электронных документов банковских операций и сделок согласно установленному Пакету операций; осуществления Банком функций агента валютного контроля; предоставления в Банк документов, необходимых для осуществления Банком функций, установленных законодательством Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма; осуществления переписки между Банком и Клиентом, а также предоставления Сторонами друг другу информации о Счете/Счетах и иных сведений и документов.	**Remote Banking Service (RBS)** – a set of services provided by the Bank to the Client for the exchange of Electronic Documents between the Client and the Bank using the System. These include conducting banking transactions and deals based on Electronic Documents in accordance with the established Package of Operations; performing the Bank's functions as a currency control agent; submitting documents required for compliance with Russian Federation legislation on anti-money laundering and counter-terrorism financing; correspondence between the Bank and the Client; and providing information about the Account(s) and other relevant details and documents.
Документация – все руководства, инструкции, технические описания и другая документация, касающаяся Системы, которые размещаются Банком в электронном виде на официальном сайте Банка в сети «Интернет» по адресу www.evrofinance.ru, а также техническое описание организации-разработчика Системы, интегрированное в раздел «Помощь» в Системе.	**Documentation** – all the manuals, instructions, functional descriptions and other documentation, relating to the System, which are placed by the Bank in electronic format at the Bank's website www.evrofinance.ru, as well as technical description of the organisation developing the System, integrated into the "Help" section in the System.
Договор ДБО – настоящие Условия в совокупности с Заявлением о присоединении к Условиям являются заключенным между Банком и Клиентом Договором об использовании электронной системы дистанционного банковского обслуживания (Договором ДБО).	**RBS Contract** – these Terms together with the Application for accession to the Terms shall constitute the Contract on the Use of the Electronic System of Remote Banking Services (RBS Contract) concluded between the Client and the Bank.

ЕИО – лицо, являющееся единоличным исполнительным органом Клиента, а также индивидуальный предприниматель и физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой.	**SEB** – a person who is the single executive body of the Client, a sole trader, or an individual engaged in private practice in accordance with the procedure established by the legislation of the Russian Federation
Запрос на создание Сертификата ключа проверки ЭП – запрос на регистрацию в Системе Ключа проверки ЭП в электронном виде, который формируется в Системе Уполномоченным представителем Клиента в процессе создания Ключей и направляется в Банк средствами Системы.	**Request for the creation of the ES verification key Certificate** – a request for registering the ES Verification Key in the System, generated in the System by the Authorized Representative of the Client during the Key creation process and sent to the Bank via the System.
Заявление об изменении Соглашения – заявление Клиента на бумажном носителе о распространении Условий на ранее заключенное между Сторонами Соглашение об использовании электронной системы дистанционного банковского обслуживания (по форме Банка).	**Application for change of Agreement** – a paper application of the Client to extend the Terms to a previously concluded between the Parties Agreement on the use of an electronic system for remote banking services (in the Bank's form).
Заявление о предоставлении права доступа в Систему «Клиент-Банк» (Заявление на доступ) – документ на бумажном носителе, подписываемый Сторонами и подтверждающий факт наделения Уполномоченного представителя Клиента правом на использование Системы в соответствии с Договором ДБО и полномочиями на совершение банковских операций и/или сделок в рамках установленного Пакета операций (по форме Банка).	**Application for granting the right of access to the Client-Bank System (Access Application)** – a paper document signed by the Parties that confirms the granting of rights to the Client's Authorized Representative to use the System in accordance with the RBS Contract and the authority to conduct banking transactions and/or deals within the established Package of Operations (in the Bank's form).
Заявление о внесении изменений в Договор ДБО – заявление, составленное Клиентом и предназначенное для внесения изменений в Договор ДБО (по форме Банка).	**Application for amendments to the RBS Contract** – an application drafted by the Client for making amendments to the RBS Contract (in the Bank's form).
Заявление об изменении сведений об Уполномоченном представителе (Заявление об изменении сведений) – заявление, составленное Клиентом и предназначенное для внесения изменений в информацию об Уполномоченных представителях, предоставленную Клиентом в Банк (по форме Банка).	**Application for change of information about the Authorized Representative** (**Application for change of information**) – an application drafted by the Client to update information about the Authorized Representatives previously provided to the Bank (in the Bank's form).
Заявление о присоединении к Условиям – письменное (на бумажном носителе)	**Application for accession to the Terms** – a written (paper) expression of the Client's intent

волеизъявление Клиента заключить Договор ДБО (по форме Банка).	to enter into the RBS Contract (in the Bank's form).
Квитанция – электронное сообщение о приеме Электронного документа Стороны-отправителя Стороной-получателем или смене статуса документа Стороной-получателем в процессе обработки. Получение Квитанции в Системе влечет за собой смену статуса документа в Системе Стороны-отправителя.	**Receipt confirmation** – an electronic message on the reception of the Electronic Document sent by the Sending party and received by the Receiving party or the change of the document status by the Receiving party during processing. Reception of the Receipt confirmation in the System entails a change in the document status in the System of the Sending party.
Клиент – юридические лица (включая кредитные организации), индивидуальные предприниматели и физические лица, занимающиеся в установленном законодательством Российской Федерации порядке частной практикой, заключившие с Банком Договор ДБО.	**Client** – legal entities (including credit organisations), sole traders and individuals engaged in private practice in accordance with the procedure established by the legislation of the Russian Federation, who have entered into the RBS Contract with the Bank.
Ключи (Комплект Ключей) – Ключ ЭП и соответствующий ему Ключ проверки ЭП.	**Keys (Set of Keys)** – ES Key and corresponding ES verification Key.
Ключ Электронной подписи (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания Электронной подписи.	**Electronic signature key (ES Key)** – a unique sequence of symbols designed to create the Electronic Signature.
Ключ проверки Электронной подписи (Ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с Ключом Электронной подписи и предназначенная для проверки подлинности Электронной подписи в Электронном документе. Срок действия Ключа проверки ЭП для УКЭП определяется выпустившим ее Удостоверяющим центром. Срок действия Ключа проверки ЭП для УНЭП, выпущенной Банком, составляет: - при использовании СКЗИ КриптоПро – 15 (пятнадцать) месяцев с даты формирования Запроса за создание Сертификата ключа проверки ЭП; - при использовании СКЗИ OpenSSL – 36 (тридцать шесть) месяцев с даты формирования Запроса на создание Сертификата ключа проверки ЭП.	**Electronic signature verification Key (ES verification Key)** – a unique sequence of symbols uniquely linked to the Electronic signature Key and designed to verify the authenticity of the Electronic Signature in the Electronic Document. The validity term of the ES verification Key for the EQES shall be determined by the Certification Authority that issued it. The validity period of the ES verification Key for the EUES issued by the Bank shall be as follows: - when using the CryptoPro ICSP – 15 (fifteen) months from the date of generating the Request for the creation of the ES verification key Certificate; - when using the OpenSSL ICSP – 36 (thirty-six) months from the date of generating the Request for the creation of the ES verification key Certificate.
Кодовое слово – последовательность символов, известная только Клиенту и Банку, используемая для Аутентификации Клиента при телефонном разговоре с Клиентом в целях	**Code word** – a symbol sequence known only to the Client and the Bank, used for Authentication of the Client during a telephone conversation with the Client in order to

подтверждения/неподтверждения возобновления исполнения операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента. Кодовое слово может использоваться многократно. Кодовое слово указывается в Договоре ДБО и может быть изменено в порядке, предусмотренном Условиями.	confirm/not confirm the resumption of a transaction with signs of money transfer without the voluntary consent of the Client. The Code Word may be used more than once. The Code Word shall be specified in the RBS Contract and may be changed in the procedure established by the Terms.
Компрометация Ключей – возникновение подозрений в том, что используемые Ключи доступны лицам, не имеющим на то полномочий, и/или процессам. К событиям, влекущим за собой Компрометацию Ключей, относятся, включая, но не ограничиваясь, следующие события: - утрата Носителей с Ключами, в том числе с последующим обнаружением; - доступ посторонних лиц (не Уполномоченных представителей Клиента) к Ключам; - сбой (поломка) Носителя с Ключами; - удаление Ключа ЭП по вине Клиента; - случаи, когда нельзя достоверно установить, что произошло с Ключом ЭП (в том числе случаи, когда Ключ ЭП/Носитель с Ключами вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий); - другие события, которые, по мнению Сторон, свидетельствуют о наличии возможности несанкционированного доступа третьих лиц к Ключам.	**Key Compromise** – suspicions that the used Keys are accessible to unauthorized third parties and/or processes. Events entailing the Key Compromise include, but not limited to the following: - loss of the Carriers with the Keys, including with their subsequent finding; - access by third parties (other than the Authorized Representatives of the Client) to the Keys - failure (breakdown) of the Carrier with Keys; - deletion of the ES Key due to the Client's fault; - situations where it is impossible to reliably determine what happened to the ES Key (including cases where the ES Key/Carrier with Keys is damaged, and the possibility of unauthorized actions cannot be definitively ruled out); - other events, which according to the Parties evidence the possibility of unauthorized access of third parties to the Keys.
Логин – уникальная последовательность буквенных/цифровых символов, используемая для Аутентификации Клиента в Системе.	**Login** – a unique sequence of alphanumeric characters used for Client Authentication in the System.
Несанкционированный доступ – наличие оснований полагать, что Система доступна неуполномоченным лицам, независимо от того, нанесен или нет ущерб Банку и/или Клиенту. К событиям, связанным с Несанкционированным доступом или подозрением на такой доступ, относятся, включая, но не ограничиваясь, следующие события: - утеря Пароля для входа в Систему;	**Unauthorized Access** – grounds to believe that the System is accessible to unauthorized persons, regardless of whether damage has occurred to the Bank and/or the Client. Events related to Unauthorized Access or suspicion thereof include, but are not limited to, the following: - loss of the Password for accessing the System;

- доступ к Системе (в том числе к Электронным документам) и ее использование лицами, не имеющими на то полномочий; - полная или временная утрата контроля доступа к Системе лиц, уполномоченных Клиентом для работы в Системе; - обнаружение использования Системы без согласия Клиента, а также в случае, если Клиент/Банк подозревает возможность возникновения подобных ситуаций; - возникновение подозрений на утечку информации или ее искажение в Системе; - заражение автоматизированного рабочего места Клиента вредоносными программами; - «хакерская» атака на информационные системы Клиента; - обнаружение попытки совершения каких-либо иных несанкционированных действий, которые могут привести к сбоям либо иным образом нанести ущерб Клиенту/Банку или другим пользователям Системы.	- access to the System (including Electronic Documents) and its use by the persons who do not have the authorization to do so; - complete or temporary loss of access control to the System by persons authorized by the Client to use the System; - detection of the System's use without the Client's consent, or when the Client/Bank suspects such situations may occur; - suspicions of information leakage or distortion within the System; - infection of the Client's automated workstation with malicious software; - "hacker" attacks on the Client's information systems; - detection of any other unauthorized actions that may lead to system failures or otherwise cause harm to the Client/Bank or other System users.
Носитель с Ключами – съемный/ отчуждаемый носитель информации, предназначенный для записи, хранения, воспроизведения Ключей ЭП. Для целей Условий под Носителем с Ключами понимается USB-Токен, USB-флеш-накопитель.	**Carrier with the Keys** – a removable/portable information carrier designed for recording, storing, and reproducing ES Keys. For the purposes of the Terms, Carrier with the Keys includes USB tokens and USB flash drives.
Пакет операций – перечень банковских операций и/или сделок, осуществляемых посредством Системы, вид которого определяется Банком в соответствии с полномочиями Уполномоченного представителя и/или Уполномоченного лица Клиента, подписавшего Заявление о присоединении к Условиям/Заявление об изменении Соглашения/Заявление о внесении изменений в Договор ДБО.	**Package of Operations** – a list of banking operations and/or transactions conducted through the System, the type of which is determined by the Bank based on the powers of the Authorized Representative and/or Authorized Person of the Client who signed the Application for accession to the Terms/Application for change of Agreement/Application for amendments to the RBS Contract.
Виды Пакетов операций:	**Types of Packages of Operations:**
«Стандартный» – включает в себя осуществление посредством Системы банковских операций (в том числе расчетных) по Счетам, осуществление депозитарных операций, заключение договоров банковского счета (далее – «**ДБС**») при открытии второго и последующих банковских счетов, заключение договоров банковского вклада (депозита), заключение дополнительных соглашений к Договору ДБО, заключение договора об	"**Standard**" – includes the execution of banking operations (including settlement operations) through the System on Accounts, depository operations, execution of Bank Account Agreements (hereinafter "**BAA**") when opening the second and subsequent bank accounts, execution of bank deposit contracts, execution of addenda to the RBS Contract, execution of acquiring service contracts, execution of loan agreements (including, but

оказании Банком услуг эквайринга, заключение кредитных договоров (в том числе, но не ограничиваясь, соглашений о предоставлении кредитной линии, кредитных договоров, заключаемых в рамках соглашений о порядке предоставления кредитов) и иных сделок (в том числе, но не ограничиваясь, залог, поручительство, соглашение о предоставлении банковских гарантий, соглашение о порядке предоставления кредитов), предложение (оферта) заключить которые с помощью Системы поступили Клиенту от Банка, а также осуществление операций и действий в соответствии с условиями заключенных между Сторонами ДБС и иных соглашений.	not limited to, credit line agreements and loan agreements executed under agreements on the procedure for providing loans), and other transactions (including, but not limited to, pledges, guarantees, and agreements on the provision of bank guarantees, agreements on the procedure for providing loans). The offers to conclude these are provided to the Client by the Bank through the System, as well as the execution of operations and actions under the terms of the BAAs and other agreements concluded between the Parties.
«Расчетный» – включает в себя осуществление посредством Системы переводов денежных средств по Счетам в рамках применяемых форм безналичных расчетов, заключение ДБС при открытии второго и последующих банковских счетов, заключение дополнительных соглашений к Договору ДБО, а также совершение других действий в соответствии с условиями заключенных между Сторонами ДБС и Договора ДБО.	"**Settlement**" – includes the execution of fund transfers through the System on Accounts within the applicable forms of cashless settlements, execution of BAAs when opening the second and subsequent bank accounts, execution of addenda to the RBS Contract, and other actions as per the terms of the BAAs and the RBS Contract concluded between the Parties.
«Расчетный Плюс» – включает в себя осуществление посредством Системы переводов денежных средств по Счетам в рамках применяемых форм безналичных расчетов, заключение ДБС при открытии второго и последующих банковских счетов, заключение между Сторонами договоров банковского вклада (депозита), их исполнение и/или расторжение, заключение дополнительных соглашений к Договору ДБО, а также совершение других действий в соответствии с условиями заключенных между Сторонами ДБС, Договора ДБО и договоров банковского вклада (депозита).	"**Settlement Plus**" – includes the execution of fund transfers through the System on Accounts within the applicable forms of cashless settlements, execution of BAAs when opening the second and subsequent bank accounts, execution, performance, and/or termination of bank deposit contracts between the Parties, execution of addenda to the RBS Contract, and other actions under the terms of the BAAs, the RBS Contract, and bank deposit contracts concluded between the Parties.
«Нестандартный» – совокупность банковских операций и/или сделок, осуществляемых посредством Системы, отличных от установленных Пакетами операций «Стандартный», «Расчетный» и «Расчетный Плюс». Описание Пакета операций «Нестандартный» содержится в Приложении № 1 к Заявлению о присоединении к Условиям/Приложении № 1 к Заявлению об	"**Non-standard**" – a set of banking operations and/or transactions conducted through the System that differ from the operations defined in the Standard, Settlement, and Settlement Plus Packages of Operations. The description of the Non-standard Package of Operations is provided in Annex No. 1 to the Application for accession to the Terms/Annex No. 1 to the Application for change of Agreement/Annex

изменении Соглашения/Приложении № 1 к Заявлению о внесении изменений в Договор ДБО.	No. 1 to the Application for amendments to the RBS Contract.
Пароль – уникальная алфавитно-цифровая последовательность символов, известная только Уполномоченному представителю Клиента, соответствующая его Логину и использующаяся для Аутентификации Уполномоченного представителя Клиента в Системе. Пароль может использоваться многократно.	**Password** – a unique alphanumeric sequence known only to the Authorized Representative of the Client, corresponding to their Login and used for the Authentication of the Authorized Representative of the Client in the System. The Password may be reused multiple times.
Плановая смена Ключей – создание Уполномоченным представителем Клиента новых Ключей, которое осуществляется до истечения срока действия действующего Ключа проверки ЭП.	**Planned change of Keys** – generation of new Keys by the Client's Authorized Representative before the expiry of the current ES verification Key.
Проверка ЭП Электронного документа – проверка соотношения, связывающего хэш-функцию Электронного документа, ЭП и Ключа проверки ЭП подписавшего абонента. Если такая проверка, произведенная с использованием Средств электронной подписи, даст положительный результат, то ЭП признается правильной, а сам Электронный документ – подлинным, без искажений, в противном случае Электронный документ считается ошибочным, а ЭП под ним – недействительной.	**Check of the Electronic Signature of an Electronic Document** – check of the interrelation between the Electronic Document connecting the hash function, Electronic Signature and an ES verification Key of the signing subscriber. If such check, conducted with using the Electronic Signature means, provides a positive result, then the Electronic Signature is acknowledged as correct, and the Electronic Document is found authentic, without distortions, otherwise the Electronic Document is found faulty, and the Electronic Signature thereto as invalid.
Рабочий день – день, не являющийся нерабочим днем согласно следующему определению. Нерабочими днями считаются субботы и воскресенья (выходные дни), за исключением объявленных рабочими днями в установленном законодательством Российской Федерации порядке, а также нерабочие праздничные дни, установленные Трудовым кодексом Российской Федерации, и те дни, на которые в силу норм законодательства Российской Федерации переносятся выходные дни.	**Business day** – a day which is not a non-business day according to the following definition. As non-business days are considered Saturdays and Sundays (weekends) with the exception of the days declared as Business Days in accordance with the procedure established by the legislation of the Russian Federation, as well as public holidays established by the Labour Code and the days to which non-working days are transfered due to provisions of the legislation of the Russian Federation.
Сертификат ключа проверки ЭП – электронный документ или документ на бумажном носителе, выданный Банком/Удостоверяющим центром и подтверждающий принадлежность Ключа проверки ЭП Владельцу сертификата ключа проверки ЭП.	**ES verification key Certificate** – an electronic or paper document issued by the Bank/Certification Authority, which confirms the belonging of the ES verification Key to the ES verification key certificates Holder.

Система «Клиент-Банк» (Система) – корпоративная информационная система дистанционного (удаленного) банковского обслуживания, организованная Банком, представляющая собой комплекс программно-технических средств и организационных мероприятий для создания, защиты, передачи и обработки Электронных документов с использованием сети «Интернет». Система используется как электронное средство платежа, а также для обмена Электронными документами между Банком и Клиентом и обеспечивает создание Комплекта Ключей, создание ЭП в Электронном документе, подтверждение подлинности ЭП в Электронном документе.	**Client-Bank System (System)** – a corporate IT system for remote banking services established by the Bank, which is a set of software and hardware and organizational measures for generating, protecting, transmitting, and processing Electronic Documents using the Internet. The System is used as electronic means of payment, as well as for exchange of Electronic Documents between the Bank and the Client, and provides the generation of Set of Keys, ES generation in an Electronic Document, confirmation of the ES authenticity in the Electronic Document.
СБП – сервис быстрых платежей платежной системы Банка России.	**FPS** – faster payments service launched by the Bank of Russia's payment system.
Средства обработки и хранения информации – программно-аппаратные средства, требования к которым приведены в Приложении №1 к Условиям.	**Products designed for processing and storage of information** – software and hardware, requirements for which are shown in Annex No. 1 to the Terms.
Средства Электронной подписи (Средства криптографической защиты информации) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание Ключа ЭП и Ключа проверки ЭП. Для создания и проверки ЭП, создания Ключей Банком используются сертифицированные криптографические средства защиты информации «КриптоПро», Клиентом используются сертифицированные криптографические средства защиты информации «КриптоПро» (далее – СКЗИ КриптоПро)[1] или криптографические средства защиты информации «OpenSSL» (далее – СКЗИ OpenSSL)[2]. Тип СКЗИ, используемого Клиентом, устанавливается Договором ДБО.	**Electronic signature means (Information cryptographic security products)** – cryptographic (coding) means or tools used to perform at least one of the following functions: creation of the Electronic Signature, verification of the same, creation of the Electronic signature Key and Electronic signature verification Key. To create and verify the Electronic Signature and to create Keys, the Bank shall use certified cryptographic tools for protection of information CryptoPro, the Client shall use certified cryptographic tools for protection of information CryptoPro (hereinafter referred to as CryptoPro ICSP)[1] or OpenSSL cryptographic tools for protection of information (OpenSSL ICSP)[2]. The type of

[1] Вывоз полученных Клиентом от Банка СКЗИ КриптоПро с территории Российской Федерации возможен только на основании решения уполномоченного органа/организации в соответствии с законодательством Российской Федерации, при отсутствии указанного решения установка Системы осуществляется по адресу, находящемуся на территории Российской Федерации. / The export of CryptoPro ICSP obtained by the Client from the Bank outside the territory of the Russian Federation is only possible based on a decision by the authorized body/organization in accordance with the legislation of the Russian Federation. Without such a decision, the System must be installed at an address located within the territory of the Russian Federation.

[2] С возможностью вывоза с территории Российской Федерации без получения соответствующего разрешения уполномоченных органов/организаций в соответствии с законодательством Российской Федерации. / With the possibility of export from the territory of the Russian Federation without obtaining the corresponding authorization from the competent authorities/organizations in accordance with the legislation of the Russian Federation.

	ICSP used by the Client shall be set by the RBS Contract.
Сторона (Стороны) – Банк и/или Клиент.	**Party (Parties)** – Bank and/or Client.
Счет – счет, открытый Банком Клиенту на момент заключения Договора ДБО или счета, которые будут открыты Банком Клиенту в будущем, на основании соответствующих ДБС, заключенных между Сторонами.	**Account** – the account opened by the Bank for the Client at the time of the conclusion of the RBS Contract or accounts which will be opened by the Bank for the Client in the future, based on the corresponding BAAs, concluded between the Parties.
Тарифы – размеры вознаграждения Банка за оказываемые по Договору ДБО работы и услуги. Тарифы устанавливаются Банком.	**Tariffs** – amount of remuneration of the Bank for the works and services rendered under the RBS Contract. Tariffs are set by the Bank.
Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Законом № 63-ФЗ.	**Certification Authority** – a legal entity, sole trader, or government/local government body that performs functions for the creation and issuance of qualified electronic signature verification certificates, as well as other functions provided for under Federal Law No. 63-FZ.
Уполномоченное лицо Клиента/Банка – лицо, действующее от имени и в интересах Клиента/Банка, полномочия которого основаны на доверенности, договоре, акте уполномоченного государственного органа или органа местного самоуправления, законе.	**Authorized Person of the Client/Bank** – a person acting on behalf of and in the interests of the Client/Bank whose authority is based on a power of attorney, contract, act of an authorized government body or local government body, or by law.
Уполномоченный представитель Клиента – физическое лицо, указанное в Заявлении на доступ, наделенное Клиентом правом подписания Электронных документов ЭП для последующей передачи посредством Системы и/или входа в Систему, создания любых Электронных документов, установления защищенного соединения с Банком для приема и отправки любых Электронных документов, подписанных ЭП Клиента, и владеющее Ключом ЭП, позволяющим создавать ЭП в Электронных документах (подписывать Электронные документы) и идентифицировать Уполномоченного представителя Клиента в Системе, а также наделенное иными полномочиями в соответствии с установленным Пакетом операций Клиента.	**Authorized Representative of the Client** – an individual specified in Access Application and empowered by the Client to sign Electronic Documents with an Electronic Signature for subsequent transfer by means of the System and/or logging in the System, to generate any Electronic Documents, to establish a secure connection with the Bank for reception and transmission of any Electronic Documents signed by the Client’s Electronic Signature, and possessing an Electronic signature Key, which allows to generate an Electronic Signature in Electronic Documents (to sign Electronic Documents) and to identify the Authorized Representative of the Client in the System, as well as endowed with other powers in accordance with the established Client's Package of Operations.

