ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

1. ИСПОЛЬЗУЕМЫЕ ПОНЯТИЯ И ТЕРМИНЫ

Договор – договор присоединения в соответствии со ст.428 ГК РФ между «Северный Народный Банк» (АО) (далее Банк) и Клиентом, состоящий из настоящих Правил с соответствующими приложениями и Заявления «На подключение счета к Системе дистанционного банковского обслуживания».

Клиент – юридическое лицо, индивидуальные предприниматель, физическое лицо, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее с банком договор об открытии счета соответствующего вида, по которому Банком предоставляется услуга Дистанционного банковского обслуживания.

Система дистанционного банковского обслуживания (далее Система ДБО) – корпоративная информационная Система Банка, представляющая собой совокупность программно-аппаратных средств, устанавливаемых у Клиента и у Банка с целью организации электронного документооборота с возможностью автоматизации расчетов посредством обработки ЭД, подписания их ЭП и проверки ЭП (электронного расчетно-кассового обслуживания).

Система электронного расчетно-кассового обслуживания «Интернет-Клиент» (далее Система «Интернет-Клиент») – Система ДБО, использующая для соединения с Банком сеть Интернет (минимальная скорость передачи данных не ниже 128 Kbps), клиентское программное обеспечение которой функционирует через веб-браузеры: Microsoft Internet Explorer, Chrome, Firefox, Opera или Safari и устанавливается при первом входе в систему (URL-адрес сайта Системы **https://dbo.sevnb.ru**).

Работа клиентского программного обеспечения Системы ДБО обеспечивается в операционных средах, которые поддерживают работу браузеров Microsoft Internet Explorer, Chrome, Firefox, Opera или Safari при использовании лицензионного программного обеспечения и настройке операционной системы, дополнительных компонентов, политики безопасности в соответствии с требованиями согласно Приложению 1 к настоящим Правилам. В случае использования операционной системы семейства Windows версия должна быть не ниже 7. Обязательно наличие устройства для подключения ключевого носителя - порта USB не ниже 2.0. Работа клиентского программного обеспечения Системы ДБО в иных системах поддерживается при условии совместимости с Системой ДБО.

Под обработкой ЭД понимается отправка ЭД Клиентом, отправка подтверждений на принятые Банком ЭД Клиента, вывод ЭД на печать и др.

Безопасность информации – состояние информации, информационных ресурсов и информационных систем, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, копирования, блокировки, нарушения конфиденциальности, доступности, достоверности и т.п.; состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних и внешних угроз.

Достоверность информации – состояние информации, информационных ресурсов и информационных систем, при котором обеспечивается отсутствие искажения, модификации, подделки, и иного изменения информации лицами, не имеющими соответствующих полномочий.

Электронный документ (далее 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 информационно-телекоммуникационным сетям или обработки в информационных системах. В Системе ДБО под электронными документами понимаются оформленные в соответствии с требованиями Центрального банка РФ платежные документы и согласованные Сторонами документы, необходимые для расчетно-кассового обслуживания и валютного контроля.

Электронная подпись (далее ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В соответствии с видами электронной подписи, установленными Федеральным законом от «6» апреля 2011 года №63-ФЗ «Об электронной подписи» (далее – Закон) в настоящих Правилах под ЭП понимается и используется в системе электронных расчетов усиленная неквалифицированная электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после его подписания; создается с использованием средств электронной подписи.

Удостоверяющий центр (далее УЦ) – Банк, осуществляющий функции по заверению сертификатов ключей проверки ЭП, а также иных функций, предусмотренных Законом.

Уполномоченное лицо (администратор) удостоверяющего центра – физическое лицо, являющееся работником УЦ и наделенное полномочиями по заверению сертификатов ключей проверки ЭП и отзыву сертификатов ключей проверки ЭП, а также иными полномочиями, предусмотренными действующим законодательством.

Средства УЦ – программные и (или) аппаратные средства, используемые для реализации функций УЦ.

Средство криптографической защиты информации (далее СКЗИ) – предназначено для электронной подписи файлов с целью подтверждения подлинности информации и ее авторства и шифрования этих файлов при передаче по открытым каналам связи для обеспечения конфиденциальности.

Средства ЭП – СКЗИ, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание секретного ключа ЭП и ключа проверки ЭП.

Владелец сертификата ключа проверки ЭП – физическое лицо, являющееся владельцем счета или физическое лицо, действующее от имени владельца счета, обладающее правом распоряжения денежными средствами с правом подписи финансовых документов, которое владеет соответствующим секретным ключом ЭП, позволяющим с помощью средств ЭП создавать ЭП в электронных документах (подписывать ЭД) и которому в установленном порядке заверен сертификат ключа проверки ЭП.

Ключевой носитель – машинный носитель информации (электронный идентификатор Rutoken, имеющий индивидуальный серийный номер), содержащий секретный ключ ЭП.

Ключ ЭП (секретный ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП.

