УТВЕРЖДЕНО/APPROVED by:

Президент АО “Денизбанк Москва”/The President JSC “Denizbank Moscow"
Осман Огуз Йалчын / Osman Oguz Yalcin

Приказ/The Order №80 от/dd 29.06.2023

ОБЩИЕ УСЛОВИЯ
предоставления услуг с использованием системы дистанционного банковского обслуживания «Клиент-Банк» в АО «Денизбанк Москва»

GENERAL TERMS AND CONDITIONS
for the provision of services using the Remote Banking system "Client-Bank" in JSC "Denizbank Moscow"

Оглавление

1. ОПРЕДЕЛЕНИЯ / DEFINITIONS

1.1. **Банк** – Акционерное общества «Денизбанк Москва» (сокращенное наименование - АО «Денизбанк Москва»), лицензия Банка России на осуществление банковских операций № 3330 от 15 декабря 2014 г.

1.2. **Клиент** – юридическое лицо или индивидуальный предприниматель, имеющее(ий) в Банке открытые банковские счета.

1.3. **Договор** – Договор о предоставлении услуг с использованием системы дистанционного банковского обслуживания «Клиент-Банк» в АО «Денизбанк Москва», заключаемый на основании представленного Клиентом в Банк Заявления на предоставление услуг «Клиент-Банк» (iBank 2) путем присоединения к настоящим Общим условиям в соответствии со статьей 428 Гражданского кодекса Российской Федерации

1.4. **Система «Клиент-Банк» (**далее по тексту **«Система»)** – корпоративная информационная система дистанционного банковского обслуживания, представляющая собой комплекс программно-технических средств, позволяющих осуществить создание, передачу по защищенному каналу связи с использованием протокола SSL и хранение платежных и иных электронных документов, а также электронных копий документов, и предназначенная для формирования электронных документов, а также электронных копий документов с помощью средств криптографической защиты информации (СКЗИ), их составления и подписания с использованием электронной подписи, и обмена ими между Клиентом и Банком.

1.5. **Электронный документ (**далее по тексту **– «ЭД»)** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по Системе, подписанная корректной ЭП и имеющая равную юридическую силу с аналогичным документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным (при необходимости) оттиском печати (если она есть), независимо от того, существуют такие документы на бумажных носителях или нет. Достоверность и конфиденциальность ЭД обеспечивается средствами ЭП, защитой от несанкционированного доступа и соблюдением установленного режима эксплуатации АРМ.

1.6. **Электронная копия документа (**далее по тексту **– «ЭКД»)** – информация в электронной форме (вид ЭД в виде сканированной копии документа на бумажном носителе), направленная через Систему в качестве вложения в сообщение, подписанное электронной подписью.

Положения настоящих Общих условий, установленные и используемые в отношении ЭД, применяются и используются в отношении ЭКД в той мере, в которой они не противоречат существу ЭКД и прямо установленным настоящими Общими условиями в отношении ЭКД положениям.

1.7. **Электронная подпись (**далее по тексту **«ЭП»)** – информация в электронной форме, созданная с

1.1. **Bank** means Joint Stock Company "Denizbank Moscow" (abbreviated name - JSC "Denizbank Moscow"), license of the Bank of Russia for banking operations No. 3330 dated December 15, 2014.

1.2. **Client** – a legal entity or individual entrepreneur who has open bank accounts with the Bank.

1.3. **Agreement** means an Agreement on the provision of services using the remote banking system in JSC "Denizbank Moscow", concluded on the basis of an Application submitted by the Client to the Bank for the provision of services "Client-Bank" (iBank 2) on accession to these General Terms in accordance with Article 428 of the Civil Code of the Russian Federation

1.4. **The "Client-Bank" system (**hereinafter referred to as **the "System")** means corporate informational system for remote banking services comprising a set of software - hardware, allowing creation, transfer through the protected communication channel with use of protocol SSL and storage of payment and other electronic documents as well as electronic copies of the documents and designed for making out and approval the electronic documents as well as electronic copies of the documents with cryptographic information protection facilities (CIPF), forming and signing of them with an electronic signature and transmission of them between the Client and the Bank.

1.5. **Electronic document (**hereinafter referred to as **the "ED")** means a documented information presented in electronic form, that is, in a form suitable for human perception using electronic computers, as well as for transmission through the System, signed by a correct ES and having equal legal force with a similar document on paper, signed with the handwritten signatures of authorized persons and certified (if necessary) by a seal impression (if any), regardless of whether such documents exist on paper media or not. The reliability and confidentiality of the ED is ensured by means of the ES, protection against unauthorized access and compliance with the established operating mode of the automated control system.

1.6. **Electronic copy of the document (**hereinafter referred to as **the "ECD")** means an information in electronic form (type of the ED as a scan copy of the document on a paper carrier) transmitted through the System as an attachment to a message signed by an electronic signature.

The provisions hereof which are established and used in relation to ED are applied and used in relation to the ECD to the extent that they do not contradict the essence of the ECD and the provisions directly established hereby regarding the ECD.

1.7. **Electronic signature (**hereinafter referred to as **the "ES")** means an information in electronic form created

использованием средств электронной подписи и полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая позволяет определить лицо, подписывающее информацию, и установить факт внесения изменений в электронный документ после момента его подписания.

1.8. **Ключ ЭП** – уникальная последовательность символов, предназначенная для создания ЭП, формируемая стороной, которая подписывает ЭД, и известная только ей.

Уникальность последовательности символов означает то, что вероятность сформировать ту же самую последовательность символов в течение времени использования ключа до его плановой замены близка к нулю.

1.9. **Ключ проверки ЭП** – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП. Ключ проверки ЭП формируется подписывающей Стороной в паре с Ключом ЭП. Уникальность последовательности символов означает то, что эта последовательность однозначно идентифицирует ЭП, выполненную с использованием только соответствующего Ключа ЭП.

1.10. **Ключевой Носитель** – физический носитель Ключа ЭП, предназначенный для формирования ЭП на ЭД и обеспечивающий неизвлекаемость Ключа ЭП.

1.11. **Владелец Сертификата Ключа проверки ЭП** – представитель Клиента или Банка, которому в установленном Федеральным законом порядке выдан Сертификат Ключа проверки ЭП.

1.12. **Сертификат Ключа проверки ЭП** – электронный документ или документ на бумажном носителе, оформляемый Клиентом и выданный Банком, подтверждающий принадлежность Ключа Проверки ЭП владельцу сертификата ключа проверки электронной подписи.

1.13. **Компрометация Ключа ЭП** – утрата доверия к Ключу ЭП по причине наступления одного или нескольких из следующих событий:

- утрата или порча Ключевого Носителя;
- утрата Ключевого Носителя с последующим обнаружением;
- утрата ключей от сейфа (в том числе с последующим обнаружением) в момент нахождения в нем Ключевого Носителя;
- доступ посторонних лиц к Ключевым Носителям либо подозрение, что такой доступ имел место;
- иные обстоятельства прямо или косвенно свидетельствующие о несанкционированном доступе третьих лиц (не Владельца Сертификата Ключа проверки ЭП) к Ключевому Носителю, Ключу ЭП или Системе или возможности такого доступа (выявленные Клиентом и/или Банком).

1.14. **Счет** – банковский счет, открытый Клиентом в Банке, проведение операций по которому производится с помощью Системы.

using electronic signature tools and obtained as a result of cryptographic transformation of information using an electronic signature key, that is attached to the other information in electronic form (information to be signed) or joined with that information by another way and that is used for identification of the person signing the information and establishing the fact of making changes to the electronic document after the moment of its signing.

1.8. **ES Key** means a unique sequence of characters designed to form an ES to be composed by the party signing ED and known to that party only.

The unique sequence of characters means that the possibility to form the same sequence of characters during the definite period of time of the key use until its planed change is nearly equal to zero.

1.9. **ES verification key** means a special unique sequence of characters, unequivocally related to the ES Key and designated for verification of ES authenticity. The ES verification key shall be formed by a signing Party together with the ES Key.

Unique sequence of characters means that that sequence unambiguously identifies the ES, formed with use of the corresponding ES Key only.

1.10. **Key Carrier** means a device containing the Key of ES and designated for forming ES on ED and ensuring anti-handling of ES Key.

1.11. **Owner of Certificate on the ES verification key** means the representative of the Client or the Bank to whom, in accordance with the procedure established by the Federal Law, a Certificate on the ES verification key was issued.

1.12. **Certificate on the ES verification key** means a document on a paper carrier, being formed by the Client and the Bank and containing a print-out of the ES verification key and designated for verification of ES authenticity on ED and identification of the User of the ES Key.

1.13. **Compromise of the ES Key** means the loss of confidence in the ES Key due to the one of the following events:

• loss or damage of a Key Carrier;
• loss of a Key Carrier with subsequent detection;
• loss of the keys to the safe (including subsequent detection) at the time when the Key Carrier is in it;
• access of unauthorized persons to Key Media or suspicion that such access took place;
• other circumstances directly or indirectly indicating the unauthorized access to the Key Carrier, the ES Key or to the System by third parties or the possibility of that access (revealed by the Owner of Certificate on the ES verification key).

1.14. **Account** means the bank account opened by the Client with the Bank operations on which are managed through the System.

1.15. **Плановая замена Ключей ЭП** – замена Ключей ЭП осуществляемая с периодичностью не менее одного раза в год с даты начала их действия.

1.16. **Внеплановая замена Ключей ЭП, принадлежащего конкретному Владельцу Сертификата Ключа проверки ЭП**, осуществляется при:

- Компрометации этого Ключа ЭП или подозрении на его Компрометацию;
- повреждении программно-технических средств, на которых установлена Система;
- получении Банком сведений из государственных и иных информационных систем о прекращении полномочий единоличного исполнительного органа и/или иных лиц, уполномоченных действовать от имени Клиента без доверенности;
- по заявлению Клиента.

1.17. **Блокировочное слово** – уникальное слово, определяемое Клиентом при регистрации в Системе, используемое Банком для идентификации Клиента при его обращении по телефону в Банк с целью срочного изменения настроек, блокировки ключа ЭП, подтверждения платежей Клиента или в иных установленных соглашением между Банком и Клиентом случаях.

В случае утраты Клиентом Блокировочного слова в ситуации, когда Система заблокирована Банком по основаниям, установленным Договором, представитель Клиента должен явиться в Банк незамедлительно и предоставить Банку новое Блокировочное слово. В противном случае Банк не будет нести ответственность за невозможность связи с Клиентом для направления Клиенту уведомлений и проведения платежей, осуществленных без согласия Клиента, а также иных предусмотренных Договором сообщений и информации.

1.15. **Planned change of the ES Key** means a change of the ES Key being executed not less than once a year since the date of the commencement of their validity.

1.16. **Extraordinary change of the ES Key belonging to a specific Owner of the Certificate of the ES Verification Key**, means:

- Compromise of the ES Key or suspicion of the Compromise of the ES Key;
- damage of a set of software – hardware on which the System is installed;
- receipt by the Bank of information from state and other information systems on the termination of the powers of the sole executive body and/or other persons authorized to act on behalf of the Client without a power of attorney;
- upon the Client's application.

1.17. **Lock word** means a unique word to be determined by the Client during its registration in the System and to be used by the Bank to identify the Client calling to the Bank in order to urgently change the settings, lock the key of the Item instance, confirm the Client's payments or in others cases set out in the agreement between the Bank and the Client.

In case of loss of the Lock word by the Client in the situation when the System is blocked by the Bank on the grounds established hereby, the Client's representative shall come to the Bank immediately and provide the Bank with a new Lock word. Otherwise, the Bank shall not be liable for the inability to communicate with the Client in order to notify the Client and make payments made without the Client's consent as well as other messages and information stipulated hereby.

2. ОБЩИЕ ПОЛОЖЕНИЯ / GENERAL PROVISIONS

2.1. Настоящие Общие условия предоставления услуг с использованием системы дистанционного банковского обслуживания «Клиент-Банк» (далее – «**Общие условия**») регулируют отношения, возникающие при подключении Банком Клиента к Системе и дальнейшем осуществлении обмена ЭД по ней. Банк обеспечивает предоставление Клиенту услуги по дистанционному банковскому обслуживанию в соответствии с Общими условиями, действующими на момент оказания услуги. В случае изменения действующего законодательства Российской Федерации, Общие условия действуют в части, не противоречащей законодательству Российской Федерации.

