Утверждены Правлением
ООО РНКО «РИБ»
Протокол №6
от 09 июня 2017 г

УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ООО РНКО «РИБ»

г. Москва

Оглавление

ВВЕДЕНИЕ

Условия предоставления услуг дистанционного банковского обслуживания ООО РНКО «РИБ» (далее Условия обслуживания) – внутренний документ ООО РНКО «РИБ», определяющий условия оказания услуг дистанционного банковского обслуживания, порядок взаимодействия между Клиентами и ООО РНКО «РИБ», описывающий правила информационной безопасности при использовании системы, процедуры доказательства подлинности электронного платежного документа, риски использования системы, а также устанавливающий общие принципы осуществления Электронного документооборота между сторонами при проведении операций по счетам и исполнении других обязательств в соответствии с заключенным (заключенными) между сторонами договором банковского счета и иными соглашениями. Условия опубликованы на сайте www.ribank.ru.

ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Если явно не оговорено иное, термины и определения, используемые в настоящем документе, имеют следующее значение:

Счета, Счет – банковские счета (банковский счет) в Российских рублях и/или в иностранной валюте, открытые (открытый) Клиенту в Банке в соответствии с действующим законодательством Российской Федерации и заключенными (заключенным) между Клиентом и Банком договорами (договором).

Договор (Договоры) банковского счета – заключенный (заключенные) между Банком и Клиентом договоры, на основании которых Банк открыл Клиенту Счет (Счета) и осуществляет расчетно-кассовое обслуживание Клиента.

Уполномоченное лицо Клиента – указанное в карточке с образцами подписей и оттиска печати (Клиента физическое лицо, имеющее право распоряжаться денежными средствами, находящимися на Счете (Счетах), с использованием электронной цифровой подписи. **Договор о ДБО** –Договор о дистанционном банковском обслуживании между Банком и Клиентом, состоящий из

Условий предоставления услуг дистанционного банковского обслуживания ООО РНКО «РИБ» и Заявления о присоединении к Условиям .

Система дистанционного банковского обслуживания (далее – Система) – корпоративная информационная система «Faktura», представляющая собой совокупность программного, информационного и аппаратного обеспечения, включая программный комплекс, состоящий из средств формирования, обработки, хранения, передачи электронных документов и средств электронной цифровой подписи, реализующая электронный документооборот между Клиентом и Банком в соответствии с настоящим Договором.

Удостоверяющий центр – Закрытое акционерное общество «Центр Цифровых Сертификатов» (ИНН 5407187087; ОГРН 1025403189602) (http://www.besafe.ru), осуществляющее следующие функции:

- создает ключи электронных цифровых подписей и удостоверяет сертификаты ключей подписи и шифрования для персонального и корпоративного пользования;
- приостанавливает и возобновляет действие сертификатов ключей подписи (шифрования), а также аннулирует их;
- ведет реестр сертификатов ключей подписи (шифрования), обеспечивает его актуальность и возможность доступа к нему участников информационных систем;
- выдает сертификаты ключей подписи в электронной форме и (или) в форме документов на бумажных носителях с информацией об их действии;
- осуществляет проверку на уникальность идентификатора владельца сертификата ключа подписи (шифрования) в реестре сертификатов ключей подписи (шифрования);
- осуществление по обращениям пользователей сертификатов ключей подписей подтверждения подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

Оператор Системы – Межбанковский процессинговый центр Faktura.ru (http://www.faktura.ru), являющийся участником Системы, созданный Закрытым акционерным обществом «Биллинговый центр» (ИНН 5401152049; ОГРН 1025400512400) в целях информационного и технологического обслуживания Системы.

Банк – ООО РНКО «РИБ», осуществляющий все или часть функций Удостоверяющего центра на основании заключенного с ним Договора о ДБО.

Электронный документ (далее - ЭД) – документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись (далее - ЭЦП) – реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в ЭД.

Средства ЭЦП – программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание ЭЦП в ЭД с использованием закрытого ключа ЭЦП, подтверждение подлинности ЭЦП в ЭД с использованием открытого ключа ЭЦП, создание закрытых и открытых ключей ЭЦП.

Закрытый ключ ЭЦП – уникальная последовательность символов, известная владельцу сертификата ключа ЭЦП и предназначенная для создания в ЭД ЭЦП с использованием Средств ЭЦП.

Открытый ключ ЭЦП – уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная Сторонам и предназначенная для подтверждения подлинности ЭЦП в ЭД с использованием Средств ЭЦП.

Сертификат ключа ЭЦП – документ на бумажном носителе или ЭД с ЭЦП Банка, которые включают в себя открытый ключ ЭЦП и которые выдаются Банком Клиенту для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа ЭЦП. **Владелец сертификата ключа ЭЦП** – уполномоченное Клиентом физическое лицо, наделенное правом распоряжения находящимися на Счете Клиента денежными средствами с использованием ЭЦП, на имя которого Банком зарегистрирован Сертификат ключа ЭЦП и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью Средств ЭЦП создавать свою ЭЦП в ЭД (подписывать ЭД).

Электронный документооборот – обмен ЭД между Сторонами в Системе в соответствии с настоящим Договором.

Электронное распоряжение на совершение переводов (далее – ЭПД) – ЭД, подписанный необходимым количеством ЭЦП представителей Клиента, уполномоченных распоряжаться находящимися на Счете Клиента денежными средствами с правом первой или второй подписи, и являющийся основанием для совершения операций по Счетам Клиента.

Электронный служебно-информационный документ (ЭСИД) – ЭД, не являющий платежным документом (выписки по счету, запросы, отчеты, информационный сообщения и т.п.).

Согласованный канал связи – сеть Интернет.

Подтверждение подлинности электронной цифровой подписи в электронном документе (проверка ЭЦП документа) –

положительный результат проверки соответствующими программными Средствами ЭЦП принадлежности ЭЦП в ЭД владельцу Сертификата ключа ЭЦП и отсутствия искажений в ЭД, подписанном данной ЭЦП.

Носитель ключевой информации – физический носитель информации определенной структуры, предназначенный для размещения на нем ключевой информации.

Автоматизированное рабочее место (АРМ) Клиента/Банка – аппаратно-программный комплекс, в состав которого входит программное обеспечение, предназначенное для:

- создания ЭД, подписания их ЭЦП, шифрования и передачи с АРМ Клиента на АРМ Банка и с АРМ Банка на АРМ Клиента;
- приёма и расшифровывания ЭД, проверки корректности ЭЦП, обработки информации из принятых ЭД;
- создания ключей ЭЦП и запросов на сертификаты открытых ключей ЭЦП;
- обработки и хранения сертификатов открытых ключей ЭЦП.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

Компрометация ключа ЭЦП – событие, в результате которого возможно несанкционированное использование неуполномоченными лицами закрытого ключа ЭЦП (в том числе несанкционированное списание или попытка списания денежных средств со счета Клиента). К таким событиям относятся, включая, но не ограничиваясь, следующие:

- утрата или порча Носителя ключевой информации;
- утрата носителя ключевой информации с последующим обнаружением;
- утрата ключей от сейфа (в том числе с последующим обнаружением) в момент нахождения в нем Носителя ключевой информации;
- временный доступ посторонних лиц к Носителям ключевой информации либо подозрение, что такой доступ имел место;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа ЭЦП;
- случаи, когда нельзя достоверно установить, что произошло с носителями электронных ключей, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к носителям ключевой информации посторонних лиц.

Прочие термины и сокращения, используемые в настоящем документе, соответствуют законодательству Российской Федерации, нормативным актам Банка России, а также заключенным между Сторонами Договорам банковских счетов.

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Дистанционное банковское обслуживание с использованием системы Клиент-Банк (Интернет-банкинг) (далее – Системы) предоставляется Клиентам Банка, с которыми заключен Договор банковского счета и (или) договор текущего валютного счета.

1.2. Настоящие Условия регламентируют порядок и условия предоставления услуги дистанционного банковского обслуживания Клиентов с использованием Системы.

1.3. Обслуживание Клиентов в Системе осуществляется Банком на основании Договора о ДБО, состоящего из настоящих Условий и Заявления о присоединении к Условиям.

1.4. Клиент присоединяется к условиям в соответствии со ст. 428 Гражданского кодекса Российской Федерации путем подписания Заявления о присоединении к Условиям.

1.5. Для обмена электронными документами (далее ЭД) Стороны используют собственные технические средства, телекоммуникационное оборудование и арендованные или принадлежащие Сторонам на ином основании каналы связи.

1.6. Обмен электронными документами с Банком может осуществляться с компьютера Клиента с установленной операционной системой Windows 2000 и выше, программой Microsoft

Internet Explorer v.5.5. и выше, настроенного для работы с Системой, при условии наличия у Клиента ключей электронной цифровой подписи (ЭЦП), необходимой для регистрации в Системе. Обмен электронными документами с Банком Клиент так же может осуществлять с использованием системы 1С: Предприятие, ни запуская при этом в Microsoft Internet Explorer, для этого необходим компьютер с установленной операционной системой не ниже Windows 2000 и 1С: Предприятие не ниже версии 8.1.