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с секретным ключом ЭП и предназначенная для проверки подлинности ЭП.

Генерация ключа – операция, предусмотренная СКЗИ, результатом которой является выработка секретного ключа ЭП, ключа проверки ЭП.

Реквизиты персонального пароля – уникальные последовательности символов (логин, пароль и идентификатор), генерируемые для каждого Пользователя Клиента, благодаря которым становится возможным вход Пользователя в Систему «Интернет-Клиент» и самостоятельная генерация Пользователем секретного ключа ЭП или доступ в Информационный сервис.

Сертификат ключа проверки ЭП – электронный документ, подписанный ЭП уполномоченного лица УЦ, или документ на бумажном носителе, выданные УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Подтверждение подлинности ЭП (далее проверка ЭП) – положительный результат проверки средством ЭП с использованием сертификата ключа проверки ЭП принадлежности ЭП в электронном документе владельцу сертификата ключа проверки ЭП и отсутствия искажений в подписанном данной ЭП электронном документе.

Компрометация секретных ключей ЭП – утрата секретных ключей ЭП и (или) ключевых носителей (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение сотрудника – владельца сертификата ключа проверки ЭП, заражение вирусом компьютера, на котором функционируют средства ЭП, или обнаружение на нем

вредоносных программ, а также любые другие виды нарушения безопасности информации, в результате которых секретные ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам.

Информационный сервис – сервис доступа Клиента к системе «Интернет-Клиент» с возможностью просмотра выписки по подключенным к системе счетам, а также возможность запроса выписки. Возможность совершать расходные операции по расчетному счету, а также обмениваться информацией с Банком посредством произвольных документов отсутствует, наличие USB порта и использование ключей ЭП не требуется.

Пользователь – уполномоченное лицо Клиента, которому на основании предоставленного в Банк Заявления на подключение счета к Системе ДБО или Заявления на подключение дополнительных пользователей (Приложение 2) предоставлен доступ к Системе ДБО.

Оперативное информирование о расходных операциях – бесплатная услуга, заключающаяся в отправке СМС-сообщений и (или) сообщений по электронной почте, содержащих реквизиты платежных документов по расходным операциям. Подключение услуги осуществляется на основании Заявления о присоединении к настоящим Правилам или на основании Заявления на подключение (Приложение 3), которое содержит параметры информирования (номер телефона, адрес электронной почты, формат сообщений). Отключение от услуги осуществляется на основании Заявления на отключение (в произвольной форме).

2. ПРЕДМЕТ ДОГОВОРА

2.1. Настоящим Договором Стороны признают юридическую силу электронных документов, подписанных ЭП соответствующей Стороны с использованием средств ЭП, созданных в соответствии с действующим законодательством об электронной подписи и средствах криптографической защиты информации.

2.2. В Системе ДБО принимаются к исполнению распоряжения о переводе денежных средств, оформленные в соответствии с действующим законодательством и необходимые для проведения операций по счетам Клиента. Для проведения операций по счету Клиента, открытому в Банке, используются полноформатные электронные документы, содержащие все реквизиты платежного документа на бумажном носителе.

При обслуживании в Системе ДБО валютных счетов Клиента, Сторонами допускается обмен электронными документами, оформляемыми при совершении валютных операций в соответствии с банковским законодательством и законодательством о валютной регулировании и валютном контроле.

2.3. Формат электронных документов определяется Банком и передается Клиенту вместе с программным обеспечением Системы ДБО.

2.4. В Системе ДБО Банком не принимаются к исполнению ЭД, направленные на возникновение, прекращение, изменение между Банком и Клиентом иных обязательств, не оговоренных настоящими Правилами.

Не принимаются сканированные копии документов, которые должны быть представлены в копиях заверенных в соответствии с действующим законодательством. Исключение составляют сканированные копии документов, обязанность предоставления которых предусмотрена действующим законодательством.

2.5. Электронные документы, принятые Банком **до 17.00 ч. по московскому времени**, считаются поступившими в пределах операционного дня. Электронные документы, поступившие **после 17.00 ч**, считаются поступившими на следующий операционный день. Временем отправки (или получения) файлов ЭД является время завершения операции записи ЭД в базу данных.

2.6. Используемый в Системе ДБО сертификат ключа проверки ЭП должен быть создан исключительно средствами ЭП, используемыми в данной Системе ДБО (для обеспечения программной и технологической совместимости).

2.7. Стороны признают, что средства УЦ и средства ЭП, применяемые в Системе ДБО, при их использовании в соответствии с мерами по обеспечению безопасности информации, предусмотренными в настоящих Правилах, не нарушают достоверность информации, обрабатываемой с их помощью.

2.8. Передача ключевого носителя и реквизитов персонального пароля производится непосредственно лицу, указанному в заявлении на подключение счета (заявлении на подключение пользователя) к Системе ДБО. Ключевой носитель на каждое физическое лицо выдается в единственном экземпляре. Обладание одним физическим лицом несколькими секретными ключами ЭП с правом подписи ЭД не допускается.