2.2. Настоящие Общие условия размещаются на сайте Банка в сети Интернет по адресу https://www.denizbank.ru.

2.3. Заключение Договора осуществляется путем направления (подачи) Клиентом в Банк Заявления на предоставление услуг «Клиент-Банк» (iBank 2) АО "Денизбанк Москва" (оферты) по установленной Банком форме и акцепта его Банком в установленном настоящими Общими условиями порядке.

2.4. Термины и определения, используемые в Общих условиях с заглавной буквы, используются в значениях,

2.1. These General Terms and Conditions for the Provision of Services using the Customer-Bank Remote Banking System (hereinafter referred to as the "**General Terms**") regulate the relations arising when the Bank when the Bank provides the Client with a connection to the System and further exchange of ED on it.

The Bank provides remote banking services to the Client in accordance with the General Terms in force at the time of rendering the service. In case of changes in the current legislation of the Russian Federation, the General Terms apply to the extent that they do not contradict the legislation of the Russian Federation.

2.2. These General Terms are posted on the Bank's website on the Internet at https://www.denizbank.ru.

2.3. The conclusion of the Agreement is carried out by sending (submitting) by the Client an Application on rendering Client-Bank services (iBank 2) JSC "Denizbank Moscow" (offer) in the form established by the Bank and its acceptance by the Bank in accordance with the procedure established hereby.

2.4. The terms and definitions used in the General Terms with a capital letter are used in the meanings set out in

установленных в Разделе 1 настоящих Общих условий.
2.5. Банк обязуется передать специальные средства защиты информации и обеспечить безопасный доступ к Системе, а Клиент обязуется принять и использовать их для передачи ЭД в установленном порядке.

Section 1 hereof.
2.5. The Bank undertakes to transfer special means of information protection and secure access to the System, and the Client undertakes to accept and use them for the transfer of ED in accordance with the established procedure.

3. ЗАЩИТА ИНФОРМАЦИИ ПРИ ОБМЕНЕ ЭД / INFORMATION PROTECTION DURING ED EXCHANGE

3.1. Система защиты информации включает:
- использование Ключа ЭП и Ключа проверки ЭП при подписании ЭД;
- систему паролей и иные средства защиты ЭД от несанкционированного просмотра, модификации или уничтожения при возможном перехвате в каналах связи;
- проверку соответствия содержимого ЭД требованиям защиты от несанкционированного доступа;
- плановую замену Ключа ЭП;
- внеплановую замену Ключа ЭП.

3.1. Information protection system hereunder includes:
- use of the ES Key and the ES verification key during ED signing;
- system of passwords and other devices for the ED protection from non-authorized reviewing, modification or elimination in case of possible intercept in communication channels;
- examination of conformity of the ED content to the requirements of protection against a non-authorized access;
- planned change of the ES key;
- extraordinary change of the ES key.

Для защиты информации Банком предоставляются услуги, указанные в Приложении № 1 к Общим условиям, согласно тарифам Банка.
Перечень конкретных услуг по дополнительной защите информации, подлежащих оказанию Банком Клиенту, Клиент указывает в заявлении на предоставление услуг «Клиент-Банк» (iBank 2) АО “Денизбанк Москва”.

For the protection of the information the Bank shall render the services indicated in Annex 1 hereto subject to the Bank’s tariffs.
The list of the services to be rendered by the Bank to the Client, the Client shall indicate in the Application on rendering Client-Bank services (iBank 2) JSC “Denizbank Moscow”.

3.2. Для признания действительности Ключа ЭП и Ключа проверки ЭП Клиента Стороны обязуются выполнить следующие действия:
3.2.1. Банк обязуется передать Клиенту устройства со встроенной системой криптозащиты и инструкции, необходимые для скачивания программного обеспечения для использования Системы;
3.2.2. Клиент обязуется загрузить программное обеспечение согласно полученным от Банка инструкциям и зарегистрировать информацию о Клиенте с указанием Блокировочного слова в Системе;
3.2.3. Клиент обязуется сформировать на Ключевом носителе в Системе Ключ ЭП и распечатать в Системе Сертификат Ключа проверки ЭП в отношении каждого Владелец Сертификата Ключа проверки ЭП;
3.2.4. Уполномоченное лицо Клиента обязуется в присутствии сотрудника Банка подписать распечатанные Сертификаты Ключа проверки ЭП в 2-х экземплярах и представить надлежаще оформленные документы, подтверждающие полномочия Владельца Сертификата Ключа проверки ЭП;
3.2.5. Банк идентифицирует представителя Клиента (заявителя) при его личном присутствии и сравнивает в Системе данные, содержащиеся в предоставленном распечатанном Сертификате Ключа проверки ЭП, с данными идентификатора Ключа проверки ЭП и представлением Ключа проверки ЭП в шестнадцатеричном виде, содержащимися в Системе;
3.2.6. При идентификации представителя Клиента (заявителя) и совпадении данных, указанных в п. 3.2.5. настоящих Общих условий, Ключ ЭП активируется;
3.2.7. После активации Ключа ЭП Банк возвращает один

3.2. In order to admit the validity of the ES key and ES verification key the Parties shall perform the following actions:
3.2.1. the Bank shall transfer to the Client the devices with imbedded cryptographic protection system and instructions for download the soft-ware needed to use the System;
3.2.2. the Client shall download the soft-ware according to the Bank’s instruction and register information about the Client with indication of the Lock word in the System;
3.2.3. the Client shall compose in the System the ES key on the Key carrier and print out in the System the Certificate on the ES verification key regarding each Owner of Certificate on the ES verification key;
3.2.4. The authorized person of the Client undertakes, in the presence of a Bank employee, to sign the printed Certificates of the EP verification key in 2 copies and submit duly executed documents, confirming the powers of the Owner of Certificate on the ES verification key;
3.2.5. the Bank shall identify the Client's representative (applicant) in his personal presence and compare in the System the data contained in the presented hard copy of the Certificate on the ES verification key with the data of the identifier of the ES verification key and expression of the ES verification key at hex contained in the System;
3.2.6. In case of successful identification of the Client's representative (applicant) and of the coincidence of the data indicated in item 3.2.5. hereof the ES key is activated;
3.2.7. Upon the activation of the ES key the Bank shall

экземпляр полученного распечатанного Сертификата Ключа проверки ЭП Клиенту с указанием даты начала и даты окончания действия Сертификата Ключа проверки ЭП.
3.3. Отмена действия Ключа ЭП и соответствующего Сертификата Ключа проверки ЭП может производиться Клиентом в Системе самостоятельно, а также путем передачи письменного заявления Клиента.
В заявлении обязательно должны быть указаны фамилия, имя, отчество Владельца Сертификата Ключа проверки ЭП и идентификатор соответствующего Сертификата Ключа проверки ЭП и дата, с которой соответствующие ключи, сертификаты и подписание ЭД, выполненное с использованием таких ключей и сертификатов, признаются недействительными.
Дата окончания действия ключей и сертификатов не может быть ранее даты отмены Клиентом действия Ключа ЭП в Системе или получения такого заявления Банком (в случае его предоставления).

3.4. Активация нового Ключа ЭП и соответствующего Ключа проверки ЭП выполняется в соответствии с п. 3.2. настоящих Общих условий.
3.5. Стороны признают, что любой ЭД, оформляемый, подписываемый и передаваемый Банком Клиенту с использованием Системы, признается подписанным действительным Ключом ЭП Банка.
3.6. Стороны признают, что используемые ими Система и программно-техническое обеспечение являются достаточными для обеспечения надежной и эффективной работы при обработке, хранении, приеме и передаче ЭД. Система обеспечивает контроль за целостностью переданных ЭД, подлинностью ЭП, шифрованием ЭД и достаточную защиту от несанкционированного доступа, а также обеспечивает идентификацию Владельца Сертификата Ключа проверки ЭП и подтверждение подлинности ЭД.
3.7. Электронный документооборот в рамках Системы осуществляется по сети Интернет. В рамках Системы ЭД Клиента формируются удаленно через сеть Интернет. Используемые в рамках Системы используемые средства криптографической защиты информации применяются для обеспечения конфиденциальности ЭД при его передаче по сети Интернет, а также для обеспечения авторства и целостности ЭД в Системе.

Клиент соглашается, что для получения услуг по Договору используется сеть Интернет, осознавая, что сеть Интернет не является безопасным каналом связи, и соглашается нести все риски, связанные с подключением его рабочего места к сети Интернет, возможным нарушением конфиденциальности и целостности информации при работе через сеть Интернет. Клиент также признает, что выход из строя его рабочего места, используемого для работы в Системе, в результате вмешательства третьих лиц через сеть Интернет, рассматривается как выход из строя по вине Клиента.
Задействованное в работе в Системе программное обеспечение использует только сертифицированные ФСБ России средства защиты информации, отвечает всем требованиям законодательства Российской Федерации и предназначено исключительно для целей, предусмотренных Общими условиями. Внесение

return one original of the received Certificate on the ES verification key to the Client with indication of the date of the validity commencement and the expiry date of the Certificate on the ES verification key.
3.3. The cancellation of the validity of the ES key and the corresponding Certificate on the ES verification key shall be executed by the Client itself in the System or by sending a written application of the Client.
In the application the name, the surname and the patronymic name of the Owner of Certificate on the ES verification key and the identifier of the Certificate on the ES verification key as well as the date from which those keys, the Certificates and ED executed with those keys and certificates are considered invalid shall be obligatory indicated.
The date of the cancellation of the keys and certificates validity must not be earlier than the date of cancellation of the validity of the ES key in the System or the date of receipt of the relevant application by the Bank (if it is provided).
3.4. Activation of a new ES key and the corresponding the ES verification key shall be performed according to the item 3.2 hereof.
3.5. The parties hereby admit that any ED being composed, signed and transferred by the Bank to the Client through the System is considered signed with valid ES key of the Bank.
3.6. The Parties hereby admit that the System, hardware and software to be used are sufficient to provide reliable and effective execution of processing, keeping, acceptance and transmission of ED. The System provides control over integrity of the transmitted ED, authenticity of ES and enciphering of the ED and effective protection against non-authorized access as well as ensures the identification of the Owner of Certificate on the ES verification key and the authenticity of the ED.

3.7. Electronic document management within the System is carried out over the Internet. Within the framework of the Client's ED System, they are generated remotely via the Internet. The cryptographic information protection tools used within the System are used to ensure the confidentiality of the ED when it is transmitted over the Internet, as well as to ensure the authorship and integrity of the ED in the System.

The Client agrees to receive services under the Contract using the Internet, realizing that the Internet is not a secure communication channel, and agrees to bear all risks associated with connecting his workplace to the Internet, possible violation of confidentiality and integrity of information when working via the Internet. The Client also acknowledges that the failure of his workplace used to work in the System, as a result of the intervention of third parties via the Internet, is considered as a failure due to the fault of the Client.

The software involved in the work in the System uses only information security means certified by the FSB of Russia, meets all the requirements of the legislation of the Russian Federation and is intended exclusively for the purposes provided for in the General Terms. Corrections, changes or additions by the Client to the software and technical

Клиентом исправлений, изменений или дополнений в программное обеспечение и техническую документацию, а также передача их третьим лицам не допускается.
3.8. Телефонный звонок в Банк, Клиенту по телефонным номерам, согласованным Сторонами при заключении настоящего Договора, с использованием Блокировочного слова является каналом связи между Клиентом и Банком, по которому Стороны уведомляют друг друга в рамках настоящего Договора при невозможности использования Системы.

documentation provided by the Bank to the Client in accordance with the General Terms, as well as their transfer to third parties are not allowed.
3.8. A telephone call to the Bank or to the Client by telephone numbers agreed upon by the Parties at the conclusion of this Agreement, using a Lock Word is a communication channel between the Client and the Bank, through which the Parties notify each other under this Agreement if it is impossible to use the System.