1.7. ЭД порождает обязательства Сторон, если он передан передающей Стороной надлежащим образом оформлен, заверен электронно-цифровой подписью (далее ЭЦП) в необходимых количествах и направлен посредством Системы, а принимающей Стороной получен, проверен и принят. Свидетельством того, что ЭД получен, проверен и принят, является надлежащим образом оформленный электронный служебно-информационный документ (далее ЭСИД), заверенный ЭЦП, содержащий положительные результаты проверки ЭЦП передающей Стороны.

1.8. Безопасность использования Системы достигается за счет предоставления доступа Клиенту к возможностям Системы путем аутентификации пользователя с использованием ключа. Обмен документами между Банком и Клиентом основывается на том, что стороны признают использование средств криптографической защиты информации достаточным для обеспечения конфиденциальности, целостности и авторства электронных документов.

1.9. В качестве электронных носителей ключей ЭЦП могут использоваться съемные электронные носители (дискеты, флэш-карты, смарт-ключи). Использование жесткого диска компьютера для хранения ключей ЭЦП не рекомендуется.

1.10. Переданные Клиенту посредством Системы и подписанные ЭЦП документы свободного формата, в т.ч. вложение в документы свободного формата, являются эквивалентными подобным документам на бумажных носителях и влекут аналогичные им права и обязанности Сторон.

1.11. На каждого сотрудника Клиента, уполномоченного работать с системой Клиент-Банк, изготавливается индивидуальный сертификат ключа ЭЦП.

1.12. Стороны признают, что получение Сторонами с использованием Системы электронных документов, подписанных ЭЦП, юридически тождественно получению аналогичных документов на бумажном носителе, с подписями уполномоченных лиц и печатью другой стороны, оформленных в соответствии с законодательством РФ и нормативными документами Банка России.

1.13. Единой шкалой времени при работе в Системе является поясное время по показаниям системных часов Банка. Временем поступления электронного документа Клиента в Банк считается время записи документа в базу данных Системы на АРМ Банка, которое указывается в соответствующем ЭСИД, направляемом Клиенту.

1.14. В соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных» Клиент дает свое согласие ООО РНКО «РИБ» (телефон (495) 232-34-34, адрес местонахождения: 119146, Москва, Фрунзенская наб., д. 24/1) на передачу всех персональных данных в ЗАО «Центр Финансовых Технологий» с целью исполнения Банком договорных обязательств перед клиентом. Согласие предоставляется с момента подписания Клиентом договора и действительно в течение пяти лет после исполнения договорных обязательств. Согласие может быть отозвано Клиентом в любой момент путем передачи Банку подписанного письменного заявления, если иное не предусмотрено законодательством РФ. Указанные Клиентом персональные данные предоставляются в целях информационного обмена с Банком, проведения операций в Системе, исполнения договорных обязательств, а также разработки Банком новых продуктов и услуги информирования Клиента об этих продуктах и услугах.

1.15. Вся документация необходимая Клиенту для работы с системой Клиент-Банк размещена на сайте Банка (www.ribank.ru).

1.16. При изменении условий оказания услуг, Банком вводится в действие новая редакции Условий.

1.17. Банком установлено следующее операционное время для перевода денежных средств на основании электронных платежных документов, поступивших в Банк и прошедших процедуру приема к исполнению распоряжений Клиентов на перевод денежных средств (контроль) в рабочие дни, установленные на территории Российской Федерации (время московское):

- в валюте Российской Федерации – с 09 часов 00 минут до 17 часов 45 минут; - в иностранной валюте – с 09 часов 00 минут до 12 часов 00 минут;

-по выполнению поручений Клиента по операциям покупки – продажи иностранной валюты – с 09 часов 00 минут до 12 часов 00 минут.

1.18. Электронные платежные документы в валюте РФ, поступившие в Банк с видом платежа «Срочно», в течении операционного времени, принимаются к исполнению и проводятся через

банковскую электронную систему переводов (БЭСП) в тот же день не позднее одного часа с момента поступления в Банк.

1.19. При недостаточности денежных средств на банковском счете Клиента распоряжения не принимаются Банком к исполнению и возвращаются не позднее рабочего дня, следующего за днем поступления распоряжения, за исключением:

- распоряжений о переводе денежных средств в бюджет Российской Федерации,
- распоряжений этой же и предыдущей очередности списания денежных средств со счета Клиента. Банк направляет Клиенту посредством Системы уведомление о неисполнении/ возврате распоряжения.

1.20. Принятые к исполнению распоряжения о переводе денежных средств в бюджет Российской Федерации, распоряжения этой же и предыдущей очередности списания денежных средств со счета Клиента, помещаются Банком в очередь не исполненных в срок распоряжений для дальнейшего контроля достаточности денежных средств и исполнения в срок и в порядке очередности списания денежных средств со счета Клиента, которые установлены Федеральным законом.

1.21. При наличии приостановлений в соответствии с Федеральным законом операций по счету Клиента распоряжения, находящиеся в очереди не исполненных в срок распоряжений, помещаются в очередь распоряжений, ожидающих разрешения на проведение операций. При отмене приостановления операций по счету Клиента указанные распоряжения подлежат исполнению.

1.22. Срок исполнения распоряжений Клиента, кроме поступивших с видом «Срочно» устанавливается договором банковского счета и/или Тарифами Банка.

1.23. Информация, которой обмениваются Стороны в рамках выполнения настоящих Условий, признается Сторонами конфиденциальной за исключением следующих случаев:

1.24.1. данная информация подлежит обязательному публичному разглашению согласно действующему законодательству Российской Федерации;

1.25.2. данная информация разрешена к публичному разглашению письменным разрешением предоставившей ее Стороны;

1.26. Стороны обязуются не разглашать конфиденциальную информацию, относящуюся к настоящим Условиям.

ПОРЯДОК ЗАКЛЮЧЕНИЯ ДОГОВОРА О ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

2.1. Информация об услуге дистанционного банковского обслуживания с использованием системы Клиент-Банк и формы документов размещены на сайте Банка (www.ribank.ru).

2.2. Заключение Договора о ДБО состоит из следующих этапов:

2.2.1. Изучение Клиентом Условий обслуживания размещенных на сайте Банка (www. ribank.ru);

2.2.2. Подготовка и передача в Банк пакета документов необходимых для заключения Договора;

2.2.2. Выбор Клиентом типа ключевого носителя;

2.2.3. Генерация Банком ключей ЭЦП;

2.2.4. Регистрация ключа ЭЦП Банком в Системе;

2.3. Типы ключевых носителей, на которых будут храниться ключи ЭЦП: дискета, флэш-карта, смарт-ключ и т.п.

От выбора типа ключевого носителя зависит степень безопасности использования Системы и процедура регистрации сеансов подключения к Системе в процессе работы:

Дискета, флэш-карта – в связи с наличием в сети Интернет специально разработанных вирусных программ, похищающих с компьютеров пользователей файлы с ключами ЭЦП систем дистанционного банковского обслуживания, степень безопасности использования системы зависит от эффективности антивирусной защиты компьютера Клиента. С целью повышения безопасности при использовании указанных выше типов ключевых носителей, после каждой авторизации клиента в Системе (ввода логина и основного пароля), предусмотрена необходимость ввода дополнительного одноразового пароля, который Клиент получает сразу после авторизации в Системе в виде SMS сообщения на номер мобильного телефона, указанный им при заключении Договора о ДБО.

Смарт-ключ – специальное электронное устройство с USB разъемом, содержащее встроенный процессор, выполняющее операцию подписания электронных документов электронной цифровой

подписью способом, исключающим возможность хищения ключей ЭЦП. При хранении ключей ЭЦП на смарт-ключе, использование одноразовых паролей носит рекомендательный характер.

2.4. Банк, являясь Агентом Удостоверяющего центра, на основании полученного от Клиента Заявления на выдачу сертификата ключа и Анкеты, инициирует выпуск сертификата ключа Клиента.

2.5. Удостоверяющий центр выпускает электронный сертификат ключа.

2.6. Банк записывает сертификат на ключевой носитель, получает Акт приема-передачи, распечатывает Акт приема-передачи в двух экземплярах, подписывает и ставит печать. Один экземпляр Акта передается Клиенту.

2.7. На каждого сотрудника Клиента, уполномоченного работать в Системе, изготавливается индивидуальный ключ ЭЦП.

2.8. В случае если уполномоченный сотрудник является представителем нескольких Клиентов и существует необходимость работать в Системе с использованием одного ранее выпущенного ключа (ключ должен быть выпущен на физическое лицо).