Усиленная квалифицированная электронная подпись (УКЭП)[3] – электронная подпись, которая соответствует всем признакам усиленной неквалифицированной электронной подписи и следующим дополнительным признакам: - Ключ проверки ЭП содержится в квалифицированном сертификате; - для создания и проверки ЭП используются Средства Электронной подписи, получившие подтверждение соответствия требованиям, установленным Законом № 63-ФЗ. УКЭП выдается Удостоверяющим центром, аккредитованным Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации/ Федеральной налоговой службой Российской Федерации, которые осуществляют функции по созданию и выдаче квалифицированных Сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Законом № 63-ФЗ.	**Enhanced qualified electronic signature (EQES)**[3] – an electronic signature that meets all the characteristics of an enhanced unqualified electronic signature and the following additional criteria: - the ES verification Key is contained in a qualified certificate; - the ES is created and verified using Electronic signature means that have been certified to meet the requirements established under Federal Law No. 63-FZ. The EQES is issued by a Certification Authority accredited by the Ministry of Digital Development, Communications, and Mass Media of the Russian Federation or the Federal Tax Service of the Russian Federation, which also performs functions for the creation and issuance of qualified ES verification Certificates and other functions provided for under Federal Law No. 63-FZ.
Усиленная неквалифицированная электронная подпись (УНЭП) – электронная подпись, выпущенная Банком, которая: - получена в результате криптографического преобразования информации с использованием Ключа ЭП; - позволяет определить лицо, подписавшее Электронный документ; - позволяет обнаружить факт внесения изменений в Электронный документ после момента его подписания; - создается с использованием Средств Электронной подписи.	**Enhanced unqualified electronic signature (EUES)** – an electronic signature issued by the Bank, which: - is generated as a result of cryptographic transformation of information using the ES Key; - allows to identify the person who signed the Electronic Document; - allows detecting the fact of making changes to an Electronic Document after the moment of its signing; - is created using the Electronic signature means.
Условия СБП – Условия предоставления сервиса по переводу денежных средств в рамках системы быстрых платежей для юридических лиц, утвержденные Банком. Условия СБП публикуются Банком в порядке, предусмотренном п. 14.7 настоящих Условий.	**FPS Terms** – Terms of providing the service for transfer of funds in the frame of the faster payments system for legal persons approved by the Bank. The FPS Terms are published by the Bank according to the procedure provided in paragraph 14.7 of these Terms.
Хэш-функция – алгоритм[4] вычисления контрольной последовательности для произвольных электронных сообщений с	**Hash function** – calculation algorithm[4] of the control sequence for the random electronic messages for the purpose of evidentiary control of their entirety.

[3] Применяется при наличии технической возможности у Банка. Одновременное использование в Системе УКЭП и УНЭП одним Уполномоченным представителем Клиента, являющимся ЕИО, не допускается./ Applies if the Bank has the technical capability. Simultaneous use of the EQES and the EUES in the System by the Authorized Representative of the Client, who is the SEB, is not permitted.

[4] Для СКЗИ КриптоПро – определенный действующим ГОСТом./ For CryptoPro ICSP – as specified in the current GOST standards.

целью доказательной проверки их целостности.	
Шифрование – преобразование данных исходных (открытых) сообщений таким образом, что их смысл становится недоступным для любого лица, не владеющего секретом обратного преобразования[5].	**Encryption** – transformation of the data of original (public) messages in such a way that their meaning becomes inaccessible to anyone who does not possess the secret of reverse transformation[5].
Расшифрование – операция обратная шифрованию.	**Decryption** – reverse operation of encryption.
Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию, рассматриваемая как аналог собственноручной подписи соответствующего Уполномоченного представителя Клиента. В рамках Условий под Электронной подписью понимается Усиленная неквалифицированная электронная подпись (УНЭП), выпущенная Банком/Усиленная квалифицированная электронная подпись (УКЭП), выпущенная Удостоверяющим центром для ЕИО.	**Electronic Signature (ES)** – an information in digital form, which is attached to another digital information (signed information) or is linked otherwise to such an information and is used to identify a person, who signs the information, considered as an analogue of the handwritten signature of the respective Authorized Representative of the Client. For the purposes of these Terms Electronic Signature refers to an Enhanced Unqualified Electronic Signature (EUES) issued by the Bank / Enhanced Qualified Electronic Signature (EQES) issued by a Certification Authority for the SEB.
Электронный документ – электронное сообщение, подписанное ЭП, а также платежное требование, требующее получения акцепта Клиента, не подписанное ЭП, и переданное одной из Сторон другой Стороне посредством Системы, в котором информация представлена в электронной форме, равнозначное документу на бумажном носителе, подписанному собственноручной подписью (собственноручными подписями) Уполномоченных лиц Сторон и скрепленному печатью.	**Electronic Document** – an electronic message, which is signed with ES, as well as a payment order which requires the Client's acceptance and not signed with ES, and transmitted by one of the Parties to the other Party via the System presenting information in an electronic form, and which is equivalent to a hard copy document signed with a handwritten signature (handwritten signatures) of the Authorized Representatives of the Parties and bearing a seal.
1. ОБЩИЕ ПОЛОЖЕНИЯ	**1. GENERAL PROVISIONS**
1.1. Настоящие Условия использования электронной системы дистанционного банковского обслуживания (далее – Условия) регулируют отношения, возникающие при предоставлении Банком Клиенту услуг ДБО, а	1.1. These Terms of use of an electronic system for remote banking services (hereinafter referred to as the Terms) regulate the relations arising from the provision of RBS services by the Bank to the Client, as well as the rights,

[5] Для СКЗИ КриптоПро – при шифровании используется алгоритм криптографического преобразования действующего ГОСТа. / For CryptoPro ICSP – encryption uses a cryptographic transformation algorithm defined by the applicable GOST standard.

также возникающие в связи с этим права, обязанности и ответственность Сторон. 1.2. Условия являются типовыми для всех Клиентов и могут быть приняты Клиентом не иначе как путем присоединения к Условиям в целом в порядке, установленном Условиями. Заключение Договора ДБО осуществляется путем присоединения Клиента к Условиям в целом в соответствии со ст.428 Гражданского кодекса Российской Федерации и производится путем подписания Клиентом Заявления о присоединении к Условиям. Датой заключения Договора ДБО является дата подписания Банком Заявления о присоединении к Условиям с проставлением на Заявлении о присоединении к Условиям подписи Уполномоченного лица и печати Банка. Далее положения Условий применяются соответственно установленному Пакету операций. 1.3. Услуги Дистанционного банковского обслуживания предоставляются Клиентам на основании Договора ДБО. 1.4. Информационный обмен в рамках Системы осуществляется с использованием сети «Интернет». 1.5. Для обеспечения конфиденциальности Электронного документа при передаче с использованием сети «Интернет», а также для обеспечения авторства, целостности и подлинности Электронного документа в Системе Клиентом используется СКЗИ КриптоПро или СКЗИ OpenSSL, а Банком – СКЗИ КриптоПро. 1.6. Клиент согласен с тем, что использование в Системе СКЗИ OpenSSL/КриптоПро в качестве средств обеспечения конфиденциальности при передаче с использованием сети «Интернет», а также для Аутентификации и обеспечения авторства, целостности и подлинности Электронного документа, являются достаточными, т.е. обеспечивающими защиту интересов Клиента. 1.7. Клиент отказывается от предъявления претензий к Банку, основанием которых является использование СКЗИ OpenSSL/СКЗИ КриптоПро в качестве средств защиты Электронного документа от несанкционированного доступа при передаче с использованием сети «Интернет», а также для	obligations and liability of the Parties arising therefrom. 1.2. The Terms are standard for all Clients and may be accepted by the Client not otherwise than by acceding to the Terms as a whole in accordance with the procedure established by the Terms. The RBS Contract shall be concluded by means of the Client's accession to the Terms as a whole in accordance with Article 428 of the Civil Code of the Russian Federation and shall be made by signing by the Client of the Application for accession to the Terms. The date of conclusion of the RBS Contract is the date of signing of the Application for accession to the Terms by the Bank with the signature of the Authorized Person and the Bank's seal affixed to the Application for accession to the Terms. Further the provisions of the Terms shall be applied according to the established Package of Operations. 1.3. Remote Banking Services are provided to the Clients on the basis of the RBS Contract. 1.4. Informational exchange within the System is made through the use of the Internet. 1.5. In order to assure confidentiality of an Electronic Document during the transfer through the use of the Internet, as well as in order to assure the authorship, the entirety and authenticity of an Electronic Document in the System, the Client uses CryptoPro ICSP or OpenSSL ICSP, and the Bank uses CryptoPro ICSP. 1.6. The Client agrees that the use of OpenSSL ICSP or CryptoPro ICSP in the System as means for the securing of the confidentiality during the transfer through the use of the Internet, as well as to Authenticate and assure the authorship, entirety and authenticity of an Electronic Document, is sufficient, i.e. assuring the protection of Client’s interests. 1.7. The Client refuses to file claims with the Bank, the motivation for which is the use of the OpenSSL ICSP or CryptoPro ICSP as products for the protection of an Electronic Document from unauthorized access during the transfer through the use of the Internet, as well as to assure the authorship and entirety of an Electronic Document.

обеспечения авторства и целостности Электронного документа.	
1.8. Система используется для обмена Электронными документами в форматах, установленных Системой. Формирование Электронных документов и обмен ими осуществляется в соответствии с требованиями Документации. Любая информация, передаваемая Сторонами по Системе, обрабатывается Средствами криптографической защиты информации.	1.8. System is used for the exchange of Electronic Documents in the formats established by the System.. Formation of the Electronic Documents and the exchange thereof is conducted in compliance with the requirements of the Documentation. Any information, transmitted by the Parties through the System, shall be processed by the Information cryptographic security products.
1.9. Банк, обладая соответствующими правами, предоставленными ему в соответствии с договором, заключенным между Банком и ООО «БСС», предоставляет Клиенту право на пользование Системой в течение действия Договора ДБО. Право на пользование предоставляется с учетом ограничений, предусмотренных законодательством Российской Федерации о правовой охране программ для ЭВМ.	1.9. The Bank, possessing the corresponding rights provided under the agreement concluded between the Bank and BSS LLC, grants the Client the right to use the System during the validity of the RBS Contract. The right to use is provided subject to the limitations stipulated by the legislation of the Russian Federation regarding the legal protection of computer software.
1.10. На отношения между Банком и Клиентом распространяются Условия СБП (Клиент считается присоединившимся к Условиям СБП), текст которых опубликован в порядке, предусмотренном п.14.7 настоящих Условий. Банк вправе вносить изменения в Условия СБП в порядке, установленном в Условиях СБП.	1.10. The relationship between the Bank and the Client is subject to the FPS Terms (the client is considered as acceded to the FPS Terms), the text of which is published according to the procedure provided in paragraph 14.7 of these Terms. The Bank has the right to amend the FPS Terms according to the procedure established by these same FPS Terms.
1.11. В случае противоречия Условий СБП условиям, изложенным в Договоре ДБО, Условия СБП имеют приоритет.	1.11. In case of contradiction of the FPS Terms with the terms set forth in the RBS Contract, the FPS Terms shall prevail.
1.12. Стороны признают, что используемые во взаимоотношениях между ними Электронные документы, подписанные ЭП, в том числе вложения в них, а также платежное требование, требующее получения акцепта Клиента, не подписанное ЭП, имеют равную юридическую силу с документами на бумажном носителе, подписанными собственноручными подписями Уполномоченных лиц Сторон и скрепленными печатями, и являются достаточным основанием для выполнения Банком операций, действий, а также для совершения Сторонами сделок.	1.12. Parties acknowledge, that the Electronic Documents, including attachments thereto, used in their mutual relations, which are signed with Electronic Signatures, as well as a payment order which requires the Client’s acceptance and not signed with ES, have an equal legal force to the documents committed on paper, signed with the handwritten signatures of the Authorized Representatives of the Parties and sealed with seals, form a sufficient basis for the execution of operations and actions by the Bank, as well as for consummation by the Parties of the transactions.
1.13. Стороны признают, что используемые ими способы доставки, указанные в Приложении №2 к Условиям, Средства обработки и хранения информации достаточны для обеспечения надежной и эффективной работы по приему, передаче и хранению информации.	1.13. The Parties acknowledge that the methods of delivery used by them under these Terms and specified in Annex No. 2 hereto, and the Information Processing and Safekeeping Means are sufficient for the assurance of a secure and efficient work on the acceptance, transfer and safekeeping of information.

1.14. Электронный документ порождает обязательства Сторон по Договору ДБО, ДБС, а также иным соглашениям между Банком и Клиентом, является офертой или акцептом, если он оформлен передающей Стороной в соответствии с Договором ДБО, ДБС, иными соглашениями между Банком и Клиентом, Документацией, а также офертой Банка, подписан ЭП (за исключением случаев, указанных в Условиях) и передан посредством Системы, а принимающей Стороной получен, и Проверка ЭП Электронного документа дала положительный результат.	1.14. An Electronic Document is binding for the Parties under the RBS Contract , BAAs, as well as other agreements between the Bank and the Client, and constitutes an offer or acceptance in case if it is drawn up by the transmitting Party in compliance with the RBS Contract, BAAs, other agreements between the Bank and the Client, Documentation and the Bank's offer, is signed with an Electronic Signature (save the cases mentioned in these Terms) and transferred through the System, and is received by the Receiving Party, and if the verification of the Electronic Signature on the Electronic Document resulted in a positive outcome.
Электронные документы не могут быть оспорены или отрицаться Сторонами и третьими лицами или быть признаны недействительными только на том основании, что они переданы в Банк с использованием Системы и способов доставки.	Electronic Documents may not be contested or denied by the Parties and third parties or be declared invalid only because they have been submitted to the Bank using the System and methods of delivery.
1.15. Банк и Клиент используют Систему для передачи Электронных документов друг другу в приоритетном порядке, при этом использование Системы не ограничивает права Клиента по предоставлению в Банк платежных, иных документов на бумажном носителе. Настоящим Стороны соглашаются с тем, что в случае поступления в Банк Электронного документа по Системе и соответствующего платежного, иного документа на бумажном носителе, содержащих идентичные условия проведения операции, осуществления соответствующих действий, в том числе по Счету, счету депо, счету по вкладу (депозиту) либо поступления в Банк идентичных Электронных документов, Банк будет рассматривать каждый из указанных документов как самостоятельный платежный, иной документ, и осуществит все действия, необходимые для проведения операции, осуществления соответствующих сделок, действий, в том числе по Счету, счету депо, счету по вкладу (депозиту), в соответствии с каждым из представленных/переданных Клиентом документов.	1.15. The Bank and the Client use the System for the transfer of Electronic Documents to each other in a priority procedure, however the use of the System does not limit the rights of the Client for the provision, to the Bank, of payment and other documents in physical format. Hereby the Parties agree that in case the Bank receives an Electronic Document transferred through the System and the corresponding payment, other document on paper, containing identical conditions for the commission of an operation, performance of relevant actions, including operations on an Account, depot-account, deposit account or the reception by the Bank of identical Electronic Documents, the Bank will consider each of the specified documents as an individual payment or other document, and will carry out all the actions, required for the commissioning of an operation, appropriate transactions and actions, including on the Account, depot-account, deposit account in compliance to each of the documents presented/transferred by the Client.
1.16. Внутренние процедуры использования Клиентом Системы и его внутренний документооборот устанавливаются Клиентом самостоятельно.	1.16. Internal procedures for the use of the System by the Client and its internal documentation management are established by the Client individually.

1.17. Стороны признают в качестве единой шкалы времени при работе с Системой местное время г. Москвы[6].	1.17. The Parties recognize Moscow local time as the sole time reference when operating the System[6].
1.18. Клиент уведомлен о том, что информация, передаваемая Банком посредством Системы, не является информацией «в реальном времени», за исключением информации об операциях в СБП.	1.18. The Client is notified that the information, transferred by the Bank through the System is not “real time” information, except for information on operations performed in the FPS.
1.19. В целях проведения Банком идентификации представителей Клиента, Клиентом предоставляются в Банк документы, удостоверяющие личность Уполномоченных лиц/Уполномоченных представителей Клиента и/или документы, подтверждающие право иностранных граждан или лиц без гражданства на пребывание (проживание в Российской Федерации). Указанные документы предоставляются в Банк в оригинале или в виде копий, заверенных нотариально (документы, выданные компетентными органами иностранных государств – при условии их легализации).	1.19. For the purpose of identifying by the Bank the Client’s representatives, the Client shall provide the Bank with documents verifying the identity of Authorized Persons/Authorized Representatives of the Client and/or documents confirming the right of foreign citizens or stateless persons to stay (reside) in the Russian Federation. The specified documents shall be submitted to the Bank in original form or as notarized copies (documents issued by competent authorities of foreign states require legalization).
Для Уполномоченных представителей Клиента с полномочиями «без права подписи» документы, удостоверяющие личность Уполномоченных представителей Клиента и/или документы, подтверждающие право иностранных граждан и лиц без гражданства на пребывание (проживание) в Российской Федерации, могут быть представлены в Банк в копиях, заверенных в порядке, установленном Банком.	For Authorized Representatives of the Client with “no signing authority,” identity documents and/or documents confirming the right of foreign citizens or stateless persons to stay (reside) in the Russian Federation may be submitted to the Bank in copies, certified in accordance with the Bank’s procedure.
Документы, представляемые Клиентом и составленные на иностранном языке, должны сопровождаться переводом на русский язык, за исключением случаев, установленных законодательством Российской Федерации. Перевод на русский язык должен быть заверен в порядке, установленном законодательством Российской Федерации.	Documents provided by the Client and drafted in a foreign language must be accompanied by a Russian translation, except as provided by the legislation of the Russian Federation. The translation must be certified in accordance with the legislation of the Russian Federaion.
1.20. В целях проверки полномочий Уполномоченных лиц/Уполномоченных представителей Клиента Клиентом предоставляются в Банк документы, подтверждающие полномочия указанных лиц на совершение банковских операций и/или сделок, осуществляемых посредством Системы в рамках установленного Пакета	1.20. To verify the authority of Authorized Persons/Authorized Representatives of the Client, the Client shall provide the Bank with documents confirming the authority of such persons to carry out banking operations and/or transactions through the System within the established Package of Operations, as well as any other necessary authorizations.

[6] Порядок приема и обработки платежей в рамках СБП определен Условиями СБП. / The procedure for accepting and processing payments under the FPS is defined by the FPS Terms.

операций, а также иные необходимые полномочия.	
1.21. Клиент, ранее заключивший с Банком Соглашение об использовании электронной системы дистанционного банковского обслуживания, вправе заключить с Банком Договор ДБО путем подачи в Банк Заявления об изменении Соглашения. С момента подписания Банком указанного заявления соответствующее соглашение (со всеми изменениями и дополнениями) считается действующим в редакции указанного заявления и Условий, а также считается заключенным между Сторонами новым Договором ДБО (номер Договора ДБО присваивается Банком, датой Договора ДБО считается дата подписания Заявления об изменении Соглашения Банком, отметки о номере и дате соответствующего Договора ДБО проставляются Банком при подписании Заявления об изменении Соглашения).	1.21. A Client who has previously concluded an Agreement on the use of an electronic system for remote banking services with the Bank has the right to enter into the RBS Contract by submitting an Application for change of Agreement to the Bank. From the moment the Bank signs the specified application, the relevant agreement (with all amendments and supplements) is considered to be in effect as amended by the application and the Terms and is deemed a new RBS Contract concluded between the Parties. The RBS Contract number is assigned by the Bank, and the date of the RBS Contract is the date the Bank signs the Application for change of Agreement. The Bank marks the RBS Contract number and date when signing the Application for change of Agreement.
Указанное в настоящем пункте заявление подается в Банк на бумажном носителе в 2 (двух) экземплярах, один из которых после подписания Банком возвращается Клиенту.	The specified application shall be submitted to the Bank in paper form in 2 (two) copies, one of which is returned to the Client after being signed by the Bank.
2. <u>ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К СИСТЕМЕ</u>	**2. <u>PROCEDURE FOR CONNECTING THE CLIENT TO THE SYSTEM</u>**
2.1. Для участия в обмене Электронными документами Клиент выполняет следующие действия: а) назначает и наделяет соответствующими полномочиями Уполномоченного представителя Клиента; б) предоставляет в Банк на бумажном носителе 2 (два) экземпляра заполненного Заявления о присоединении к Условиям; в) для каждого Уполномоченного представителя Клиента предоставляет в Банк на бумажном носителе 2 (два) экземпляра заполненного Заявления на доступ с приложением документов, по форме и содержанию соответствующих п.1.19, п.1.20 настоящих Условий; г) в случае использования УКЭП ЕИО: - самостоятельно получает в Удостоверяющем центре Средство ЭП и Сертификат ключа проверки УКЭП для ЕИО. Процедура получения УКЭП определяется требованиями Удостоверяющего центра;	2.1. For participation in the exchange of Electronic Documents, the Client performs the following actions: a) appoints and delegates the respective authorities to Authorized Representative of the Client; b) submits to the Bank 2 (two) paper copies of the completed Application for accession to the Terms; c) for each Authorized Representative of the Client submits to the Bank 2 (two) paper copies of the completed Access Application with attached documents in form and content compliant with paragraphs 1.19, 1.20 of these Terms; d) in the case of using the EQES of the SEB: - independently obtains the ES tools and the EQES verification key Certificate for the SEB from the Certification Authority. The procedure for obtaining the EQES is determined by the requirements of the Certification Authority;