2.9. Формирование секретных ключей ЭП Клиента производится исключительно самим Клиентом, таким образом, что единственным владельцем секретного ключа ЭП является лицо, его сформировавшее. Сведения о секретном ключе ЭП в Банке отсутствуют. Ключи проверки ЭП, хранящиеся в Банке, не могут быть использованы для подписи ЭД или восстановления (вычисления) сгенерированных Клиентом секретных ключей ЭП.

2.10. Подключение каждого счета Клиента к Системе ДБО производится на основании отдельного Заявления «На подключение счета к Системе дистанционного банковского обслуживания».

2.11. В Системе ДБО не установлены ограничения по параметрам операций при направлении ЭД. Клиент может установить перечень ограничений при работе с системой «Интернет-клиент», заполнив заявление на установку ограничений в системе дистанционного банковского обслуживания (ДБО) (Приложение 4). Ограничения на операции начинают действовать не ранее второго операционного дня после регистрации заявления в Банке.

2.12. Приостановление/возобновление обслуживания счета в Системе ДБО осуществляется Банком по заявлению Клиента (Приложение 6,7) в порядке, предусмотренном настоящими правилами. В период приостановления комиссия за обслуживания счета в Системе ДБО Банком не взимается, за исключением месяцев, в которых были поданы заявления о приостановлении/возобновлении обслуживания счета в Системе. Пересчет комиссии за месяц, в котором было подано заявление о приостановлении/возобновлении обслуживания счета в системе ДБО, Банком не производится и уплачивается Клиентом в полном размере.

3. ОБЯЗАТЕЛЬСТВА СТОРОН

3.1. Банк обязуется:

3.1.1. Передать Клиенту по Акту приема-передачи при подключении:

3.1.1.1. Зарегистрированный в Системе «Интернет-Клиент» носитель ключа ЭП;[1]

3.1.1.2. Реквизиты персонального пароля.

3.1.2. Хранить не менее трех лет материалы по предмету Договора для разрешения споров, в том числе:

3.1.2.1. Файлы ЭД, полученные от Клиента.

3.1.2.2. Сертификат ключа проверки ЭП в бумажном виде и в форме электронного документа.

3.1.3. Принимать к исполнению ЭД, подлинность которых подтверждена положительным результатом проверки ЭП Клиента, за исключением случаев, оговоренных п. 3.3. настоящих Правил.

3.1.4. Немедленно сообщить Клиенту о факте не подтверждения подлинности его ЭП, посредством уведомления в Системе ДБО.

3.1.5. Информировать Клиента посредством Системы ДБО о принятии (непринятии) документов в электронном виде с указанием в уведомлении даты отправления и датой принятия (непринятия) сообщения, причиной отказа в принятии.

3.1.6. Информировать Клиента о проведенных по счету операциях, в том числе с использованием ЭД, путем направления по Системе ДБО электронной выписки на следующий операционный день, следующий за днем передачи ЭД в Банк, после 9.30 утра.

3.1.7. Приостановить/возобновить обслуживание счета в Системе ДБО на следующий день со дня указанного в заявлении Клиента в порядке, предусмотренном настоящими Правилами.

[1] В случае использования клиентом информационного сервиса носитель ключа ЭП не передается

3.2. Клиент обязуется:

3.2.1. Знакомиться с изменениями и дополнениями, внесенными в настоящие Правила и Тарифы Банка, актуальной эксплуатационной документацией Системы ДБО. Не реже одного раза в календарном месяце обращаться в Банк или на сайт Банка **www.sevnb.ru** для получения информации о внесенных изменениях в настоящие Правила и Тарифы. При несогласии с внесенными изменениями Клиент уведомляет об этом Банк в письменной форме в течение 5-ти дней с момента ознакомления.

3.2.2. Соблюдать установленные Банком форматы ЭД.

3.2.3. Соблюдать регламент отправки ЭД.

3.2.4. Исключить доступ к ключевому носителю и Реквизитам персонального пароля неуполномоченных лиц.

3.2.5. Не передавать, не копировать, не разглашать секретный ключ ЭП третьим лицам.

3.2.5.1. Не передавать Ключевой носитель третьим лицам и не совершать с ним иные действия, влекущие наступление административной или уголовной ответственности, в том числе предусмотренной ст. 187 УК РФ.

3.2.6. Клиент самостоятельно осуществляет установку и настройку Системы ДБО, а также последующую генерацию секретного ключа ЭП на принадлежащем ему оборудовании, согласно пользовательской документации.

3.2.6.1. Доступ к документации Системы «Интернет-Клиент» осуществляется посредством сайта **https://dbo.sevnb.ru**.

3.2.7. Обновлять компоненты Системы ДБО.

3.2.8. Принять меры по обеспечению безопасности информации, обрабатываемой посредством составляющих Системы ДБО, расположенных на его территории, не противоречащие действующему законодательству и положениям настоящих Правил, достаточные для недопущения и (или) нейтрализации последствий рисков, указанных в пункте 6.3 настоящих Правил.