2.9. С целью подключения к системе Клиент передает в Банк следующие документы, оформленные с его стороны и достаточные для его подключения к Системе:

Заявление о присоединении к Условиям предоставления услуг дистанционного банковского обслуживания ООО РНКО «РИБ» – 1 экз.; Анкету уполномоченного сотрудника – 1 экз. на каждого сотрудника;

2.10. Договор о ДБО считается заключенным с момента его подписания Банком.

2.11. Обслуживание Клиента с использованием Системы начинается не позднее следующего банковского дня после подписания Банком Акта приема передачи сертификата (ключа ЭЦП).

2.12. В случае просрочки Клиентом оплаты комиссии за регистрацию в Системе и выдачу ключа ЭЦП на срок более 30 (Тридцать) календарных дней Банк вправе приостановить обслуживание Клиента на срок до момента погашения Клиентом задолженности. 2.13. В случае непогашения Клиентом задолженности в течении 3 (Три) месяцев, Договор расторгается.

ПОРЯДОК ЭКСПЛУАТАЦИИ СИСТЕМЫ

3.1. Если не оговорено особо, в рамках Договора о ДБО Клиент может:

3.1.1. работать со следующими документами:

- выписка по счету;
- платежное поручение;
- перевод валюты;
- покупка, продажа, конверсия валюты;
- уведомление о получении валютной выручки;
- подтверждение остатка на счете клиента;
- документы свободного формата;
- документы валютного контроля.

3.1.2. получать SMS уведомления (Системой может взиматься дополнительная плата):

- о входе в Систему;
- одноразовые пароли;
- содержащие информацию о снятии/поступлении на расчетный счет.

3.1.3. получать E-mail уведомления:

- о входе в систему;
- об исполнении документов, отправленных в Банк;
- о поступлении из Банка выписки или промежуточной информации об операциях по счету;
- о поступлении валютной выручки;
- о поступлении документов свободного формата;
- о замене Банком ранее присланной выписки по счету;
- о поступлении новых почтовых сообщений;
- о поступлении из Банка запроса на подтверждение остатка;
- об увеличении остатка средств на счете;
- об уменьшении остатка средств на счете;
- об остатке средств на счете в указанное время (ежедневно).

Осуществлять обмен электронными документами с Банком непосредственно из 1С: Предприятие, не запуская Microsoft Internet

Explorer.

3.2. Отправка и прием электронных документов должны осуществляться только владельцем ключа ЭЦП.

3.3. Для предоставления доступа к счетам новым сотрудникам, Клиент в отношении каждого сотрудника предоставляет в Банк Анкету в одном экземпляре на бумажном носителе.

3.4. Для изменения прав доступа владельцев ключей ЭЦП к счетам Клиента открытым в Банке, Клиент предоставляет в Банк Заявление о замене ключа ЭЦП в одном экземпляре на бумажном носителе.

3.5. Для подключения к Системе новых счетов, открытых в Банке, Клиент предоставляет в Банк Заявление на подключение\отключение счетов к системе Клиент-Банк в одном экземпляре на бумажном носителе.

3.6. Электронный документ считается принятым Банком к исполнению, если его статус изменен с «Доставлен в банк» на иной.

3.7. Клиент вправе отозвать отправленный электронный документ, если Банком не начата его обработка (статус документа, отправленного в Банк изменен на «Исполнен»). Отзыв переданного в Банк платежного документа может быть произведен Клиентом только после устного распоряжения (по телефону) с последующей обязательной отправкой Банку отзыва по Системе («Прочие документы») с полным указанием реквизитов отзываемого документа. После исполнения Банком распоряжения Клиента об отзыве платежного документа, документ приобретает статус «Возвращен» с указанием причины возврата.

3.8. Электронные документы вместе с их ЭЦП должны храниться Сторонами в течение времени, установленного для аналогичных документов на бумажном носителе, если иное не предусмотрено действующим законодательством РФ.

РЕКОМЕНДАЦИИ ДЛЯ СНИЖЕНИЯ РИСКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СИСТЕМЕ:

Подключите e-mail или SMS/PUSH-уведомления об отправке платежей и при обнаружении подозрительных операций незамедлительно обращайтесь в банк!

Используйте встроенные средства блокировки и разблокировки устройства для мобильной связи (логин/пароль для входа в ОС, логин/пин код/отпечаток пальца) которые используются для входа в Систему.

На устройствах для мобильной связи для работы с Системой следует использовать безопасный способ подключения с помощью специального приложения, а не браузера. Загружать и устанавливать специальное приложение следует только с официальных сайтов – Google Play или Apple AppStore (ссылки для скачивания размещены на сайте https://www.faktura.ru/f2b/).

В случае утери устройства для мобильной связи, с установленным специальным приложением, используемым для работы с Системой, необходимо незамедлительно заблокировать SIM-карту у оператора сотовой связи и обратиться в Банк для блокировки доступа в Систему;

В случае изменения номера телефона устройства для мобильной связи для работы в Системе, обратитесь в Банк для изменения доступа со старого номера на новый номер телефона. Необходимо помнить, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время;

Если у Вас неожиданно перестала работать SIM-карты – незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как в отношении Вас третьими лицами возможно проведение мошеннических действий;

Для работы с Системой используйте защищенные устройства для мобильной связи – не пытайтесь обходить установленные производителем защитные механизмы (например, через джейлбрейк (Jailbreak) или рутинг (Rooting)). Не перепрошивайте свое устройства для мобильной связи прошивками сторонних лиц, не являющихся производителями устройства, т.к. это может сделать Ваше устройство уязвимым к заражению вредоносным кодом.

Не допускается работать в Системе через публичные беспроводные сети (Wi-Fi), незащищенные беспроводные сети. Специальные приложения применяют механизмы защиты своих данных при передаче, а так как публичные беспроводные сети сравнительно труднее контролировать, то у злоумышленников появляется больше возможностей для попыток обхода защитных механизмов. Для работы необходимо использовать подключение к сети Интернет через мобильного оператора (3G, 4G) или через доверенную защищенную беспроводную сеть;

Используйте только доверенные компьютеры с лицензионными программами, установленным антивирусом. Регулярно проверяйте компьютер на вирусы, обновляйте операционную систему, браузеры и антивирусные базы.

При работе с электронной почтой не открывайте письма, полученные от неизвестных отправителей, и вложения к ним, не переходите по ссылкам из таких писем.

Не используйте права администратора без крайней необходимости. В повседневной практике входите в систему, как пользователь без прав администратора.

При работе в Интернет не соглашайтесь на установку дополнительных программ.

Рекомендуется использовать выделенный компьютер только для работы с Системой.

Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Банком Системы, и (или) использующих зарегистрированные товарные знаки и наименование Банка, необходимо удостовериться, чтобы при подключении к Системе защищённое SSL-соединение было установлено исключительно с официальным сайтом Системы Faktura - https://www.faktura.ru/f2b/. Перед началом работы в Системе, необходимо убедиться, что в адресной строке браузера совпадает с вышеуказанным адресом соответствующего сервиса.

Прежде чем ввести имя пользователя и пароль в системе Faktura, проверьте подлинность сайта https://www.faktura.ru/f2b/ по информации из SSL-сертификата. Для этого в адресной строке браузера, например Internet Explorer, щелкните мышкой на символ замка, далее «Просмотр сертификатов», перейти на закладку «Состав», встать на строку «Субъект», в окне просмотра убедитесь в наличии следующей информации: CN = www.faktura.ru, O = CJSC Billingovyi center. Аналогичным образом можно посмотреть эту информацию и в других браузерах. Центром сертификации, подтверждающим подлинность сайта https://www.faktura.ru/f2b/, является Thawte EV RSA CA 2018. При установке мобильного приложения из репозитория убедитесь, что разработчиком данного программного обеспечения является компания JSC Center of Financial Technologies.

При создании паролей придерживайтесь следующих правил:

-не допускается использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в другие системы,

- пароль должен соответствовать следующим требованиям – длина пароля должна быть не менее 8 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.), пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, год рождения, номер телефона и т.п.).

Необходимо хранить логин и пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать пароль к Системе там, где доступ к нему могут получить посторонние лица включая устройство для мобильной связи. Исключите запись пароля на стикерах, носителях ключей и т.п..

Не сообщайте пароль, SMS-коды, необходимые для проведения операций, посторонним лицам, в том числе сотрудникам Банка по телефону, электронной почте или иным способом. При наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом по контактным телефонам, указанным на официальном сайте Банка;

Не оставляйте устройства для мобильной связи без присмотра. Необходимо установить пароль на доступ к устройству для мобильной связи и/или на доступ к SMS-сообщениям. Это затруднит доступ злоумышленникам к устройству для мобильной связи в случае его утраты;

Необходимо корректно завершать работу в Системе, используя для этого пункт меню «Выход»;

Храните носители ключей (смарт-ключи, USB-флеш, CD) в месте, недоступном посторонним лицам. Исключите хранение ключей на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах, либо используйте крипто-контейнеры.

ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

4.1. Электронный документооборот между Клиентом и Банком может включать в себя следующие этапы:

4.1.1. Формирование электронного документа;

4.1.2. Отправку и доставку электронного документа;

4.1.3. Проверку электронного документа;

4.1.4. Подтверждение получения электронного документа;

4.1.5. Отзыв электронного документа;

4.1.6. Хранение электронных документов (ведение архивов).

4.2. Система позволяет использовать несколько вариантов формирования электронных документов:

4.2.1. Подготовка электронных документов в режиме on-line, путем заполнения типовых экранных форм документов, реализованных в Системе. Этот вариант подходит для Клиентов, работающих с небольшим количеством документов в день и использующих типовые формы документов, реализованных в Системе.

4.2.2. Подготовка документов, в том числе платежных, в off-line с использованием специализированного программного обеспечения (приложения Microsoft, бухгалтерские программы и прочее) с последующим импортом данных в Систему.

4.2.3. Для некоторых бухгалтерских программ (например, 1С - бухгалтерия) существуют интегрированные в Систему модули сопряжения, позволяющие экспортировать и импортировать документы в Систему.

4.3. Электронные документы могут отправляться Клиентом в Банк только после их подписания ЭЦП. В случае неверного оформления документа, отправленного Клиентом в Банк или в случае подписания документа неверным ЭЦП, документ к обработке не принимается, о чем Клиент извещается средствами Системы с указанием причины отказа.

4.4. При любом изменении ЭД, совершенном после подписания такого документа ЭЦП одной из Сторон, ЭЦП становится некорректной;

4.5. Система позволяет Клиенту отслеживать статус каждого отправленного в Банк документа, который может иметь следующие состояния:

4.5.1. Подготовлен – документ подготовлен, но не отправлен в Банк. На данном этапе электронный документ можно исправить или удалить;

4.5.2. Подписан – такой статус возникает, если под документом должно быть несколько подписей (первая и/или вторая и/или подтверждающая);

4.5.3. Отправлен в банк – документ отправлен в Банк, но еще не получен Банком;

4.5.4. Принят банком – документ получен Банком, прошел проверку на подлинность подписи, но еще не обработан;

4.5.5. Исполнен – документ исполнен Банком;

4.5.6. Возвращен – документ возвращен Клиенту с указанием причины.

4.6. Клиент и Банк самостоятельно ведут архив документов, отправленных\полученных с использованием Системы, обеспечивая целостность помещенных в них документов. Подписанные ЭЦП документы, помещенные в архив, должны храниться вместе с необходимой для подтверждения подписи ключевой информацией.

4.7. В Системе предусмотрена возможность информирования Клиентов о всех входах в Систему и о получении Банком платежных документов от имени Клиента, путем отправки на номер мобильного телефона, указанный им при заключении Договора, соответствующих SMS-сообщений. Активация услуги информирования может быть выполнена и после заключения Договора о ДБО, путем подачи соответствующего заявления.

4.8. В случае изменения номеров контактных телефонов или адресов e-mail, используемых для информирования Клиентов о получении Банком платежных документов от имени Клиента и о всех входах в Систему, Клиенты обязаны немедленно направить в Банк Заявление об изменении контактных данных.

4.9. К исполнению ЭД принимаются только при их аутентификации в соответствии с настоящими Условиями.

ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ (РАСПОРЯЖЕНИЯМИ)

5.1.Банк и Клиент устанавливают между собой порядок передачи распоряжений в электронном виде к счету, который включает в себя:

5.1.1. подготовку и передачу Клиентом в Банк электронных платёжных распоряжений,

5.1.2. формирование Банком по запросу Клиента информации о состоянии счёта Клиента за запрашиваемый период (выписка по счету),

5.1.3. обмена сообщениями посредствам системы,

5.1.4. информирования Банком Клиента о совершенных операциях по счету,

5.1.5. направления Банком Клиенту уведомлений о приеме распоряжений к исполнению.

5.2. Клиент в соответствии с «Правилами осуществления перевода денежных средств Российской Федерации» оформляет электронное распоряжение о переводе и передает его в Банк для исполнения по установленным каналам связи. После получения электронного платежного документа Банк принимает его к исполнению. Клиенту передается служебное электронное сообщение о принятии или отказе в принятии электронного распоряжения. Статус документов, переданных в Банк, отслеживается Клиентом самостоятельно при проведении очередного сеанса связи.

5.3. Процедура признания аналога собственноручной подписи Клиента заключается в расшифровании поступившего от него электронного документа с использованием уникального ключа. В случае успешного завершения процедуры расшифрования документа и электронной цифровой подписи, присвоенной Клиенту, а также соответствия электронной цифровой подписи документа электронной цифровой подписи Клиента, электронная цифровая подпись Клиента считается подтвержденной, а документ поступившим от уполномоченного лица Клиента.

5.4. Принятые от Клиента ЭД и запросы проходят обработку службами Банка с 09 до 18 часов.

5.5. Списание средств производится в пределах остатка на счёте Клиента.

СЕРТИФИКАТЫ КЛЮЧЕЙ ЭЦП И КЛЮЧИ ЭЦП

6.1. Изготовление Сертификатов ключей ЭЦП осуществляется на основании Заявления Клиента, поданного им Банку. Заявление формируется в соответствии с типовой формой, разработанной Банком и подписывается собственноручно Клиентом или его уполномоченным лицом. Содержащиеся в Заявлении сведения подтверждаются предъявлением соответствующих документов (для физических лиц – паспорт, для представителей юридических лиц – паспорт, а также письменный документ, заверенный подписью руководителя и печатью организации, подтверждающий право представителя действовать от имени данной организации).

6.2. Сертификат ключа ЭЦП содержит следующие данные:

6.2.1. Уникальный идентификатор владельца сертификата ключа (ФИО или псевдоним, или учетный идентификатор владельца сертификата ключа подписи, дополнительные сведения);

6.2.2. Открытый ключ;

6.2.3. Идентификатор сертификата ключа Удостоверяющего центра, создавшего сертификат ключа;

6.2.4. Уникальный регистрационный номер сертификата ключа, присвоенный Удостоверяющим центром;

6.2.5. Дату начала и окончания срока действия сертификата ключа;

6.2.6. Идентификатор Удостоверяющего центра, выдавшего сертификат ключа;

6.2.7. Подпись Удостоверяющим центром данных Сертификата ключа.

6.3. Клиент обязан обеспечить конфиденциальность и безопасность закрытых ключей ЭЦП используемых в Системе.

6.4. Знание информации, которая передается между Сторонами по каналу связи Системы, не приводит к компрометации закрытых ключей ЭЦП Сторон;

6.5. Каждая Сторона несет ответственность за сохранение в тайне своих закрытых ключей ЭЦП, паролей, за правильность заполнения и оформления ЭД и за действия своего персонала при работе с Системой;

6.6. Подделка одной Стороной ЭЦП другой Стороны (т.е. создание корректной ЭЦП) невозможна без знания закрытого ключа ЭЦП;

6.7. Закрытый ключ ЭЦП уполномоченного лица Клиента, созданный в единственном экземпляре в рамках настоящего Договора, уникален. Создание дубликата закрытого ключа ЭЦП технически невозможно;

6.8. Произведенная замена ключей ЭЦП с соблюдением требований настоящих Условий не влияет на юридическую силу ЭД, если он был подписан рабочим на момент подписания ключом ЭЦП;

6.9. В силу особенностей формирования закрытых ключей ЭЦП Удостоверяющим центром, Банк не имеет к ним доступа, в случае выявления фактов компрометации ключей, претензии к Банку не могут быть предъявлены.

6.10. С целью обеспечения конфиденциальности и безопасности закрытых ключей ЭЦП, используемых в Системе, Клиент должен соблюдать следующие меры предосторожности:

6.10.1. использовать и своевременно обновлять на компьютере, с которого осуществляется работа с Системой, антивирусное программное обеспечение;

6.10.2. применять технические и организационные меры, исключающие возможность доступа посторонних лиц к ключевым носителям;

6.10.3. при наличии малейших подозрений о компрометации ключей, уведомлять об этом Банк и инициировать блокирование ключей до выяснения обстоятельств и/или выполнить мероприятия по смене ключей ЭЦП.

6.11. Банк настоятельно рекомендует не использовать в качестве ключевого носителя жесткий диск компьютера, так же рекомендует не использовать отчуждаемые носители (дискеты, флэш-карты т.п.) и настоятельно рекомендует использовать смарт-ключи.

СМЕНА СЕРТИФИКАТА КЛЮЧА ЭЦП И КЛЮЧЕЙ ЭЦП. ОБЩИЕ ПОЛОЖЕНИЯ

7.1. При изменении данных, идентифицирующих Владельца сертификата ключа ЭЦП, содержащихся в документах, предоставленных при выдаче Сертификата ключа ЭЦП, смене ключей ЭЦП, в случаях Компрометации ключей ЭЦП, Владельцу сертификата ключа ЭЦП надлежит получить новый Сертификат ключа ЭЦП в порядке, предусмотренном настоящим разделом. Все риски, связанные с невозможностью использования Сертификата ключа ЭЦП в связи с изменением данных, идентифицирующих Владельца сертификата ключа ЭЦП, несет Владелец сертификата ключа ЭЦП.