- предоставляет в Банк Сертификат ключа проверки УКЭП в электронном виде (на отчуждаемом носителе или путем направления на адрес электронной почты Центра технической поддержки клиентов dbo@efbank.ru (только в заархивированном виде));	- provides the Bank with the EQES verification key Certificate in electronic form (on a portable carrier or by sending it to the Customer Technical Support Center email address dbo@efbank.ru (only in archived form));
д) обеспечивает наличие и приведение оборудования, предназначенного для установки Системы, в соответствие с требованиями к аппаратно-программным средствам, приведенными в Приложении №1 к Условиям.	e) ensures the availability and compliance of the equipment, required for the installation of the System, with the requirements for hardware and software stipulated in Annex No. 1 to the Terms;
2.2. Банк, после принятия от Клиента документов, по форме и содержанию соответствующих подп. б), в) и г) п.2.1 настоящих Условий, предоставляет Клиенту доступ в Систему и выполняет следующие действия: а) регистрирует Клиента в Системе; б) создает в Системе учетные записи Уполномоченных представителей Клиента; в) передает Клиенту Временные Пароли для входа в Систему в соответствии с Заявлением на доступ; г) в случае использования УКЭП ЕИО загружает в Систему электронный Сертификат ключа проверки УКЭП, полученный от Клиента, и ограничивает возможность работы с Ключом ЭП сроком действия Сертификата ключа проверки УКЭП, выданного Удостоверяющим центром; д) проставляет отметки на каждом экземпляре Заявления на доступ и передает один экземпляр указанного заявления Клиенту; е) проставляет отметки на каждом экземпляре Заявления о присоединении к Условиям и передает один экземпляр указанного заявления Клиенту; ж) консультирует Клиента по вопросам установки и эксплуатации Системы после проведения Клиентом подготовительных мероприятий, перечисленных в п.2.1 настоящих Условий.	2.2. The Bank, upon receiving from the Client the documents corresponding in form and content to subparagraphs b), c), and d) of paragraph 2.1 of these Terms, grants the Client access to the System and performs the following actions: a) registers the Client in the System; b) creates System accounts for the Authorized Representatives of the Client; c) provides the Client with Temporary Passwords to access the System in accordance with the Access Application; d) in the case of using the EQES of the SEB uploads the EQES verification key Certificate received from the Client into the System and restricts the use of the ES Key to the validity period of the EQES verification key Certificate issued by the Certification Authority; e) marks each copy of the Access Application and returns one signed copy to the Client; f) marks each copy of the Application for accession to the Terms and returns one signed copy to the Client; g) provides consultations to the Client on the System installation and operation after the Client has completed the preparatory measures listed in paragraph 2.1 of these Terms.
2.3. Клиент после получения от Банка Временного Пароля выполняет следующие действия: а) в случае использования УНЭП: - авторизуется в Системе с помощью Логина и Временного Пароля; - формирует Ключи и записывает их на свой Носитель с Ключами;	2.3. After receiving the Temporary Password from the Bank, the Client performs the following actions: a) in the case of using the EUES: - logs into the System using the Login and Temporary Password; - generates Keys and records them onto the Client's Carrier with the Keys;

- создает и направляет в Банк по Системе электронный Запрос на создание Сертификата ключа проверки ЭП; - предоставляет в Банк по каждому из Уполномоченных представителей Клиента Акт признания, распечатанный из Системы, в 2 (двух) экземплярах, подписанный собственноручными подписями Уполномоченного лица Клиента и соответствующего Уполномоченного представителя Клиента; б) в случае использования УКЭП ЕИО: - авторизуется в Системе с помощью Логина и Временного Пароля; - меняет Временный Пароль, полученный от Банка, на свой Пароль. 2.4. Банк (в случае использования УНЭП) после проверки полученного от Клиента надлежащим образом оформленного Акта признания в 2 (двух) экземплярах выполняет следующие действия: - в течение 2 (двух) Рабочих дней с даты приема Акта признания активирует Ключ проверки ЭП на основании электронного Запроса Клиента на создание Сертификата ключа проверки ЭП; - проставляет отметку о дате начала и окончания срока действия Ключа проверки ЭП на каждом экземпляре принятого от Клиента Акта признания и передает Клиенту один экземпляр указанного акта. 2.5. Клиент (в случае использования УНЭП) после активации Банком в Системе Ключа проверки ЭП осуществляет следующие действия: - авторизуется в Системе с помощью Логина и Временного Пароля; - меняет Временный Пароль, полученный от Банка, на свой Пароль. 2.6. Процесс подключения Клиента к Системе считается завершенным: а) в случае использования УНЭП – с момента активации Банком в Системе первого Ключа проверки ЭП Уполномоченного представителя Клиента из имеющегося у Клиента набора Ключей, выпущенных Банком одному/нескольким Уполномоченным представителям Клиента; б) в случае использования УКЭП ЕИО – с момента загрузки Банком в Систему	- creates and sends to the Bank via the System the electronic Request for the creation of the ES verification key Certificate; - submits to the Bank for each of the Authorized Representatives of the Client the Act of acknowledgement printed out from the System, in 2 (two) copies, bearing handwritten signatures of the authorized person of the Client and of the corresponding Authorized Representative of the Client. b) in the case of using the EQES of the SEB: - logs into the System using the Login and Temporary Password; - changes the Temporary Password received from the Bank to their own Password. 2.4. The Bank, in the case of using the EUES, after verifying the properly executed Act of acknowledgement provided by the Client in 2 (two) copies, performs the following actions: - within 2 (two) Business Days of the Bank from the date of the acceptance of the Act of acknowledgement activates the ES verification Key on the basis of the Client's electronic Request for creation of the ES verification key Certificate; - makes a note on the date of the commencement and completion of the ES verification Key validity period on each copy of the Act of acknowledgement of the ES verification key and delivers to the Client one copy of the said act. 2.5. The Client, in the case of using the EUES, after activation of the ES verification Key by the Bank in the System, performs the following actions: - logs into the System using the Login and Temporary Password; - changes the Temporary Password received from the Bank to their own Password. 2.6.The process of connecting the Client to the System is considered complete: a) in the case of using the EUES – from the moment the Bank activates the first ES verification Key of the Authorized Representative of the Client in the System, from the set of Keys issued by the Bank to one or more of the Authorized Representative of the Client; b) in the case of using the EQES of the SEB – from the moment the Bank uploads into the

электронного Сертификата ключа проверки УКЭП для ЕИО, полученного от Клиента.	System the EQES verification key Certificate for the SEB, received from the Client.
3. ПОРЯДОК ПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ И ПРЕДОСТАВЛЕНИЯ ПРАВА ДОСТУПА В СИСТЕМУ УПОЛНОМОЧЕННОМУ ПРЕДСТАВИТЕЛЮ КЛИЕНТА	**3. PROCEDURE FOR PLANNED CHANGE OF KEYS AND GRANTING THER RIGHT OF ACCESS TO THE SYSTEM TO THE AUTHORIZED REPRESENTATIVE OF THE CLIENT**
3.1. Плановая смена Ключей осуществляется в связи с истечением срока их действия. При Плановой смене Ключей Стороны осуществляют следующие действия: 3.1.1. Клиент: а) в случае использования УНЭП: - формирует в Системе новые Ключи и записывает их на свой Носитель с Ключами; - создает и направляет в Банк электронный Запрос на создание нового Сертификата ключа проверки ЭП; - предоставляет в Банк на бумажном носителе Акт признания в 2 (двух) экземплярах; б) в случае использования УКЭП ЕИО самостоятельно получает в Удостоверяющем центре новый Сертификат ключа проверки УКЭП для ЕИО и передает его в Банк в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@efbank.ru (только в заархивированном виде)). Процедура получения УКЭП определяется требованиями Удостоверяющего центра. 3.1.2. Банк: а) в случае использования УНЭП: - в течение 2 (двух) Рабочих дней с даты получения от Клиента надлежащим образом оформленного Акта признания в 2 (двух) экземплярах активирует новый Ключ проверки ЭП на основании электронного Запроса Клиента на создание Сертификата ключа проверки ЭП; - проставляет отметку о дате начала и окончания срока действия Ключа проверки ЭП на каждом экземпляре принятого от Клиента Акта признания и передает Клиенту один экземпляр указанного акта. б) в случае использования УКЭП ЕИО загружает в Систему новый электронный Сертификат ключа проверки УКЭП, полученный от Клиента, и ограничивает возможность работы с Ключом ЭП сроком	3.1. The Planned change of Keys is performed when the Keys expire. During the Planned change of Keys, the Parties perform the following actions: 3.1.1. Client: a) in the case of using the EUES: - generates new Keys in the System and records them onto their Carrier with the Keys; - creates and submits to the Bank an electronic Request for the creation of a new ES verification Key Certificate; - submits to the Bank 2 (two) paper copies of the Act of acknowledgement; b) in the case of using the EQES of the SEB independently obtains a new EQES verification key Certificate for the SEB from the Certification Authority and submits it to the Bank in electronic form (on a portable carrier or via the System/by email to the Customer Technical Support Center at dbo@efbank.ru (only in archived form)). The procedure for obtaining the EQES is determined by the Certification Authority's requirements. 3.1.2. The Bank: a) in the case of using the EUES: - activates a new ES verification Key based on the Client's electronic Request for the creation of the ES verification key Certificate within 2 (two) Business Days from the date of the receipt from the Client of 2 (copies) of the duly executed Act of acknowledgement ; - makes a note on the date of the commencement and completion of the ES verification Key validity period on each copy of the Act of acknowledgement accepted from the Client and gives one copy of the said act to the Client.. b) in the case of using the EQES of the SEB uploads the new EQES verification key Certificate received from the Client into the System and restricts the use of the ES Key to the validity period of the new EQES

действия нового Сертификата ключа проверки УКЭП, выданного Удостоверяющим центром, при условии совпадения информации, предоставленной Клиентом в Банк с информацией, содержащейся в Сертификате ключа проверки УКЭП.

3.2. Для предоставления права доступа в Систему новому Уполномоченному представителю Стороны совершают действия, перечисленные в подп. в), г) п.2.1, подп. б) – д) п.2.2, п.2.3 – п.2.5 настоящих Условий, при этом новый Сертификат ключа проверки УКЭП для ЕИО, полученный Клиентом в Удостоверяющем центре, также может быть передан в Банк посредством Системы.

4. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ДОГОВОР ДБО/ СВЕДЕНИЯ ОБ УПОЛНОМОЧЕННЫХ ПРЕДСТАВИТЕЛЯХ

4.1. В целях внесения изменений в условия Договора ДБО, Клиент, по мере внесения соответствующих изменений, незамедлительно представляет в Банк документы, подтверждающие соответствующие изменения, и Заявление о внесении изменений в Договор ДБО, форма которого размещена на официальном сайте Банка.

В целях внесения изменений в сведения об Уполномоченных представителях, Клиент, по мере внесения соответствующих изменений, незамедлительно представляет в Банк документы, подтверждающие соответствующие изменения и Заявление об изменении сведений, форма которого размещена на официальном сайте Банка.

Случаи предоставления Клиентом вышеуказанных заявлений установлены данными документами.

4.2. Заявление о внесении изменений в Договор ДБО/Заявление об изменении сведений может быть представлено в Банк в 2 (двух) экземплярах на бумажном носителе или направлено по Системе за ЭП Уполномоченного представителя Клиента (при наличии у него соответствующих полномочий).

В случае изменения телефонного номера Клиента, Кодового слова, а также при установлении Клиенту Пакета операций

verification key Certificate issued by the Certification Authority, provided that the information submitted by the Client to the Bank matches the details in the EQES verification key Certificate.

3.2. To grant access to the System to a new Authorized Representative, the Parties shall perform the actions listed in subparagraphs c) and d) of paragraph 2.1, subparagraphs b) – e) of paragraph 2.2, and paragraph 2.3 – 2.5 of these Terms. Additionally, the new EQES verification key Certificate for the SEB, obtained by the Client from the Certification Authority, may also be submitted to the Bank through the System.

4. PROCEDURE FOR AMENDING THE RBS CONTRACT/INFORMATION ABOUT AUTHORIZED REPRESENTATIVES

4.1. To amend the terms of the RBS Contract, the Client, as corresponding amendmaents are made, shall immediately submit to the Bank the documents confirming the respective changes and an Application for amendments to the RBS Contract, the form of which is available on the Bank's official website.

To change information about the Authorized Representatives, the Client, as corresponding changes are made, shall immediately submit to the Bank the documents confirming the respective changes and an Application for change of information, the form of which is available on the Bank's official website.

The cases in which the Client is required to submit the aforementioned applications are established by these documents.

4.2. The Application for Amendments to the RBS Contract/Application for change of information may be submitted to the Bank in two (2) paper copies or sent through the System with the ES of the Authorized Representative of the Client (provided they have the necessary authority).

In the case of changing the Client’s phone number, Code Word, or when establishing the Non-standard Package of Operations, the

«Нестандартный», Заявление о внесении изменений в Договор ДБО предоставляется Клиентом в Банк только на бумажном носителе. Во всех остальных случаях Заявление о внесении изменений в Договор ДБО/Заявление об изменении сведений может быть направлено в Банк посредством Системы в виде вложения в Электронный документ «Письмо в банк» в формате Word или в виде сканированного образа Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений на бумажном носителе, при этом ЭП в Электронном документе «Письмо в банк» и подпись в сканированном образе Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений на бумажном носителе должны принадлежать одному Уполномоченному представителю Клиента.	Application for amendments to the RBS Contract must be submitted in paper form only. In all other cases, the Application for amendments to the RBS Contract/Application for change of information may be sent to the Bank via the System as an attachment to the Electronic Document “Letter to the Bank” in Word format or as a scanned image of the Application for amendments to the RBS Contract/Application for change of information on paper. In this case, the ES in the Electronic Document “Letter to the Bank” and the signature on the scanned image of the Application for amendments to the RBS Contract/Application for change of information must belong to the same Authorized Representative of the Client.
Датой внесения изменений в Договор ДБО считается дата подписания Банком Заявления о внесении изменений в Договор ДБО с проставлением на нем подписи Уполномоченного лица и печати Банка/направления Банком по Системе письма о принятии (акцепте) Банком Заявления о внесении изменений в Договор ДБО.	The date on which amendments to the RBS Contract take effect shall be considered the date on which the Bank signs the Application for amendments to the RBS Contract with the signature of the Bank’s Authorized Person and the Bank’s seal or the date the Bank sends a letter via the System acknowledging acceptance (approval) of the Application for amendments to the RBS Contract.
В случае поступления Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений в Банк посредством Системы в виде вложения в Электронный документ Банк осуществляет следующие действия: - при положительном решении о принятии указанных заявлений проставляет в Системе статус «Письмо в банк» «Обработан» с указанием информации о принятии указанных заявлений и дате их принятия, а также направляет Клиенту (в качестве акцепта) по Системе письмо о принятии Заявления о внесении изменений в Договор ДБО; - при отрицательном решении о принятии указанных заявлений проставляет в Системе статус «Письма в банк» «Отказано» с указанием причины отказа.	When the Application for amendments to the RBS Contract/Application for change of information is submitted to the Bank through the System as an attachment to an Electronic Document, the Bank performs the following actions: - in the case of a positive decision, the System status of the “Letter to the Bank” is updated to “Processed” with information on the acceptance of the application and the date of acceptance. The Bank also sends the Client a letter through the System confirming acceptance of the Application for amendments to the RBS Contract. - in case of a negative decision regarding the acceptance of the specified statements, sets the status in the System as «Letters to the Bank» «Rejected» with an indication of the reason for the rejection.
4.3. В случае изменения фамилии, имени, отчества (при наличии) Уполномоченного представителя Клиента, Клиент совершает все действия, предусмотренные Условиями для предоставления Уполномоченному представителю права доступа в Систему, и	4.3. In the event of a change in the surname, first name, or patronymic (if applicable) of the Authorized Representative of the Client, the Client performs all actions stipulated by the Terms to grant the Authorized Representative rights of access to the System, and submits to

предоставляет в Банк Заявление об изменении сведений, в котором указывает прежнюю фамилию, имя или отчество (при наличии) соответствующего Уполномоченного представителя.	the Bank an Application for change of information, indicating the previous surname, first name, or patronymic (if applicable) of the respective Authorized Representative.
Банк на основании полученных документов и Заявления об изменении сведений:	The Bank, based on the received documents and the Application for change of information:
- создает в Системе новую учетную запись Уполномоченного представителя Клиента, в которой указывает его новую фамилию, имя или отчество (при наличии);	- creates a new account in the System for the Authorized Representative of the Client, indicating their new surname, first name, or patronymic (if any);
- осуществляет все действия, предусмотренные Условиями для предоставления Уполномоченному представителю права доступа в Систему;	- performs all actions stipulated by the Terms to grant the Authorized Representative the right of access to the System;
- аннулирует в Системе учетную запись Уполномоченного представителя Клиента с прежней фамилией, именем, отчеством (при наличии) и блокирует соответствующий Сертификат ключа проверки ЭП.	- cancels in the System the account of the Authorized Representative of the Client with the previous surname, first name, patronymic (if any) and blocks the corresponding ES verification key Certificate.
В случае изменения иных данных Уполномоченного представителя Клиента, Клиент предоставляет в Банк надлежащим образом заверенные копии документов, по форме и содержанию соответствующих п.1.19 настоящих Условий, и Акт признания в 2 (двух) экземплярах (в случае использования УНЭП), при этом создание нового Комплекта Ключей не требуется.	In the event of changes to other information about the Authorized Representative of the Client, the Client provides the Bank with duly certified copies of documents, in form and content corresponding to paragraph 1.19 of these Terms, and an Act of acknowledgement in 2 (two) copies (in case of using the EUES), while the creation of a new Set of Keys is not required.
4.4. В случае прекращения полномочий Уполномоченного представителя, а также при изменении его фамилии, имени или отчества (при наличии), направление Заявления об изменении сведений означает требование Клиента прекратить прием и исполнение любых Электронных документов, подписанных ЭП, сформированной с использованием Ключа ЭП такого Уполномоченного представителя.	4.4. In the event of the termination of the powers of the Authorized Representative, as well as in the case of a change in their surname, first name, or patronymic (if any), the submission of an Application for change of information signifies the Client's demand to cease the acceptance and execution of any Electronic Documents signed with an ES Key generated using the ES Key of such an Authorized Representative.
4.5. В случае изменения наименования и организационно-правовой формы Клиент:	4.5. In the event of a change in the name and organizational-legal form of the Client:
- при использовании УНЭП: формирует в Системе Запрос на создание Сертификата ключа проверки ЭП, при этом самостоятельно изменяет свое наименование/организационно-правовую форму в Системе, и направляет его в Банк в электронном виде посредством Системы, а также предоставляет в Банк на бумажном носителе Акт признания в 2 (двух) экземплярах;	- when using the EUES: generates a Request for the creation of the ES verification key Certificate in the System, independently changes its name/organizational-legal form in the System, and sends it to the Bank electronically via the System, as well as provides the Bank with the Act of acknowledgement in 2 (two) copies on paper;
- при использовании УКЭП ЕИО: самостоятельно получает в Удостоверяющем	- when using the EQES of the SEB: independently obtains the EQES verification

центре Сертификат ключа проверки УКЭП для ЕИО с новым наименованием/организационно-правовой формой Клиента и передает его в Банк в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@efbank.ru (только в заархивированном виде)).	key Certificate for the SEB with the new name/legal form of the Client from the Certification Authority and submits it to the Bank in electronic form (on a portable carrier, by sending it via the System/to the email address of the Customer Technical Support Center dbo@efbank.ru (only in archived form)).
4.6. В случае смены Средства криптографической защиты информации Банк на основании полученного от Клиента Заявления о внесении изменений в Договор ДБО изменяет в Системе Средство криптографической защиты информации, после чего Клиент (в случае использования УНЭП) осуществляет действия по созданию Уполномоченному представителю нового Ключа проверки ЭП с использованием соответствующего Средства криптографической защиты информации и предоставляет в Банк Акт признания в 2 (двух) экземплярах в соответствии с подп. а) п.3.1.1 настоящих Условий.	4.6. In the event of a change in the Information cryptographic security product, the Bank, based on the Application for amendments to the RBS Contract received from the Client, modifies the Information cryptographic security product in the System. Subsequently, the Client (in the case of using the EUES) performs actions to create a new ES verification Key for the Authorized Representative using the appropriate Information cryptographic security product and provides the Bank with the Act of acknowledgement in 2 (two) copies in accordance with subparagraph a) of paragraph 3.1.1 of these Terms.
После получения от Клиента Акта признания Банк осуществляет действия, указанные в подп. а) п.3.1.2 настоящих Условий.	After receiving the Act of acknowledgement from the Client, the Bank performs the actions specified in subparagraph a) of paragraph 3.1.2 of these Terms.
В случае необходимости использования в Системе УКЭП, выпущенной Удостоверяющим центром для ЕИО, Клиент одновременно с Заявлением о внесении изменений в Договор ДБО предоставляет в Банк Сертификат ключа проверки УКЭП ЕИО в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@efbank.ru (только в заархивированном виде)).	In case of the necessity to use the EQES issued by the Certification Authority for the SEB in the System, the Client simultaneously with the Application for amendments to the RBS Contract provides the Bank with the EQES verification key Certificate of the SEB in electronic form (on a portable carrier, by sending it through the System/to the email address of the Customer Technical Support Center dbo@efbank.ru (only in archived form)).
4.7. В случае использования в Системе УКЭП, выпущенной Удостоверяющим центром для ЕИО, вместо УНЭП, ранее выпущенной Банком для ЕИО, Клиент предоставляет в Банк письмо в произвольной форме на бумажном носителе или посредством Системы с приложением Сертификата ключа проверки УКЭП ЕИО в электронном виде (на отчуждаемом носителе, путем направления по Системе/на адрес электронной почты Центра технической поддержки клиентов dbo@efbank.ru (только в заархивированном виде)).	4.7. In case the EQES issued by the Certification Authority for the SEB is used in the System instead of the EUES previously issued by the Bank for the SEB, the Client provides the Bank with a letter in free form on paper or via the System, attaching the EQES verification key Certificate of the SEB in electronic form (on a portable carrier, by sending it through the System/to the email address of the Customer Technical Support Center dbo@efbank.ru (only in archived form)).
Банк на основании полученного письма Клиента:	The Bank, based on the letter received from the Client:

- загружает в Систему Сертификат ключа проверки УКЭП ЕИО, полученный от Клиента;	- uploads into the System the EQES verification key Certificate of the SEB, received from the Client;
- блокирует в Системе Сертификат ключа проверки УНЭП, выпущенный Банком для ЕИО.	- blocks in the System the EUES verification key Certificate, issued by the Bank for the SEB.
4.8. В случае выпуска Банком УНЭП для ЕИО вместо ранее использовавшейся в Системе УКЭП, выпущенной Удостоверяющим центром для ЕИО, Клиент предоставляет в Банк письмо в произвольной форме на бумажном носителе или посредством Системы.	4.8. In the event that the Bank issues the EUES for the SEB instead of the previously used the EQES in the System, issued by the Certification Authority for the SEB, the Client provides the Bank with a letter in free form on paper or via the System.
Банк на основании полученного письма Клиента:	The Bank, based on the letter received from the Client:
- производит в Системе настройки, позволяющие Клиенту осуществить создание Ключа проверки УНЭП для ЕИО;	- configures the System to enable the Client to create the EUES verification Key for the SEB;
- блокирует в Системе Сертификат ключа проверки УКЭП, выпущенный Удостоверяющим центром для ЕИО.	- blocks in the System the EQES verification key Certificate issued by the Certification Authority for the SEB.
Далее Стороны осуществляют действия, указанные в подп. а) п.3.1.1 и подп. а) п.3.1.2 настоящих Условий.	The Parties shall then perform the actions specified in subparagraph a) of paragraph 3.1.1 and subparagraph a) of paragraph 3.1.2 of these Terms.
4.9. В целях получения нового Временного Пароля для входа в Систему Клиент запрашивает его в Заявлении о Компрометации в момент уведомления Банка о наступлении события Компрометации либо предоставляет в Банк Заявление об изменении сведений в порядке, определенном п.4.2 настоящих Условий.	4.9. For the purpose of obtaining a new Temporary Password to access the System, the Client requests it in the Compromise Statement at the moment of notifying the Bank about the occurrence of a Compromise event or submits to the Bank an Application for change of information in the manner specified in paragraph 4.2 of these Terms.
5. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ И НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ	**5. PROCEDURE FOR ACTIONS IN CASE OF COMPROMISE AND UNAUTHORIZED ACCESS**
5.1. В случае Компрометации Ключей и/или Несанкционированного доступа к Системе/к информационным системам Клиента, Клиент обязан незамедлительно уведомить об этом Банк любым возможным способом и направить в Банк Заявление о Компрометации (по форме Банка) вложенным файлом на официальный адрес электронной почты (e-mail) Банка, указанный в Договоре ДБО, с последующим предоставлением в Банк оригинала указанного заявления.	5.1. In the event of a Compromise of the Keys and/or Unauthorized Access to the System/to the Client's information systems, the Client is obliged to immediately notify the Bank by any possible means and send a Compromise Statement (in the Bank's form) as an attached file to the official email address of the Bank, specified in the RBS Contract, with subsequent provision of the original of the said statement to the Bank.
Банк на основании полученного на официальный адрес электронной почты (e-mail) Банка Заявления о Компрометации:	The Bank, based on the Compromise Statement received at the official email address of the Bank:
а) при Компрометации Ключей:	a) in case of Compromise of the Keys:

- прекращает прием и исполнение любых Электронных документов (полученных, но не исполненных Банком), подписанных ЭП, сформированной с использованием скомпрометированного Ключа ЭП Уполномоченного представителя Клиента; - приостанавливает использование Системы Уполномоченным представителем Клиента и блокирует скомпрометированный Комплект Ключей указанного Уполномоченного представителя Клиента; - аннулирует действующий Пароль Уполномоченного представителя Клиента, формирует Временный Пароль и передает его Клиенту способом, указанным в Заявлении о Компрометации; б) при Несанкционированном доступе к Системе/к информационным системам Клиента: - прекращает прием и исполнение любых Электронных документов (полученных, но не исполненных Банком); - приостанавливает использование Системы Клиентом и блокирует Комплекты Ключей всех Уполномоченных представителей Клиента; - аннулирует действующие Пароли всех Уполномоченных представителей Клиента, формирует Временные Пароли и передает их Клиенту способом, указанным в Заявлении о Компрометации. Клиент, после получения Временных Паролей и устранения последствий Компрометации Ключей и/или Несанкционированного доступа к Системе/информационным системам Клиента, для восстановления доступа в Систему осуществляет действия, перечисленные в подп. г) п.2.1, п.2.3, п.2.5 настоящих Условий.	- ceases the acceptance and execution of any Electronic Documents (received but not executed by the Bank), signed with an ES formed using the compromised ES Key of the Authorized Representative of the Client; - suspends the use of the System by the Authorized Representative of the Client and blocks the compromised Set of Keys of the specified Authorized Representative of the Client; - cancels the current Password of the Authorized Representative of the Client, generates a Temporary Password, and delivers it to the Client in the manner specified in the Compromise Statement; b) in case of Unauthorized Access to the System/to the Client's information systems: - ceases the acceptance and execution of any Electronic Documents (received but not executed by the Bank); - suspends the use of the System by the Client and blocks the Sets of Keys of all Authorized Representatives of the Client; - cancels the active Passwords of all Authorized Representatives of the Client, generates Temporary Passwords, and delivers them to the Client in the manner specified in the Compromise Statement. The Client, after receiving the Temporary Passwords and eliminating the consequences of the Compromise of the Keys and/or Unauthorized Access to the System/information systems of the Client, performs the actions listed in subparagraph d) of paragraph 2.1, paragraph 2.3, paragraph 2.5 of these Terms to restore access to the System.
6. ПРАВА И ОБЯЗАННОСТИ СТОРОН	**6. RIGHTS AND OBLIGATIONS OF THE PARTIES**
6.1. Взаимные права и обязанности Сторон	**6.1. Reciprocal rights and obligations of the Parties**
6.1.1. Стороны при обмене Электронными документами с использованием Системы обязуются руководствоваться правилами и требованиями, установленными законодательством Российской Федерации, ДБС, Договором ДБО, Условиями СБП, иными соглашениями между Банком и Клиентом.	6.1.1. Parties, during the exchange of the Electronic Documents through the use of the System, undertake to be guided by the rules and requirements as set by the legislation of the Russian Federation, BAAs, the RBS Contract, the FPS Terms and other agreements between the Bank and the Client.

6.1.2. Стороны обязуются не разглашать третьей стороне (за исключением случаев, предусмотренных законодательством Российской Федерации и Договором ДБО) информацию о Средствах криптографической защиты информации, используемых в Системе.	6.1.2. Parties undertake not to disclose to a third party (except for cases, as under the legislation of the Russian Federation and the RBS Contract) the information about the Information cryptographic security products used in the System.
6.1.3. Каждая из Сторон обязуется немедленно информировать другую Сторону обо всех случаях Компрометации Ключей, Несанкционированного доступа к Системе, а также повреждения/утраты программно-аппаратных средств обработки, хранения, передачи Электронных документов, Средств криптографической защиты информации, а также Ключей, и не использовать Ключи при наличии оснований полагать, что они скомпрометированы.	6.1.3. Each Party undertakes to immediately inform the other Party about all the cases of Key Compromise, Unauthorized access to the System, as well as the damage to the software and hardware designed for processing, storage and transfer of Electronic Documents, as well as the Information cryptographic security products and Keys, and not to use Keys if there are the reasons to assume that they are compromised.
6.1.4. Любые Электронные документы, передаваемые по Системе, подлежат шифрованию.	6.1.4. Any Electronic Documents transferred within the System, are subject to encryption.
6.1.5. Любые Электронные документы, передаваемые по Системе, должны быть заверены ЭП Стороны-отправителя, за исключением платежного требования, требующего получения акцепта Клиента, не подписанного ЭП. При этом Стороны согласны, что в этом случае Система используется как способ достоверного определения Банка, направившего такое платежное требование Клиенту.	6.1.5. Any Electronic Documents transferred within the System must be certified by an Electronic Signature of the Sending party, except the payment order, which requires the Client’s acceptance not signed with ES. Meanwhile the Parties agree that in this case the System should be used as a mean of reliably defining the Bank, which has sent such a payment order to the Client.
6.1.6. Клиент уведомлен и согласен, что письмо, направленное Клиентом в Банк в соответствии с Договором ДБО со своего официального адреса электронной почты (e-mail) на официальный адрес электронной почты (e-mail) Банка, считается полученным Банком с момента его регистрации как входящего документа во внутренней системе документооборота Банка.	6.1.6. The Client is aware and agrees that the letter sent by the Client to the Bank in accordance with the RBS Contract from its official e-mail address to the Bank's official e-mail address shall be deemed received by the Bank upon its registration as an incoming document in the internal document management system of the Bank.
6.2. Права и обязанности Клиента	**6.2. Rights and obligations of the Client**
6.2.1. Клиент не имеет права тиражировать и передавать третьей стороне программное обеспечение, предоставляемое Банком по Договору ДБО и все конфиденциальные данные, относящиеся к нему.	6.2.1. The Client has no right to replicate and transfer, to a third party, the software, granted by the Bank under the RBS Contract and all the confidential information relating to the Contract.
6.2.2. Клиент имеет право, при необходимости, воспользоваться помощью специалиста Банка по предоставлению права доступа в Систему, направив в Банк письменное заявление.	6.2.2. The Client has the right, if required, to use the assistance of an expert from the Bank in order to obtain the right to access to the System, by directing a written request to the Bank.

6.2.3. Клиент обязуется в сроки, предусмотренные Условиями, обеспечить на Счете остаток денежных средств в размере, необходимом для оплаты услуг Банка в соответствии с Договором ДБО и Тарифами.	6.2.3. The Client within the term specified by the Terms, undertakes to assure that its Account indicate a balance of funds in the amount, required for the payment of services rendered by the Bank as in compliance with the RBS Contract and Tariffs.
6.2.4. Клиент обязуется обеспечивать сохранность и целостность установленной Системы, включая Средства криптографической защиты информации, а также выполнять требования к эксплуатации Системы, изложенные в Документации.	6.2.4. The Client undertakes to assure security and entirety of the installed System, including Information cryptographic security products, as well as implement the requirements for the operation of the System, as specified in the Documentation.
6.2.5. Клиент по требованию Банка обязан предоставить заверенные подписями Уполномоченных лиц Клиента и оттиском печати Клиента (при необходимости ее проставления) копии (на бумажном носителе) Электронных документов, переданных по Системе, в течение 5 (пяти) календарных дней с момента направления ему требования.	6.2.5. The Client, at the request of the Bank, shall present copies (in paper) of Electronic Documents, certified by signatures of the Client's Authorized Persons and the Client's seal impression (if necessary), transmitted through the System, within a period of 5 (five) calendar days from the moment the Bank sends such a requirement.
6.2.6. Клиент обязан незамедлительно информировать Банк об изменении информации, касающейся исполнения Сторонами Договора ДБО, в т.ч. обо всех изменениях в адресах/контактной информации, указанных в Заявлении о присоединении к Условиям/иных документах, предоставленных в Банк в соответствии с Договором ДБО.	6.2.6. The Client is obliged to immediately inform the Bank of any changes in the information related to the performance of the Parties under the RBS Contract, including all changes in addresses/contact information specified in the Application for accession to the Terms/other documents provided to the Bank in accordance with the RBS Contract.
6.2.7. Клиент обязан незамедлительно предоставлять в Банк Заявление об изменении сведений при смене ЕИО в целях подтверждения прав действующих Уполномоченных представителей Клиента или изменения их состава, а также при прекращении полномочий действующего Уполномоченного представителя Клиента.	6.2.7. The Client is obliged to promptly provide the Bank with an Application for change of information in the event of a change of the SEB to confirm the rights of the current Authorized Representatives of the Client or to modify their composition, as well as in the event of termination of the powers of the current Authorized Representative of the Client.
6.2.8. Все риски неблагоприятных последствий, связанных с несвоевременным уведомлением Банка о произошедших изменениях, в том числе, указанных в главе 4, п.6.2.6, п.6.2.7, п.7.10 настоящих Условий, несет Клиент.	6.2.8. All risks of adverse consequences associated with the untimely notification of the Bank about changes that have occurred, including those specified in Chapter 4, paragraphs 6.2.6, 6.2.7, 7.10 of these Terms, are borne by the Client.
6.2.9. Клиент обязан самостоятельно контролировать сроки действия Ключей УНЭП и УКЭП и своевременно инициировать процедуру Плановой смены Ключей до истечения их срока действия.	6.2.9. The Client must independently monitor the validity periods of the EUES and the EQES Keys and timely initiate the Planned change of Keys procedure before their expiration.
Соответствующие уведомления о Плановой смене Ключей размещаются Банком в виде оповещения при каждом входе Клиента в Систему в течение двух месяцев до истечения срока действия Ключей проверки ЭП.	Relevant notifications about the Planned change of Keys are provided by the Bank as a notice each time the Client logs into the System within two months before the expiration of the ES verification Keys.

Действие Ключей прекращается, если до истечения срока их действия: а) в случае использования УНЭП: Клиентом не направлен в Банк по Системе Запрос на создание Сертификата ключа проверки ЭП и/или не предоставлен в Банк на бумажном носителе Акт признания, а также в случае несоответствия указанного акта, полученного Банком от Клиента на бумажном носителе, положениям настоящих Условий; б) в случае использования УКЭП: Клиентом не предоставлен в Банк новый Сертификат ключа проверки УКЭП ЕИО в электронном виде. Для возобновления работы в Системе Клиент создает новый Комплект Ключей, после чего Стороны осуществляют действия, предусмотренные п.3.1 настоящих Условий. 6.2.10. При расторжении Договора ДБО Клиент обязуется уничтожить все предоставленное ему в пользование программное обеспечение (исполняемые и вспомогательные файлы) Системы. 6.2.11. Клиент обязуется не передавать третьим лицам свои права и обязанности по Договору ДБО без письменного согласия Банка. 6.2.12. Клиент обязан проверять наличие новых Электронных документов от Банка, направленных в адрес Клиента, ежедневно, за исключением нерабочих дней Банка, а также ежедневно проверять SMS-сообщения, направленные Банком в связи с выявлением им операций, соответствующих признакам осуществления перевода денежных средств без добровольного согласия Клиента[7]. Клиент обязан не реже одного раза в 5 (пять) календарных дней знакомиться с информацией, публикуемой Банком в соответствии с п.14.7 настоящих Условий. За убытки, возникшие в результате неисполнения Клиентом вышеуказанных обязанностей, Банк ответственности не несет. 6.2.13. Клиент обязуется по требованию и форме Банка предоставлять документы, подтверждающие данные об Уполномоченном представителе Клиента, а также документы, подтверждающие его полномочия на совершение банковских операций и/или сделок, осуществляемых посредством	The Keys' operation ceases if, before their expiration date: a) in the case of using the EUES: The Client has not sent a Request for the creation of the ES verification key Certificate to the Bank through the System and/or has not provided the Bank with the Act of acknowledgement on paper, as well as in the event of a discrepancy between the said act received by the Bank from the Client on paper and the provisions of these Terms; b) in case of using the EQES: The Client has not provided the Bank with a new EQES verification key Certificate of the SEB in electronic form. To resume work in the System, the Client creates a new Set of Keys, after which the Parties perform the actions stipulated in paragraph 3.1 of these Terms. 6.2.10. In case of the termination of the RBS Contract, the Client undertakes to destroy all the software of the System granted to the latter for use (executable and auxiliary files). 6.2.11. The Client undertakes not to transfer its rights and obligations under the RBS Contract, to third parties without a written consent of the Bank. 6.2.12. The Client shall check, on the daily basis, the availability of the new Electronic Documents from the Bank, directed to the Client, except for the Bank's non-working days, as well as daily check SMS messages sent by the Bank in relation to any discovered transaction with signs of money transfer without the voluntary consent of the Client[7]. The Client must at least once every 5 (five) calendar days review the information published by the Bank in accordance with paragraph 14.7 of these Terms. The Bank shall not be liable for losses incurred as a result of the Client’s failure to fulfill the above obligations. 6.2.13. The Client undertakes to provide documents certifying data on the Authorized Representative of the Client on demand and in the form of the Bank, as well as documents confirming its authorisation to perform banking operations and/or transactions carried out via the System within the established

[7] При наличии технической возможности у Банка. / Subject to the Bank's technical capability.

Системы в рамках установленного Пакета операций, а также иные необходимые полномочия.	Package of Operations, as well as other necessary authorisations.
6.2.14. Клиент обязуется соблюдать требования информационной безопасности при работе с Системой, указанные в Приложении № 4 к Условиям, а также направляемые Банком по Системе и размещаемые на официальном сайте Банка в сети «Интернет».	6.2.14. The Client undertakes to comply with information safety requirements specified in Annex No. 4 to the Terms, distributed by the Bank in the System, and posted on the Bank's official website in the Internet in the course of working with the System.
6.2.15. Клиент обязуется немедленно информировать Банк о направлении Электронных документов по Системе под влиянием обмана или при злоупотреблении его доверием.	6.2.15. The Client undertakes to immediately inform the Bank about sending Electronic Documents via the System under the influence of fraud or by breach of trust.
6.2.16. В случае использования УКЭП ЕИО Клиент, помимо обязанностей, установленных настоящими Условиями, обязуется: - самостоятельно получать в Удостоверяющем центре Средство ЭП для создания УКЭП ЕИО; - самостоятельно контролировать сроки действия Сертификатов ключей проверки ЭП, полученных в Удостоверяющем центре, своевременно производить их замену и предоставлять данную информацию Банку в порядке, предусмотренном настоящими Условиями; - незамедлительно сообщать Банку о случаях прекращения действия Сертификата ключа проверки ЭП, в порядке, установленном настоящими Условиями, и прекратить использование УКЭП ЕИО при направлении Электронных документов в Банк по Системе; - обеспечивать конфиденциальность Ключей; - не использовать Ключ ЭП при наличии оснований полагать, что его конфиденциальность нарушена; - незамедлительно уведомлять Банк и Удостоверяющий центр, выдавший Сертификат ключа проверки ЭП, о нарушении конфиденциальности Ключа ЭП при получении информации о таком нарушении; - использовать для создания и проверки УКЭП ЕИО, создания Ключей ЭП и Ключей проверки ЭП Средства Электронной подписи, имеющие подтверждение соответствия требованиям, установленным Законом № 63-ФЗ.	6.2.16. In case of using the EQES of the SEB, the Client, in addition to the obligations established by these Terms, undertakes: - independently obtain an ES tool for creating the EQES of the SEB at the Certification Authority; - independently monitor the validity periods of the ES verification key Certificates obtained from the Certification Authority, promptly replace them, and provide this information to the Bank in the manner prescribed by these Terms; - immediately notify the Bank of any termination of the ES verification key Certificate, in the manner established by these Terms, and cease using the EQES of the SEB when sending Electronic Documents to the Bank through the System; - ensure the confidentiality of the Keys; - do not use the ES Key if there are grounds to believe that its confidentiality has been compromised; - promptly notify the Bank and the Certification Authority that issued the ES verification key Certificate about a breach of confidentiality of the ES Key upon receiving information about such a breach; - use ES Tools with confirmation of compliance with the requirements established by the Law No. 63-FZ for creation and verification of the EQES of the SEB, creation of ES Keys and ES Verification Keys.
6.3. Права и обязанности Банка	**6.3. Rights and obligations of the Bank**
6.3.1. Банк не принимает к исполнению Электронные документы, оформленные с	6.3.1. The Bank does not accept Electronic Documents for execution, drawn up in

нарушением требований законодательства Российской Федерации, Договора ДБО, ДБС, Условий СБП, иных соглашений между Сторонами.	violation of the requirements of the legislation of the Russian Federation, the RBS Contract, BAAs, the FPS Terms and other agreements between the Parties.
6.3.2. Банк имеет право отказать Клиенту в приеме к исполнению Электронного документа, если Клиент заполнил поля Электронного документа с ошибками. В этом случае Клиенту направляется Квитанция с указанием причины отказа[8].	6.3.2. The Bank has the right to refuse the Client in the acceptance for execution of an Electronic Document, if the Client omitted mistakes when filling in such Electronic Document. In this case a Receipt confirmation is sent to the Client specifying the reason for refusal[8].
6.3.3. Банк не имеет права самостоятельно корректировать реквизиты Электронных документов Клиента.	6.3.3. The Bank may not independently correct details of Electronic Documents of the Client.
6.3.4. В случае непредоставления Клиентом документов, указанных в п.4.3 настоящих Условий, Банк не будет нести ответственность за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Клиентом Электронного документа, подписанного Уполномоченным представителем Клиента, данные о котором были предоставлены Клиентом в Банк ранее.	6.3.4. If the Client fails to provide the documents specified in paragraph 4.3 of these Terms, the Bank shall not be liable for the consequences of performing transactions, other actions, deals on the basis of an Electronic Document duly executed by the Client, signed by the Authorized Representative of the Client, details of which were provided by the Client to the Bank earlier.
6.3.5. Банк прекращает прием/исполнение любых Электронных документов в следующих случаях: - если они подписаны ЭП, сформированной с использованием скомпрометированного Ключа ЭП Уполномоченного представителя Клиента; - если они подписаны Ключом ЭП Уполномоченного представителя Клиента после прекращения его полномочий; - если они подписаны УКЭП в случае прекращения действия Сертификата ключа проверки УКЭП; - в случае прекращения действия аккредитации Удостоверяющего центра, выдавшего Клиенту Сертификат ключа проверки УКЭП.	6.3.5. The Bank shall stop accepting and executing any Electronic Documents in the following cases: - if they are signed with an ES generated using a compromised ES Key of the Authorized Representative of the Client; - if they are signed with the ES Key of the Authorized Representative of the Client after their authority has been terminated; - if they are signed with the EQES in the event of the termination of the EQES verification key Certificate; - in the event of the termination of accreditation of the Certification Authority that issued the Client the EQES verification key Certificate.
Все Электронные документы, поступившие в Банк до принятия Банком Заявления о внесении изменений в Договор ДБО/Заявления об изменении сведений/Заявления о Компрометации, исполняются в порядке, установленном Условиями или иными соглашениями между Сторонами.	All Electronic Documents received by the Bank prior to the Bank's acceptance of the Application for amendments to the RBS Contract/Application for change of information/Compromise Statement shall be executed in accordance with the procedure established by the Terms or other agreements between the Parties.

[8] Порядок приема и обработки платежей в рамках СБП определен Условиями СБП. / The procedure for acceptance and processing of payments in the frame of FPS is established by the FPS Terms.

В случае непредоставления оригинала Заявления о Компрометации на бумажном носителе Банк не будет нести ответственность за убытки, причиненные Клиенту в результате прекращения приема и исполнения Электронных документов, подписанных ЭП, сформированной с использованием соответствующего скомпрометированного Ключа ЭП.	In the event that the original Compromise Statement is not provided on paper, the Bank shall not be held liable for losses incurred by the Client as a result of the termination of acceptance and execution of Electronic Documents signed with an ES generated using the corresponding compromised ES Key.
6.3.6. Банк имеет право отказать Клиенту в приеме/приостановить исполнение любого Электронного документа по своему усмотрению, в том числе, но не ограничиваясь, в случае возникновения у него подозрений, что Электронный документ подписан не Уполномоченным представителем Клиента, Компрометации Ключей, Несанкционированного доступа к Системе и/или в случае какого-либо нарушения Клиентом Договора ДБО, при этом Клиент вправе передать в Банк соответствующий платежный, иной документ на бумажном носителе[9].	6.3.6. The Bank has the right to refuse the Client in the acceptance/suspend execution of any Electronic Document at its own discretion, including, but not limited to, the cases when it suspects that the Electronic Document is signed by somebody other than the Authorized Representative of the Client, Key Compromise, Unauthorized Access to the System and/or in case of the Client's default of the RBS Contract, in which case the Client has the right to present the Bank with the corresponding payment or other document on paper[9].
О своем отказе в приеме Электронного документа Банк обязуется уведомить Клиента не позднее Рабочего дня, следующего за днем поступления Электронного документа в Банк, путем направления сообщения Клиенту по Системе.	The Bank shall notify the Client about its refusal to accept the Electronic Document no later than the Business Day, following the day of reception of an Electronic Document by the Bank, by sending a message to the Client via the System.
6.3.7. Банк имеет право отказать Клиенту в приеме Электронных документов/ приостановить их исполнение для проведения расчетных операций по Счету, счету по вкладу (депозиту), подписанных ЭП, а также перевести Клиента в Информационный режим функционирования Системы, при котором Клиенту доступен ограниченный функционал (режим «просмотра», а также направление в Банк сообщений свободного формата), в случаях, предусмотренных законодательством Российской Федерации, в том числе в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.	6.3.7. The Bank has the right to refuse the Client in the acceptance/suspend execution of Electronic Documents for carrying out settlement transactions on the Account, a deposit account signed with ES and also to switch the Client to the Information mode of the System functions, when the Client's access is restricted to the browsing mode and sending to the Bank of free form messages in cases provided for by the legislation of the Russian Federation, including in the field of countering the legalization (laundering) of criminal proceeds and terrorism funding.
6.3.8. Банк имеет право запрашивать у Клиента подтверждение данных об Уполномоченном представителе Клиента, а также документы, подтверждающие его полномочия на совершение банковских операций и/или сделок, осуществляемых посредством	6.3.8. The Bank has the right to require from the Client confirmation of data on the Authorized Representative of the Client, as well as documents confirming their authority to perform banking operations and/or transactions carried out via the System within the

[9] Платежные документы в рамках СБП могут передаваться только посредством Системы. / Payment documents in the frame of FPS should be transferred only through the System.