3.2.9. Рассматривать всю информацию, полученную от Банка в ходе выполнения Договора, (за исключением сведений, доступ к которым не может быть ограничен в соответствии с законодательством) как конфиденциальную и не использовать ее в целях иных, чем определено условиями Договора.

3.2.10. Обязательства по сохранению конфиденциальности имеют силу после истечения срока действия Договора или его досрочного расторжения в течение последующих трех лет.

3.2.11. При не подтверждении подлинности ЭП полученных из Банка ЭД, сохранить эти документы с одновременным сообщением об этом в Банк.

3.2.12. При возникновении споров, связанных с использованием Системы ДБО, предоставлять по письменному запросу Банка все необходимые документы.

3.2.13. Немедленно уведомить Банк о прекращении полномочий владельца сертификата ключа проверки ЭП и не осуществлять отправку в Банк ЭД, подписанных ЭП владельца сертификата ключа проверки ЭП, не обладающего соответствующими полномочиями.

3.2.14. Не реже одного раза в течение рабочего дня проверять исполнение Банком платежных ЭД и проведение операций по счету в соответствии с информацией, представленной Банком в соответствии с пунктом п. 3.1.6 или содержащейся в самостоятельно запрашиваемой Клиентом выписке по Системе ДБО.

3.2.15. Не передавать клиентское программное обеспечение Системы ДБО и права по Договору третьим лицам.

3.2.16. В случае компрометации секретных ключей ЭП, а также при возникновении подозрений о возможном нарушении безопасности Системы ДБО:

3.2.16.1. Немедленно сообщить об этом в УЦ Банка по телефонам 40-97-07, 40-97-03, 40-95-95, 40-97-25 или явиться лично, после чего в исполнении всех электронных документов Клиента, переданных по системе Интернет-Клиент, будет отказано. Любая информация, переданная Клиентом по Системе ДБО с использованием скомпрометированных секретных ключей ЭП Банком, игнорируется. Возобновление работы в Системе ДБО возможно только с санкции Банка после выдачи Клиенту новых ключей ЭП.

3.2.16.2. Представить в Банк письменное уведомление, содержащее изложение обстоятельств, относящихся к случаю компрометации ключей ЭП или подозрений о возможном нарушении безопасности Системы ДБО, а также Заявление об отзыве соответствующих сертификатов ключей проверки ЭП (Приложение 5).

3.2.17. Клиент обязуется использовать средства ЭП и обеспечить выполнение Пользователями в соответствии с правилами пользования ими и положениями Договора, а также принимать меры по обеспечению безопасности информации при работе в Системе ДБО согласно Приложению 1 к настоящим Правилам.

Клиент обязуется обеспечить выполнение указанных правил и требований уполномоченными Пользователями.

3.2.18. При расторжении Договора вернуть Банку переданные во временное пользование носители (или возместить их стоимость согласно Тарифам Банка), удалить (уничтожить) все экземпляры переданного по Договору программного обеспечения Системы ДБО (в том числе СКЗИ).

3.2.19. Не осуществлять в отношении клиентского программного обеспечения, его модулей и подсистем, а также СКЗИ:

3.2.19.1. Декомпилирование и (или) изучение кода, его модификацию или улучшение.

3.2.19.2. Использование не в составе соответствующей Системы ДБО.

3.2.19.3. Передачу третьим лицам каких-либо прав не в составе соответствующей Системы ДБО.

3.2.19.4. Не использовать каким-либо образом компоненты, модули и подсистемы программного обеспечения Системы ДБО в других программах для ЭВМ.

3.2.20. Проводить плановую замену секретных ключей ЭП и соответствующих им ключей проверок ЭП один раз в год.

3.2.21. Владелец сертификата ключа проверки ЭП при подаче Сертификата ключа проверки ЭП на бумажном носителе обязан явиться в Банк (Филиал Банка), имея при себе документ, удостоверяющий личность и собственноручно подписать бланк Сертификата в присутствии уполномоченного сотрудника Банка.

3.3. **Права Банка:**

3.3.1. Банк вправе не принять к исполнению ЭД или не исполнить принятый ЭД в случаях:

3.3.1.1. Наличии сомнений в полномочиях владельца сертификата ключа проверки ЭП.

3.3.1.2. При получении сообщения о возможной компрометации ключей ЭП в соответствии с п. 3.2.16. настоящих Правил.

3.3.1.3. При несоответствии ЭД формату, установленному Банком.

3.3.1.4. В иных случаях, предусмотренных действующим законодательством.

3.3.2. Запрашивать у Клиента документы при возникновении спорных ситуаций при исполнении Договора.

3.3.3. Расторгнуть в одностороннем порядке Договор при нарушения Клиентом условий настоящих Правил.

3.3.4. Банк вправе обновлять компоненты Системы ДБО.