7.2. Сертификаты ключей ЭЦП, выдаваемые в Системе, действительны в течение одного года, после чего они должны быть обновлены, т.е. должны быть сгенерированы новые ключи ЭЦП и изготовлены новые Сертификаты ключей ЭЦП.

7.3. Если срок действия Сертификата ключа ЭЦП еще не истек, Клиент может обновить Сертификат ключа ЭЦП, передав в Банк Анкету и носитель ключевой информации, после чего Банк продлит срок действия закрытого ключа, подготовит Акт и передаст Клиенту.

7.4. Если срок действия Сертификата ключа ЭЦП не истек Клиент праве самостоятельно произвести продление срока действия Сертификата ЭЦП используя пункт меню «Обновление Сертификата ключа ЭЦП» в Личном кабинете. В этом случае Акт, подписанный ЭПЦ Банка придет на электронную почту Клиента. Клиент подпишет Акт своим ЭЦП.

7.5. Если срок действия Сертификата ключа ЭЦП истек, Клиенту необходимо передать в Банк Анкету и носитель ключевой информации, при этом Банком будут выполнены действия как при регистрации нового сотрудника.

7.6. Банк вправе отказать в выдаче Клиенту нового Сертификата ключа ЭЦП, с указанием причины отказа.

7.7. Смена Сертификата ключа ЭЦП, смена ключей ЭЦП в связи с Компрометация ключей ЭЦП может произойти в следующих случаях:

7.7.1. увольнение сотрудников, имевших доступ к ключевым носителям, если ЭЦП было выпущено, но на юридическое лицо;

7.7.2. неисправность ключевого носителя;

7.7.3. ключ стал известен третьим лицам.

7.8. В случае компрометации рабочих ключей ЭЦП, Клиент обязан в кратчайшие сроки уведомить Банк о факте компрометации. Для этого Клиент должен не позднее следующего рабочего дня предоставить в Банк Заявления о компрометации ключа ЭЦП на бумажном носителе в двух экземплярах, заверенных подписью и печатью Клиента, либо сканирует его, подписывает своей ЭЦП и направляет посредством Системы. Дата и время получения

заявления о компрометации фиксируется Администратором Системы по отметке времени получения Заявления. Один экземпляр Заявления, полученного на бумажном носителе, с отметкой времени возвращается Клиенту, другой - остается в Банке для использования его в дальнейшей работе.

Если Клиент не может оперативно приехать в офис Банка и подать заявление, Клиент вправе направить на электронный адрес Банка скан-копию Заявления о компрометации ключа.

Банк снимает в системе права на использование данного счета. После того, как Клиент принес в Банк оригинал Заявления о компрометации ключа, Банк инициирует процедуру компрометации.

7.9. По истечении не более чем 2 (двух) часов со времени получения Банком уведомления о компрометации ключа ЭЦП в рабочие дни, или не более чем 2 (двух) часов с начала первого рабочего дня для случая, когда уведомление о компрометации ключа ЭЦП было получено в электронном виде в нерабочие дни, все документы, полученные по Системе с использованием скомпрометированных ключей, считаются недействительными, не принимаются Банком в обработку и возвращаются Клиенту с указанием причины возврата.

7.10. Банк не несет ответственности за возможный ущерб, вызванный компрометацией ключа ЭЦП Клиента, в течение 2 (двух) часов с момента получения Банком уведомления о компрометации ключа ЭЦП в рабочие дни, или 2 (двух) часов с начала первого рабочего дня, если уведомление о компрометации ключа ЭЦП было получено в электронном виде в нерабочие дни.

7.11. После передачи в Банк Заявления о компрометации ключа ЭЦП, для возобновления работы уполномоченного лица Клиента в Системе, Клиенту необходимо выполнить действия, как при регистрации нового сотрудника.

7.12. Новый ключ уполномоченному сотруднику Клиента, в отношении ключа ЭЦП которого в Банк поступило уведомление о компрометации ключа ЭЦП, может быть выдан только после получения Банком Заявления о компрометации ключа ЭЦП.

ПОРЯДОК ИЗГОТОВЛЕНИЯ (ПЕРЕИЗГОТОВЛЕНИЯ) СЕРТИФИКАТОВ КЛЮЧА ЭЦП И КЛЮЧЕЙ ЭЦП

8.1. Банк изготавливает Сертификат ключа ЭЦП, а также ключи ЭЦП, руководствуясь следующими правилами:

87.1.1. Получив Заявление Клиента в соответствии с п. 5.1, Банк формирует запрос на создание Сертификата ключа ЭЦП. Запрос формируется в виде ЭД, подписанного ЭЦП Банка и направляется в Удостоверяющий центр с использованием программно-аппаратных средств Банка, подключенных через каналы связи к программно-техническим средствам Удостоверяющего центра. Запрос содержит Закрытый ключ ЭЦП, а также Уникальный идентификатор владельца сертификата ключа, сформированный на основе проверенных Банком данных Клиента.

8.1.2. Создание Сертификатов ключа ЭЦП для Банка/Клиентов осуществляется Удостоверяющим центром в течение 3 (Трех) рабочих дней с момента получения от Банка электронного запроса. Передача Удостоверяющим центром или уполномоченными им лицами Банку Носителей ключевой информации, содержащих Ключ ЭЦП и Сертификат ключа ЭЦП, созданных Удостоверяющим центром без получения Заявления от Клиента, осуществляется в порядке и на условиях, определяемых Удостоверяющим центром и Банком дополнительно.

8.1.3. При изготовлении Сертификатов ключа ЭЦП всегда проверяется уникальность Идентификаторов владельцев сертификатов ключа, принадлежащих разным Владельцам сертификатов ключа, и Открытых ключей ЭЦП в реестре и архиве Удостоверяющего центра. Программно-аппаратные средства Удостоверяющего центра исключают возможность изготовления одинаковых Сертификатов ключа ЭЦП. При изготовлении Носителей ключевой информации, Удостоверяющий центр самостоятельно формирует уникальный Идентификатор владельца сертификата и присваивает его созданному Сертификату ключа ЭЦП.

8.1.4.Удостоверяющий центр предоставляет Банку созданные по Заявлению/запросу Банка Сертификаты ключа ЭЦП для Банка/Клиентов в форме ЭД.

8.1.5. Банк при выдаче Криптографических ключей Клиента распечатывает на бумажном носителе Акт приема-передачи Сертификата ключа ЭЦП Клиента в двух экземплярах и обеспечивает проставление в них собственноручной подписи Клиента или уполномоченного лица Клиента. Второй экземпляр Акта приема-передачи на бумажном носителе хранится у Банка. По требованию Удостоверяющего центра Банк обязан направить в Удостоверяющий центр заверенную копию Акта. Направление заверенной копии осуществляется Банком за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от Удостоверяющего центра. В случае не направления вышеуказанного Акта в предусмотренный срок, Удостоверяющий центр вправе приостановить деятельность такого Банка по формированию запросов на создание Сертификатов ключа ЭЦП и их выдачи Клиентам, письменно уведомив об этом Банк.

8.2. Клиент, уже являющийся Владельцем Сертификата ключа ЭЦП, изготавливает Сертификат ключа ЭЦП, посредством удаленного обращения на страницу сервера Удостоверяющего центра, предназначенную для удаленной выдачи Сертификатов ключа ЭЦП, руководствуясь следующими правилами:

8.2.1. Банк обращается на сервер Удостоверяющего центра и подтверждает выдачу нового Сертификата ключа ЭЦП Клиента.

8.2.2. Удостоверяющий центр изготавливает новый Сертификат ключа ЭЦП по запросу Клиента. Класс нового Сертификата ключа ЭЦП совпадает с Классом действующего Сертификата ключа ЭЦП Клиента.

8.2.3. Банк обращается на сервер Удостоверяющего центра и получает Акт приема-передачи нового Сертификата ключа ЭЦП Клиента.

8.2.4. Банк заверяет Акт приема-передачи нового Сертификата ключа ЭЦП Клиента Электронной подписью и передает его Удостоверяющему центру, подтверждая тем самым выдачу нового Сертификата ключа ЭЦП Клиенту.

8.2.5. Банк или Удостоверяющий центр сообщает Клиенту адрес выдачи нового Сертификата ключа ЭЦП.

8.2.6. Клиент обращается по указанному адресу, получает заверенный Банком Акт приема-передачи нового Сертификата ключа ЭЦП.

8.2.7. Клиент заверяет действующей ЭП Акт приема-передачи нового Сертификата и передает Акт в УЦ.

8.2.8. Клиент получает новый Сертификат ключа ЭЦП.