Системы в рамках установленного Пакета операций, а также иные необходимые полномочия.	established Package of Operations, as well as other necessary authorities.
6.3.9. Банк имеет право заблокировать в Системе Ключ ЭП Уполномоченного представителя Клиента в случае прекращения действия его полномочий до момента предоставления в Банк документов, подтверждающих продление его полномочий на новый срок. При продлении полномочий создание новых Ключей ЭП не требуется.	6.3.9. The Bank has the right to block the ES Key of the Authorized Representative of the Client in the System in case their authority is terminated until documents confirming the extension of their authority for a new term are provided to the Bank. When extending the authority, creating new ES Keys is not required.
6.3.10. Банк имеет право ограничить право подписи Электронных документов (наделить правом подписи «без права подписи») Уполномоченного представителя Клиента в случае недействительности/истечения срока действия документа, удостоверяющего его личность.	6.3.10. The Bank has the right to restrict the right to sign Electronic Documents (grant the right to sign "without the right to sign") for the Authorized Representative of the Client in case of invalidity/expiration of the document confirming their identity.
6.3.11. Банк имеет право с учетом полномочий, предоставленных Уполномоченному представителю Клиента, ограничить перечень банковских операций и/или сделок, осуществляемых им посредством Системы.	6.3.11. The Bank reserves the right, taking into account the powers granted to the Authorized Representative of the Client, to limit the range of banking operations and/or transactions they may perform through the System.
6.3.12. Банк имеет право вносить в одностороннем порядке изменения в порядок функционирования Системы и сообщать об этом Клиенту в письменном уведомлении на бумажном носителе или посредством Системы.	6.3.12. The Bank shall have the right to amend unilaterally the procedure of the System functioning and inform the Client about it via a written notification or the System.
6.3.13. Банк имеет право приостановить обслуживание Клиента с использованием Системы: - на время спорных ситуаций с уведомлением об этом Клиента. - для выполнения неотложных, аварийных и регламентных работ, связанных с обслуживанием Системы.	6.3.13. The Bank shall have the right to suspend services for the Client rendered with the use of the System: - for duration of disputable situations, upon a corresponding notice given to the Client. - for the performance of urgent, emergency and scheduled works associated with servicing of the System.
6.3.14. Банк приостанавливает использование Клиентом Системы при получении от Банка России информации, содержащейся в Базе данных, на период нахождения в ней указанных сведений о Клиенте. При этом Банк незамедлительно уведомляет об этом Клиента, а также о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России (в том числе через Банк) об исключении сведений, относящихся к Клиенту, из Базы данных.	6.3.14. The Bank shall suspend use of the System by the Client in case of receiving from the Bank of Russia of the information contained in the Database for the period of presence in the Database of the mentioned data about the Client. The Bank shall immediately notify the Client thereof, as well as about the Client’s right to submit an application to the Bank of Russia (including via the Bank) for deletion of the data related to the Client from the Database.
6.3.15. Банк имеет право по своей инициативе блокировать действие Ключей в случае их Компрометации.	6.3.15. The Bank may on its own initiative block the operation of the Keys in case of their Compromise.

6.3.16. Банк имеет право по своей инициативе приостановить использование Клиентом Системы при Несанкционированном доступе к Системе.	6.3.16. The Bank has the right, at its sole discretion, to suspend the Client's use of the System in the event of Unauthorized Access to the System.
6.3.17. Банк информирует Клиента о приостановлении обслуживания в Системе (перевод в Информационный режим)/приостановлении использования Системы/блокировке Ключей/ограничении банковских операций и/или сделок, осуществляемых посредством Системы/о возобновлении использования Системы путем направления сообщения по Системе и/или на адрес официальной электронной почты Клиента, указанный в Договоре ДБО или полученный в рамках исполнения Банком требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма.	6.3.17. The Bank informs the Client of service suspension within the System (switching to Information Mode)/suspension of System use/blocking of Keys/restriction of banking operations and/or transactions performed through the System/resumption of System use by sending a notification via the System and/or to the official email address of the Client as specified in the RBS Contract or provided as part of the Bank's compliance with anti-money laundering and counter-terrorism financing legislation.
6.3.18. Банк обязуется принимать от Клиента Электронные документы, подписанные Уполномоченным(и) представителем(лями) Клиента в соответствии с условиями Договора ДБО, требованиями законодательства Российской Федерации и осуществлять операции, сделки, иные действия на основании таких Электронных документов в сроки, предусмотренные ДБС, Договором ДБО, Условиями СБП, иными соглашениями между Сторонами, законодательством Российской Федерации.	6.3.18. The Bank undertakes to accept Electronic Documents from the Client, which have been signed by the Authorized Representative(s) of the Client in compliance with the terms of the RBS Contract and the requirements of the legislation of the Russian Federation and implement operations, transactions and other actions in time stipulated in BAAs, legislation of the Russian Federation, the RBS Contract, the FPS Terms and other agreements between the Parties, on the basis of such Electronic Documents.
6.3.19. После подключения к Системе Банк начинает информировать Клиента о совершении каждой операции по Счету, счету депо с использованием Системы или без ее использования путем предоставления Клиенту выписки по Счету, счету депо не позднее Рабочего дня, следующего за днем совершения операции по Счету, счету депо, путем направления их только посредством Системы. Днем выдачи (получения) указанных выписок считается день их направления Банком по Системе. В случае необходимости получения Клиентом выписок по Системе за период до момента подключения к Системе, Клиент вправе обратиться в Банк с соответствующим заявлением, направленным в Банк по Системе либо предоставленным на бумажном носителе. В случае, если использование Клиентом Системы приостановлено, уведомление Клиента о совершении указанных операций осуществляется путем предоставления	6.3.19. After connection to the System the Bank shall start informing the Client about each transaction on the Account, depot account with or without the use of the System by providing to the Client statements of the Account and the depot account not later than the Bank’s Business Day following the date of the transaction on the Account and depot account with said statements to be forwarded exclusively via the System. The date of issue (receipt) of said statements shall be the date of their forwarding by the Bank via the System. If the Client requires System statements for the period prior to connection to the System, the Client has the right to submit a corresponding request to the Bank, either through the System or in paper form. If the Client’s use of the System is suspended, the Client shall be notified of the above transactions by way of sending the Client statements of the Account, depot account via

Клиенту выписки по Счету, счету депо по Системе незамедлительно после восстановления доступа к ней или другим способом и в сроки, предусмотренные соответствующим ДБС/договором счета депо.	the System immediately after recovery of the access thereto or in any other manner and within the terms fixed by corresponding BAA/depot account agreement.
Направление Банком указанных выписок по Системе (или другим способом и в сроки, предусмотренные соответствующим ДБС/договором счета депо) является надлежащим уведомлением Клиента о совершении операции с использованием электронного средства платежа в соответствии с законодательством Российской Федерации, и не требует дополнительного направления Банком Клиенту каких-либо иных уведомлений.	The said statements forwarded by the Bank via the System (or in any other manner and within the terms fixed by the corresponding BAA/depot account agreement) shall be deemed the proper notification of the Client about the transaction using the electronic means of payment in accordance with the legislation of the Russian Federation, and shall not require any additional notification from the Bank to the Client.
6.3.20. Банк обязуется консультировать Клиента по вопросам работы с Системой (с 10.00 до 16.00 московского времени в Рабочие дни), предоставлять Клиенту новые версии Системы, а также информировать Клиента обо всех изменениях порядка функционирования Системы в течение всего срока действия Договора ДБО.	6.3.20. The Bank undertakes to consult the Client on the issues of operations in the System (from 10 a.m. till 4 p.m. Moscow time on Business Days), grant the Client with the new versions of the System, as well as inform the Client about all the changes in the functions of the System during the entire period of validity of the RBS Contract.
6.3.21. В целях противодействия осуществлению переводов денежных средств без добровольного согласия клиента, Банк на основании заявления Клиента, составленного по форме Банка на бумажном носителе или направленного с помощью Системы, устанавливает не позднее Рабочего дня, следующего за днем принятия Банком данного заявления:	6.3.21. With the purpose to prevent the transfer of money without the voluntary consent of the Client, on the basis of the Client's request elaborated in paper and in accordance with the Bank's form or sent through the System, not later than the Business day following the receiving of this request:
- соответствующие ограничения (лимиты) по сумме одной операции и/или по общей сумме всех операций за календарный день, проводимых по Счету с помощью Системы;	- the Bank establishes respective restrictions (caps) on the amount of one operation and/or on the whole amount of daily operations performed in the Account through the System.
- соответствующие ограничения по предоставлению Банком Клиенту с помощью Системы кредита либо ограничение максимальной суммы одного кредита и/или кредитов за определенный период времени, определяемые Клиентом.	- the respective restrictions are also established on the credit provision by the Bank to the Client through the System, or a restriction on the maximum amount of one credit and/or credits for a specific lapse of time defined by the Client.
Отмена установленных ограничений осуществляется Банком после принятия им соответствующего заявления Клиента, представленного в Банк на бумажном носителе.	The abolition of established restrictions will be implemented once the Bank receives the respective Client's request submitted in paper.
7. ПРАВА, ОБЯЗАННОСТИ И ПОРЯДОК ДЕЙСТВИЯ СТОРОН ПРИ ВЫЯВЛЕНИИ БАНКОМ ОПЕРАЦИЙ, СООТВЕТСТВУЮЩИХ ПРИЗНАКАМ	**7. RIGHTS, OBLIGATIONS AND PROCEDURES OF THE PARTIES WHEN THE BANK DISCOVERS TRANSACTIONS WITH SIGNS OF**

ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА	**MONEY TRANSFER WITHOUT THE VOLUNTARY CONSENT OF THE CLIENT**
7.1. Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, обязан при приеме к исполнению распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, приостановить его исполнение на срок, предусмотренный законодательством Российской Федерации.	7.1. If the Bank discovers a transaction with signs of money transfer without the voluntary consent of the Client, the Bank when accepting for execution of the Client's order to perform a transaction with signs of money transfer without the voluntary consent of the Client shall suspend the execution of the order for a term stipulated by the legislation of the Russian Federation.
7.2. О приостановлении исполнения распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента Банк обязуется уведомить Клиента незамедлительно путем направления сообщения Клиенту по своему усмотрению по Системе или по номеру мобильного телефона[10], указанному Клиентом в Договоре ДБО или сообщенному Клиентом Банку в порядке, предусмотренном настоящими Условиями.	7.2. The Bank shall immediately notify the Client about the suspension of the Client's order to perform such transaction with signs of money transfer without the voluntary consent of the Client by sending a message to the Client at its own discretion via the System or to the mobile phone number[10] specified by the Client in the RBS Contract or notified by the Client to the Bank in the procedure established by these Terms.
7.3. Клиент подтверждает/не подтверждает исполнение Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без добровольного согласия Клиента, в установленные законодательством Российской Федерации сроки по номеру телефона Банка, указанному на официальном сайте Банка в сети «Интернет», с произнесением Кодового слова Клиента.	7.3. The Client confirms/does not confirm the performance by the Bank of the order suspended due to signs of money transfer without the voluntary consent of the Client within the timeframe established by the legislation of the Russian Federation by calling on the Bank's phone number specified on the official web-site of the Bank in the Internet and using the Client's Code Word.
При наличии технической возможности, подтвердить исполнение Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без добровольного согласия Клиента, Клиент может по Системе путем ввода кода – подтверждения, предварительно запрошенного Клиентом по Системе и полученного на номер мобильного телефона, указанный в Договоре ДБО или сообщенный Клиентом Банку в	If technically possible, the Client may confirm the performance by the Bank of the order suspended due to signs of money transfer without the voluntary consent of the Client, using the System and entering the confirmation code preliminarily requested by the Client via the System and received on the mobile phone number specified in this Contract on the use of RBS or advised by the Client to the Bank in the procedure established by the Terms. Until

[10] Клиентам, указавшим при заключении Договора ДБО два номера мобильных телефонов, SMS-сообщение направляется на номер мобильного телефона, указанный в первой строке пункта «Мобильный телефон клиента для приема сообщений в формате SMS-сообщений». / The Clients specifying two mobile phone numbers when entering the Contract on the Use of RBS, SMS messages shall be sent to the mobile phone number specified in the first line of "Mobile phone number of the client for SMS messages".

порядке, предусмотренном Условиями. До подтверждения исполнения Банком соответствующего платежа Клиент обязан сверить реквизиты распоряжения, отправленного Клиентом, с реквизитами, указанными в уведомлении, направленном Банком по номеру мобильного телефона, указанному Клиентом в Договоре ДБО или сообщенному Клиентом Банку в порядке, предусмотренном Условиями.

При поступлении. в установленные законодательством Российской Федерации сроки, в Банк подтверждения исполнения Банком соответствующего платежа в течение операционного дня, указанного в ДБС, денежные средства списываются со Счета в текущий Рабочий день Банка. При поступлении вышеуказанного подтверждения после операционного дня, денежные средства списываются со Счета не позднее следующего Рабочего дня Банка.

В случае, если Клиент соглашается с сообщением Банка о том, что операция по Счету соответствует признакам осуществления перевода денежных средств без добровольного согласия Клиента, Клиент вправе незамедлительно направить в Банк отзыв соответствующего распоряжения.

При неполучении, в установленные законодательством Российской Федерации сроки, от Клиента соответствующего подтверждения, Банк отказывает в исполнении распоряжения по истечении данного срока.

Клиент уведомлен о том, что все телефонные разговоры записываются и хранятся в Банке в течение срока, установленного законодательством Российской Федерации. Записи указанных телефонных разговоров могут быть использованы при разрешении любых споров, а также предоставлены в суд.

7.4. В случае, если, несмотря на направление Клиентом подтверждения распоряжения в соответствии с п.7.3. настоящих Условий, Банк получил от Банка России информацию, содержащуюся в Базе данных, его исполнение приостанавливается Банком на срок, предусмотренный законодательством Российской Федерации.

О приостановлении исполнения подтвержденного распоряжения Банк обязуется уведомить Клиента незамедлительно путем направления сообщения Клиенту по

confirmation of performance by the Bank of the corresponding payment, the Client shall check the details in the order sent by the Client against the details specified in the notification sent by the Bank to the mobile phone number specified by the Client in the Contract on the Use of RBS or otherwise advised by the Client to the Bank in the procedure established by the Terms.

If the Client confirms within the timeframe established by the legislation of the Russian Federation the above payment to the Bank within the transaction hours specified in the BAA, funds shall be debited from the Account on the current Business Day of the Bank. If the above confirmation is received after the transaction hours, the funds shall be debited from the Account no later than on the next Bank's Business Day.

If the Client agrees with the Bank's message that the transaction on the Account bears signs of money transfer without the voluntary consent of the Client, the Client may immediately revoke the respective order from the Bank.

If the Client fails to send the corresponding confirmation within the timeframe established by the legislation of the Russian Federation, the Bank shall refuse to execute the order after the expiry of the defined timeframe.

The Client is hereby notified that all telephone conversations shall be recorded and stored by the Bank within the period established by the laws of the Russian Federation. The recordings of such telephone conversations may be used when resolving any disputes and may be presented to court.

7.4. Despite the confirmation of the order being sent by the Client in accordance with paragraph 7.3 of these Terms, if the Bank receives from the Bank of Russia information from the Database, the execution of the order shall be suspended by the Bank for a term stipulated by the legislation of the Russian Federation.

The Bank shall immediately notify the Client about suspension of execution of the confirmed order by sending a message to the Client at its own discretion via the System or to

своему усмотрению по Системе или по номеру мобильного телефона[11], указанному Клиентом в Договоре ДБО или сообщенному Клиентом Банку в порядке, предусмотренном Условиями.	the mobile phone number[11] specified by the Client in the Contract on the Use of RBS or provided by the Client to the Bank in the procedure established by the Terms.
7.5. При неполучении, в установленные законодательством Российской Федерации сроки, от Клиента соответствующего отказа в исполнении Банком подтвержденного распоряжения, по истечении данного срока Банк исполняет подтвержденное распоряжение Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не принимать его к исполнению.	7.5. If the Bank does not receive from the Client the respective revocation of the order within the timeframe established by the legislation of the Russian Federation, after expiry of the defined term the Bank shall exectute the confirmed order of the Client if there are not other reasons not to execute it stipulated by the legislation of the Russian Federation.
7.6. Днем получения Клиентом сообщений, указанных в п.7.2. и п.7.4. настоящих Условий, является день направления Банком указанного сообщения по Системе или день направления Банком SMS-сообщения на номер мобильного телефона Клиента, указанный им в Договоре ДБО или сообщенный Клиентом Банку в порядке, предусмотренном Условиями.	7.6. The day the Client receives the messages specified in the paragraph 7.2 and 7.4 of these Terms is considered the day the Bank sends that message via the System or the day the Bank sends SMS message to the Client's phone number specified by the Client in the Contract on the Use of RBS or provided by the Client to the Bank in the procedure established by the Terms.
7.7. Клиент подтверждает/не подтверждает исполнение/отказывается от исполнения Банком распоряжения, приостановленного из-за признаков осуществления перевода денежных средств без добровольного согласия Клиента, в Рабочие дни.	7.7. The Client confirms/does not confirm /revokes the execution by the Bank of the order suspended due to signs of money transfer without the voluntary consent of the Client on Business Days of the Bank.
7.8. Клиент уведомлен и согласен с тем, что Банк проводит Проверку ЭП Электронного документа (процедуру удостоверения права распоряжения денежными средствами Клиента) каждый раз, когда проводится проверка Электронного документа Клиента на соответствие признакам осуществления перевода денежных средств без добровольного согласия Клиента, а также на наличие информации, содержащейся в Базе данных. В этом случае Банк не несет ответственность за убытки Клиента, которые могут возникнуть у него вследствие неисполнения Электронного документа из-за отрицательного результата Проверки ЭП Электронного документа.	7.8. The Client has been notified and agrees that the Bank conducts Check of the Electronic Signature of an Electronic Document (the procedure of verification of the right to manage Client's money funds) every time the Bank conducts Check of Electronic Document of the Client for signs of money transfer without the voluntary consent of the Client, as well as for the presence of information contained in the Database. In this case, the Bank shall not be liable for the losses of the Client, which the Client may suffer as a result of non-execution of the Electronic Document due to the negative result of the Check of the Electronic Signature of an Electronic Document.
7.9. Банк вправе в одностороннем порядке изменить Кодовое слово Клиента, направив Клиенту уведомление на бумажном носителе с	7.9. The Bank may unilaterally change the Client's Code Word by sending a notification to the Client on paper with a handwritten

[11] Клиентам, указавшим при заключении Договора ДБО два номера мобильных телефонов, SMS-сообщение направляется на номер мобильного телефона, указанный в первой строке пункта «Мобильный телефон клиента для приема сообщений в формате SMS-сообщений». / To the Clients specifying two mobile phone numbers when entering into the RBS Contract, SMS messages shall be sent to the mobile phone number specified in the first line of "Mobile phone number of the client for SMS messages".

собственноручной подписью руководителя Банка (Уполномоченного им лица) об изменении Кодового слова.

7.10. В случае утраты Клиентом контроля над номером мобильного телефона, а также утраты Клиентом уверенности в том, что Кодовое слово и/или номер мобильного телефона не могут быть использованы неуполномоченными лицами (далее – компрометация), Клиент обязан незамедлительно направить в Банк Заявление о Компрометации (вложенным файлом) на официальный адрес электронной почты (e-mail) Банка, указанный в Договоре ДБО, с последующим немедленным предоставлением в Банк оригинала указанного заявления.

Все распоряжения Клиента о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, поступившие после получения Банком Заявления о Компрометации по электронной почте и до принятия Банком от Клиента последующего Заявления о внесении изменений в Договор ДБО в 2 (двух) экземплярах на бумажном носителе с собственноручной подписью Уполномоченного лица Клиента с указанием нового Кодового слова и/или номера мобильного телефона, считаются автоматически отозванными.

В случае замены Клиентом номера мобильного телефона и/или Кодового слова, Клиент обязан незамедлительно предоставить в Банк Заявление о внесении изменений в Договор ДБО на бумажном носителе в 2 (двух) экземплярах с собственноручной подписью Уполномоченного лица Клиента с указанием нового Кодового слова и/или номера мобильного телефона.

До момента принятия Банком вышеуказанного заявления Банк использует в соответствии с Условиями ранее сообщенный Банку Клиентом номер мобильного телефона, ранее сообщенное Клиентом Банку/Банком Клиенту (в соответствии с п.7.9 настоящих Условий) Кодовое слово.

7.11. Банк не несет ответственности за ущерб, причиненный Клиенту вследствие несанкционированного использования третьими лицами (в том числе, но не ограничиваясь, при компрометации) Кодового

signature of the Bank Manager (his Authorized Representative) on the change of the Code Word.

7.10. If the Client loses control over the mobile phone number or loses confidence that the Code Word and/or mobile phone number cannot be used by unauthorized persons ("compromise"), the Client shall immediately send to the Bank the Compromise Statement (as an enclosed file) to the Bank's official e-mail address specified in the RBS Contract, subject to the subsequent immediate sending of the original of the said statement to the Bank.

All the Client's orders on the performance of the transaction having signs of money transfer without the voluntary consent of the Client which are delivered after the Bank receives the Compromise Statement by e-mail and before the Bank accepts from the Client the subsequent Application for amendments to the RBS Contract in 2 (two) copies on paper with a handwritten signature of the Client's Authorized Person specifying the new Code Word and/or mobile phone number, shall be deemed automatically revoked.

If the Client changes the mobile phone number and/or the Code Word, the Client shall immediately submit to the Bank the Application for amendments to the RBS Contract in 2 (two) copies on a paper bearing the handwritten signature of the Authorized Person of the Client specifying a new Code Word and/or mobile telephone number.

Until the Bank accepts the above mentioned application, the Bank shall use the mobile phone number previously provided to the Bank by the Client and the Code Word previously provided to the Bank by the Client/to the Client by the Bank (as per paragraph 7.9 of these Terms) in accordance with the Terms.