3.3.5. Банк вправе изменять Тарифы за использование Системы ДБО и за предоставляемые услуги.

3.4. Права Клиента:

3.4.1. Клиент вправе, но не чаще чем 1 раз в год, обратиться в Банк с заявлением о приостановлении обслуживания счета в системе ДБО в порядке, предусмотренном настоящими Правилами. При этом приостановление обслуживания счета в системе ДБО не приостанавливает течение срока действия ключа ЭП.

4. ПОРЯДОК ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

4.1. Проверка ЭП в ЭД, передаваемых Сторонами Договора в Системе ДБО, является обязательной и осуществляется средствами ЭП автоматически при поступлении новых ЭД, результат проверки ЭП храниться в лог-файле Системы ДБО.

4.1.1. В Системе «Интернет-Клиент» проверка ЭП проводится автоматически, результат проверки ЭП можно получить, воспользовавшись кнопкой в панели инструментов «Проверка подписи» у конкретного ЭД.

4.2. Исходными данными для процедуры проверки ЭП являются:

4.2.1. ЭД, переданный одной из Сторон в формате Системы ДБО и подписанный ее ЭП.

4.2.2. Сертификат ключа проверки ЭП Стороны, подписавшей ЭД.

4.3. ЭП в электронных документах, передаваемых Сторонами Договора в Системе ДБО, признается действительной при одновременном соблюдении следующих условий:

4.3.1. Сертификат ключа проверки ЭП заверен УЦ Банка.

4.3.2. Сертификат ключа проверки ЭП действителен на момент подписания ЭД.

4.3.3. Положительный результат проверки принадлежности сертификата ключа проверки ЭП участнику Системы ДБО.

4.3.4. Подтверждено отсутствие изменений, внесенных в ЭД, после его подписания.

4.4. Проверка ЭП должна осуществляться средствами ЭП в соответствии с правилами пользования ими.

5. УСЛОВИЯ ОПЛАТЫ

5.1. За обслуживание в Системе ДБО счетов взимается ежемесячная абонентская плата за каждый подключенный к Системе ДБО счет согласно действующим Тарифам Банка.

5.2. Оплата происходит путем списания денежных средств со счета Клиента. При подключении к Системе ДБО нескольких счетов, Банк вправе списать денежные средства с любого счета (счетов), на котором(ых) имеются средства.

5.3. В случае невозможности взимания (списания) платы из-за отсутствия средств на счете Клиента в течение 30 календарных дней, Банк вправе расторгнуть Договор. При этом Банк отправляет по Системе ДБО требование об оплате задолженности. При невыполнении Клиентом данного требования по оплате в течение 5-дней со дня его направления Договор считается расторгнутым, и Клиент отключается от Системы ДБО.

6. ФОРС-МАЖОР И РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ЭП

6.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств, если это неисполнение явилось следствием обстоятельств непреодолимой силы, а также действий и решений высших государственных органов, забастовок, военных действий любого характера, возникших после заключения Договора.

6.2. Сторона, ссылающаяся на форс-мажорные обстоятельства, обязана в течение двух банковских дней письменно информировать другую Сторону о наступлении подобных обстоятельств.

6.3. Клиент несет все возможные неблагоприятные последствия (риски), связанные с использованием электронной подписи, в том числе:

6.3.1. Риски, возможные при хищении или утере секретного ключа ЭП.

6.3.2. Риски, возможные при получении доступа третьих лиц к информационным системам, в которых используется секретный ключ ЭП.

6.3.3. Риски, возможные при нецелевом использовании сертификата ключа проверки ЭП при подписании электронной подписью документов организации.

6.3.4. Риски, возможные при отказе от оперативного информирования Клиента о расходных операциях.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Ответственность за содержание, полноту и правильность оформления ЭД несет Сторона, составившая и подписавшая указанный документ своей ЭП.

7.2. Клиент несет ответственность за действия в Системе уполномоченных им Пользователей.

7.3. Банк не несет ответственности за техническое состояние компьютерного оборудования Клиента, возможные технические помехи в телефонных линиях и (или) каналах связи, предоставляемых сторонними организациями (провайдерами связи), прекращение использования Системы ДБО из-за отключения электроэнергии и (или) по иным техническим причинам, не зависящим от Банка, а также за последствия, которые являются следствием неприменения Клиентом мер по обеспечению информационной безопасности при работе с Системой ДБО.

7.4. Банк не несет ответственности за проверку регистрационных данных указанного Клиентом номера телефона, в частности за проверку факта принадлежности номера телефона Клиенту.

7.5. Банк не несет ответственности за доставку и скорость передачи SMS-сообщений и (или) уведомлений по электронной почте и не гарантирует сохранение конфиденциальности и целостности передаваемой с их помощью информации.

7.6. Банк не несет ответственность за убытки, возникшие у Клиента вследствие непринятия к исполнению или при отказе в исполнении ЭД.