4. УСЛОВИЯ ОБМЕНА ЭД И ПОРЯДОК ПРОВЕРКИ ЭП / CONDITIONS OF ED EXCHANGE AND ES EXAMINATION PROCEDURE

4.1. ЭД признается документом, равнозначным документу на бумажном носителе, подписанному собственноручными подписями уполномоченных лиц и заверенному печатью, и имеет равную с ним юридическую силу.
ЭКД, полученная по Системе, признается Сторонами копией, равнозначной соответствующей копии документа на бумажном носителе, заверенной собственноручными подписями уполномоченных лиц и печатью, и имеет равную с ней юридическую силу, если иное не будет прямо установлено в ином соглашении Сторон.
4.2. Одной ЭП могут быть подписаны несколько связанных между собой ЭД (включая ЭКД) (далее по тексту – «**Пакет электронных документов**»).
Каждый из ЭД (включая ЭКД), входящий в Пакет электронных документов, считается подписанным (заверенным) ЭП, которой подписан соответствующий Пакет электронных документов.
4.3. Ответственность за идентичность информации, содержащейся в ЭД/ЭКД, информации в соответствующем документе/копии на бумажном носителе, несет Владелец ЭП, подписавший данный ЭД/ЭКД.
4.4. Банк в случае необходимости изготавливает копию полученного ЭД (ЭКД) на бумажном носителе в порядке, позволяющем идентифицировать данную копию с полученным ЭД (ЭКД), и заверяет ее в установленном порядке.
4.5. Любой ЭД, содержащий ЭП одной Стороны и полученный по Системе другой Стороной, считается направленным другой Стороной и подлежит исполнению в соответствии с Договором или иными соглашениями, в соответствии с которыми возможен обмен электронными документами.
4.6. Убытки, которые могут быть причинены вследствие исполнения ЭД, отправленного неуполномоченным лицом с использованием действительной ЭП, покрываются за счет Стороны, с использованием чьей ЭП такой ЭД был направлен.
4.7. При работе с ЭД должна обеспечиваться возможность его воспроизведения на бумажном носителе с сохранением всех реквизитов в соответствии с требованиями действующего законодательства.
4.8. Направленный для исполнения ЭД должен содержать все обязательные реквизиты соответствующего документа в соответствии с требованиями действующего законодательства (включая текстовые реквизиты, в соответствии с которыми совершаются операции по

4.1. The ED is considered the document equal to the document on a paper carrier signed with handwriting signatures of the authorized persons and verified with the seal and has validity equal to the document on a paper carrier.
The ECD received via the System is considered the document equal to the document on a paper carrier signed with handwriting signatures of the authorized persons and verified with the seal and has validity equal to the document on a paper carrier unless otherwise expressly provided in another agreement of the Parties.
4.2. Several ED (including ECD) connected to each other may be signed with one ES (hereinafter referred to as **the** "**Package of electronic documents**").
Each of the EDs (including ECD) included in the Package of electronic documents is considered signed (verified) with ES by which the relevant Package of electronic documents has been signed.
4.3. The ES owner to have signed the ED/ECD is held responsible for the identity of the information in the ED/ECD with the information in the relevant document/copy on a paper carrier.

4.4. If it is necessary, the Bank makes a copy of received ED (ECD) on a paper carrier according to the procedure that allows to identify the copy with received ED (ECD) and verifies the copy in the established order.

4.5. Any ED containing the ES of the Party and received through the System by the other Party is considered transmitted by the other Party and shall be executed according hereto or other agreements, in accordance with which the established procedure for the exchange of electronic documents is possible.
4.6. Losses that might be caused due to performance of the ED, transmitted by unauthorized person but signed with valid ES, shall be covered at the expense of the Party on behalf of which the ED has been transmitted.

4.7. During work with the ED the possibility to reproduce the ED on a paper carrier with all the elements in accordance with the current legislation must be ensured.

4.8. The ED transmitted for the execution must contain all the obligatory elements of the relevant document according to the current legislation (including the text elements in accordance with which the operations on the Account are executed).

Счету).

4.9. Наряду с обязательными реквизитами ЭД может содержать дополнительные реквизиты, состав которых определяется Банком.

4.10. Ответственность за содержание реквизитов ЭД несет Владелец ЭП, подписавший данный ЭД.

4.11. ЭД передается в Банк в виде полноформатного ЭД, обеспечивающего сохранение всех его реквизитов.

4.12. Осуществление операций по Счету Клиента на основании ЭД не сопровождается передачей документов на бумажном носителе.

4.13. ЭД порождает права и обязанности Сторон по Договору, Договору банковского счета или другим соглашениям, в рамках которых происходит взаимодействие с использованием Системы, если передающей Стороной ЭД оформлен надлежащим образом (в соответствии с требованиями законодательства РФ, Общими условиями, Договором банковского счета, другими соглашениями), заверен корректными ЭП в необходимом количестве и передан по системе ДБО, а принимающей Стороной - получен, проверен в соответствии с требуемыми процедурами и принят. Свидетельством того, что ЭД получен, проверен и принят, является квитанция, содержащая положительный результат проверки ЭП передающей Стороны.

4.14. Стороны устанавливают следующий порядок проверки ЭД:

ЭД, полученный от Клиента, проверяется на подлинность ЭП Клиента, количество ЭП Клиента, а также путем осуществления иных процедур контроля, предусмотренных действующим законодательством и Договором.

Процедура проверки подлинности ЭП и количества ЭП Клиента осуществляется Системой в автоматическом режиме с фиксацией в Системе результата проверки путем применения криптографического алгоритма Ключа проверки ЭП.

Достоверность ЭД, подписанного ЭП, считается подтвержденной, если выполнение Банком вышеназванного порядка проверки подлинности ЭП дает положительный результат.

4.15. Причины отказа в приеме ЭД:

а) ЭП идентифицируется как недействительная,

б) при отрицательном результате осуществления процедур контроля;

в) ЭД не соответствует требованиям защиты от несанкционированного доступа;

г) в иных случаях, предусмотренных действующим законодательством.

4.16. Датой отправления ЭД считается дата, в которой Сторона осуществила меры, необходимые для отправки по Системе другой Стороне сформированного ЭД, подписанного ЭП.

Датой приема (неприема) ЭД считается дата, в которой Сторона завершила все меры, необходимые для проверки ЭД, полученного по Системе от другой Стороны.

Прием ЭД подтверждается посредством отражения в Системе соответствующего статуса ЭД с информацией об отправителе и о получателе ЭД.

Отказ в приеме ЭД подтверждается посредством отражения в Системе статуса ЭД "Отвергнут" с

4.9. In addition to the obligatory elements the ED might contain the additional elements to be determined by the Bank.

4.10. The ES owner to have signed the ED is held responsible for the information in the ED.

4.11. The ED shall be transmitted to the Bank as a full-format ED proving keeping of all its details of the information.

4.12. The execution of the operations on the Client’s Account on the grounds of ED is not accompanied with the transfer of the documents on a paper carrier.

4.13. An ED generates the rights and obligations of the Parties under an Agreement, a Bank Account Agreement or other agreements within which interaction with the use of the System takes place, if the transmitting Party has the ED properly executed (in accordance with the RF legislation, General Terms, Bank Account Agreement, other agreements), certified by correct EP in the necessary It was received and transmitted via the DBO system, and received, verified and accepted by the receiving Party. The evidence that the ED has been received, verified and accepted is a receipt containing a positive result of the verification of the transmitting Party's EP.

4.14. The Parties have determined the ED verification procedure as follows:

The ED received from the Client shall be verified for authenticity of ES of the Client, quantity of ES of the Client as well as with execution of other control procedures stipulated in the current legislation and the Agreement.

The procedure of the ES verification and verification of quantity of the ES of the Client shall be executed automatically with recording of the result of the verification in the System with use of a cryptographic algorithm of the ES verification key.

The authenticity of the ED signed with the ES is considered verified if the execution by the Bank of the set ES verification procedure shows the positive result.

4.15. The reasons for refusal to accept the ED:

a) the ES is identified as invalid;

b) if the control procedure shows the negative result;

c) the ED does not comply with the requirements on the protection against a non-authorized access;

d) in other cases stipulated in the current legislation.

4.16. The date of ED transmitting means a date during which a party has executed measures to transfer a formed ED signed with the ES via the System to the other party.

The date of accepting (non-accepting) of the ED means a date during which a party has completed execution of all the measures on verification of the ED received via the System from the other party.

The accepting of the ED shall be confirmed by means of showing the status of the ED with information about a sender and a recipient in the System.

The refusal to accept the ED shall be confirmed by means of showing the status of the ED “Rejected” in the System

указанием причины отказа.
4.17. При положительном результате проверки ЭД такой ЭД исполняется в срок, предусмотренный соответствующим соглашением, для целей исполнения которого ЭД направлялся по Системе.
4.18. Банк блокирует работу Клиента в Системе в следующих случаях:
4.18.1. указанном в п. 8.3. настоящих Общих условий;
4.18.2. в случаях необходимости осуществления плановой или внеплановой замены Ключей ЭП до проведения соответствующей замены Ключей ЭП;
4.18.3. в случаях, установленных в разделе 7 настоящих Общих условий;
4.18.4. в иных случаях, установленных Договором.
4.19. Банк уведомляет Клиента о совершении операции посредством отражения в Системе соответствующего статуса ЭД с информацией об исполнении ЭД. Моментом получения Клиентом такого уведомления считается время, указанное для соответствующего статуса ЭД в истории ЭД в Системе.

with indication of the reason for the refusal.
4.17. Upon the positive result of the ED verification, that ED shall be executed within the term stipulated in the relevant agreement, for the purposes of which the ED was sent through the System.
4.18. The Bank shall suspend the activity of the Client in the System in the following cases:
4.18.1. indicated in item 8.3. hereof;
4.18.2. necessity of execution of the Planned change of the ES Key or Extraordinary change of the ES Key until the execution of the relevant change of the ES Key;
4.18.3. in the cases specified in Section 7 hereof;
4.18.4. in other cases stipulated by the Agreement.

4.19. The Bank shall notify the Client of the transaction by means of showing the status of the ED in the System with information on the execution of the ED. The time when the Client receives such notification is considered the time indicated for the corresponding status of ED in the history of ED in the System.

5. ХРАНЕНИЕ И УНИЧТОЖЕНИЕ ЭД / KEEPING AND ELIMINATION OF ED

5.1. Клиент, составивший ЭД, и Банк, его получивший, обязаны обеспечить его хранение в течение срока, установленного действующим законодательством.
5.2. Архивы ЭД ведутся в Банке и у Клиента в разрезе всех входящих и исходящих ЭД.

Архив Сертификатов Ключа проверки ЭП ведется в Банке. Архивы ведутся в течение сроков хранения, установленных для документов на бумажных носителях.

Правила ведения указанных архивов регулируются действующим законодательством, включая нормативные акты Банка России и Договором.
5.3. ЭД и их бумажные копии, практическая необходимость в которых отпала и установленные сроки хранения которых истекли, могут быть уничтожены.
5.4. Уничтожение ЭД производится в отношении соответствующих программных данных с одновременным уничтожением копий этих ЭД на бумажных носителях.

5.1. The Client to have formed the ED and the Bank to have received it shall secure the ED storage within the term stipulated by the current legislation.
5.2. Archives of the ED shall be kept by the Bank and by the Client from the point of view of all incoming and outgoing ED.
Archive of Certificates on the ES verification key shall be kept by the Bank. The archives shall be kept in accordance with the term for keeping prescribed for the documents on paper carriers.
The procedure of keeping of the above-mentioned archives is regulated by the current legislation including the regulative acts of the Bank of Russia and hereby.
5.3. The ED and their copies on paper which are not necessary any longer and keeping periods of which have expired, can be destroyed.
5.4. The destruction of the ED shall be made simultaneously with elimination of the correspondent copies of the ED on paper carriers.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН / RIGHTS AND OBLIGATIONS OF THE PARTIES

6.1. Стороны обязаны:
6.1.1. Уведомлять друг друга о фактах возникновения проблем при отправке ЭД в день его отправки.
6.1.2. При проведении обмена ЭД руководствоваться действующим законодательством и Договором.
6.1.3. За свой счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для работы Системы в соответствии с Договором.
6.1.4. Оградить Систему от несанкционированного доступа третьих лиц.
6.1.5. Сохранять в тайне используемую систему защиты информации.
6.1.6. Предоставлять по письменному запросу другой Стороны надлежащим образом оформленные бумажные

6.1. The Parties are obliged:
6.1.1. To inform each other about the occurrence of problems when sending ED on the date of sending.
6.1.2. When conducting an ED exchange, follow the current legislation and the Contract.
6.1.3. To keep in working condition their hardware and software being used during the process of the ED exchange in accordance herewith at their own expense.
6.1.4. To prevent an unauthorized access of the third parties to the System.
6.1.5. To keep secret the System on information protection being used.
6.1.6. To provide to the other Party at its written request the copies of the ED (ECD) on paper carries duly drawn.