7.11. The Bank shall not be liable for damage caused to the Client due to unauthorized use by third parties (including but not limited to compromising) of the Code Word/mobile phone number, to which the Bank sends SMS

слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента.	messages about transactions with signs of money transfer without the voluntary consent of the Client.
7.12. Банк не несет ответственности за негативные последствия, в том числе убытки Клиента, которые могут возникнуть у Клиента вследствие неполучения уведомлений от Банка об операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, приостановлении исполнения подтвержденного распоряжения или о приостановлении использования Системы, в том числе, в связи с недостоверностью/неактуальностью информации, указанной Клиентом, а также в связи с недоступностью для Клиента указанных способов связи, а также по вине Клиента или мобильного оператора, в случае утраты Клиентом Кодового слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, их компрометации.	7.12. The Bank shall not be liable for negative consequences, including losses of the Client, which the Client may suffer as a result of non-receipt of notifications from the Bank about a transaction with signs of money transfer without the voluntary consent of the Client, suspension of execution of the confirmed order or suspension of use of the System, including, but not limited to, for the reason of inaccuracy/outdated nature of the information specified by the Client, unavailability of the specified communication methods for the Client, fault of the Client or the mobile operator, loss of the Code Word/mobile phone number, to which the Bank sends SMS messages on transactions with signs of money transfer without the voluntary consent of the Client, by the Client or the compromise thereof.
7.13. Банк не несет ответственности за убытки Клиента, возникшие в результате утраты (порчи, передачи, утери, разглашении) Клиентом Кодового слова/номера мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента.	7.13. The Bank shall not be liable for the Client's losses resulting from the loss (damage, transfer, disclosure) of the Code Word/mobile phone number, to which number the Bank sends SMS messages on transactions with signs of money transfer without the voluntary consent of the Client, by the Client.
7.14. Банк не несет ответственности за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку об утрате Клиентом контроля над номером мобильного телефона, а также утрате Клиентом уверенности в том, что Кодовое слово, номер мобильного телефона, на который Банком направляется SMS-сообщение о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, не могут быть использованы неуполномоченными лицами.	7.14. The Bank shall not be liable for losses of the Client arising out of the late notification of the Bank about the loss of control over the mobile phone number by the Client, as well as the loss by the Client of confidence that the Code Word, mobile number, to which the Bank sends SMS messages on transactions with signs of money transfer without the voluntary consent of the Client, cannot be used by unauthorized persons.
7.15. Клиент обязуется предоставить Банку действительный номер мобильного телефона и обеспечить постоянную доступность номера	7.15. The Client shall provide the Bank with a valid mobile phone number and ensure that the

мобильного телефона для приема сообщений в формате SMS-сообщений на русском/английском языке.	mobile phone number is always available for receiving SMS messages in Russian/English.
7.16. Клиент несет ответственность за достоверность номера мобильного телефона, обязан не допускать создание дубликатов (клонов) sim-карты, а также не допускать получение, использование и замену sim-карты и/или номера мобильного телефона, Кодового слова неуполномоченными лицами.	7.16. The Client shall be liable for the accuracy of the mobile phone number, shall prevent any duplication (cloning) of the SIM card, and prevent the receipt, use, and replacement of the SIM card and/or mobile phone number, the Code Word by unauthorized persons.
7.17. Клиент обязуется обеспечить хранение информации о Кодовом слове способом, делающим Кодовое слово недоступным третьим лицам.	7.17. The Client shall ensure the safekeeping of information about the Code Word in a manner that makes the code word inaccessible to third parties.
Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения невозможности доступа неуполномоченных лиц к информации о Кодовом слове, номере мобильного телефона Клиента, находящейся в распоряжении Банка.	The Bank shall take all the necessary measures of the organizational and technical nature to ensure that unauthorized persons cannot access the information on the Code Word and the Client's mobile phone number available to the Bank.
7.18. Клиент подтверждает, что ему известно о том, что в процессе передачи информации путем направления SMS-сообщения возможен риск несанкционированного доступа третьих лиц к такой информации и настоящим выражает свое согласие с тем, что Банк не несет ответственности за разглашение информации о Клиенте, операциях по его Счетам в случае такого несанкционированного доступа.	7.18. The Client is hereby aware of the risk of unauthorized access by third parties to the information communicated by SMS messages and hereby agrees that the Bank shall not be liable for any disclosure of such information about the Client and transactions on the Client's Accounts in the event of such unauthorized access.
7.19. Клиент соглашается с тем, что Банк не несет ответственности за какие-либо аварии, сбои и перебои в обслуживании, связанные с оборудованием, системами передачи электроэнергии и/или линий связи, сети «Интернет», которые обеспечиваются, подаются, эксплуатируются и/или обслуживаются третьими лицами в связи с направлением Банком Клиенту SMS-сообщения, в том числе убытки, понесенные в связи с неправомерными действиями или бездействием третьих лиц. Банк не несет ответственность за доступность и работоспособность средств связи, с помощью которых Банк осуществляет уведомление Клиента.	7.19. The Client hereby agrees that the Bank shall not be liable for any emergencies, malfunctions and interruptions in the services due to equipment, electricity systems and/or communication lines, the Internet, which are provided, supplied, operated and/or maintained by third parties, as related to the SMS messages sent by the Bank to the Client, including losses incurred due to illegal actions or inaction of third parties. The Bank shall not be liable for the availability and operability of the means of communication used by the Bank to notify the Client.
8. КОНФИДЕНЦИАЛЬНОСТЬ	**8. CONFIDENTIALITY**
8.1. Условия и информация, содержащаяся в Договоре ДБО, а также вся переписка, связанная с его исполнением, считаются обеими Сторонами конфиденциальной	8.1. Terms and information, contained in the RBS Contract, as well as all the correspondence, relating to its execution, are considered as confidential by both Parties,

информацией, составляющей, в том числе, банковскую и коммерческую тайну, которую Стороны не вправе разглашать третьим лицам без предварительного письменного согласия другой Стороны, за исключением случаев, предусмотренных Договором ДБО и законодательством Российской Федерации, предоставления такой информации независимым аудиторским организациям по их требованию в ходе проведения аудита бухгалтерского учета и финансовой (бухгалтерской) отчетности; когда она оказалась известной третьим лицам до того, как Стороны ее разгласили.

constituting, inter alia, a bank and commercial secret, which the Parties have no right to disclose to third parties without preliminary written consent thereto of the other Party, only in case and in the manner, as under the RBS Contract and the legislation of the Russian Federation and provision of such kind of information to independent audit organizations on their demand in the process of audit of accounting and financial (accounting) reports; when it has been disclosed to the third parties before it was disclosed by the Parties.

9. ФИНАНСОВЫЕ ВЗАИМООТНОШЕНИЯ

9. MUTUAL FINANCIAL RELATIONS

9.1. Порядок оплаты, стоимость работ и услуг, оказываемых Банком Клиенту по настоящему Договору ДБО, устанавливаются Тарифами и Условиями. Расчеты производятся в рублях путем списания Банком (без дополнительных распоряжений Клиента) денежных средств с расчетного и/или иных счетов Клиента, открытых в Банке, с которых такое списание допускается законодательством Российской Федерации, предварительно полностью до оказания услуг. Если денежные средства списываются со счета Клиента в иностранной валюте, а сумма, причитающаяся Банку в соответствии с Тарифами, выражена в рублях, Банк самостоятельно производит конверсию указанных средств по курсу Банка России на день совершения операции и направляет полученную сумму для оплаты услуг Банка.

9.1. Manner of payment, price of works and services, rendered by the Bank to the Client as under the RBS Contract, are set by the Tariffs and the Terms. Settlements are conducted in rubles through the direct debiting by the Bank (without additional Client's orders) of the funds from the settlement and/or other accounts held by the Client in the Bank, from which such debiting is permitted by the legislation of the Russian Federation, preliminarily in full prior to the provision of services. If the funds are debited from a foreign currency account of the Client, and the amount due to the Bank, as in compliance to the Tariffs, is expressed in rubles, Bank individually converts the specified funds at the exchange rate of the Bank of Russia as at the day of the commission of the operation and directs the received amount for payment for the Bank's services.

9.2. В случае, если остаток денежных средств на расчетном и/или иных счетах Клиента не позволяет Банку в срок и в размере, определенных Договором ДБО и действующими Тарифами, произвести списание платы за услуги Банка, Банк имеет право не оказывать запрашиваемые Клиентом услуги и/или приостановить обслуживание Клиента по Системе до момента полной оплаты задолженности Клиентом, соответственно уведомив об этом Клиента не менее чем за 5 (пять) Рабочих дней. Клиент отказывается от любых претензий к Банку за возникновение в этом случае возможных убытков, включая реальный ущерб и упущенную выгоду, связанных с задержками в

9.2. In case if the balance of funds in the settlement and/or other accounts of the Client does not allow the Bank, within the term and in the amount set by the RBS Contract and the effective Tariffs, to debit the amount of payment for the services of the Bank, the Bank shall have the right not to render the services requested by the Client and/or suspend the servicing of the Client in the System until the full payment of the Client's debt has been made, correspondingly notifying the Client of such at least 5 (five) Business Days in advance. The Client refuse to file any claims with the Bank for the occurrence, in such case, of possible losses, including real damage and lost profits, related to the delays in commissioning Client

проведении Клиентом операций по Счету, счету депо, счету по вкладу (депозиту), осуществления иных действий, сделок.	operations on the Account, depot account, deposit account, or other actions or transactions.
9.3. В случае расторжения Клиентом Договора ДБО в одностороннем порядке, Клиент обязан не позднее 3 (трех) Рабочих дней от даты направления уведомления о расторжении оплатить стоимость оказанных услуг.	9.3. In case the Client terminates the RBS Contract in a unilateral manner, Client shall no later than 3 (three) Business Days from the date of the sending of the notification about the termination, cover the cost of rendered services.
9.4. Клиент настоящим дает согласие (заранее данный акцепт) на исполнение (в том числе частичное) Банком, в полной сумме платежных требований/инкассовых поручений Банка или иных документов, установленных Банком России, для осуществления прав, предусмотренных п.9.1 настоящих Условий, в течение срока действия Договора ДБО.	9.4. Hereby the Client gives his consent (pre-authorization) to the execution (including partial execution) by the Bank of Bank's payment requests/collection orders or other documents stipulated by the Bank of Russia, in full, for the implementation of rights specified in the paragraph 9.1 of these Terms within the validity period of the RBS Contract.
10. ОТВЕТСТВЕННОСТЬ СТОРОН	**10. LIABILITY OF THE PARTIES**
10.1. За неисполнение и/или ненадлежащее исполнение обязательств по Договору ДБО Стороны несут ответственность в соответствии с законодательством Российской Федерации и Договором ДБО.	10.1. The Parties shall be held liable for non-performance and/or improper performance of the duties under the RBS Contract, as in compliance to the legislation of the Russian Federation and the RBS Contract.
10.2. Клиент несет ответственность за: - сохранность и целостность установленного программного обеспечения, включая Средства криптографической защиты информации, Носителей с Ключами; - выполнение требований к эксплуатации Системы, изложенных в Условиях и Документации; - надлежащее выполнение условий Договора ДБО, а также за использование Ключей только Уполномоченным представителем Клиента, указанным в соответствующем Заявлении на доступ.	10.2. The Client shall be responsible for: - the security and entirety of the installed software, including the Information cryptographic security products, Carriers with Keys, - the observance of the requirements for the operation of the System, specified in the Terms and the Documentation, - due execution of the terms of the RBS Contract, as well as for the use of Keys only by the Authorized Representative of the Client specified in the corresponding Access Application.
10.3. Банк несет ответственность перед Клиентом в соответствии с законодательством Российской Федерации, при наличии вины за реальный ущерб, но не за упущенную выгоду, с учетом ограничений, предусмотренных п.10.4 настоящих Условий, за точное, своевременное и полное исполнение поручений и инструкций Клиента по проведению банковских, депозитарных операций, по совершению иных действий, сделок, на основании надлежащим образом оформленных и своевременно переданных по Системе Электронных документов Клиента.	10.3. The Bank shall be held liable before the Client, as in compliance to the legislation of the Russian Federation, in case of its fault for real damage, but not for lost profits, in light of the restrictions, as under paragraph 10.4 of these Terms, for the exact, timely and full execution of the orders and instructions presented by the Client for the commission of banking operations, custody transactions and other actions or transactions on the basis of the duly drawn up and timely transferred, within the System, Electronic Documents of the Client.
10.4. Банк не несет ответственности:	10.4. The Bank shall not be liable for the following:

- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Электронного документа, признанного верным и принятого Банком к исполнению (любой Электронный документ, подписанный ЭП Уполномоченного представителя Клиента в соответствии с Договором ДБО и полученный Банком по Системе, в любом случае признается Электронным документом, исходящим от Клиента, что не допускает отказ Клиента от того, что такой документ направлен с его стороны, ни при каких обстоятельствах);	- for the consequences of operations, other actions or transactions on the basis of a duly drafted Electronic Document, acknowledged as accurate and accepted by the Bank for execution (any Electronic Document signed by the ES of the Authorized Representative of the Client in compliance to the RBS Contract and received by the Bank through the System, is in any case found as an Electronic Document received from the Client, which excludes Client's refusal from the fact that such document was sent on its behalf, under any circumstances);
- за последствия совершения операций, иных действий, сделок на основании надлежащим образом оформленного Электронного документа, подписанного прежним Уполномоченным представителем Клиента, до принятия Банком от Клиента Заявления об изменении сведений, касающихся прекращения полномочий соответствующего Уполномоченного представителя Клиента;	- for the consequences of operations, other actions or transactions on the basis of a duly drafted Electronic Document from the Client, signed by the former Authorized Representative of the Client, until the Bank accepts the Application for change of information from the Client regarding termination of authorisation of the respective Authorised Representative of the Client;;
- за последствия отказа Банка в соответствии с п.6.3.2, п.6.3.5 – п.6.3.7 настоящих Условий от приема к исполнению Электронного документа, переданного Клиентом по Системе;	- for the consequences of the Bank's refusal, in compliance to paragraph 6.3.2, paragraphs 6.3.5 – 6.3.7 of these Terms, to accept for execution an Electronic Document, transferred by the Client via the System;
- за последствия использования Системы, установленной у Клиента, посторонними, а также неуполномоченными на это лицами;	- for the consequences of use of the System, installed for the Client, by third parties, as well as by persons not authorized for such use;
- за последствия разглашения Клиентом информации о порядке работы Системы, включая порядок использования Средств криптографической защиты информации;	- for the consequences of the disclosure by the Client of the information on the procedure of operation of the System, including the procedure for the use of Information cryptographic security products;
- за нарушение работы Системы и возникновение трудностей в осуществлении операций, иных действий посредством Системы в результате ошибок и неточностей, допущенных Клиентом;	- for the malfunction of the System and occurrence of difficulties in the commission of operations in the System as a result of errors inaccuracies, admitted by the Client;
- за нарушение работы Системы в результате неисправности Средств обработки и хранения информации Клиента, используемых для доступа к Системе;	- for the malfunction of the System as a result of an error in the products designed for processing and storage of information of the Client, used to access the System;
- за сбои в работе Системы, произошедшие не по вине Банка и повлекшие для Клиента невозможность передачи Электронных документов;	- for System failures not caused by the Bank that result in the inability of the Client to transmit Electronic Documents;
- за нарушение работы Системы в результате действий третьих лиц;	- for the malfunction of the System as a result of actions of third parties;
- за последствия нарушения Клиентом требований и правил, приведенных в Договоре ДБО и Документации;	- for the consequences of Client's violation of rules and requirements, as presented in the RBS Contract and the Documentation;

- за последствия нарушения работоспособности телекоммуникационных линий связи, сети «Интернет»;	- for the consequences of malfunctions in the telecommunication lines and the Internet;
- за убытки Клиента, возникшие вследствие несвоевременного сообщения Банку о событии Компрометации;	- for the losses sustained by the Client, arising as a result of untimely message to the Bank about the Compromise event;
- за убытки, возникшие в результате утраты (порчи, передачи, утери, разглашении) Клиентом применяемых в Системе Паролей, Ключей, Носителей с Ключами, конфиденциальной информации и/или программного обеспечения;	- for the losses, arising as a result of loss (damage, transfer, loss, disclosure) by the Client of the Passwords, Keys, Carriers with Keys, confidential information and/or software used in the System;
- за правильность заполнения и оформления Электронных документов Клиентом;	- for the accuracy and proper completion of Electronic Documents by the Client;
- за исполнение ЭД, направленных и подписанных УКЭП Клиента, в случае прекращения сертификата ключа проверки ЭП по использованию УКЭП и несообщения данной информации Банку;	- for the execution of Electronic Documents sent and signed with the Client's EQES in cases where the ES verification key Certificate for EQES usage has been revoked, and the Bank was not informed of this;
- за убытки, возникшие в результате использования Системы в нарушение каких-либо требований законодательства Российской Федерации, применимого к деятельности Клиента;	- for the losses, arising as a result of the use of the System in violation of any requirements of the legislation of the Russian Federation, applicable to the operations of the Client.
- за последствия решений органов государственной власти Российской Федерации и других стран, Банка России, которые делают невозможным надлежащее исполнение Банком своих обязательств по Договору ДБО;	- for consequences arising from decisions made by government authorities in the Russian Federation or other countries, or by the Bank of Russia, that make it impossible for the Bank to properly fulfill its obligations under the RBS Contract;
- за несанкционированный вывоз Клиентом на территорию иностранного государства СКЗИ КриптоПро.	- for the unauthorized export of CryptoPro ICSP by the Client to a foreign country.
11. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ	**11. SETTLEMENT OF DISPUTES**
11.1. Стороны примут все меры к разрешению всех споров и разногласий, связанных с толкованием Сторонами Договора ДБО и его выполнением, путем переговоров.	11.1. The Parties shall undertake all the possible measures for the resolution of all the disputes and disagreements, relating to the interpretation, by the Parties, of the RBS Contract and its execution, through negotiations.
11.2. В случае, если Стороны не придут к взаимоприемлемому решению путем переговоров, Сторона, предъявившая претензию, официально вручает другой Стороне уведомление о претензии в письменном виде на бумажном носителе. Сторона, получившая уведомление, проводит расследование по факту претензии в течение 7 (семи) календарных дней от даты получения уведомления, по истечении которых на	11.2. In case if Parties will fail to reach a mutually beneficial solution through negotiations, Party, which has filed the claim, will officially present the other Party with a notification on the claim submitted in writing on paper. Party that received the notification shall conduct an investigation on the fact of the claim, within a period of 7 (seven) calendar days from the date of reception of the notification, upon the expiry of which it shall

бумажном носителе уведомляет другую Сторону о результатах расследования.	notify the other Party, on paper, about the results of the investigation.
11.3. В случае, если результаты расследования не удовлетворяют Сторону, предъявившую претензию, либо если такое уведомление не получено Стороной, предъявившей претензию, Стороны формируют Техническую комиссию для разбора конфликтной ситуации в течение 5 (пяти)[12]/15 (пятнадцати)[13] календарных дней с момента истечения срока, указанного в п.11.2 настоящих Условий. Целью работы Технической комиссии является установление правомерности и обоснованности претензии. Порядок разбора конфликтной ситуации приведен в Приложении № 3 к Условиям. В состав Технической комиссии включаются в равном количестве представители Банка и представители Клиента, а также представители организации-разработчика Системы и, в случае необходимости, независимые эксперты. Их полномочия подтверждаются доверенностями. Лица, входящие в состав Технической комиссии, должны обладать необходимыми знаниями в области обеспечения защиты информации и работы компьютерных информационных систем. Состав Технической комиссии согласовывается Сторонами в акте. Срок действия Технической комиссии составляет не более 14 (четырнадцати) календарных дней.	11.3. If the results of the investigation will not satisfy the Party which has filed the claim, or if such notification was not received by the Party, which filed the claim, Parties shall organize a Technical committee for the for the resolution of the conflict situation, within a period of 5 (five)[12]/15 (fifteen)[13] calendar days from the moment of the expiration of the term specified in paragraph 11.2. of these Terms. Work objective of the Technical committee is the establishment of legitimacy and justification of the claim. Procedure for the resolution of the conflict situation is shown in Annex No. 3 to the Terms. The Technical committee shall include, equally, the representatives of the Bank and the representatives of the Client, as well as representatives of the System developer company, and if such is required, independent experts. Their authority is confirmed by powers of attorney. Members of the Technical committee must possess the necessary knowledge in information protection and computer information systems. Composition of the Technical committee is agreed by the Parties with an act. Validity period of the Technical committee constitutes a maximum of 14 (fourteen) calendar days.
Стороны согласны с тем, что оплачивать услуги привлеченных экспертов должна Сторона, предъявившая претензию.	The Parties agree that the Party filing the claim shall bear the costs of paying for the services of the engaged experts.
11.4. Работа Технической комиссии проходит на территории Банка.	11.4. Work of the Technical committee takes place on the territory of the Bank.
11.5. В случае отсутствия у одной из Сторон каких-либо материалов, требуемых для установления правомерности и обоснованности претензии (перечень материалов приведен в Приложении №3 к Условиям), спор решается в пользу другой Стороны.	11.5. In case one of the Parties lacks any materials, required for the establishment of legality and justification of the claim (list of materials in presented in Annex No. 3 to the Terms), the dispute shall be resolved in favor of the other Party.
Бремя доказывания лежит на Стороне, заявившей о нарушении ее прав и законных интересов.	The burden of proof lies with the Party claiming a violation of its rights and legitimate interests.
11.6. Результат работы Технической комиссии оформляется актом, в котором фиксируются выводы, к которым Техническая комиссия пришла в результате проведенных мероприятий, и определяются последующие	11.6. The result of the work conducted by the Technical committee is documented by an act, which records the conclusions reached by the Technical committee as a result of the conducted activities and defines the follow-up

[12] Применимо только для СКЗИ КриптоПро. / Applicable only for the CryptoPro ICSP.
[13] Применимо только для СКЗИ OpenSSL. / Applicable only for the OpenSSL ICSP.