8. РАЗРЕШЕНИЕ СПОРОВ

8.1. Споры и разногласия разрешаются Сторонами путем переговоров в разумные сроки.

8.2. Обязанность по доказыванию обстоятельств повлекших возникновение убытков лежит на Стороне, которой эти убытки причинены.

8.3. Если Стороны не пришли к взаимному согласию, спор передается в Арбитражный суд РК, при этом ЭД признаются Сторонами в качестве доказательств, наравне с документами на бумажных носителях.

8.4. Ответственность за действия (бездействие) в результате которых ключевой носитель (секретный ключ ЭП) стал известен неуполномоченным лицам и последствия таких действий (бездействия) несет владелец сертификата ключа проверки ЭП.

9. СРОК ДЕЙСТВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА

9.1. Договор считается заключенным с момента подписания его Сторонами и действует до его расторжения Сторонами.

9.2. В случае отключения (снятия) всех счетов Клиента с обслуживания по Системам ДБО, Договор считается расторгнутым.

9.3. Любая из Сторон вправе расторгнуть Договор в любое время, предупредив об этом другую Сторону письменно не мене чем за пять календарных дней до предполагаемой даты расторжения Договора. До даты расторжения Договора Клиент обязан оплатить задолженность перед Банком, возникшую вследствие исполнения Договора.

9.4. При несогласии Клиента с внесенными изменениями в Тарифы Банка Договор считается расторгнутым с момента поступления в Банк уведомления Клиента, направленного в соответствии с п. 3.2.1.

КЛИЕНТ:

Наименование:

ИНН_____, КПП _____

Юридический адрес: _____

Телефон: _____

Р/с № _____ в «Северный Народный Банк» (АО)

С вышеуказанными Правилами ознакомлен и полностью согласен

_____

(подпись)

М.П.

Правила использования СКЗИ и ЭП

1. Общие положения

Средства криптографической защиты информации (СКЗИ) предназначены для подписи файлов электронной подписью (ЭП) с целью подтверждения подлинности информации и ее авторства (данные СКЗИ называются также средствами ЭП) и шифрования этих файлов при передаче по открытым каналам связи для обеспечения конфиденциальности.

По истечении срока действия ключей ЭП Клиент обязан обратиться в УЦ Банка для их замены.

Переданные в рамках Договора средства ЭП и СКЗИ не предназначены для обработки сведений, составляющих государственную тайну и не подлежат использованию для их обработки.

Клиент обязуется осуществлять использование СКЗИ в соответствии с настоящими Правилами использования СКЗИ и ЭП и эксплуатационно-технической документацией к нему.

Клиент обязуется осуществлять хранение файлов регистрации (протоколов, журналов, лог-файлов) событий операционной системы и приложений, СКЗИ (Криптоплагина) и т.д. на рабочих местах, с которых осуществлялся доступ в Систему, в течение 1 года с момента последнего доступа.

2. Работа со средствами ЭП и СКЗИ

Для работы со средствами ЭП и СКЗИ привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации-Клиента. Должностные лица, уполномоченные данным приказом и эксплуатирующие СКЗИ, использующие секретные ключи ЭП (далее - Пользователи), несут персональную ответственность за: сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы со средствами ЭП и СКЗИ; сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭП; сохранность ключевых носителей и других документов, выдаваемых с ключевыми носителями.

Клиент должен обеспечить условия хранения и использования ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования информации ключевого носителя и паролей.

Не допускается:

а) Разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным, выводить содержимое ключевых носителей на дисплей и принтер, или копировать его на другие носители;

б) Вставлять ключевой носитель в компьютер при проведении работ, не являющихся штатными процедурами использования ключей (шифрование и (или) расшифровывание информации, проверка ЭП и т.д.), а также в другие компьютеры, не предназначенные для работы с Системой ДБО;

в) Записывать на ключевой носитель постороннюю информацию;

г) Вносить какие-либо изменения в программное обеспечение (далее ПО) СКЗИ и средств ЭП;

д) Использовать бывшие в работе ключевые носители для записи посторонней информации;

2.1. Правила эксплуатации и хранения электронного идентификатора Rutoken.

а) Оберегайте электронный идентификатор от механических воздействий (падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения; все это может привести к его поломке.

б) Не прилагайте излишних усилий при подсоединении устройства к порту компьютера.

в) Не допускайте попадания на электронный идентификатор (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема примите меры для их очистки. Для очистки корпуса и разъема устройства используйте сухую ткань. Использование органических растворителей недопустимо.

г) Не разбирайте электронный идентификатор! Такие действия могут привести к поломке корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие, к ненадежной работе или выходу из строя самого идентификатора.

д) Разрешается подключать идентификатор только к исправному оборудованию. Параметры USB порта должны соответствовать спецификации для USB.

е) Запрещается использовать длинные переходники или USB хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для идентификатора, может подаваться несоответствующее напряжение.