копии ЭД (ЭКД).

6.2. Стороны имеют право:
6.2.1. Запрашивать надлежаще оформленные на бумажном носителе копии ЭД.
6.2.2. В любое время заменить свои Ключи ЭП в соответствии с порядком, установленным настоящими Общими условиями.
6.2.3. Передавать по Системе другой Стороне любую информацию, в том числе не относящуюся к расчетным операциям (документы валютного контроля, уведомления и т.д.).

6.3. Банк обязан:
6.3.1. Уведомить Клиента о приостановлении работы Системы дольше чем на 1 рабочий день не позднее чем за 3 (Три) рабочих дня, а также консультировать Клиента по вопросам работы с Системой.
6.3.2. В порядке, предусмотренном заключенным с Банком договором банковского счета, осуществлять проведение операций по Счету Клиента на основании ЭД, поступивших от последнего по Системе.
6.3.3. Информировать Клиента о совершении операций с использованием Системы в порядке, установленном в п. 4.19 настоящих Общих условий.

6.4. Банк имеет право:
6.4.1. Оформлять копии ЭД Клиента на бумажном носителе и заверять их собственноручными подписями уполномоченных лиц и печатью Банка в соответствии с требованиями внутренних документов Банка.
6.4.2. Отказать Клиенту в приеме от него ЭД по Системе с указанием причины отказа. В случае такого отказа Клиент вправе представить в Банк надлежащим образом оформленный документ на бумажном носителе, который исполняется Банком в соответствии с заключенным с Банком договором банковского счета и действующим законодательством.
6.4.3. Не принимать к исполнению ЭД Клиента, если они подписаны некорректными ЭП или подписаны ЭП, сформированными с использованием скомпрометированных ЭП, после получения Банком уведомления о компрометации ключа ЭП в порядке, предусмотренном Условиями.
6.4.4. Приостанавливать исполнение ЭД в случаях, предусмотренных законодательством и настоящим Договором, в т.ч. в случае непредставления Клиентом запрошенных Банком документов, вплоть до их представления.
6.4.5. Приостанавливать функционирование системы в рабочие дни для планового обслуживания Системы, с уведомлением Клиента за 24 часа о планируемом обслуживании.
6.4.6. В одностороннем порядке отказаться от исполнения Договора в случае отсутствия Клиента по указанному им адресу (месту нахождения), а также в случае нарушения Клиентом условий Договора и/или настоящих Общих условий.
6.4.7. В одностороннем внесудебном порядке изменять:
- настоящие Общие условия;
- тарифы;
- порядок обслуживания Клиента, включая график работы Банка.

6.2. The Parties are entitled:
6.2.1. To ask for presentation of the duly drawn copies of the ED on paper carries.
6.2.2. To change its ES Keys according to the procedure determined hereby at any time.

6.2.3. To transmit through the System to the other Party any information including that not related to the settlement operations (documents on currency control, notifications and so on).

6.3. The Bank is obliged:
6.3.1. To inform the Client about the suspension of the System more than 1 business day no later than 3 (three) business days prior such suspension as well as to consult the Client about the operation of the System.
6.3.2. According to the procedure stipulated in the bank account agreement concluded with the Bank to execute operations on the Client’s account on the grounds of the ED received from the Client via the System.
6.3.3. To inform the Client about transactions using the System in the manner specified in item 4.19 hereof.

6.4. The Bank is entitled:
6.4.1. To make the paper copies of the Client’s ED and verify them with handwriting signatures of the authorized persons of the Bank and the Bank’s seal in accordance with the requirements of internal documents of the Bank.
6.4.2. To refuse the Client in receiving an ED from the Client through the System with indication of a reason of the refusal. In case of the refusal the Client is entitled to present to the Bank document duly drawn up on a paper carrier that shall be executed by the bank in accordance with the bank account agreement concluded with the Bank and the current legislation.
6.4.3. Not to accept the Client's ED for execution if they are signed by incorrect ES or signed by ES formed using compromised ES, after the Bank receives notification of the compromise of the ES key in accordance with the procedure provided for herein the.

6.4.4. To suspend execution of the ED in cases stipulated by the legislation and hereby including the case of a failure to provide the Bank with the requested documents until presentation thereof.

6.4.5. To suspend operation of the System during business days for routine maintenance of the System, with notification to the Client with a 24 hours prior notice before the planned suspension.
6.4.6. To terminate this Agreement unilaterally in the event of the absence of the Client at the address indicated by it (place of registration) as well in the event of violation by the Client of the Agreement and/or hereof.

6.4.7. Unilaterally change out of court:
- these General Terms;
- tariffs;
- the order of customer service, including the work schedule and operating time of the Bank.

Информация об изменениях Общих условий, тарифов, порядка обслуживания Клиента, включая график работы Банка, доводится до сведения Клиента не менее чем за 5 (пять) календарных дней до даты вступления в силу указанных изменений путем размещения соответствующей информации на сайте Банка в сети Интернет по адресу https://www.denizbank.ru.

6.4.8. Приостановить использование Клиентом Системы в случае нарушения Клиентом своей обязанности по предоставлению Банку достоверной информации для связи с ним (обновленной информации в случае ее изменения) в соответствии с п.6.5.10 настоящих Общих условий, а также в иных случаях, установленных законом и Договором.

6.4.9. По заявлению Клиента устанавливать ограничения по параметрам операций, которые могут осуществляться Клиентом с использованием Системы, перечень которых указан в Приложении № 1 к настоящим Общим условиям.

6.4.10. Осуществлять иные права в соответствии с действующим законодательством и Договором.

6.5. Клиент обязан:

6.5.1. В течение 30 (Тридцати) календарных дней с даты заключения Договора настроить и ввести в эксплуатацию программно-технические средства, необходимые для работы Системы, и выполнить обязательства, указанные в п. 3.2.4. настоящих Общих условий.

В случае, если в течение срока, указанного в настоящем пункте, Клиент не выполнит обязательства, указанные в п. 3.2.4. настоящих Общих условий, сформированные в Системе неактивированные Ключи ЭП Клиента из Системы будут удалены.

6.5.2. Не допускать использование Ключей ЭП третьими лицами, не являющимися Владельцем Сертификата Ключа проверки ЭП, и обеспечить сохранность и нераспространение Ключей ЭП и Ключевых носителей.

В случае Компрометации Ключа ЭП или подозрения на Компрометацию Ключа ЭП, утраты доступа к Системе и (или) ее использования (подозрений об использовании) без согласия Клиента, а также повреждения программно-технических средств, на которых установлена Система, включая средства обработки, хранения и защиты информации, Клиент обязан прекратить использование Ключей ЭП, обесточить компьютер, на котором установлена Система, и незамедлительно проинформировать об этом Банк с использованием Блокировочного слова по телефону и (или) электронным письмом с предоставлением письменного подтверждения не позднее следующего рабочего дня со дня получения такой информации.

При этом Банк блокирует Систему до проведения замены ключей ЭП.

6.5.3. Осуществлять замену Ключей ЭП в случаях и по процедуре, установленных настоящими Общими условиями, в противном случае любые убытки, возникшие вследствие невыполнения замены, должны погашаться за счет Клиента.

6.5.4. Контролировать правильность оформления направляемых ЭД.

6.5.5. Применять при проведении обмена ЭД систему обработки, хранения и защиты информации и телекоммуникации только на исправном и проверенном на отсутствие компьютерных вирусов персональном

Information on changes in General Terms, tariffs, customer service procedures, including the Bank's work schedule, is brought to the attention of the Customer at least 5 (five) business days before the date of entry into force of these changes by posting relevant information on the Bank's website on the Internet at https://www.denizbank.ru.

6.4.8. To suspend the use by the Client of the System in case the Client violates his obligation to provide the Bank with reliable information to contact him (updated information in case of change) in accordance with clause 6.5.10 hereof as well as in other cases established by law and the Agreement.

6.4.9. To establish restrictions on the parameters of operations that can be carried out by the Client using the System, the list of which is indicated in Appendix No. 1 hereto, according to the request of the Client.

6.4.10. To effect other rights in accordance with the current legislation and the Agreement.

6.5. The Client is obliged:

6.5.1. To install and put into operation the hardware and software necessary for the operation of the System within 30 (thirty) calendar days from the date of conclusion the Agreement and perform the obligations indicated in item 3.2.4. hereof.

If within the term stipulated in this paragraph the Client has failed to perform the obligation indicated in item 3.2.4. hereof, the Client's ES Keys formed in the System but not activated shall be deleted from the System.

6.5.2. To prevent using ES Keys by the third parties which are not the Owner of Certificate on the ES verification key hereunder and provide storage and non-spreading of the ES Keys and Key carrier.

The Client is obliged to suspend the use of the ES Keys, to disconnect from energy the computer on which the System is installed and immediately inform the Bank with use of the Lock word on phone and (or) e-mail about any case of the Compromise of the ES Key or suspicions of Compromising the ES Key, loss of access to the System and (or) its use (suspicion of use) without the Client's consent, as well as a damage of hardware and software on which the System is installed including the devices for processing, keeping and protection of the information with presentation of the written confirmation not later than the following business day after receiving the information.

The Bank shall suspend the operation of the System until the ES Keys change.

6.5.3. To make the change of the ES Key and the Extraordinary change of the ES Key in cases and in accordance with the procedure set out herein, otherwise any losses arisen from a failure to fulfill such change shall be covered at the Client's expense.

6.5.4. To control the correctness of drawing up the obligatory elements of the ED being transmitted.

6.5.5. To use the systems of processing, storage and protection of the information and the telecommunications during the exchange of the ED only on the personal computer examined for the computer viruses.

компьютере.

Применять антивирусные программы на устройствах, на которых используется Система, и обновлять их. Список антивирусных программ, подлежащих обязательной установке на компьютере Клиента, постоянно обновляется Банком и публикуется на сайте Банка.

To apply anti-virus programs on devices that use the System and update them. The list of the antivirus programs to be obligatory installed on the Client's personal computer shall be constantly updated by the Bank and published on the Bank's web-site.

6.5.6. При получении уведомления от Банка об изменении программного обеспечения Системы принимать меры для своевременного получения и установки новых версий Системы.

6.5.6. Upon receipt of the Bank's notice about the changes in the System's software to undertake measures for the timely receipt and installation of the new versions of the System.

6.5.7. Не допускать тиражирование и передачу третьей стороне программно-технического обеспечения, предоставляемого Клиенту Банком для проведения обмена ЭД.

6.5.7. To prevent copying and assigning to the third parties the hardware and software provided by the Bank to the Client for the ED exchange execution.

6.5.8. Предоставлять представителям Банка допуск в помещение, где размещаются программно-технические средства, на которых установлена Система, для проведения проверок соблюдения Клиентом условий настоящих Общих условий.

6.5.8. To ensure the admission for the Bank's representatives into the premises in which the hardware with the installed System is located for execution of the examination of the observance by the Client of the terms and conditions hereof.

6.5.9. При прекращении действия Договора уничтожить все принадлежащие ему конфиденциальные данные и все программное обеспечение (исполняемые и вспомогательные файлы) Системы, относящиеся к Договору, и не передавать их третьим лицам.

6.5.9. To destroy all the disposed confidential information, software (executed and subsidiary files) of the System related to the Agreement and abstain from assigning them to any third parties upon the termination of the Agreement.

6.5.10. Предоставить Банку достоверную информацию для связи с ним, а в случае ее изменения своевременно предоставить обновленную информацию.

6.5.10. To provide the Bank with reliable information to contact him, and in case of change, provide timely information in a timely manner.