8.2.9. Сертификат ключа ЭЦП помещается в реестр Сертификатов, который ведет Удостоверяющий центр.

8.2.10. Так как Акт приема-передачи формируется в электронном виде и сохраняется Удостоверяющим центром, Банк может в этом случае Акт не хранить.

8.2.11 Банк может отказаться от подтверждения выдачи нового Сертификата ключа ЭЦП Клиента, при этом Банк или Удостоверяющий центр направляет Клиенту сообщение об отказе.

8.3. Правила, указанные в п. 8.2. (включая соответствующие подпункты 8.2.1. - 8.2.11.), применяются, только в случаях, когда:

- Клиент, уже являющийся Владельцем сертификата ключа ЭЦП Удостоверяющего центра, срок действия которого не истек, формирует новую пару Открытого ключа ЭЦП и Закрытого ключа ЭЦП, а также запрос на новый Сертификат ключа ЭЦП;
- Клиент подписывает запрос на новый Сертификат ключа ЭЦП действующим Закрытым ключом ЭЦП. Идентификаторы владельца сертификата нового и действующего Сертификата ключа ЭЦП должны совпадать;
- Клиент передает заверенный действующим Закрытым ключом ЭЦП запрос на новый Сертификат ключа ЭЦП серверу Удостоверяющего центра. Запрос равнозначен Заявлению Клиента на выдачу Сертификата ключа ЭЦП, заверенному собственноручной подписью Клиента или уполномоченного лица Клиента.

ПРАВА И ОБЯЗАННОСТИ СТОРОН

9.1. СТОРОНЫ обязуются:

9.1.1. Принимать на себя в полном объеме все обязательства, связанные с ЭД, удостоверенным от их имени корректной ЭЦП.

9.1.2. При проведении электронных расчетов с использованием Системы руководствоваться действующим законодательством Российской Федерации, нормативными актами Банка России, определяющими порядок и правила проведения переводов денежных средств, настоящими Условиями, а также Договором (Договорами) банковского счета.

9.1.3. За собственный счет приобретать и поддерживать в работоспособном состоянии технические средства и общесистемное программное обеспечение, необходимые для функционирования Системы, а также обеспечивать функционирование Системы в частях, относящихся к АРМ каждой из Сторон.

9.1.4. Самостоятельно обеспечивать безопасность функционирования своих АРМ, контролировать сохранность ключей ЭЦП и не допускать к ним посторонних лиц.

9.1.5. Информировать друг друга обо всех случаях невозможности расшифровки ЭД или не подтверждения подлинности ЭЦП не позднее следующего рабочего дня после их получения.

9.2. БАНК обязуется:

9.2.1. В порядке, определенном в настоящих Условиях, подключить Клиента к Системе.

9.2.2. Обеспечить конфиденциальность и защиту от несанкционированного доступа к информации о Счете Клиента и операциям по нему со стороны Банка при условии выполнения Клиентом условий настоящего Договора.

9.2.3. Обеспечивать защиту банковской части Системы от несанкционированного доступа.

9.2.4. Сообщать Клиенту об обнаружении попытки несанкционированного доступа в Систему, если это затрагивало интересы Клиента.

9.2.5. Незамедлительно приостанавливать операции по Счету Клиента с использованием Системы при получении от Клиента информации о компрометации ключа ЭЦП.

9.2.6. Не принимать к исполнению ЭД, если они подписаны некорректными ЭЦП Клиента или подписаны ЭЦП, сформированными на скомпрометированном ключе ЭЦП, после получения Банком уведомления о компрометации ключа ЭЦП в порядке, предусмотренном настоящим Договором и Условиями.

9.2.7. Исполнять электронные распоряжения Клиента в сроки, установленные Договором банковского счета, если электронное распоряжение составлено в соответствии с требованиями настоящих Условий, Договора банковского счета и нормативных документов Банка России, а также подписан корректными ЭЦП Клиента.

9.2.8. Направлять Клиенту посредствам Системы уведомления о принятии распоряжения, а также о статусе принятого распоряжения.

9.2.9. Осуществлять архивное хранение электронных документов, переданных Клиентом в Банк посредством Системы, в течение срока, установленного законодательством Российской Федерации.

9.2.10. Не менее чем за 1 (один) рабочий день уведомлять Клиента о планируемых технических изменениях в Системе, прямо или косвенно влияющих на передачу или получение Клиентом электронных документов, или иным образом затрагивающих интересы Клиента.

9.2.11. В случае приостановки приема, регистрации и исполнения ЭД, а также их передачи посредством Системы на время производства плановых технических работ принимать разумные меры для уведомления Клиента об этом не менее, чем за 1 (Один) рабочий день до начала работ, если иные сроки не установлены настоящими Условиями, в том числе путем опубликования соответствующего сообщения в Системе.

9.2.12. В случае внеплановой приостановки приема, регистрации и исполнения ЭД, а также их передачи посредством Системы по техническим причинам и в случае наступления форс-мажорных обстоятельств, принимать разумные меры для незамедлительного уведомления Клиента об этом, в том числе путем опубликования соответствующего сообщения в Системе (при наличии такой возможности) или на сайте Банка в сети Интернет по адресуwww.ribank.ru.

9.2.13. В случае приостановки приема, регистрации и исполнения ЭД, а также их передачи посредством Системы по основаниям выявления признаков нарушения безопасности или подозрения на возможный несанкционированный доступ к Системе от имени Клиента, принимать разумные меры для уведомления Клиента об этом не позднее 1 (Одного) рабочего дня с даты такой приостановки.

9.2.14. Осуществлять консультирование и техническое сопровождение Клиента в порядке, предусмотренном в настоящем Договоре и Условиях.

9.2.15. Банк несет иные обязанности, предусмотренные действующим законодательством Российской Федерации, настоящими Условиями.

9.3. БАНК имеет право:

9.3.1. Производить замену программного обеспечения, необходимого для использования Системы, с предварительным уведомлением Клиента об этом путем направления соответствующего уведомления Клиенту по Системе и/или путем опубликования соответствующего сообщения на сайте Банка в сети Интернет по адресу www.ribank.ru, не менее чем за 5 (Пять) календарных дней до даты начала работы в новых условиях.

9.3.2. Не принимать к исполнению полученные от Клиента электронные распоряжения в случае их несоответствия требованиям, установленным настоящими Условиями, Договором банковского счета, другими соглашениями Сторон, действующим законодательством Российской Федерации и нормативными актами Банка России, определяющими порядок и правила проведения переводов денежных средств. Об отказе в принятии электронного документа Банк сообщает Клиенту в течение 1 (одного) рабочего дня со дня получения Банком таких документов с указанием причины отказа (в случае если иной срок не установлен действующим законодательством Российской Федерации). Настоящая информация доводится до Клиента, в том числе с использованием Системы.

9.3.3. Не проводить операции по счету Клиента при недостатке средств на нем.

9.3.4. При необходимости оформлять от имени Клиента распоряжения на бумажном носителе на основе полученных Банком распоряжений Клиента посредствам Системы.

9.3.5. Банк вправе списывать со Счета Клиента вознаграждение за оказание услуги по обслуживанию Счета Клиента с использованием Системы в соответствии с Тарифами размещенными на сайте Банка.

9.3.6. В одностороннем порядке отказаться от настоящего Договора в случае неподключения Клиента к Системе в течение 30 (Тридцати) календарных дней с даты заключения настоящего Договора по причинам, не зависящим от Банка.

9.3.7. В одностороннем порядке отказаться от настоящего Договора при задержке уплаты Клиентом в течение 2 (двух) календарных месяцев вознаграждения за услуги Банка в соответствии с настоящими Условиями.

9.3.8. БАНК обладает иными правами, предусмотренными действующим законодательством Российской Федерации, настоящими Условиями.

9.4. КЛИЕНТ обязуется:

9.4.1. Организовать автоматизированное рабочее место для работы Системы в соответствии с требованиями, установленными Условиями.

9.4.2. Своевременно устанавливать на свои программно-аппаратные средства, используемые для работы в Системе, текущие пакеты обновлений и новые версии программного обеспечения Системы, при наличии.

9.4.3. Предоставлять уполномоченным лицам Банка необходимый доступ к программно-техническим средствам Клиента для настройки автоматизированного рабочего места Клиента.

9.4.4. Использовать свое АРМ для подключения к Системе, исключительно в целях, предусмотренных настоящими Условиями.

9.4.5. Обеспечивать защиту своего АРМ от несанкционированного доступа.

9.4.6. Не вносить исправления, изменения или дополнения в специализированное программное обеспечение (при наличии), техническую документацию, ЭЦП, предоставляемые Банком по настоящему Договору, а также не передавать их третьим лицам.

9.4.7. Хранить закрытые ключи ЭЦП на Носителях ключевой информации в месте, исключающем их несанкционированное использование или хищение. КЛИЕНТ самостоятельно и за свой счет обеспечивает сохранность, неразглашение и нераспространение ключей ЭЦП.