действия Сторон. Акт подписывается членами Технической комиссии. Стороны признают решение, оформленное актом, обязательным для участников конфликтной ситуации, и обязуются добровольно исполнять решение Технической комиссии в установленные указанным актом сроки.	actions of the Parties. The act shall be signed by the members of the Technical committee. The parties acknowledge the decision formalized by the act as binding for the participants of the conflict situation and undertake to voluntarily comply with the decision of the Technical committee within the timeframes specified in the said act.
11.7. Уклонение какой-либо Стороны от участия в создании или работе Технической комиссии может привести к невозможности ее создания и работы, но не может привести к невозможности урегулирования конфликта в судебном порядке. В случае, если Техническая комиссия не будет создана в сроки, предусмотренные Условиями, либо, если в течение 14 (четырнадцати) календарных дней с момента создания Технической комиссии, ее работа не даст результата, либо, если Стороны не придут к взаимоприемлемому решению, спор передается на рассмотрение в Арбитражный суд г. Москвы в соответствии с законодательством Российской Федерации.	11.7. The refusal of any Party to participate in the creation or operation of the Technical committee may result in its inability to be created or to function, but it cannot lead to the impossibility of resolving the conflict in court. If the Technical committee will not be established within the terms, as defined by the Terms, or if during 14 (fourteen) calendar days from the moment of the establishment of the Technical committee its operations will not provide any results, or, if the Parties fail to reach a mutually acceptable solution, the dispute shall be transferred for consideration by the Arbitration court of Moscow as in compliance to the legislation of the Russian Federation.
11.8. Стороны признают, что: - основополагающим документом при рассмотрении конфликтной ситуации, связанной с обменом Электронными документами посредством Системы, является протокол работы Системы, сформированный Банком;	11.8. The Parties acknowledge that: - the fundamental document when reviewing a conflict situation related to the exchange of Electronic Documents via the System is the protocol of the System's operation, generated by the Bank;
- Электронные документы, направленные Сторонами друг другу по Системе или хранящиеся в Банке в соответствии с Условиями, а также соответствующие протоколы почтовых серверов и/или сведения из баз данных, фиксирующих отправку каждого уведомления с его содержанием, сформированные на бумажных носителях, подписанные Уполномоченным лицом и скрепленные печатью (при необходимости ее проставления), записи телефонных разговоров между Сторонами являются достаточным доказательством соответствующего факта и могут быть представлены в качестве надлежащего доказательства в суд в случае рассмотрения спора, возникшего в результате применения Системы, а также при рассмотрении споров в досудебном порядке в соответствии с Условиями.	- the Electronic Documents, directed by the Parties to each other through the System or the ones stored in the Bank in compliance to the Terms, as well as the corresponding protocols of mail servers and/or information from the databases recording the sending of each notification with its content on paper signed by the Authorized Person and sealed (if necessary), records of telephone conversations between the Parties shall be sufficient evidence of the respective fact and may be presented as an adequate evidence before the court, in case of the consideration of the dispute, arising as a result of the application of the System, as well as during the consideration of disputes in a pre-trial proceedings as in compliance with the Terms.
12. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ	**12. VALIDITY PERIOD OF THE AGREEMENT**

12.1. Договор ДБО действует до момента прекращения обязательств по всем ДБС.	12.1. The RBS Contract shall remain valid until the end of the obligations under all BAAs.
12.2. Банк вправе отказаться от исполнения Договора ДБО полностью в одностороннем порядке, письменно уведомив об этом Клиента, в случае, если по истечении 6 (шести) месяцев с даты заключения Договора ДБО Клиент не выполнил действия, предусмотренные п.2.3 настоящих Условий (в случае использования УНЭП) или не предоставил в Банк Сертификат ключа проверки УКЭП ЕИО в электронном виде.	12.2. The Bank shall have the right to fully repudiate this RBS Contract unilaterally upon a written notice to the Client, if following six (6) months after the date of signing of the RBS Contract the Client did not undertake any action stipulated in paragraph 2.3 of these Terms (in case of using the EUES) or did not provide the Bank with the EQES verification key Certificate of the SEB in electronic form.
12.3. Договор ДБО может быть расторгнут по письменному заявлению одной из Сторон (односторонний отказ от исполнения Договора ДБО полностью). В случае расторжения Договора ДБО по инициативе Банка, Банк уведомляет об этом Клиента не позднее, чем за 14 (четырнадцать) календарных дней до даты расторжения, с указанием наименования Клиента, причины расторжения, даты и номера Договора ДБО.	12.3. The RBS Contract may be terminated under the written application of one of the Parties (a unilateral repudiation of the RBS Contract in its entirety). In case of the RBS Contract termination at the Bank’s initiative, the Bank shall notify the Client thereof no later than 14 (fourteen) calendar days prior to the date of termination, specifying the Client's name, reason for termination, date and number of the RBS Contract.
В случае расторжения Договора ДБО по инициативе Клиента, Клиент в письменной форме на бумажном носителе уведомляет об этом Банк не позднее, чем за 3 (три) Рабочих дня до даты расторжения.	In case of the RBS Contract termination at the Client’s initiative, the Client shall notify the Bank thereof no later than 3 (three) Bank’s Business Days prior to the date of termination in writing on paper.
Расторжение Договора ДБО до истечения срока его действия не освобождает Стороны от выполнения обязательств, предусмотренных Договором ДБО и не исполненных до даты его расторжения, и не лишает Сторону, чьи права по Договору ДБО нарушены в результате невыполнения обязательств другой Стороной, требовать защиты своих прав в соответствии с законодательством Российской Федерации и Договором ДБО.	Termination of the RBS Contract prior to the end of its validity does not free the Parties from the execution of the obligations, as under the RBS Contract and which were left un-executed before the date of its termination, and does not deprive the Party, whose rights under the RBS Contract have been violated as a result of the non-execution of the obligations by the other Party, of the right to demand protection of its rights as in compliance to the legislation of the Russian Federation and the RBS Contract.
12.4. Уведомление о расторжении Договора ДБО может быть направлено Банком Клиенту одним или несколькими из нижеперечисленных способов: - под расписку ЕИО или Уполномоченному лицу Клиента при наличии соответствующей доверенности; - посредством Системы; - с официального адреса электронной почты (e-mail) Банка на официальный адрес электронной почты (e-mail) Клиента, указанный в Договоре ДБО или полученный в рамках исполнения Банком требований	12.4. The notification on the RBS Contract termination should be sent to the Client by the Bank in one or more of following manners: - against signature to the SEB or the Authorized Person of the Client, provided that there is a relevant power of attorney; - through the System; - from the official email address of the Bank to the Client's official e-mail address, specified in the RBS Contract, or received in the frame of execution by the Bank of the requirements established by the anti-money laundering,

законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма, исключая сведения, содержащие банковскую, коммерческую тайны и персональные данные;	terrorism financing legislation, except the information which contains the bank, commercial secrets and personal data;
- почтой России заказным письмом с уведомлением на официальный почтовый адрес Клиента или на почтовый адрес, указанный в Договоре ДБО/иных документах, предоставленных в Банк в соответствии с Договором ДБО;	- via the Russian Post by a registered letter with notification to the official Client's domicile or to the mail address specified in the RBS Contract/other documents submitted to the Bank in accordance with the RBS Contract;
- почтовой службой DHL или иной курьерской службой доставки на почтовый адрес, указанный в Договоре ДБО/иных документах, предоставленных в Банк в соответствии с Договором ДБО.	- via DHL courier service or another courier service to the mail address specified in the RBS Contract/other documents submitted to the Bank in accordance with the RBS Contract;
12.5. С момента расторжения Договора ДБО на отношения между Банком и Клиентом не распространяются Условия СБП.	12.5. Since the termination of the RBS Contract the FPS Terms are not applied to the relationship between the Bank and the Client.
13. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ	**13. FORCE MAJEURE**
13.1. Стороны освобождаются от ответственности за неисполнение и/или ненадлежащее исполнение обязательств по Договору ДБО, если такое неисполнение явилось результатом действий или обстоятельств непреодолимой силы (далее – Форс-мажор), то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств.	13.1. The Parties shall be freed from liability for non-performance and/or improper performance of the obligations under the RBS Contract, if such non-performance was a result of the actions or effect of force majeure (hereinafter the Force Majeure), i.e. extraordinary and unavoidable, in the given conditions, circumstances.
13.2. Под термином Форс-мажор понимаются наводнение, пожар, землетрясение, ураган, взрыв, оседание почвы, эпидемии и иные подобные явления, а также война или военные действия в месте нахождения Банка или Клиента, забастовки в отрасли или регионе, принятие органом законодательной, исполнительной или судебной власти акта, повлекшие за собой невозможность надлежащего исполнения Договора ДБО Сторонами.	13.2. Force Majeure is understood as a flood, fire, earthquake, hurricane, explosion, soil shrinkage, epidemic and other similar occurrences, as well as war or military actions at the location of the Bank or the Client, strikes in the industry or the region, adoption of an act by the authority of legislative, enforcement or judicial power entailing the impossibility of execution of the RBS Contract by the Parties.
13.3. Сторона, для которой возникли обстоятельства непреодолимой силы, обязана в течение 7 (семи) Рабочих дней от даты возникновения Форс-мажора уведомить другую Сторону о наступлении таких обстоятельств, с приложением соответствующих доказательств. Доказательством Форс-мажора может служить официальный документ компетентной	13.3. The Party, who is faced with the Force Majeure, shall within a period of 7 (seven) Business Days from the date of occurrence of the Force Majeure, inform the other Party about the occurrence of such circumstances, with an annex of the corresponding evidence. Evidence of Force Majeure can be an official document from a competent organization, confirming the

организации, подтверждающий факт наступления обстоятельств непреодолимой силы.	fact of occurrence of the Force Majeure circumstances.
13.4. В случае наступления обстоятельств непреодолимой силы срок выполнения Сторонами обязательств по Договору ДБО переносится соразмерно времени, в течение которого действуют такие обстоятельства и их последствия. После прекращения действия Форс-мажора обязательства Сторон возобновляются.	13.4. In case of occurrence of the Force Majeure circumstances the term for the execution of the obligations by the Parties as under the RBS Contract shall be transferred commensurate to the time, during which such circumstances and their consequences take effect. After the end of the Force Majeure the obligations of the Parties resume.
14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	**14. FINAL PROVISIONS**
14.1. Условия составлены на русском и английском языках. В случае противоречий между версиями Условий на русском и английском языке, преимущественную силу имеет версия Условий на русском языке.	14.1. The Terms are executed in Russian and English. In the event of a conflict between the Russian and English versions of the Terms, the Russian version of the Terms shall prevail.
14.2. Если отдельное положение Договора ДБО теряет силу или становится неисполнимым, это не приводит к недействительности других его положений.	14.2. If a separate provision of the RBS Contract becomes invalid or unenforceable, this shall not invalidate other provisions of the RBS Contract.
14.3. С даты заключения Договора ДБО вся переписка и договоренности между Сторонами, касающиеся условий Договора ДБО и предшествующие его заключению, теряют силу.	14.3. From the date of conclusion of the RBS Contract, all the correspondence and arrangements between the Parties concerning the terms and conditions of the RBS Contract before the above date shall become null and void.
14.4. Вся переписка в рамках исполнения Договора ДБО осуществляется Сторонами на русском/английском/испанском языке и может быть осуществлена посредством Системы.	14.4. All the correspondence within the framework of the execution of the RBS Contract shall be carried out by the Parties in Russian/English/Spanish and may be carried out through the System.
14.5. Условия могут быть изменены по инициативе Банка путем внесения изменений и/или дополнений в Условия, в том числе путем утверждения новой редакции Условий, в порядке, установленном настоящим разделом Условий.	14.5. The Terms may be amended by the Bank through modifications and/or additions to the Terms, including by approving a new edition of the Terms, in the manner prescribed by this section of the Terms.
14.6. Изменения и/или дополнения в Условия, внесенные Банком, вступают в силу по истечении 5 (пяти) календарных дней с даты опубликования Банком информации об этих изменениях и/или дополнениях либо с даты вступления изменений и/или дополнений в силу, если такая дата указана в опубликованной информации, но не ранее 5 (пяти) календарных дней с даты опубликования информации.	14.6. Amendments and/or additions made by the Bank to the Terms come into effect 5 (five) calendar days after the Bank publishes information about these amendments and/or additions, or from the date of their effectiveness if such date is indicated in the published information, but not earlier than 5 (five) calendar days from the date of publication.
В случае изменения законодательства Российской Федерации Условия, до момента их изменения Банком, применяются в части, не	In case of any change in laws of the Russian Federation, the Terms shall be applicable to the extent compliant with the

противоречащей требованиям законодательства Российской Федерации.	requirements of the legislation of the Russian Federation, until they are changed by the Bank.
14.7. Банк с целью ознакомления Клиентов с Условиями публикует их на официальном сайте Банка в сети «Интернет» по адресу: www.evrofinance.ru.	14.7. To make the Terms available to the Clients for review, the Bank shall publish them on the Bank's official website on the Internet at: www.evrofinance.ru.
Моментом публикации Условий, Тарифов и информации для ознакомления Клиентов, в т.ч. Документации, а также моментом ознакомления Клиента с опубликованными Условиями, Тарифами и информацией для ознакомления Клиентов, в т.ч. Документацией, считается момент их первого размещения на официальном сайте Банка в сети «Интернет» по адресу: www.evrofinance.ru.	As a moment of publication of the Terms, Tariffs and of information for clients, the Documentation included, as well as a moment of the Client´s familiarization with the published Terms, Tariffs and Documentation, is considered the moment of its primary placement at the Bank´s official website www.evrofinance.ru.
14.8. Действие изменений, внесенных в Условия, и вступивших в силу, распространяется на всех лиц, присоединившихся к Условиям, независимо от даты присоединения к Условиям (даты заключения Договора ДБО). В случае несогласия с изменениями, вносимыми в Условия, Клиент вправе расторгнуть Договор ДБО в одностороннем порядке до вступления таких изменений в силу в порядке, установленном в п.12.3 настоящих Условий.	14.8. Effective amendments to the Terms shall apply to all the persons who have joined the Terms, regardless of the date when they joined the Terms (date of the conclusion of the RBS Contract). In case the Client disagrees with the amendments to the Terms, the Client may terminate the RBS Contract unilaterally before such changes take effect in the accordance with the procedure established by paragraph 12.3 of these Terms.
14.9. В случае, если до вступления в силу опубликованных Банком изменений и/или дополнений, внесенных в Условия, Договор ДБО не расторгнут, Стороны признают, что указанные изменения и/или дополнения в Условия приняты Клиентом.	14.9. If the RBS Contract is not terminated before the effective date of the amendments and/or supplements to the Terms published by the Bank, the Parties shall deem such amendments and/or supplements to the Terms accepted by the Client.
14.10. Банк не несет ответственности, если информация об изменении и/или дополнении Условий, опубликованная в порядке и в сроки, установленные Условиями, не была получена и/или изучена и/или правильно истолкована Клиентом.	14.10. The Bank shall not be liable if the information on the amendments and/or supplements to the Terms published in the manner and within the period established by the Terms has not been received and/or studied and/or correctly interpreted by the Client.
14.11. Для целей Условий Акт признания открытого ключа (сертификата) для обмена сообщениями, подписанный между Сторонами до введения в действие настоящей редакции Условий, признается равнозначным Акту признания Сертификата ключа проверки ЭП для обмена сообщениями.	14.11. For the purposes of these Terms, the Act of acknowledgement of the public key (certificate) for message exchange signed by the Parties before the entry into force of the present version of these Terms is considered as equal to the Act of acknowledgement of the ES verification key Certificate for message exchange.
14.12. Для целей Условий Данные о владельце сертификата ключа проверки ЭП, подписанные Сторонами до введения в действие настоящей редакции Условий, признаются равнозначными Заявлению о предоставлении права доступа.	14.12. For the purposes of the Terms, information about the ES verification key certificate Holder signed by the Parties prior to the enactment of this version of the Terms is considered equivalent to an Application for granting the right of access.

14.13. Для целей Условий Договоры об использовании электронной системы дистанционного банковского обслуживания, предусматривающие присоединение к Соглашению об использовании электронной системы дистанционного банковского обслуживания (размещенному на официальном сайте Банка в сети «Интернет»), подписанные между Сторонами до введения в действие настоящей редакции Условий, признаются равнозначными Договору ДБО с Пакетом операций «Стандартный».	14.13. For the purposes of the Terms, Contracts on the use of the Electronic System of Remote Banking Services that include accession to the Agreement on the use of an electronic system for remote banking services (published on the Bank's official website) signed by the Parties prior to the enactment of this version of the Terms are considered equivalent to the RBS Contract with the Standard Package of Operations.
14.14. Список Приложений, являющихся неотъемлемой частью Условий: - Приложение №1 «Требования к аппаратно-программным средствам». - Приложение №2 «Способы доставки информации». - Приложение №3 «Порядок разбора конфликтных ситуаций». - Приложение №4 «Требования информационной безопасности».	14.14. List of Annexes, constituting an integral part of the Terms: - Annex No. 1 «Requirements to hardware and software». - Annex No. 2 «Means for the delivery of information». - Annex No. 3 «Procedure for the resolution of conflict situations». - Annex No. 4 «Information safety requirements».

Приложение №1 **к Условиям использования электронной системы дистанционного банковского обслуживания**	**Annex No. 1** **To the Terms of the Use of the Electronic System for Remote Banking Services**
ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНЫМ СРЕДСТВАМ	**REQUIREMENTS FOR THE SOFTWARE AND HARDWARE.**
1. Операционная система Windows 7 и выше. 2. Яндекс.Браузер, Chrome, Mozilla или Firefox. 3. Наличие подключенного сетевого или локального принтера. 4. Наличие подключения к сети Internet. 5. Перед установкой Системы необходимо установить программное обеспечение Средства криптографической защиты информации[14]. 6. При обмене информацией с бухгалтерскими системами (далее – БС) «1С», «Парус», БЭСТ-4 и с другими БС, в которых есть возможность экспорта документов в текстовый формат, необходимо, чтобы формат дат и чисел импортируемых документов соответствовал форматам дат и чисел, задаваемым в региональных настройках операционной системы компьютера.	1. Operating system Windows 7 or higher. 2. Yandex.Browser, Chrome, Mozilla or Firefox. 3. Availability of connected network or local printer. 4. Internet connection. 5. Before installing the System, it is necessary to install the software for the Information cryptographic security product[14]. 6. When exchanging information with accounting systems (ASs) "1C", "Parus", BEST-4, and with other ASs, in which it is possible to export documents in text format, the format of dates and numbers of imported documents must coincide with the formats of dates and numbers set in the regional settings of the computer operating system.

[14] Применимо только для СКЗИ КриптоПро. / Applicable only for the CryptoPro ICSP.

Приложение №2 **к Условиям использования электронной системы дистанционного банковского обслуживания**	**Annex No. 2** **To the Terms of the Use of the Electronic System for Remote Banking Services**
СПОСОБЫ ДОСТАВКИ ИНФОРМАЦИИ	**MEANS OF DELIVERY OF INFORMATION**
Работа осуществляется через подключение к своему провайдеру услуг сети «Интернет».	**Work is carried out through a connection to your Internet service provider**
Параметры подключения: открытый TCP порт 443 на сайт https://corp.efbank.ru	Connection parameters: open TCP port 443 to website https://corp.efbank.ru
Параметры подключения могут быть изменены и сообщены Клиенту в письменном уведомлении или направлены Клиенту посредством Системы.	Connection parameters may be changed and communicated to the Client by a written notification or sent to the Client via the System.
Настройка Клиентом данной транспортной схемы осуществляется на рабочем месте самостоятельно согласно требованиям провайдера.	**The Client shall set this delivery mechanism independently at the workstation according to the provider's requirements.**

Приложение №3
к Условиям использования электронной системы дистанционного банковского обслуживания

ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ

1. Общие положения

1.1. В настоящем Порядке под конфликтной ситуацией понимается возникновение у Сторон претензий, связанных с обменом Электронными документами (далее – ЭД) посредством Системы.
1.2. Ниже приведен перечень конфликтных ситуаций по поводу исполнения ЭД, рассматриваемых Технической комиссией, действующей в соответствии с порядком, предусмотренным Условиями:
- ЭД исполнен, а Клиент утверждает, что ЭД не посылал и не подписывал;

- Клиент утверждает, что он направил ЭД, а ЭД не исполнен, причем, по утверждению Клиента, от Банка получена Квитанция об исполнении;
- Клиент утверждает, что он направил один ЭД, а исполнен другой ЭД;
- не подтверждена подлинность ЭД средствами проверки ЭП принимающей Стороны;
- оспаривается факт идентификации Уполномоченного представителя Клиента, которому предоставлено право подписания от имени Клиента направляемых в Банк ЭД;
- другие конфликтные ситуации, связанные с функционированием Системы.
1.3. При возникновении разногласий Сторон в связи с обменом ЭД посредством Системы, а также в иных случаях возникновения конфликтных/спорных ситуаций, связанных с эксплуатацией Системы, обмен ЭД немедленно прекращается.
1.4. До разрешения конфликтной ситуации Клиенту рекомендуется не использовать в работе персональный компьютер, на который установлено программное обеспечение Системы.
1.5. При разрешении конфликтных ситуаций Стороны обязуются руководствоваться следующими принципами:

Annex No. 3
To the Terms of the Use of the Electronic System for Remote Banking Services

PROCEDURE FOR THE RESOLUTION OF CONFLICT SITUATIONS

1. General Provisions

1.1. In this Procedure, a conflict situation is understood as the occurrence of claims by the Parties related to the exchange of Electronic Documents (hereinafter referred to as ED) via the System.
1.2. Below is the list of conflict situations regarding the execution of EDs, considered by the Technical committee, acting in compliance to the procedure, as under the Terms:
- The ED was performed, and the Client insists that the ED was not sent and was not signed by the latter;
- The Client asserts that he directed the ED but the ED was not performed, however, according to the Client, Bank provide a confirmation receipt for the above document;
- The Client asserts, that he sent one ED, but a different ED was performed;
- the authenticity of the ED has not been confirmed by the ES verification tools of the receiving Party;
- the fact of identifying the Authorized Representative of the Client, who has been granted the right to sign ED sent to the Bank on behalf of the Client, is being disputed;
- other conflict situations related to the functioning of the System.
1.3. In the event of disagreements between the Parties related to the exchange of EDs via the System, as well as in other cases of conflict/disputed situations associated with the operation of the System, the exchange of ED is immediately suspended.
1.4. Until the conflict situation is resolved, the Client is advised not to use the personal computer on which the System software is installed.

1.5. During the resolution of conflict situations Parties undertake to be guided by the following principles:

- Сторона-получатель обязуется признать подлинным и действительным ЭД, переданный ей посредством Системы и имеющий ЭП, сформированную на Ключах ЭП Стороны-отправителя, при условии положительного результата проверки ЭП на соответствующих им Ключах проверки ЭП;	- Receiving party undertakes to acknowledge, as authentic and valid, the ED transferred thereto through the System and which has an Electronic Signature, formed on the ES Keys of the Sending party, subject to the positive result of the Electronic Signature verification on the corresponding ES verification Keys;
- Сторона-отправитель обязуется признать подлинным (переданным ею посредством Системы) и действительным ЭД, имеющий ЭП, сформированную на ее Ключах ЭП, при условии положительного результата проверки ЭП на соответствующих им Ключах проверки ЭП;	- Sending party undertakes to acknowledge as authentic (transferred thereto through the System) and valid the ED which has an Electronic Signature, formed under its ES Keys, subject to the positive result of the Electronic Signature verification on the corresponding ES verification Keys;
- ответственность возлагается на Сторону-отправителя при получении Стороной-получателем ложного ЭД с успешно подделанной ЭП, так как в этом случае Сторона-отправитель не обеспечила сохранность Ключей ЭП.	- the responsibility is borne with the Sending party in case the Receiving party receives a false ED with successfully falsified Electronic signature, as in this case the Sending party did not assure the security of the ES Keys.
1.6. Стороны признают, что математические свойства алгоритма ЭП[15] гарантируют невозможность подделки значения ЭП любым лицом, не обладающим Ключом ЭП.	1.6. Parties agree that the mathematical features of the ES algorithm[15], guarantee impossibility of falsification of the ES value by any person, who does not possess the ES Key.
1.7. Стороны должны представить Технической комиссии следующие материалы:	1.7. Parties must present the following materials to the Technical committee:
– уведомление о претензии в письменном виде на бумажном носителе с подробным изложением обстоятельств и предполагаемых причин возникновения конфликтной ситуации;	– a written notice of claim on paper with a detailed description of the circumstances and the presumed causes of the conflict situation;
– носители информации с файлами, содержащими спорный ЭД, выгруженный из Системы, а также распечатанный из Системы спорный ЭД на бумажном носителе или Квитанция на него. Описание процедуры выгрузки данных для проверки ЭП приведено в Документации;	– data carriers with the files, containing the disputed ED downloaded from the System, as well as the printed disputed ED from the System on paper or the Receipt confirmation received for it. Description of the procedures for the downloading of data for the verification of the ES is provided in the Documentation;
– выписка из протокола работы Системы, подтверждающая прием/отправку спорного ЭД, на бумажном носителе, за согласованный Сторонами период;	– an extract from the System's protocol confirming the receipt/sending of the disputed ED, in hard copy, for the period agreed upon by the Parties;
– в случае использования УНЭП: подписанные собственноручными	– in case of using the EUES: original copies of the Acts of acknowledgement

[15] Для СКЗИ КриптоПро – реализованного в соответствии с требованиями стандартов Российской Федерации действующих ГОСТов. / For the CryptoPro ICSP – implemented in accordance with the requirements of the standards of the Russian Federation and applicable GOSTs.