6.5.11. Регулярно (не реже одного раза в 3 (три) рабочих дня) проверять Систему на предмет получения от Банка информационных сообщений (информации), в том числе касающихся изменений в порядке работы и взаимодействия Сторон, внесения изменения в указанные в п. 6.4.7 настоящих Общих условий документы и другой информации, ознакамливаться с направленной информацией и принимать ее во внимание и/или в работу.

6.5.11. Regularly (at least once every 3 (three) business days) check the System for receiving information messages from the Bank, including those concerning changes in the working procedure and interaction of the Parties, in the documents specified in clause 6.4.7 of these General Terms and others, get acquainted with the information sent and take it into account and/or work.

По истечении 3 (трех) рабочих дней с момента направления по Системе информации Клиент считается ознакомленным и согласным с ней (включая изменения, о которых информация сообщает) и принимает на себя риск последствий, связанных с неознакомлением с направленной информацией.

After 3 (three) working days from the date of sending the information through the System, the Client is considered to be familiar with and agrees with it (including the changes reported by the information) and assumes the risk of consequences associated with not knowing the information sent.

6.4.12. Исполнять иные обязательства, установленные настоящим Договором.

6.4.12. To fulfill other obligations established by this Agreement.

7. ДЕЙСТВИЯ СТОРОН В СЛУЧАЕ ВЫЯВЛЕНИЯ ОПЕРАЦИИ, СООТВЕТСТВУЮЩЕЙ ПРИЗНАКАМ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА / ACTIONS OF THE PARTIES IN CASE OF IDENTIFICATION OF AN OPERATION CORRESPONDING TO THE SIGNS OF A MONEY TRANSFER WITHOUT THE CONSENT OF THE CLIENT

7.1. Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, обязан:

7.1. If the Bank identifies a transaction that corresponds to the characteristics of money transfer without a Client's consent, the Bank shall be obliged to:

7.1.1. до осуществления списания денежных средств с банковского счета Клиента на срок не более двух рабочих дней приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента. Признаки осуществления перевода денежных средств без согласия Клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети

7.1.1. suspend the execution of the order on execution of the operation corresponding to the signs of money transfer without a client's consent for a period of not more than two business days prior to the debiting of funds from the bank account of the Client. Signs of money transfer without a client's consent are established by the Bank of Russia and placed on its official website in the information and telecommunication network "Internet";

"Интернет";
7.1.2. приостановить использование Клиентом Системы.
7.2. Незамедлительно после приостановления исполнения распоряжения о переводе денежных средств Банк обязан позвонить Клиенту по телефону, указанному Клиентом в качестве контактного по Договору, и при использовании Клиентом Блокировочного слова:
7.2.1. предоставить Клиенту информацию:
а) о приостановлении Банком исполнения распоряжения Клиента о совершении операции по переводу денежных средств, которое, по мнению Банка, соответствует признакам осуществления перевода денежных средств без согласия Клиента;
б) о рекомендациях Банка по снижению рисков повторного осуществления перевода денежных средств без согласия Клиента;
7.2.2. незамедлительно запросить у Клиента подтверждение возобновления исполнения распоряжения.
7.3. При получении от Клиента подтверждения, указанного в подпункте 7.2.2 настоящих Общих условий, Банк обязуется:
7.3.1. незамедлительно возобновить исполнение распоряжения;
7.3.2. незамедлительно возобновить доступ Клиента к Системе.
При неполучении от Клиента подтверждения, указанного в подпункте 7.2.2 настоящих Общих условий, Банк возобновляет исполнение распоряжения, а также возобновляет использование Клиентом Системы по истечении двух рабочих дней после дня совершения им действий, указанных в пунктах 7.1 и 7.2 настоящих Общих условий.
7.4. В случае утраты Системы, при компрометации ключа ЭП или при подозрении на компрометацию ключа ЭП и (или) использования Системы без согласия Клиента Клиент обязан направить соответствующее уведомление Банку путем телефонного звонка с использованием Блокировочного слова незамедлительно после обнаружения факта утраты Системы, при компрометации ключа ЭП или при подозрении на компрометацию ключа ЭП и (или) использования Системы без согласия Клиента, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции, направленного в порядке, установленном настоящими Общими условиями.
7.5. При получении от Клиента уведомления, указанного в пункте 7.4 настоящих Общих условий, после осуществления списания денежных средств с банковского счета Клиента Банк обязан незамедлительно направить оператору по переводу денежных средств, обслуживающему получателя средств, уведомление о приостановлении зачисления денежных средств на банковский счет получателя средств (далее - уведомление о приостановлении) по форме и в порядке, которые установлены нормативным актом Банка России.
7.6. В случае получения от Банка уведомления о приостановлении до осуществления зачисления денежных средств на банковский счет получателя средств оператор по переводу денежных средств, обслуживающий получателя средств, обязан приостановить на срок до пяти рабочих дней со дня получения такого уведомления зачисление денежных

7.1.2. suspend the Client's use of the System.
7.2. Immediately after the suspension of execution of the order for the transfer of funds, the Bank is obliged to call the Client at the phone number specified by the Client as a contact under the Agreement and when the Client uses the Lock word:
7.2.1. provide information to the Client about:
a) suspending the Bank's execution of the Client's order on a transaction for transfer of funds, which, in the opinion of the Bank, corresponds to the characteristics of money transfer without a client's consent;
b) recommendations of the Bank to reduce the risks of re-execution of money transfers without the Client's consent;
7.2.2. immediately request the Client to confirm the resumption of execution of the order.
7.3. Upon receipt of confirmation from the Client specified in sub-paragraph 7.2.2 hereof, the Bank shall:
7.3.1. immediately resume execution of the order;
7.3.2. immediately resume the use of the System by the Client.
In case of failure to receive confirmation from the Client specified in sub-paragraph 7.2.2 hereof, the Bank shall resume the execution of the order, as well as resume the use of the System by the Client after two business days after the date of the actions specified in items 7.1 and 7.2 hereof.
7.4. In case of loss of the System, in case of compromise of the ES Key or in case of suspicion of compromise of the ES Key and (or) use of the System without the Client's consent, the Client is obliged to send a corresponding notification to the Bank by phone call using the Lock word immediately after the fact of loss of the System, in case of compromise of the ES Key or in case of suspicion of the compromise of the ES Key and (or) use of the System without the Client's consent, but not later than one day, following the day of receipt from the Bank of the notification on the made operation directed in the order established hereby.
7.5. Upon receipt from the Client of the notification specified in item 7.4 hereof, after the funds have been debited from the Client's bank account, the Bank shall immediately send to the money transfer operator servicing the funds recipient a notification on the suspension of the funds transfer to the bank account of the funds recipient (further - the suspension notification) in the form and in the manner prescribed by the regulatory act of the Bank of Russia.
7.6. In case of receipt from the Bank of the notification on suspension before transfer of money to the bank account of the recipient of means the operator on transfer of money servicing the recipient of means is obliged to suspend for a period of up to five business days from the date of receipt of such notification transfer of money to the bank account of the recipient in the amount of transfer of money and

средств на банковский счет получателя средств в сумме перевода денежных средств и незамедлительно уведомить получателя средств в порядке, установленном договором, заключенным с получателем средств, о приостановлении зачисления денежных средств и необходимости представления в пределах указанного срока документов, подтверждающих обоснованность получения переведенных денежных средств.

7.7. В случае представления в течение пяти рабочих дней со дня совершения оператором по переводу денежных средств, обслуживающим получателя средств, действий, предусмотренных пунктом 7.6 настоящих Общих условий, получателем средств документов, подтверждающих обоснованность получения переведенных денежных средств, оператор по переводу денежных средств, обслуживающий получателя средств, обязан осуществить зачисление денежных средств на банковский счет получателя средств.

7.8. В случае непредставления в течение пяти рабочих дней со дня совершения оператором по переводу денежных средств, обслуживающим получателя средств, документов, подтверждающих обоснованность получения переведенных денежных средств, оператор по переводу денежных средств, обслуживающий получателя средств, обязан осуществить возврат денежных средств Банку не позднее двух рабочих дней после истечения указанного пятидневного срока. Банк обязан осуществить зачисление денежных средств на банковский счет Клиента не позднее двух дней со дня их получения.

7.9. В случае получения от Банка уведомления о приостановлении после осуществления зачисления денежных средств на банковский счет получателя средств оператор по переводу денежных средств, обслуживающий получателя средств, обязан направить Банку уведомление о невозможности приостановления зачисления денежных средств на банковский счет получателя средств по форме и в порядке, которые установлены нормативным актом Банка России. Банк не несет ответственности перед Клиентом за убытки, возникшие в результате надлежащего исполнения обязательств, установленных пунктами 7.6 – 7.8 настоящих Общих условий.

7.10. Банк настоящим уведомляет Клиента, что в случае, когда Клиент будет выступать получателем денежных средств, а Банк, соответственно, будет выступать банком получателя средств, к правоотношениям Сторон будут применены положения пунктов 7.5 – 7.9 настоящих Общих условий.

immediately notify the recipient of means in the order established by the agreement concluded with the recipient of funds about suspension of transfer of money and need of submission within the specified term of the documents confirming validity of receipt of the transferred money.

7.7. In the case of submission within five business days from the date of the transfer of funds by the operator serving the recipient of funds, the actions provided for in item 7.6 hereof, the recipient of the funds of the documents confirming the validity of the receipt of the transferred funds, the operator of the transfer of funds serving the recipient is obliged to transfer the funds to the bank account of the recipient.

7.8. In case of failure to submit within five business days from the date of the money transfer operator, serving the recipient of funds, documents confirming the validity of the receipt of the transferred funds, the money transfer operator, serving the recipient of funds, is obliged to make a refund to the Bank no later than two business days after the expiration of the specified five-day period. The Bank is obliged to transfer funds to the Client's bank account not later than two days from the date of their receipt.

7.9. In case of receipt from the Bank of the notification on suspension after implementation of transfer of money to the Bank account of the recipient of means the operator on transfer of money serving the recipient of means is obliged to send to the Bank the notification on impossibility of suspension of transfer of money to the bank account of the recipient of means in the form and in the order which are established by the regulatory act of Bank of Russia. The Bank shall not be liable to the Client for losses arising as a result of the proper performance of the obligations set out in items 7.6 – 7.8 hereof.

7.10. The Bank hereby notifies the Client that in the event that the Client will be the recipient of funds and the Bank, respectively, will be the recipient's bank, the provisions of items 7.5 – 7.9 hereof will be applied to the legal relations of the Parties.

8. ВОЗНАГРАЖДЕНИЕ И ПОРЯДОК ЕГО УПЛАТЫ / FEE AND PROCEDURE OF THE FEE PAYMENT

8.1. Оплата подключения Клиента к Системе, консультации его сотрудников, установки системы телекоммуникаций, систем обработки, хранения и защиты информации, оплата иных услуг, оказываемых Банком, осуществляется Клиентом в размере и сроки, установленные тарифами Банка и Договором.

8.2. Банк осуществляет подключение Клиента к Системе, а также подключение соответствующих услуг на следующий рабочий день после оплаты Клиентом услуг Банка за текущий месяц.

8.1. The payment for connection of the Client to the System, for consultation to its employees, for installation of the telecommunication system, system of processing, storage and protection of the information, the payment for the other services being rendered by the Bank hereunder shall be effected by the Client in the amount and within the term stipulated by the Bank's tariffs and the Agreement.

8.2. The Bank shall connect the Client to the System on the following business day after the payment by the Client of the Bank's services for the current month.

8.3. Клиент обязан обеспечить необходимый остаток денежных средств на своих счетах в Банке, доступных для списания Банком, не позднее последнего рабочего дня текущего месяца для взимания Банком платы за оказываемые услуги в следующем месяце.
В случае невыполнения Клиентом обязательства, указанного в настоящем пункте в установленный срок, Банк приостанавливает прием платежных ЭД Клиента в Системе до момента поступления полной оплаты на счет Банка.
Если период неоплаты составляет более 2 (двух) месяцев подряд, Договор прекращает свое действие.
8.4. Клиент настоящим уполномочивает Банк списывать с любых своих счетов, открытых в Банке, без его распоряжения денежные средства в оплату услуг, оказываемых по настоящему Договору, в размере и сроки, определенные тарифами Банка и Договором.