9.4.8. Соблюдать порядок совершения электронного документооборота в соответствии с настоящими Условиями.

9.4.9. Передавать в Банк надлежащим образом оформленные электронные распоряжения, контролировать выписки по счетам и статусы ЭД, направленных в БАНК. После направления ЭД через Систему сформировать и получить запрос о состоянии счёта и для контроля прохождения ЭД.

9.4.10. В случае утери или выхода из строя носителя ключевой информации обращаться в Банк для замены носителя и принятия необходимых мер, в том числе блокировки ЭЦП Клиента.

9.4.11. Хранить в тайне пароль входа в Систему. Изменять свой пароль входа в Систему по первому требованию Банка.

9.4.12. Незамедлительно сообщать Банку об обнаружении попытки несанкционированного доступа к Системы.

9.4.13. Строго соблюдать требования по подготовке, оформлению и передаче электронных документов в Банк посредством системы, изложенные в настоящих Условиях и предоставленной Банком документации.

9.4.14. Не позднее чем за 3 (три) рабочих дня до даты фактического истечения срока действия полномочий Владельца сертификата ключа ЭЦП Клиента на использование ключей ЭЦП в Системе предоставить в Банк документы, подтверждающие продление срока их действия.

9.4.15. В течение одного банковского дня уведомить Банк в письменной форме об отстранении от подписания платежных документов по любым основаниям (увольнения, перевода на др. работу и т.д.) лиц, имеющих право первой, второй подписи на платежных документах. Банк производит блокировку ЭЦП в день получения такого уведомления.

9.4.16. В случае внесения каких-либо изменений в документы, подтверждающие полномочия Владельца сертификата ключа ЭЦП Клиента на использование ключей ЭЦП в Системе, в течение 3 (трех) рабочих дней с момента внесения в них изменений, предоставить в Банк указанные документы, а также при необходимости внести изменения в параметры подключения к Системе.

9.4.17. По первому требованию Банка, но не позднее 2 (двух) рабочих дней с даты получения такого требования, предоставить копии отправленных или полученных ЭД на бумажном носителе, заверенные собственноручной подписью уполномоченных лиц и печатью Клиента.

9.4.18. Уплачивать Банку вознаграждение за оказание услуги по обслуживанию Счета Клиента с использованием Системы в соответствии с Тарифами размещенными на сайте Банка.

9.4.19. В период приостановки обслуживания Счета Клиента с использованием Системы, Клиент оформляет и направляет в Банк расчетные и иные документы в порядке, предусмотренном Договором банковского счета и соглашениями, заключенными между Сторонами.

9.4.20. Клиент несет иные обязанности, предусмотренные действующим законодательством Российской Федерации и настоящими Условиями.

9.5. Клиент имеет право:

9.5.1. Формировать и передавать в Банк посредством Системы электронные распоряжения, предусмотренные настоящими Условиями, а также иные документы.

9.5.2. Получать от Банка в электронном виде посредством Системы информацию об исполнении ЭД, переданных Клиентом в Банк посредством Системы, а также иные документы, предусмотренные настоящими Условиями.

9.5.3. Отзывать свои ЭД, переданные в Банк посредством Системы, в случае, если на момент поступления требования Клиента об отзыве электронного документа Банком еще не были совершены действия по его исполнению, делающие невозможным отзыв электронного документа Клиента.

9.5.4. Получать бесплатные консультации специалистов Банка по вопросам, связанным с эксплуатацией Системы.

9.5.5. На платной основе в соответствии с Тарифами вызывать специалистов Банка для настройки программного обеспечения на АРМ Клиента, а также для оказания специалистами Банка услуг по иным вопросам, связанным с функционированием и эксплуатацией Системы.

9.5.6. Клиент обладает иными правами, предусмотренными действующим законодательством Российской Федерации и настоящими Условиями.

ПРАВА БАНКА ПО ОГРАНИЧЕНИЮ В СИСТЕМЕ

10.1. Банк оставляет за собой право отказать Клиенту в заключении Договора о ДБО и не предоставлять обслуживание в Системе.

10.2. Приостановить обслуживание Клиента с использованием Системы, а также отказывать Клиенту в приеме ЭД и совершении операции по Счету, если при осуществлении внутреннего контроля согласно действующему законодательству Российской Федерации и нормативным документам Банка России не представлены документы, необходимые для фиксирования информации в соответствии с положениями Федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", а также в случае, если в результате реализации правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма у работников Банка возникают подозрения, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

При этом для совершения операции по Счету Банк принимает от Клиента надлежащим образом оформленные распоряжения на перевод денежных средств на бумажном носителе, переданные в Банк лично из рук лица, наделенного правом первой подписи.

10.3. Отказать Клиенту в отзыве его ЭД (электронного распоряжения), если на момент поступления требования Клиента об отзыве его ЭД Банком были совершены действия по исполнению указанного ЭД, делающие его отзыв невозможным.

10.4. Отказать Клиенту в отзыве ЭД с момента списания денежных средств со Счета Клиента.

10.5. Не исполнять полученные от Клиента ЭД в случае их несоответствия требованиям, установленным настоящими Правилами, Договором(ами) банковского счета, другими соглашениями Сторон, действующим законодательством Российской Федерации и нормативными актами Банка России, определяющими порядок и правила проведения безналичных расчетов. Возврат (аннулирование) неисполненных ЭД осуществляется Банком не позднее рабочего дня, следующего за днем, в который возникло основание для возврата (аннулирования) ЭД, включая поступление заявления об отзыве.

10.6. Приостановить обслуживание Клиента с использованием Системы:

- при несоблюдении Клиентом настоящих Правил, в том числе по оплате услуг и возмещение расходов Банка;
- при предоставлении недостоверной (некорректной) информации, указанной Клиентом при регистрации в Системе или изменении сведений, в том числе информации о номере мобильного телефона и адреса электронной почты.
- при несоблюдении Клиентом действующего законодательства Российской Федерации;

•при возникновении разногласий и конфликтных ситуаций, возникших в рамках настоящих Правил;

• при возникновении событий, связанных с компрометацией ключей ЭП или использования Системы без согласия Клиента;

• для выполнения неотложных аварийных и ремонтно-восстановительных работ, связанных с обслуживанием Системы, с уведомлением Клиента о сроках проведения этих работ. В период приостановки предоставления услуги, связанной с эксплуатацией Системы, Клиент оформляет и направляет в Банк распоряжения на перевод денежных средств и иные документы в порядке, предусмотренном Договором(-ами) банковского/их счета(-ов) и соглашениями, заключенными между Сторонами.

10.7. В одностороннем порядке изменять:

•Тарифы;

•Правила;

• порядок и график обслуживания Клиента, включая график работы Банка, операционное время и операционный день Банка, условия приема и проверки электронных документов (в том числе по исполнению распоряжений на перевод электронных денежных средств). Информация об указанных изменениях доводится до Клиента за 5 (пять) календарных дней до даты их введения в действие одним из следующих путей:

• размещения информационного сообщения на официальном сайте Банка www.ribank.ru

• рассылкой сообщений через Систему,

• размещения информации на информационном стенде в помещении Банка. Дополнительно указанная информация может доводиться до сведения Клиента любым иным способом по усмотрению Банка.

10.8. Банк вправе устанавливать ограничения на сумму операций, совершаемых Клиентом в Системе;

10.9. Банк вправе отказать Клиенту в совершении операции, в случае обнаружения операций, не соответствующих настоящим Условиям или действующему законодательству;

10.10. Клиент уполномочивает Банк в случае компрометации Средств доступа или SMS-ключей/Кодовой даты либо обнаружения незаконно проводимых операций или возникновения у Банка подозрений в незаконности проводимых посредством Системы, приостановить доступ Клиента к Системе и не исполнять его распоряжения до полного выяснения обстоятельств;

10.11. Банк вправе приостановить дистанционное обслуживание Клиента в Системе в одностороннем порядке, если Клиент нарушает порядок использования систем, предусмотренный настоящими Условиями.

ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ ВОЗНИКАЮЩИХ В ХОДЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

11.1. Споры, возникающие в ходе электронного документооборота между Клиентом и Банком следующего характера:

11.1.1. оспаривание факта формирования Клиентом или Банком электронного документа;

11.1.2. оспаривание времени и даты отправки\доставки электронного документа одной из сторон;

11.1.3. заявление одной из сторон об искажении электронного документа;

11.1.4. другие споры требующие проверки подлинности ЭЦП, передаются на рассмотрение Комиссии, формируемой на основании письменного заявления Клиента или Банка другой Стороне.

11.2. В состав Комиссии входят в равных количествах представители Сторон.

11.3. Основанием для проведения разбора конфликтных ситуаций является письменное заявление от одной из Сторон направленное в адрес другой Стороны, о возникновении конфликтной ситуации.

11.4. Целью проведения разбора конфликтной ситуации является подтверждение или не подтверждение подлинности ЭЦП под документом, являющимся предметом спора Сторон.