ж) Запрещается извлекать электронный идентификатор из порта компьютера, если на устройстве моргает индикатор, поскольку это обозначает работу с данными и прерывание работы может негативно сказаться как на данных, так и на работоспособности идентификатора.

з) Запрещается оставлять идентификатор подключенным к компьютеру во время перезагрузки, ухода в спящий или ждущий режимы, поскольку в это время возможны перепады напряжения на USB порте и, как следствие, выход устройства из строя.

и) Запрещается оставлять идентификатор подключенным к компьютеру, когда необходимость в работе с ЭП и СКЗИ отсутствует.

к) Рекомендуется отключать другие USB устройства на время работы с электронным идентификатором. Большое количество USB устройств может приводить к значительным изменениям в режимах питания USB портов компьютера и, как следствие, к выходу из строя электронных идентификаторов.

л) В случае неисправности или неправильного функционирования электронного идентификатора обращайтесь в УЦ Банка.

3. Обеспечение информационной безопасности на рабочем месте

Клиент обязан обеспечивать безопасное функционирование СКЗИ в соответствии с переданной ему документацией СКЗИ и следующими требованиями по безопасности:

С целью защиты от угроз, связанных с появлением в сети Интернет ложных (фальсифицированных) ресурсов, имитирующих программный интерфейс Системы ДБО, необходимо осуществлять доступ к ней только по указанному в Договоре URL-адресу.

Защита информации от несанкционированного доступа (далее НСД) должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором безопасности.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку.

При размещении технических средств с установленным СКЗИ:

а) Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

б) Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

При установке программного обеспечения СКЗИ следует:

а) На технических средствах, предназначенных для работы с СКЗИ использовать только лицензионное ПО фирм-изготовителей.

б) На ЭВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности.

При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ защищаемой информации и (или) при загруженной ключевой информации.

в) Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатывания системного блока и разъемов ЭВМ).

г) ПО, устанавливаемое на ЭВМ с СКЗИ, не должно содержать возможностей, позволяющих: модифицировать содержимое произвольных областей памяти; модифицировать собственный код и код других подпрограмм; модифицировать память, выделенную для других подпрограмм; передавать управление в область собственных данных и данных других подпрограмм; несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске; повышать предоставленные привилегии; модифицировать настройки операционной системы (далее ОС); использовать недокументированные фирмой-разработчиком функции ОС.

д) Рекомендуется периодически проверять на отсутствие аппаратных закладок аппаратуру, на которой устанавливается и работает СКЗИ. Необходимость таких проверок определяется решением руководства эксплуатирующей организации.

При организации работ по защите информации от НСД необходимо учитывать следующие требования:

а) Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- 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 и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

б) Средствами BIOS должна быть исключена возможность работы на ЭВМ с СКЗИ, если во время ее начальной загрузки не проходят встроенные тесты. Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- Не использовать нестандартные, измененные или отладочные версии ОС.
- Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.
- Исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек.
- На ЭВМ должна быть установлена только одна операционная система.
- Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.
- ОС должна быть настроена только для работы с СКЗИ. Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).
- Режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень.
- Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.
- Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части): системный реестр; файлы и каталоги; временные файлы; журналы системы; файлы подкачки; кэшируемая информация (пароли и т.п.); отладочная информация.
- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.
- Необходимо организовать и использовать комплекс мероприятий антивирусной защиты (включающий в себя установку антивирусного программного обеспечения).
- Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
- При использовании СКЗИ на ЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN и т.п.).

4. Действия в случае компрометации ключей ЭП

Клиент самостоятельно определяет факт компрометации принадлежащего ему секретного ключа ЭП. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, обрабатываемой с помощью средств СКЗИ и ЭП в информационных системах, принадлежащих Клиенту, организует сам Клиент.

При компрометации секретного ключа ЭП Клиент должен немедленно прекратить все работы, связанные с передачей документов в электронном виде по каналам связи, и сообщить в Банк о факте компрометации. Информация о компрометации может передаваться по телефону или непосредственно уполномоченному лицу УЦ Банка. Не позднее 1 часа после поступления сообщения о компрометации ключа, будут заблокированы электронные документы в Системе ДБО, подписанные скомпрометированным секретным ключом ЭП Клиента. Продолжение работы в Системе ДБО возможно только после замены скомпрометированных ключей.

Для генерации новых секретных ключей ЭП владелец сертификата ключа проверки ЭП, у которого были скомпрометированы ключи ЭП, должен обратиться к уполномоченному лицу УЦ Банка, предоставив Заявление об отзыве сертификата (Приложение 5) и документы, удостоверяющие личность.

С настоящими правилами ознакомлен(а), их содержание мне понятно:

«__»_____20__г. _____/_____

подпись *ФИО*

ОБЯЗАТЕЛЬСТВА

владельца сертификата ключа проверки ЭП и СКЗИ

Я, _____

ФИО

ОБЯЗУЮСЬ:

не разглашать конфиденциальную информацию, к которой имею допуск, рубежи ее защиты, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

сообщать в Удостоверяющий центр Банка и непосредственному руководителю по месту работы о ставших мне известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

немедленно уведомить Удостоверяющий центр Банка и непосредственного руководителя по месту работы о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Я предупрежден(а), что в случае нарушения данных обязательств я несу ответственность согласно действующему законодательству; ко мне могут быть применены административные меры, в том числе прекращение отношений с использованием СКЗИ, а в случае причинения материального ущерба Банку – меры материальной ответственности в соответствии с действующим законодательством.