8.3. The Client shall ensure the balance on its accounts with the Bank not later than the last business day of the current month for the payment of the fee to the Bank for the Bank's services hereunder to be rendered within the next month.
If the Client fails to perform its obligation indicated in the present paragraph at maturity, the Bank shall suspend acceptance of the Client payment ED in the System until the moment of crediting the funds in full to the Bank's account.
If the period of non-payment is longer than 2 months in a row, the Agreement will become ineffective.
8.4. The Client hereby authorizes the Bank to charge from the Client's accounts without the Client's order the funds to pay for the services being rendered hereunder (under the Agreement) in the amount and within the term determined by the Bank's tariffs and by the Agreement.

9. ОТВЕТСТВЕННОСТЬ СТОРОН / LIABILITY OF THE PARTIES

9.1. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств по Договору в случае возникновения обстоятельств непреодолимой силы (форс – мажор).
Освобождение Клиента от ответственности в случае отключения электроэнергии, повреждения линий связи, аварии и других явлений, в результате которых связь между Банком и Клиентом была нарушена, может иметь место только в том случае, если он использовал все возможности доставить платежные документы в Банк с курьером на бумажных носителях.
9.2. Каждая Сторона несет ответственность за содержание, в том числе достоверность, любого ЭД, подписанного его ЭП.
9.3. Банк не несет ответственности за неисполнение или ненадлежащее исполнение своих обязанностей по Договору, если в Системе произошел сбой вследствие неисправности персонального компьютера Клиента (включая компьютерный вирус) или неисправности каналов связи, предоставленных третьими лицами.
Банк не несет ответственности за последствия исполнения распоряжений, выданных неуполномоченными лицами, а также в тех случаях, когда с использованием предусмотренных банковскими правилами и Договором процедур Банк не мог установить факта выдачи распоряжения (направления ЭД) неуполномоченными лицами.
9.4. Сторона, несвоевременно сообщившая о случае Компрометации Ключа ЭП, несет связанные с этим убытки.
9.5. В случае возникновения ущерба Сторона, не исполнившая (ненадлежащим образом исполнившая) обязательства по Договору, несет ответственность перед другой Стороной за возникшие убытки. При отсутствии доказательств неисполнения (ненадлежащего исполнения) Сторонами обязательств по настоящему Договору, риск убытков несет Сторона, подписавшая ЭП ЭД, исполнение которого повлекло за собой убытки.
9.6. Банк не несет ответственность в случаях финансовых потерь, понесенных Клиентом в связи с нарушением и (или) ненадлежащим исполнением им требований по

9.1. The Parties shall not bear any responsibility for failure to fulfil their liabilities or improper fulfilment their liabilities hereunder, if such a failure has been caused by force-majeure circumstances.
In the event of power disconnection, damage of communication channel, damages and other accidents due to which connection between the Bank and the Client has been broken, the Client can be released from the responsibility only if the Client has done its best to present the payment documents on a paper carrier to the Bank with a messenger.
9.2. Each party is responsible for the content including authenticity of any ED signed with its ES

9.3. The Bank is not liable for failure to fulfil their liabilities or improper fulfilment their liabilities hereunder if a lineout in the operation of the System has arisen due to the Client's personal computer trouble (including an infection with a computer virus) or faultiness of the communications channels provided by the third parties.
The Bank is not liable for the consequences of the execution of the orders issued by non-authorized persons as well as in case when the Bank is not able to determine the fact of issuance of the order by non-authorized persons using the procedures stipulated by the Bank's rules and by the Agreement.

9.4. The Party to have untimely informed about the case of the Compromise of the ES Key is liable for the losses arisen due to that fact.
9.5. In case of occurrence of any damage the Party to have failed to perform (not properly performed) its obligations under the Agreement is liable towards the other Party for the losses. If the evidence about the failure of the performance (not proper performance) of the Parties hereto is absent, the risk on the losses is borne by the Party that signed with the ES that ED the execution of which entailed the losses.
9.6. The Bank shall not be liable in cases of financial losses incurred by the Client in connection with violation and (or) improper fulfillment by him of requirements for

защите от вредоносного кода (вируса) клиентских устройств, где используется Система, а также за компрометацию аутентификационной и идентификационной информации, используемой Клиентом для доступа к Системе, произошедшую не по вине Банка.

protection against malicious code (virus) of client devices where the System is used, as well as for the compromise of authentication and identification information used by the Client to access to the System that occurred through no fault of the Bank.

10. ПОРЯДОК РАЗРЕШЕНИЯ РАЗНОГЛАСИЙ ПРИ ОБМЕНЕ ЭД / DISPUTE SETTLEMENT PROCEDURE DURING THE ED EXCHANGE

10.1. В случае возникновения разногласий при обмене ЭД по Договору, Сторона обязуется направить другой Стороне соответствующую претензию в письменной форме.

10.1. In the event of arising disputes during the ED exchange hereunder the Party shall send to the other Party the relevant claim in written form.

10.2. Получив претензию, другая Сторона обязуется в течение 10 (Десяти) рабочих дней с даты получения претензии проинформировать в письменной форме Сторону, направившую претензию, о результатах ее рассмотрения.

10.2. Having received the claim, the other Party shall inform the Party which sent the claim about the result of consideration of the claim within 10 (ten) business days from the date of the receipt of the claim.

10.3. Сторона, направившая претензию, в течение 10 (Десяти) рабочих дней после получения письменного ответа на претензию от другой Стороны, должна рассмотреть представленные объяснения и письменно уведомить другую Сторону об отказе от претензии или о несогласии с результатами ее рассмотрения.

В случае неполучения другой Стороной в течение указанного срока уведомления об отказе от претензии или о несогласии с результатами ее рассмотрения, претензия считается снятой, а спор – урегулированным.

10.3. The Party to have sent the claim within 10 (ten) business days from the date of the receipt of the written reply to the claim from the other Party shall consider the received explanations and notify the other Party about the waiver of the claim or disagreement on the result of its consideration.

If the other Party haven't received notice about the waiver of the claim or about the disagreement on the result of its consideration within the stipulated term, the claim is considered is withdrawn and the dispute is settled.

10.4. Если Сторона, направившая претензию, не согласна с результатами ее рассмотрения, Стороны обязаны в течение 5 (Пяти) рабочих дней с даты получения другой Стороной уведомления о несогласии с результатами рассмотрения претензии сформировать экспертную комиссию для рассмотрения спора (далее по тексту – «Комиссия»).

10.4. If the Party to have sent the claim doesn't agree to the result of the consideration of the claim, the Parties shall form expert committee for the dispute consideration (hereinafter referred to as the "Committee") within 5 (five) business days from the date of the receipt by the other Party the notice of disagreement on the result of consideration of the claim written reply to the claim.

10.5. Комиссия создается из уполномоченных представителей Сторон в составе 5 (Пяти) членов. В Комиссию входят 3 представителя Банка и 2 представителя Клиента.

10.5. The Committee shall be formed consisting of authorized representatives of the Parties and composed of 5 (five) members. The Committee includes 3 representatives of the Bank and 2 representatives of the Client.

10.6. В случае уклонения одной из Сторон от участия в работе Комиссии, другая Сторона вправе самостоятельно привлечь экспертов, указанных в п. 10.8. настоящих Общих условий, для рассмотрения спора с обязательным предварительным уведомлением об этом другой Стороны.

10.6. In case of evasion by one of the Parties from participation in the Committee work the other Party is entitled to involve the experts indicated in item 10.8. hereof for consideration of the dispute with obligatory prior notification about that to the other Party.

10.7. Техническая экспертиза спорного ЭД осуществляется Комиссией в помещении Клиента, где находится компьютер Клиента, с IP адреса которого был подписан спорный ЭД, если Банком не рекомендуется иное.

10.7. Technical examination of the arguable ED shall be executed by the Committee in the Client's premises where the Client's computer with IP address from which the arguable ED was signed is located, if the Bank doesn't recommend otherwise.

10.8. Стороны вправе привлекать к работе Комиссии согласованных экспертов в области защиты информации. Стороны согласны с тем, что в качестве экспертов, могут привлекаться следующие организации:

10.8. The Parties are entitled to involve to the Committee work agreed experts on information protection. The Parties have agreed that the following expert companies might be involved:

- разработчик Системы;
- разработчик средств криптографической защиты информации (СКЗИ);
- Центр Федеральной службы безопасности по лицензированию, сертификации и защите государственной тайны;
- сотрудники Федерального агентства

- vendor of the System;
- vendor of cryptographic information protection facilities (CIPF);
- the Center of the Federal security service on licensing, certification and official secret protection;
- employees of the Federal Agency for Government Communications and Information;

правительственной связи и информации;
• иные сертифицированные эксперты в области средств криптографической защиты информации.
Стороны согласны с тем, что оплачивать услуги привлеченных экспертов в области защиты информации должна Сторона, предъявившая претензию.
10.9. Комиссия обязуется приступить к работе не позднее рабочего дня, следующего за днем ее формирования.
10.10. Член Комиссии со стороны Банка в присутствии остальных членов Комиссии снимает образ диска с компьютера, с IP адреса которого был подписан спорный ЭД.
10.11. Член Комиссии со стороны Банка в присутствии остальных членов Комиссии проверяет, что на компьютере, с IP адреса которого был подписан спорный ЭД, не нарушена целостность программного обеспечения (в результате сбоев аппаратуры, воздействия компьютерных вирусов, в том числе полученных через Интернет). Для анализа наличия компьютерных вирусов используется антивирусное программное обеспечение, рекомендуемое Банком, позволяющее произвести проверку на вирусы без загрузки операционной системы компьютера Клиента.
10.12. В случае, если целостность программного обеспечения на компьютере, с IP адреса которого был подписан спорный ЭД, не нарушена, то действия, указанные в п. 10.14 – 10.18 настоящих Общих условий, выполняются на компьютере, с IP адреса которого был подписан спорный ЭД.
10.13. В случае, если целостность программного обеспечения на компьютере, с IP адреса которого был подписан спорный ЭД, нарушена, то действия, указанные в п. 10.14 – 10.18. настоящих Общих условий выполняются на другом компьютере, предоставленном Клиентом.
В случае, предусмотренном в настоящем пункте, член Комиссии со стороны Банка в присутствии остальных членов Комиссии устанавливает программное обеспечение Системы на другом компьютере, предоставленном Клиентом (свободном от вирусов и программных закладок), используя для этого стандартную процедуру установки для подтверждения работоспособности Системы.
10.14. Член Комиссии со стороны Банка в присутствии остальных членов Комиссии с использованием установленного программного обеспечения Системы распечатывает спорный ЭД с идентификаторами ЭП на бумажном носителе.
10.15. Член Комиссии со стороны Банка в присутствии остальных членов Комиссии с помощью установленного программного обеспечения Системы распечатывает действующие на момент подписания спорного ЭД Сертификаты Ключей проверки ЭП, используя Ключевые носители Клиента.
10.16. Члены Комиссии сравнивают распечатанные Сертификаты ключей проверки ЭП с соответствующими подписанными экземплярами Сертификатов ключей проверки ЭП, ранее переданными Клиентом Банку согласно п. 3.2.4 настоящих Общих условий.
Члены Комиссии проверяют:
- срок действия подписанных Сертификатов Ключа проверки ЭП;
- совпадение в распечатанных Сертификатах Ключей

• other certified experts on cryptographic information protection facilities.

The Parties have agreed that the service to be rendered by the involved experts shall be paid by the Party which presented the claim.
10.9. The Committee shall start to work not later the business day following the day of its forming.
10.10. The member of the Committee on the Bank's side in the presence of the other members of the Committee shall copy a disk image of the computer with IP address from which the arguable ED was signed.
10.11. The member of the Committee on the Bank's side in the presence of the other members of the Committee shall check that the software integrity of the computer with IP address from which the arguable ED was signed has not been disrupted (due the failures of the equipment, an impact of computer viruses, including those obtained via the Internet).
For the analysis of the computer antivirus presence the software, recommended by the Bank, shall be used which allows to execute a virus scan without downloading the Client's computer operating system.
10.12. If the software integrity of the computer with IP address from which the arguable ED was signed has not been disrupted, the actions indicated in items 10.14 – 10.18 hereof shall be executed on the computer with IP address from which the arguable ED was signed.