11.5. Рассмотрение конфликтных ситуаций выполняется специально создаваемой Комиссией, состоящей из представителей Банка и представителей Клиента, при необходимости могут быть дополнительно привлечены специалисты Удостоверяющего центра и / или Оператора Системы.

11.6. Все виды конфликтных ситуаций, описываемых в данном документе, связаны с доказательством целостности, подлинности электронных документов, факте, либо времени его получения или отправки.

11.7. Электронный документ считается подлинным, если он был одной Стороной надлежащим образом сформирован, подписан и отправлен, а другой Стороной - получен, проверен и принят. Свидетельством факта получения документа является наличие уведомления о получении электронного документа, сформированного и отправленного системой Клиент-Банк. Свидетельством времени получения, отправки или факта подписания электронного документа является метка времени в электронном документе, содержащая время системы Клиент-Банк и связанная с использованием криптографических протоколов с электронным документом, для которого требуется освидетельствование.

11.8. Комиссия по разбору конфликтных ситуаций создается по письменному заявлению одной из участвующих в конфликте Сторон не позднее 5 (Пять) рабочих дней с момента получения Стороной письменного заявления для разрешения конфликтов, предметом которых являются:

11.8.1. отказ подписывающей Стороны от факта подписи электронного документа;

11.8.2. отказ подписывающей Стороны от содержания электронного документа;

11.8.3. отказ Стороны-получателя электронного документа от факта получения электронного документа;

11.8.4. отказ Стороны-отправителя электронного документа от факта отправки электронного документа;

11.8.5. отказ Стороны-получателя электронного документа от времени получения электронного документа;

11.8.6. отказ Стороны-отправителя электронного документа от времени отправки электронного документа.

11.9. Комиссия созывается Банком. В состав Комиссии входят равное количество представителей Сторон. Рекомендуемым числом членов Комиссии с каждой стороны является по 3 человека: 2 человека представляют руководство и финансовое подразделение, 1 человек – службу информационных технологий. Комиссия осуществляет свою работу на территории Банка.

11.10. До подачи заявления, заявитель должен убедиться, что причиной возникновения конфликта не является нарушение целостности программного обеспечения, произошедшего в результате сбоев аппаратуры, действия компьютерных вирусов или троянских программ.

11.11. Для участия в работе Комиссии, представители Сторон должны иметь с собой Акт приема-передачи сертификата ключа и ключевой носитель, на котором хранится закрытый ключ ЭЦП.

11.12. Для работы Комиссии Банк предоставляет необходимое оборудование и программное обеспечение.

11.13. Перед проведением разбора конфликтной ситуации, Комиссия проверяет ЭЦП сертификатов ключей Сторон, для чего из архива сертификатов получаются эталонные копии сертификатов, и Комиссия сверяет их с сертификатами представленными сторонами. 9.14. Проверка подлинности документа, подписанного закрытым ключом ЭЦП и достоверность идентификации Сертификата, выполняются с использованием Эталонного Модуля Проверки подписи документа, хранящегося у Удостоверяющего центра. Результатом работы Эталонного Модуля Проверки является:

11.14.1. установление факта создания спорного документа с использованием Системы;

11.14.2. установление факта подписи спорного документа в соответствии с технологией Системы;

11.14.3. установление факта целостности спорного документа.

11.15. Подтверждение подлинности ЭЦП под спорным документом означает, что документ действительно подписан владельцем закрытого (секретного) ключа ЭЦП и электронный документ юридически тождественен аналогичному документу на бумажном носителе заверенному подписью уполномоченных лиц и печатью Стороны-отправителя документа.

11.16. Не подтверждение подлинности ЭЦП под спорным документом означает, что электронный документ не имеет юридической силы.

11.17. После проведения разбора конфликтной ситуации, Комиссия составляет протокол проверки. Решение Комиссии в виде Акта, отражающего результаты проверки, оформляются в письменном виде и подписывается собственноручно членами Комиссии. Решение Комиссии является окончательным и пересмотру не подлежит. Действия, вытекающие из решения, являются обязательными для обеих Сторон конфликта.

11.18. Возмещение пострадавшей Стороне принесенного ущерба выполняется в установленном действующим законодательством Российской Федерации порядке.

ОТВЕТСТВЕННОСТЬ СТОРОН

12.1. За неисполнение или ненадлежащее исполнение обязательств по Договору ДБО Стороны несут ответственность в соответствии с действующим законодательством.

12.2. Банк несет ответственность за несоблюдение сроков проведения операций по счету Клиента на основании надлежащим образом оформленных и своевременно доставленных документов Клиента в соответствии с действующим законодательством и Договором банковского счета.

12.3. Каждая из Сторон несет ответственность за достоверность информации, представляемой по Системе другой Стороне.

12.4. Банк не несёт ответственности за списание средств со счёта Клиента, не подтверждённое в последствии документально, при условии, что электронные документы Клиентом были составлены правильно, а также, если Банк не был своевременно информирован о смене лиц, имеющих право первой, второй подписи на платежных документах.

12.5. Банк не несет ответственность за задержку и/или искажение ЭД, возникающие по не зависящим от Банка причинам в сетях передачи данных, используемых в Системе, и находящихся вне компетенции Банка, а также вследствие выхода из строя технических средств и общесистемного программного обеспечения, установленных Клиентом на своем АРМ.

12.6. Сторона не несет ответственность за убытки другой Стороны, возникшие вследствие несвоевременного сообщения другой Стороной о компрометации ее ключей ЭЦП.

12.7. Банк не несет ответственности за наступившие негативные последствия для Клиента в случае несвоевременного прочтения полученных им информационных сообщений, переданных Банком через Систему.

12.8. Стороны не несут ответственности за неисполнение или ненадлежащее исполнение обязательств в соответствии с настоящими Условиями, если надлежащее исполнение оказалось невозможным вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств. К таким обстоятельствам относятся: стихийные бедствия (землетрясение, наводнение, ураган и т.д.), обстоятельства общественной жизни (военные действия, террористические акты, пожары, эпидемии, забастовки и т.д.), введение чрезвычайного положения уполномоченными органами Российской Федерации и/или субъектов Российской Федерации при условии, что такие обстоятельства непосредственно повлияли на выполнение обязательств по Договору о ДБО, запретительные меры государственных органов, принятие решений органами государственной власти (законодательной и/или исполнительной) Российской Федерации, которые делают невозможным для одной из Сторон продолжать исполнение своих обязательств по Договору о ДБО, сбои и повреждения электрических и телефонных сетей, компьютерных систем и т.д. При этом срок исполнения обязательств отодвигается соразмерно времени, в течение которого действовали такие обстоятельства, если исполнение обязательств остается возможным.

ПРОЧИЕ УСЛОВИЯ

13.1. Договор о ДБО вступает в силу с момента его подписания Банком подписанного Клиентом Заявления о присоединении к Условиям и действует в течение срока действия Договоров банковского счета по всем счетам Клиента, указанным в названном Заявлении о присоединении к Условиям, или иного договора в рамках исполнения которого была установлена Система либо до расторжения Договора о ДБО.

13.2. Если ни одна из Сторон письменно не заявит о своем желании его расторгнуть Договор о ДБО за 10 (Десять) рабочих дней до таты истечения срока его действия, то Договор автоматически продлевается (пролонгируется) на каждый последующий календарный год.

13.3. Стороны вправе расторгнуть Договор о ДБО в одностороннем порядке. Сторона, инициирующая расторжение обязана письменно уведомить об этом другую Сторону не позднее, чем за 10 (Десять) рабочих дней до предполагаемой даты расторжения. Кроме того, настоящий Договор автоматически (без направления Сторонами друг другу соответствующих письменных уведомлений) прекращается в следующих случаях:

- в связи с прекращением деятельности одной из Сторон – в дату прекращения деятельности Стороны, определяемую в соответствии с законодательством Российской Федерации;
- в связи с закрытием всех Счетов Клиента, подключенных к Системе – в дату закрытия последнего Счета Клиента, подключенного к Системе;
- в иных случаях, предусмотренных действующим законодательством Российской Федерации.

13.4. Односторонний отказ от исполнения настоящих Условий допускается в случаях, установленных действующим законодательством Российской Федерации и настоящими Условиями.

13.5. Все другие конфиденциальные сведения хранятся и уничтожаются Сторонами в соответствии с порядком и сроками хранения и уничтожения документов, установленных действующим законодательством Российской Федерации.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА КЛИЕНТОВ

14.1. Клиент вправе обратиться для получения необходимых консультаций, технической и методической помощи в работе с Системой по телефонам, указанным на сайте Банка (www.ribank.ru) в рабочее время. Дистанционные консультации по телефону оказываются бесплатно.

14.2. Клиент вправе вызвать сотрудника Банка в свой офис для настройки Системы и обучения принципам работы в Системе. Данные услуги оказываются Банком при наличии у Банка возможности и оплачиваются отдельно.