Я предупрежден (а) и осознаю, что изготовление, передача (сбыт) третьим лицам сертификата ключа проверки ЭП и СКЗИ, ключевого носителя, а также иных технических устройств, компьютерных программ для неправомерного осуществления операций с денежными средствами на счете (ах), влечет уголовную ответственность, предусмотренную действующим законодательством, в том числе ст. 187 УК РФ.

Подтверждаю принятие на себя указанных выше обязательств, их содержание мне понятно.

«___»_____20__ г. _____

(подпись)

Второй экземпляр обязательств получил(а):

«___»_____20__ г. _____

(подпись)

к Заявлению на подключение расчетного счета к Системе дистанционного банковского обслуживания от 10.11.2022 года

АКТ ПРИЕМА-ПЕРЕДАЧИ

г. Сыктывкар «___» _____202_года

«Северный Народный Банк» (акционерное общество), именуемое в дальнейшем «Банк», в лице _____, _____, с одной стороны, **и** _____, **именуемый в дальнейшем «Клиент»,** с другой стороны, составили настоящий акт о том, что Банк произвел подключение к системе электронного расчетно-кассового обслуживания «Интернет-Клиент», а Клиент принял подключение, согласно заключенному между сторонами Договору о «Дистанционном банковском обслуживании по счетам юридических лиц и индивидуальных предпринимателей».

Банк уведомляет о возможной уголовной ответственности уполномоченных лиц, обладающих доступом и правом пользования системой дистанционного банковского обслуживания, за сбыт электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств (ст.187 УК РФ).

Банк осуществил регистрацию следующего ключевого носителя в Системе «Интернет-Клиент» и передал его в исправном состоянии Клиенту:

Ключевой носитель _____, предоставленный Банком

Ключевой носитель _____, принадлежащий Клиенту

Банк передал, а Клиент принял:

Реквизиты персонального пароля – 1 шт.

Стороны претензий друг к другу не имеют.

Принял: Передал:

«Северный Народный Банк (АО)

_____ _____

М.П. М.П.

Приложение 2

Заявление
на подключение дополнительных Пользователей к Системе дистанционного банковского обслуживания (ДБО)

г. Сыктывкар

Заявитель (указывается владелец счета) _____, ИНН_____, тел.:_____, просит подключить к счет(ам) в Системе ДБО Интернет-Клиент следующих Пользователей:

Фамилия, имя, отчество	**Счет(а)**	**С правом подписи платежных документов (Да/Нет)***

*** Возможность получения права подписи ЭД и сочетание подписей определяется в соответствии с карточкой образцов подписей. По банковским счетам физических лиц, по которым карточка образцов подписей не оформляется, электронная подпись оформляется на владельца счета и (или) на представителя, предоставившего доверенность, удостоверенную нотариально.**

Заявитель _____ (_____)
(подпись) *(расшифровка)*

М.П.

«___»_____ 202__г.

ОТМЕТКИ БАНКА

Полномочия Заявителя на распоряжение денежными средствами на счете Клиента проверил

_____ (_____)

Подключить счет к Системе ДБО согласно заявлению

_____ (_____)
М.П.

Приложение 4

Заявление

на установку ограничений в Системе дистанционного банковского обслуживания (ДБО)

Заявитель (указывается владелец счета)_____, *ИНН* _____, *тел.:* _____ , просит установить ограничения при работе в системе ДБО Интернет-клиент.

Перечень вариантов ограничений:

на максимальную сумму перевода денежных средств за одну операцию		
на максимальную сумму переводов денежных средств за 1 день		
на перечень возможных получателей денежных средств	☐ Установить Перечень возможных получателей прилагаю	
на временной период, в который могут быть совершены переводы денежных средств;	с:	до:
на перечень идентификаторов устройств, с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений;	☐ Установить Перечень идентификаторов устройств прилагаю	
Ограничения НЕ устанавливать (снять)		

Отметьте галочкой ограничение и(или) укажите, если надо, дополнительные параметры ограничения.

Все предыдущие заявления на установку ограничений в Системе дистанционного банковского обслуживания (ДБО), если таковые имели место быть, считаются утратившими силу (недействительными).

Заявитель _____ (_____)

(подпись) *(расшифровка)*

М.П.

«___» _____ 202__г.

ОТМЕТКИ БАНКА

Полномочия Заявителя на распоряжение денежными средствами на счете Клиента проверил

_____ (_____)

Подключить счет к Системе ДБО согласно заявлению

_____(_____)

М.П.