10.13. If the software integrity of the computer with IP address from which the arguable ED was signed has been disrupted, the actions indicated in items 10.14 – 10.18 hereof shall be executed on another computer provided by the Client.

In the case stipulated in this paragraph the member of the Committee on the Bank's side in the presence of the other members of the Committee shall install the software on the other computer provided by the Client (free from viruses and program bookmarks) using the standard installation procedure for confirmation of the operation of the System.

10.14. The member of the Committee on the Bank's side in the presence of the other members of the Committee shall print out the arguable ED with identifier on a paper carrier using the software installed.

10.15. The member of the Committee on the Bank's side in the presence of the other members of the Committee shall print out the Certificate on the ES verification key that was valid at the moment of the signing the arguable ED using the Key carriers of the Client.

10.16. The members of the Committee shall compare the printed out Certificates on the ES verification key with the corresponding signed originals of the Certificate on the ES verification key given to the Bank earlier according to item 3.2.4 here.
The members of the Committee examine:
- the validity of the signed originals of the Certificates on the ES verification key;
- coincidence of the expression of the ES verification key

проверки ЭП и соответствующих подписанных Сертификатах Ключей проверки ЭП данных представления Ключа проверки ЭП в шестнадцатеричном виде и данных идентификатора Ключа проверки ЭП.
10.17. Члены Комиссии проверяют совпадение данных идентификатора Ключа проверки ЭП спорного ЭД, распечатанного из Системы, с идентификатором Ключа проверки ЭП, содержащимся в распечатанном Сертификате Ключа проверки ЭП.
10.18. По решению Комиссии компьютер, с IP адреса которого был подписан спорный ЭД, опечатывается Комиссией с целью невозможности дальнейшего подключения к нему внешних устройств, невозможности включения питания компьютера и исключения возможности доступа к жесткому диску компьютера.
10.19. Претензия Клиента считается снятой, а спор урегулированным в пользу Банка, если:
10.19.1. Клиент отказывается формировать Комиссию для осуществления технической экспертизы;
10.19.2. члены Комиссии со стороны Клиента отказываются осуществлять техническую экспертизу согласно процедуре, изложенной в п. 10.7 – 10.18 настоящего раздела.
10.19.3. по результатам проведенной технической экспертизы установлено, что на момент подписания спорного ЭД Ключ проверки ЭП был действителен; данные представления Ключа проверки ЭП в шестнадцатеричном виде и данные идентификатора Ключа проверки ЭП в распечатанных Сертификатах Ключей проверки ЭП и подписанных Сертификатах Ключей проверки ЭП совпали.
10.20. Спор считается урегулированным в пользу Клиента, если по результатам проведенной технической экспертизы установлено, что на момент подписания спорного ЭД срок действия Ключа проверки ЭП истек и/или данные представления Ключа проверки ЭП в шестнадцатеричном виде и данные идентификатора Ключа проверки ЭП в распечатанных Сертификатах Ключей проверки ЭП и подписанных Сертификатах Ключа проверки ЭП не совпали.
10.21. Все действия, предпринимаемые Комиссией для выяснения спорной ситуации, а также выводы, сделанные Комиссией, заносятся в Протокол Комиссии.
Протокол Комиссии должен содержать следующие данные:
- дату и место составления Протокола;
- время начала и окончания работы Комиссии;
- состав Комиссии;
- краткое изложение обстоятельств возникшей спорной ситуации;
- подробное описание мероприятий, осуществляемых Комиссией для установления причин и последствий возникшей спорной ситуации;
- выводы, к которым пришла Комиссия в результате проведенных мероприятий;
- о наличии (отсутствии) особого мнения членов Комиссии;
- подписи всех членов Комиссии.

В случае, если вывод члена Комиссии не совпадает с выводом других членов Комиссии, указанный член Комиссии обязуется изложить особое мнение письменно, которое подписывается соответствующим членом Комиссии и прикладывается к Протоколу.

at hex and the data of the identifier of the ES verification key in the printed out Certificates on the ES verification key with the ones in the corresponding signed Certificates on the ES verification key.
10.17. The members of the Committee examine coincidence of the data of the identifier of the ES verification key of the arguable ED with the identifier of the ES verification key in the printed out Certificates on the ES verification key.
10.18. By the decision of the Commission the computer with IP address from which the arguable ED was signed shall be sealed in order to prevent any possibility to connect any external devices to it, to switch it on and to eliminate any possibility of the access to the hard drive of the computer.
10.19. The claim is considered withdrawn and the dispute is solved in favour of the Bank, if:
10.19.1. The Client refuses to form the Committee for the technical examination execution;
10.19.2. the Committee members on the Client's side refuse to execute the technical examination procedure according to the items 10.7 – 10.18 hereof;

10.19.3. on the results of the technical expertise it has been determined that during the signing of the arguable ED the ES verification key was valid; the expression of the ES verification key at hex and the data of the identifier of the ES verification key in the printed out Certificates on the ES verification key match with the ones in the corresponding signed Certificates on the ES verification key.

10.20. The dispute is considered solved in favour of the Client, if on the results of the technical expertise it has been determined that during the signing of the arguable ED the ES verification key was invalid or/and the expression of the ES verification key at hex and the data of the identifier of the ES verification key in the Certificates on the ES verification key printed out don't match with the ones in the corresponding signed Certificates on the ES verification key.
10.21. All the actions taken by the Committee for the dispute clarification as well as the conclusions made by the Committee shall be recorded in the Committee Minutes.
The Committee Minutes shall contain the following information:
- date and place of the Minutes composition;
- time of the commencement and completion of the work by the Committee;
- composition of the Committee;
- brief description of the dispute;
- detailed description of the actions carried out by the Committee to establish the reasons and consequences of the dispute arose;
- conclusions made by the Committee as a result of the executed actions;
- existence (absence) of the special opinion of the Committee members;
- signatures of all Committee members.

If the opinion of a Committee member doesn't match with the opinions of the other Committee members that Committee member shall write his/her special opinion which to be signed by the Committee member and attached to the Minutes.

10.22. Протокол Комиссии составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу, один экземпляр для Банка, другой – для Клиента.
10.23. Протокол Комиссии является окончательным и пересмотру не подлежит. Выводы Комиссии являются обязательными для Сторон.
Протокол Комиссии является основанием для предъявления претензий к лицам, виновным в возникновении спорной ситуации.
Протокол Комиссии является доказательством при дальнейшем разбирательстве спора в суде.

10.22. The Committee Munities shall be made on a paper carrier in two copies being of the same force, one copy - for the Bank, the other copy – for the Client.
10.23. The Committee Munities is final and is not the subject to any appeal. The Committee conclusions are obligatory for the Parties.
The Committee Munities shall be the ground for presentation of the claims to the persons by whose fault the dispute has arisen.
The Committee Munities shall be a prove during the further litigation in court.

11. ПРОЧИЕ ПОЛОЖЕНИЯ / MISCELLANEOUS

11.1. Договор вступает в силу в момент акцепта Банком направленного Клиентом в соответствии с п.2.3 настоящих Общих условий Заявления на предоставление услуг «Клиент-Банк» (iBank 2) АО “Денизбанк Москва” и прекращает свое действие в установленных законом или Договором порядке.
Любая Сторона может отказаться от исполнения Договора с письменным уведомлением об этом другой Стороны за 15 (Пятнадцать) календарных дней до желаемой даты его прекращения, а также в других случаях, предусмотренных Договором.
В случае прекращения действия Договора Банк отключает Клиента от Системы (за исключением случаев, когда отношения сторон сохраняют силу на основании иного соглашения сторон, регулирующего использование системы «Клиент-Банк»).
11.2. Изменения в настоящие Общие условия и Тарифы вносятся в порядке, установленном в п.6.4.7 Общих условий.
11.3. Если какое-либо из положений настоящих Общих условий или Договора становится недействительным, другие положения настоящих Общих условий/Договора остаются в силе.
11.4. Банк и Клиент настоящим подтверждают, что Банком ведется запись телефонных переговоров с Клиентом, и запись указанных разговоров будет иметь юридическую силу и будет использована в качестве доказательства в суде при разрешении споров.
11.5. К настоящим Общим условиям прилагаются и являются их неотъемлемой частью следующие приложения:
11.5.1. Перечень услуг, оказываемых для защиты информации (Приложение № 1);
11.5.2. Памятка Клиенту о мерах информационной безопасности при обмене ЭД (Приложение № 2).

11.1. The Agreement comes into force at the moment of acceptance by the Bank of the Application for the provision of services "Client-Bank" (iBank 2) of JSC "Denizbank Moscow" sent by the Client in accordance with clause 2.3 of these General Terms and terminates in accordance with the procedure established by law or the Agreement.
This Agreement may be terminated by any Party with 15 (fifteen) calendar days prior notice to the other Party about its intention to terminate it as well as in the other cases stipulated in the Agreement.
In case of the Agreement termination the Bank shall disconnect the Client from the System (except for the cases in which the relations of the parties remain in force under another agreement between the parties to be concluded to regulate the “Client-Bank” system use).
11.2. Changes to the General Terms and Tariffs are made in accordance with the procedure established in clause 6.4.7 hereof
11.3. If any provision hereof or of the Agreement is null and void, the other provisions hereof/ of the Agreement shall be considered valid.

11.4. The Bank and the Client hereby confirm that the Bank keeps a record of telephone conversations with the Client and the recording of such conversations will have legal force and will be used as evidence in court in resolving disputes.
11.5. The following annexes are attached hereto and are integral part hereof:
11.5.1. The list of the services to be rendered for the information protection (Annex 1);
11.5.2. Informational letter to the Client about measures on informational security during the ED exchange (Annex 2).

Приложение/Annex №1.

Перечень услуг, оказываемых для защиты информации / The list of the services to be rendered for the information protection

Перечень услуг, оказываемых для защиты информации	**The list of the services to be rendered for the information protection**
1. Определения, используемые в настоящем Приложении:	1. Definitions being used herein:
1.1. Услуга по защите ЭП – защищенное хранение и неизвлекаемость (невозможность считывания) секретного ключа ЭП с использованием ключевого носителя – USB-токена.	1.1. Service on digital signature protection means protected storage and anti-handling (impossibility to read) of confidential key of digital signature with application of the Key carrier – USB-token device.
1.2. Услуга по дополнительной защите с использованием устройств по защите ЭП (MAC-токен, OTP-токен и т.п.) – двухфакторная аутентификация клиента и дополнительное подтверждение платежных поручений на сумму, превышающую указанную Клиентом, одноразовыми паролями с использованием устройства – токена.	1.2. Service on additional protection with use of devices for the protection of ES (MAC token, OTP token, etc.) means a two-factor authentication of the Client and additional confirmation of payment orders for amount increasing that indicated by the Client, by one-time passwords with application of token device.
1.3. Услуга по дополнительной защите с использованием SMS и/или push-уведомлений – двухфакторная аутентификация Клиента и дополнительное подтверждение платежных поручений на сумму, превышающую указанную Клиентом, одноразовыми паролями с использованием SMS или push-уведомлений, полученных из специального мобильного приложения.	1.3. Service on additional protection with SMS and/or push notifications use means a two-factor authentication of the Client and additional confirmation of payment orders for amount increasing that indicated by the Client, by one-time passwords with use of SMS or push notifications received from the special mobile application.
1.4. Услуга по информированию об операциях по счету с использованием SMS и e-mail – дополнительное информирование Клиента об операциях по счету и работе Системы.	1.4. Service on informing about operations on account with use of SMS or e-mail means additional informing the Client about operations on account and work of the System.
1.5. Услуга по IP-фильтрации адресов – установленные в Системе ограничения на заданные Клиентом IP адреса, с которых возможен доступ в Систему, и/или на географическое местоположение устройств, с использованием которых может осуществляться подготовка и (или) подтверждение Клиентом электронных сообщений.	1.5. Service on IP-filtration of addresses – restrictions on IP addresses specified by the Client from which access to the System is possible and/or on geographical location of devices set in the System that can be used for preparing and (or) confirming electronic messages by the Client.
1.6. Услуга установления лимита по операциям – установление максимальной суммы перевода денежных средств за одну операцию и (или) за определенный в Системе период времени (лимит на день, месяц, др.) – возможность установления лимита, при превышении которого Система откажет в осуществлении перевода.	1.6. Service for setting transfer limits – setting the maximum amount of money transfer by one operation and (or) by a period of time stipulated by the System (limit per day, month, etc), if exceeded, the System will refuse to make the transfer.
1.7. Услуга ограничения по перечню предоставляемых услуг, связанных с осуществлением переводов денежных средств – ограничение по набору прав Клиента на работу с типами документов.	1.7. Service of limit for all services related to the implementation of money transfers – limitation in the rights of the Client to work with document types.
2. В Системе используется ЭП, соответствующая признакам, установленным законом для усиленной неквалифицированной ЭП с использованием Сертификата Ключа проверки ЭП, выдаваемого удостоверяющим центром корпоративной информационной системы.	2. ES being used in the System meets the requirements set for the reinforced non-qualified electronic signature with use of the certificate of the verification key of an electronic signature issued by certificatory center of corporate informational system
3. Защита информации осуществляется путем: • предоставления Услуги по защите ЭП и Услуги по дополнительной защите с использованием устройств по защите ЭП или • предоставления Услуги по защите ЭП и Услуги по дополнительной защите с использованием SMS и/или push-уведомлений; • предоставления Услуги по информированию об операциях по счету с использованием SMS или e-mail;	3. The protection of the information is executed by means of: • rendering Service on digital signature protection and Service on additional protection with use of devices for the protection of ES or • rendering Service on digital signature protection and Service on additional protection with SMS use; • rendering Service on informing about operations on account with use of SMS or e-mail;