подписями Уполномоченных лиц Сторон оригиналы Актов признания; – в случае использования УКЭП: Сертификат ключа проверки УКЭП, выданный Удостоверяющим центром, подтверждающий факт действительности ЭП под оспариваемым ЭД; – оригиналы заявлений об изменении состава Уполномоченных представителей Клиента, аннулировании действия Ключа проверки ЭП Уполномоченного представителя Клиента (при наличии); – Ключ проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка, с помощью которых проводилась проверка ЭП оспариваемого ЭД; – распечатки Ключа проверки УНЭП/Сертификата ключа проверки УКЭП Клиента, распечатку Ключа проверки УНЭП Уполномоченного лица Банка на бумажном носителе; – Носители с Ключами; – другие материалы, имеющие отношение к сути рассматриваемой претензии. 1.8. Стороны обязаны способствовать работе Технической комиссии и не допускать необоснованного отказа от предоставления необходимых документов. В случае непредоставления в установленный срок Технической комиссии одной из Сторон каких-либо из вышеперечисленных материалов к рассмотрению принимаются аналогичные материалы, предоставленные другой Стороной.	signed with the handwritten signatures of the Authorized Persons of the Parties; – in case of using the EQES: the EQES verification key Certificate issued by the Certification Authority, confirming the validity of the ES on the disputed ED; – original statements on changes to the composition of the Authorized Representatives of the Client, cancellation of the validity of the Client's Authorized Representative's ES verification Key (if any); – The ES verification Key of the Authorized Representatives of the Client/Bank's Authorised Person used to verify the ES of the disputed ED. – printouts of the Client’s EUES verification key/EQES verification key Certificate and the Bank’s Authorized Person’s EUES verification key on paper; – Carriers with the Keys; – other materials relevant to the essence of the claim under consideration. 1.8. The Parties are obligated to facilitate the work of the Technical committee and to avoid unjustified refusal to provide the necessary documents. In the event that one of the Parties fails to provide any of the aforementioned materials to the Technical committee within the established timeframe, similar materials provided by the other Party shall be considered.
2. Процедура проверки подлинности Электронных документов 2.1. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка. 2.2. При разборе конфликтных ситуаций используется стороннее эталонное программное обеспечение проверки подлинности ЭП и Сертификатов ключа проверки ЭП. 2.3. Проверка подлинности ЭП под спорным ЭД Клиента осуществляется посредством:	**2. Procedure for the verification of the authenticity of the Electronic Documents** 2.1. The procedure for verifying the authenticity of ED is carried out using the Bank's equipment and on its premises. 2.2. When resolving conflict situations, third-party reference software is used for the authentication of the ES and ES verification key Certificates. 2.3. Verification of the authenticity of the ES on the disputed ED of the Client is carried out by:

- программного средства «КриптоАРМ», установленного в Банке[16]. либо - программы OpenSSL.exe[17]. Описание программы приведено в документации на официальном сайте разработчика в сети «Интернет»: http://openssl.org/docs/.	- the CryptoARM software installed at the Bank[16]. or - the OpenSSL.exe[17] program. The program description is provided in the documentation on the developer's official website on the Internet: http://openssl.org/docs/.
2.4. Проверка подлинности ЭП под спорным ЭД Банка осуществляется посредством программного средства «КриптоАРМ», установленного в Банке.	2.4. Verification of the ES under a disputed Bank ED is conducted using the CryptoARM software installed at the Bank.
2.5. Процедура проверки Технической комиссией УНЭП, выпущенной Банком/УКЭП, выпущенной в соответствии с внутренним регламентом Удостоверяющего центра, под спорным ЭД включает следующие действия:	2.5. The procedure for the Technical committee's verification of the EUES issued by the Bank or the EQES issued in accordance with the Certification Authority's internal regulations under a disputed ED includes the following steps:
- установление времени подписания и отправки оспариваемого ЭД Уполномоченным представителем Клиента/Уполномоченным лицом Банка;	- establishing the time of signing and sending the disputed ED by the Authorized Representative of the Client/Bank’s Authorized Person;
- сверка даты и времени регистрации, а также срока действия Ключей проверки ЭП Уполномоченного представителя Клиента/Уполномоченного лица Банка, подписавших спорный ЭД, с датой и временем подписания спорного ЭД;	- cross-checking the date and time of registration, as well as the validity period of the ES verification Keys of the Authorized Representative of the Client/Bank’s Authorized Person who signed the disputed ED, against the date and time of signing the disputed ED;
- сверка даты и времени регистрации в Банке заявлений об изменении состава/ аннулировании действия ключей ЭП Уполномоченных представителей Клиента, подписавших спорный ЭД (при наличии), с датой и временем подписания спорного ЭД;	- cross-checking the registration date and time of statements submitted to the Bank regarding changes in the composition or revocation of the ES Keys of the Authorized Representatives of the Client who signed the disputed ED (if applicable) against the date and time of signing the disputed ED;
- проверка действительности полномочий лиц, подписавших спорный ЭД, на дату его подписания, осуществляемая по результатам рассмотрения соответствующих документов, подтверждающих их полномочия;	- verifying the validity of the signing authority of individuals who signed the disputed ED as of the signing date, based on the review of relevant documents confirming their authority;
- проверка подлинности УНЭП/УКЭП под выгруженным спорным ЭД с использованием Ключа проверки ЭП Стороны-отправителя спорного ЭД;	- verifying authenticity of the EUES/ EQES on the downloaded disputed ED with the use of a ES verification Key of the Sending party of the disputed ED;
- проверка подлинности и целостности Ключей проверки ЭП Уполномоченных представителей Клиента/Уполномоченных лиц Банка:	- verifying the authenticity and integrity of the ES verification Keys of the Authorized Representatives of the Client/Bank's Authorized Persons:

[16] Применимо только для СКЗИ КриптоПро. / Applicable only for the CryptoPro ICSP.
[17] Применимо только к СКЗИ OpenSSL. / Applicable only for the OpenSSL ICSP.

• В случае использования УНЭП: - проверка соответствия экземпляров Актов признания, предоставленных Сторонами в соответствии с п.1.7. настоящего Порядка; - сверка соответствия ключевых полей Ключа проверки ЭП из Актов признания с распечаткой протокола проверки ЭП, полученной при помощи программы OpenSSL.exe[18]/ посредством программного средства «КриптоАРМ»[19], установленного в Банке. • В случае использования УКЭП: - сверка соответствия ключевых полей Ключа проверки ЭП из файла Сертификата ключа проверки УКЭП, направленного Клиентом в Банк, с распечаткой протокола проверки ЭП, полученной посредством программного средства «КриптоАРМ»[20], установленного в Банке; - в случае необходимости подтверждения УКЭП Техническая комиссия направляет запрос в Удостоверяющий центр о подтверждении действительности УКЭП на дату подписания оспариваемого ЭД. 2.6. Подтверждением корректности УНЭП/УКЭП под оспариваемым ЭД является одновременное выполнение следующих условий: - Ключи проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка, с помощью которых проверялись УНЭП/УКЭП, в момент поступления ЭД в Банк/Клиенту и его проверки являлись действующими, т.е. были зарегистрированы в установленном Банком или внутренним регламентом работы Удостоверяющего центра порядке, сроки их действия не истекли и они не были отменены; - подтверждена подлинность и целостность Ключей проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка, с помощью которых проводилась проверка УНЭП/УКЭП; - проверка УНЭП/УКЭП под спорным ЭД с использованием Ключей проверки ЭП Уполномоченных представителей Клиента/Уполномоченного лица Банка дала	• In case of using the EUES: - verifying conformity of the copies of the Acts of acknowledgement provided by the Parties as per paragraph 1.4 of this Procedure; - cross-cheking the key fields of the ES verification Key from the Acts of acknowledgement against the printed out ES verification protocol from OpenSSL.exe[18]/CryptoAPM[19], installed in the Bank. • In case of using the EQES: - verification of the key fields of the ES verification Key from the EQES verification key Certificate file sent by the Client to the Bank against the printout of the ES verification protocol obtained using the CryptoARM[20] software installed at the Bank; - If the EQES confirmation is required, the Technical committee sends a request to the Certification Authority to confirm the validity of the EQES as of the date the disputed ED was signed. 2.6. Confirmation of the correctness of the EUES/EQES under the disputed ED is established if the following conditions are simultaneously met: - the ES verification Keys of the Authorized Representatives of the Client/Bank's Authorized Persons used to verify the EUES/EQES were valid at the time of receipt of the ED by the Bank/Client and its verification was valid, i.e., they were registered in accordance with the procedures established by the Bank or the Certification Authority's internal regulations, their validity period had not expired, and they had not been revoked. - the authenticity and integrity of the ES verification Keys of the Authorized Representatives of the Client/Bank's Authorized Persons used to verify the EUES/EQES were confirmed; - verification of the EUES/EQES under the disputed ED using the ES verification Keys of the Authorized Representatives of the Client/Bank's Authorized Persons yielded a

[18] Применимо только к СКЗИ OpenSSL. / Applicable only for the OpenSSL ICSP.
[19] Применимо только к СКЗИ КриптоПро. / Applicable only for the CryptoPro ICSP.
[20] Применимо только к СКЗИ КриптоПро. / Applicable only for the CryptoPro ICSP.

положительный результат, то есть подтвердила подлинность УНЭП/УКЭП под спорным ЭД; - действия Банка по обработке ЭД проведены в соответствии с информацией, содержащейся в ЭД.	positive result, confirming the authenticity of the EUES/EQES under the disputed ED; - the Bank's actions in processing the ED were conducted in accordance with the information contained in the ED.
2.7. В случае выполнения всех условий, перечисленных в п.2.6 настоящего Порядка, Стороны соглашаются с тем, что корректность УНЭП/УКЭП под оспариваемым ЭД подтверждена, то есть проверяемый ЭД подписан корректными УНЭП/УКЭП.	2.7. If all the conditions listed in paragraph 2.6 of this Procedure are met, the Parties agree that the correctness of the EUES/EQES under the disputed ED is confirmed, i.e., the disputed ED was signed with the valid EUES/EQES.
2.8. В случае невыполнения любого из условий, перечисленных в п.2.6 настоящего Порядка, Стороны соглашаются с тем, что корректность УНЭП/УКЭП не подтверждена, то есть проверяемый ЭД подписан некорректными УНЭП/УКЭП.	2.8. If any of the conditions listed in paragraph 2.6 of this Procedure is not met, the Parties agree that the correctness of the EUES/EQES is not confirmed, i.e., the disputed ED was signed with the invalid EUES/EQES.
2.9. В том случае, если Банк принял к исполнению ЭД, подписанный УНЭП/УКЭП Уполномоченного представителя Клиента, корректность которого установлена Технической комиссией (Стороны согласны с выводами Технической комиссии), Стороны соглашаются с тем, что претензии Клиента к Банку, связанные с последствиями исполнения указанного ЭД, являются необоснованными.	2.9. If the Bank accepts for execution an ED signed with the EUES/EQES of the Authorized Representative of the Client, the correctness of which is established by the Technical committee (the Parties agree with the conclusions of the Technical committee), the Parties agree that the Client's claims against the Bank related to the consequences of executing the said ED are unfounded.
2.10. В том случае, если Банк принял к исполнению ЭД, подписанный УНЭП/УКЭП Уполномоченного представителя Клиента, корректность которого не подтверждена Технической комиссией (Стороны согласны с выводами Технической комиссии), претензии Клиента к Банку, связанные с последствиями исполнения указанного документа признаются обоснованными.	2.10. If the Bank accepts for execution an ED signed with the EUES/EQES of the Authorized Representative of the Client, the correctness of which is not confirmed by the Technical committee (the Parties agree with the conclusions of the Technical committee), the Client's claims against the Bank related to the consequences of executing the said ED are considered justified.
2.11. Результаты работы Технической комиссии отражаются в акте, составленном в 2 (двух) экземплярах, по одному экземпляру для каждой Стороны, и являющимся основанием принятия Сторонами окончательного решения об урегулировании конфликтной ситуации.	2.11. The results of the Technical committee's work are recorded in an act drawn up in two (2) copies, one for each Party, which serves as the basis for the Parties to make a final decision on resolving the conflict situation.
Акт о результатах проведения технической экспертизы должен содержать следующую информацию: - состав Технической комиссии; - дата и место составления акта;	The Act on the results of the technical examination must include the following information: - composition of the Technical committee; - date and place of the act's preparation;

- дата и время начала и окончания работы Технической комиссии; - суть претензии; - перечень мероприятий, проведённых Технической комиссией; - фактические обстоятельства, установленные Технической комиссией; - выводы, к которым пришла Техническая комиссия в результате проведённых мероприятий; - подписи членов Технической комиссии на каждом листе акта. 2.12. Акт подписывается всеми членами Технической комиссии. Члены Технической комиссии, не согласные с выводами большинства, подписывают акт с возражениями, который прилагается к основному акту, либо излагают свое несогласие и выводы в письменном виде в отдельном документе, который прилагается к основному акту. 2.13. В случае несогласия одной из Сторон с выводами Технической комиссии, отражёнными в акте о результатах проведения технической экспертизы, уклонения от формирования Технической комиссии либо участия в её работе, препятствования участию второй Стороны в работе Технической комиссии, вторая Сторона вправе передать спор на рассмотрение в Арбитражный г. Москвы.	- start and end dates and times of the Technical committee’s work; - nature of the claim; - list of measures undertaken by the Technical committee; - factual circumstances established by the Technical committee; - conclusions reached by the Technical committee as a result of the measures undertaken; - signatures of the members of the Technical committee on each page of the act. 2.12. The act shall be signed by all the members of the Technical committee. Members of the Technical committee, who disagree with the conclusions made by the majority, sign a report of objection, which is annexed to the main report, or shall state their disagreement and conclusions in writing in a separate document, which shall be attached to the main report. 2.13 In the event one Party disagrees with the conclusions of the Technical committee as reflected in the act on the results of the technical examination, or if a Party refuses to form the Technical committee, participate in its work, or obstructs the other Party’s participation in the Technical committee's work, the other Party has the right to submit the dispute to the Arbitration Court of Moscow for resolution.

Приложение №4 **к Условиям использования электронной системы дистанционного банковского обслуживания**	**Annex No. 4** **To the Terms of the Use of the Electronic System for Remote Banking Services**
ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	**INFORMATION SAFETY REQUIREMENTS**
Для минимизации рисков Несанкционированного доступа к Системе, к Счетам, счету по вкладу (депозиту) Клиента со стороны злоумышленников и компрометации ключевой информации, Банк настоятельно просит Клиентов соблюдать следующие меры информационной безопасности:	In order to minimize the risks of Unauthorized access to the System, to the Client's Accounts, deposit account by law violators and the compromise of key data, the Bank strongly recommends its Clients to comply with the following information safety measures:
• Выделить отдельный компьютер, который не будет использоваться в иных целях, кроме как для установки и работы в Системе, и предоставить доступ к нему ограниченному кругу лиц	• To choose a separate computer that shall be used solely for the purposes of installation and working with the System, and provide access to it to a limited number of persons.
• Не осуществлять, а при наличии технической возможности, запретить выход в сеть «Интернет» с этого компьютера на иные адреса, за исключением адресов серверов Банка.	• Not to access the Internet from such a computer and, if possible, to prevent all Internet connection from such a computer, except for the connection with the Bank services.
• Ограничить или полностью запретить удаленный доступ к выделенному компьютеру с других компьютеров локальной сети. Не использовать средства удаленного администрирования на выделенном компьютере. При наличии технических средств, поместить выделенный компьютер в отдельную сеть, контролируемую межсетевым экраном и системами обнаружения атак.	• To limit or prohibit remote access to such a computer from all other computers of the local network. Not to use remote administration tools on such a computer. Technical assets permitting, to create a specified network controlled by a network firewall and an intrusion detection system for such a computer.
• Заменить все стандартные Пароли, заданные при установке Системы, на уникальные собственные, производить периодическую смену Паролей (не реже одного раза в три месяца); не оставлять в легкодоступных местах и не передавать неуполномоченным лицам записи, содержащие сведения о Паролях для входа в Систему, хранить записи о Паролях в месте, защищенном от несанкционированного доступа.	• To replace all default Passwords set out at the moment of System installation with unique passwords; to change Passwords regularly (not less than once in three months), do not leave in easily accessible places and do not transfer to unauthorised persons records containing information about the Passwords for entering the System, keep records about the Passwords in a place protected from unauthorised access;
• Использовать на постоянной основе антивирусное программное обеспечение с последней актуальной версией баз.	• To constantly use anti-virus software with the latest versions of databases;
• Регулярно (не реже одного раза в неделю) выполнять антивирусную проверку для	• To carry out anti-virus checks on a regular basis (not less than once a week)

своевременного обнаружения вредоносных программ.	in order to timely detect malicious software;
• Использовать на компьютере исключительно лицензионное программное обеспечение.	• To use only licensed software on the computer;
• Регулярно (не реже одного раза в месяц или по факту публикации) устанавливать обновления операционной системы.	• To update the operating system regularly (not less than once a month or upon launching);
• Проверить группу «Администраторы» на выделенном компьютере, исключить всех рядовых пользователей из этой группы, не работающих с Системой.	• To check the Administrator's group on the selected computer and to remove all users that do not operate the System;
• При наличии технической возможности, для пользователей, работающих с Системой, создать отдельную групповую политику, разрешающую запуск только определенных приложений.	• Technical assets permitting, develop a separate group policy for the users working with the System and allow the use of specific applications only.
• Для доступа к серверам Банка использовать только заведомо известные Вам адреса интернет серверов Банка.	• To use only known Internet addresses of Bank servers to access them.
• В случае отсутствия возможности подключения к серверу Банка незамедлительно сообщать об этом Банку.	• To inform the Bank immediately, in case Bank servers are unavailable.
• Хранить в безопасном месте (в сейфе) и никому не передавать Носители с Ключами электронной подписи и Ключами проверки электронной подписи (далее – Ключи), обеспечив к ним доступ только Уполномоченных представителей.	• To store Carriers with Electronic signature Keys and Electronic signature verification Keys (hereinafter – the Keys) in a safe place (a vault), never to transfer them to third parties, to limit access to them only to Authorized Representatives;
• Никогда не осуществлять копирование Ключей на локальный жесткий диск компьютера, даже с последующим его удалением.	• Never to copy Keys on the local hard drive of the computer, even in case the copies are deleted immediately;
• Регулярно (не реже одного раза в месяц) проверять целостность Носителей с Ключами, проводя проверку наличия на них файлов электронной подписи.	• To check the integrity of Carriers with the Keys cheking the presence of electronic signature files on them on a regular basis (not less than once a month);
• Своевременно (в соответствии с положениями Условий) проводить Плановую смену Ключей.	• Timely (according to the provisions of the Terms) perform the Planned change of Keys;
• Не оставлять Носители с Ключами без присмотра, подключать их к компьютеру только на время использования и незамедлительно их отключать после проведения банковских операций. При оставлении рабочего места Системы без присмотра всегда блокировать экран с последующим вводом пароля для его разблокировки.	• Not to leave the Carriers with the Keys unattended; to connect them to the computer only for the time of use and immediately disconnect after the completion of banking operations. In case a work place with the System is left unattended, to block the screen and to use a password for its further unlocking;

• Производить незамедлительную замену Ключей в случае их компрометации или подозрении на компрометацию.	• To immediately replace Keys in case of their actual or alleged compromise;
• Принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства на компьютере и в Системе, появление на компьютере и в Системе компьютерных вирусов, а также программ, направленных на разрушение и модификацию программного обеспечения Системы, Электронных документов, либо на перехват Паролей, Ключей и другой конфиденциальной информации.	• Take necessary measures to prevent unauthorized changes to technical and software tools on the computer and in the System, the appearance of computer viruses in the System, and programs aimed at damaging or modifying the System's software, Electronic Documents, or intercepting Passwords, Keys, and other confidential information.
• Своевременно устанавливать все обновления Системы.	• Timely update the System;
• Не устанавливать обновления, а также не открывать ссылки в почтовых сообщениях, полученных от имени Банка по электронной почте; получив такое сообщение, незамедлительно сообщать об этом Банку.	• Not to install updates and not to open links received in the e-mail from the Bank; to inform the Bank about receiving any such e-mails;
• Ежедневно, в течение операционного дня Банка и по окончании Рабочего дня, осуществлять дополнительный вход в Систему для контроля перечня исходящих документов за текущий день. При обнаружении подозрительных документов, незамедлительно обращаться в Банк.	• To access the System additionally in order to check the list of the documents for the current day in a daily basis during a banking day and at its end. In case of detection of any suspicious documents, to inform the Bank immediately;
• В случае подозрений на замедление работы компьютера отключить компьютер физически от локальной сети и сети «Интернет» и обратиться к системному администратору с просьбой о необходимости проведения полной антивирусной проверки сканированием всех файлов и памяти компьютера.	• In case of suspicious delays in the computer's operations, to physically disconnect the computer from the local network and the Internet and to request complete anti-virus scanning of all files and computer memory from the system administrator;
• В случае, если инцидент информационной безопасности все же произошел, ни в коем случае не выключать компьютер, а отключить его физически только от локальной сети и сети «Интернет», незамедлительно обратиться к системному администратору и сообщить об инциденте в Банк для проведения оперативного расследования и принятия необходимых мер для сбора доказательств.	• In case of a breach of information security, never to turn the computer off, but to disconnect it physically from the local network and the Internet, to address the system administrator immediately and to inform the Bank about the incident in order to carry out on-the-spot investigation and take measures to collect evidence.
• В случае выявления Клиентом подозрительных операций в Системе незамедлительно сообщать об этом в Банк.	• In case the Client detects suspicious operations with the System, he should immediately inform the Bank about it.