• предоставления Услуги по IP-фильтрации адресов; • предоставления Услуги установления лимита по операциям; • предоставления Услуги ограничения по перечню предоставляемых услуг, связанных с осуществлением переводов денежных средств. Банк оказывает соответствующие услуги на основании Заявления Клиента.	• providing a Service on IP-filtration of addresses; • providing a Service of setting transfer limits; • provision a Service of restrictions on the list of services provided related to the implementation of money transfers. The Bank renders the relevant services according to the Client's application.

Приложение/Annex №2.

Памятка Клиенту о мерах информационной безопасности при обмене ЭД / Informational letter to the Client about measures on informational security during the ED exchange

1. Меры, необходимые для обеспечения безопасности электронных подписей:	***1. Measures necessary to ensure information security of electronic signatures:***
1.1. На компьютере, с которого производится работа, должно быть установлено только лицензионное программное обеспечение. Установленное программное обеспечение (система «Клиент-Банк», операционная система, web-браузер) должно регулярно обновляться.	1.1 On the computer that is used for work, the licensed software only shall be installed. The installed software ("Client-Bank" system, operational system, web browser) shall be updated regularly.
1.2. Должна быть установлена система антивирусной защиты, рекомендуемая Банком, с регулярными обновлениями.	1.2 Anti-virus protection system recommended by the Bank shall be installed. Anti-virus protection system shall be updated on regular basis.
1.3. Для подписания электронного документа рекомендуется использовать две подписи.	1.3. Two signatures shall be used for signature of the electronic document.
1.4. Доступ в систему «Клиент-Банк» должен быть разделен между двумя разными компьютерами: на одном из них должен осуществляться ввод электронного документа в систему «Клиент-Банк», а на другом - подписание электронного документа и его отправка.	1.4. The access to "Client-Bank" system shall be separated between two different computers: entering of the electronic document shall be executed with the first one; signing and transmission of the electronic document shall be executed with the second one.
1.5. Все загружаемые из Интернета файлы и программы должны проверяться на наличие вирусов.	1.5. All files and the programs to be loaded from the Internet shall be checked on the presence of the viruses.
1.6. Рекомендуется использовать программные средства блокировки сетевых атак (персональный/корпоративный сетевой экран).	1.6. It is recommended to use the software tools for block network attacks (the personal/corporate network firewall).
1.7. Запрещается использовать съемные носители и компакт диски, кроме ключевых носителей.	1.7. It is forbidden to use removable carriers and CD's except for the key carriers.
1.8. Рекомендуется использовать специальное программное обеспечение, контролирующее использование съемных носителей.	1.8. It is recommended to use special software to control the use of removable carriers.
1.9. Запрещается использовать ключевые носители на иных компьютерах, за исключением компьютера Клиента, предназначенного для работы с системой «Клиент-Банк». Запрещается работать в системе «Клиент-Банк» с общедоступных компьютеров, например, из интернет-кафе.	1.9. It is forbidden to use the key carrier on the other computers, except for the Client's computer destined for work with "Client-Bank" system. It is forbidden to work with "Client-Bank" system from the computers available to all, for example, at an Internet-cafe.
1.10. Пользователь ключа электронной подписи должен осуществлять вход в систему «Клиент-Банк» только с помощью собственного ключевого носителя. Во время работы ключевой носитель подключается к компьютеру, после работы в системе «Клиент-Банк» необходимо закрыть программу, отключить ключевой носитель от компьютера и убрать его в сейф или в запираемый шкаф.	1.10. The electronic signature key user shall login to "Client-Bank" system only with his/her own key carrier. During work the key carrier to be connected to the computer, after completion of work with "Client-Bank" system the program shall be closed, the key carrier shall be disconnected from the computer and put into a safe or in a locked case.
1.11. Запрещается оставлять ключевые носители подключенными к компьютеру, если работа в системе «Клиент-Банк» завершена.	1.11. It is forbidden to leave the key carriers connected to the computer if work in "Client-Bank" system has been completed.

1.12. Следует исключить доступ неуполномоченных лиц к ключевым носителям и иным устройствам системы «Клиент-Банк», включая устройства по дополнительной защите ЭП. Не разрешается оставлять ключевые носители и иные устройства системы «Клиент-Банк» лежащими на рабочем месте во время отсутствия пользователя ключа электронной подписи.	1.12. It is necessary to exclude any access of unauthorized persons to the key carriers and other devices of «Client-Bank» system, including devices for additional protection of ES. It is not allowed to leave the key carriers and other devices of “Client-Bank” system on a workplace during the absence of electronic signature key user.
1.13. Для работы системы «Клиент-Банк» должна быть предусмотрена отдельная учетная запись для каждого пользователя операционной системы компьютера с ограничением прав пользователя.	1.13. For work with “Client-Bank” system a separate registration account for each user of the computer operational system with restriction of the rights of the user shall be created.
1.14. Следует исключить доступ лиц, не уполномоченных работать с системой «Клиент-Банк», к компьютеру, на котором установлена система «Клиент-Банк».	1.14. It is necessary to exclude any access of unauthorized persons to work with "Client-Bank" system, to the computer on which “Client-Bank” system is installed.
1.15. Запрещается доступ к внешним Интернет ресурсам (сайтам), непосредственно не связанным с работой системы «Клиент-Банк», с компьютера, на котором установлена система «Клиент-Банк».	1.15. It is forbidden to use the computer on which “Client-Bank” system is installed for any access to the external Internet resources (sites) which are not connected directly with work of “Client-Bank” system.
1.16. Запрещается устанавливать программы из недостоверных источников, открывать файлы от неизвестных отправителей и пр.	1.16. It is forbidden to setup programs from doubtful sources, to open files from unknown senders and so forth.
1.17. Запрещается передавать ключи электронной подписи сотрудникам Банка под каким бы то ни было предлогом.	1.17. It is forbidden to transfer the confidential electronic signature keys to employees of the Bank, under any pretext.
1.18. Запрещается использовать ключевой носитель в случае Компрометации ключа электронной подписи. В случае Компрометации ключа электронной подписи Клиент обязан обесточить компьютер, на котором установлена Система, и незамедлительно уведомить об этом Банк с указанием Блокировочного слова электронным письмом по адресу: support.ru@denizbank.com и (или) телефону 8 (495) 725-10-20 доб. 194 и произвести Внеплановую замену ключей электронной подписи.	1.18. It is forbidden to use the key carrier in case of the Compromise of electronic signature key. In case of the Compromise of electronic signature key the Client shall disconnect the computer on which the System is installed from electric power and notify immediately the Bank with providing the Lock word by e-mail: support.ru@denizbank.com and (or) on phone 8 (495) 725-10-20 ext. 194 and make the Extraordinary change of electronic signature keys.
1.19. Обстоятельства, которые могут свидетельствовать о Компрометации ключа электронной подписи: • утеря Ключевого носителя с последующим обнаружением или без; • обнаружение факта несанкционированного доступа к Ключевому носителю; • нарушение правил хранения и использования Ключевого носителя; • обнаружение вредоносного программного обеспечения на компьютере, на котором установлена система «Клиент-Банк» или на ином компьютере, входящим с ним в локальную сеть; • обнаружение нарушения целостности топологии локальной сети клиента (временное или постоянное); • обнаружение попыток сетевых атак на компьютер, на котором установлена система «Клиент-Банк» или иной компьютер, входящий с ним в локальную сеть; • невозможность входа в систему «Клиент-Банк» при наличии Интернет соединения; • невозможность входа в систему «Клиент-Банк» в	1.19. Circumstances which can testify about the Compromise of electronic signature key: • loss of the key carrier with the subsequent detection or without; • detection of unauthorized access to the key carrier; • infringement of the rules on storage and use of the Key carrier; • detection of the virus software on the computer on which “Client-Bank” system is installed or on another computer connected with it to the local network; • detection of any infringement of the integrity topology in the local network of the Client (temporary or constant); • detection of network attacks attempts to the computer on which “Client-Bank” system is installed or another computer connected with it to the local network; • impossibility to login in "Client-Bank" system if the Internet connection is available;

результате неавторизованной смены пароля ключевого носителя; • нестабильное функционирование компьютера, на котором установлена система «Клиент-Банк» (медленная работа, произвольная перезагрузка и др.) или его выход из строя; • появление на экране сообщений с требованием ввода кодов, паролей, не предусмотренных функциональными свойствами системы «Клиент-Банк»; • DDoS-атака на ИТ- инфраструктуру Клиента; • несоответствие порядковых номеров платежных поручений; • в целях работы в системе «Клиент-Банк» переход по ссылкам, не принадлежащим официальному сайту Банка или порталу iBank2.RU (www.ibank2.ru); • иные обстоятельства.	• impossibility to login in "Client-bank" system due to unauthorized change of the Key carrier password; • unstable operating of the computer on which “Client-Bank” system is installed (slow work, unauthorized restart, etc.) or its failure; • occurrence on the screen of the messages with requirements to enter codes, passwords which are not stipulated by the functional properties of "Client-Bank" system; • DDoS-atack to IT infrastructure of the Client; • discrepancy of outgoing numbers of payment orders; • with a view to work in "Client-Bank" system transition under the references which are not belong to the official site of the Bank or to the iBank2.RU (www.ibank2.ru) portal; • the other circumstances.
1.20. Необходимо немедленно заменить/аннулировать ключи электронной цифровой подписи в случаях их компрометации или подозрения на компрометацию, а также во всех случаях увольнения или смены лиц, допущенных к этим ключам, а также руководителей Клиента, которые подписывали решения (доверенности) о допуске пользователей к ключам электронной цифровой подписи.	1.20. It is necessary to immediately replace/cancel the electronic digital signature keys in cases of their compromise or suspicion of compromise, as well as in all cases of dismissal or change of persons admitted to these keys, as well as the Client's managers who signed decisions (powers of attorney) on the admission of users to the electronic digital signature keys.
2. Риски, связанные с использованием электронных подписей: Следование вышеизложенным правилам полностью является ответственностью Клиента. Если при расследовании спорной ситуации будет установлено, что спорная ситуация возникла вследствие их нарушения Клиентом и/или Компрометации ключа электронной подписи, ответственность за возникновение спорной ситуации и соответствующий ущерб возлагается на Клиента.	***2. Risks related to use of electronic signatures:*** The observance of the rules set out above is the responsibility of the Client. If during the investigation of a dispute it is established that the dispute arose due an infringement of the rules by the Client and (or) the Compromise of electronic signature key, the Client shall be liable for occurrence of the incident and the damage related to it.