ПОРЯДОК
обмена электронными документами с использованием системы ДБО

В настоящем Порядке обмена электронными документами с использованием системы ДБО (далее – Порядок) дополнительно применяются следующие термины:

1С:DirectBank[1] (прямой обмен с банком) – технология, позволяющая Клиенту при соблюдении Договора ДБО осуществлять электронный документооборот с Банком из системы 1С:Предприятие, установленной на ПК Клиента, в Систему ДБО.
1С:Предприятие – система программ, являющаяся программным продуктом компании ООО «1С» ОГРН 1107746695980, предназначенным для автоматизации деятельности Клиента, поддерживающая технологию 1С:DirectBank.
АБС – автоматизированная банковская система.
Адрес электронной почты Уполномоченного лица (Адрес электронной почты УЛ) - адрес электронной почты Уполномоченного лица, используемый для всех выбранных для Уполномоченного лица услуг/опций, предусматривающих получение электронных сообщений на адрес электронной почты.
Дистрибутив - совокупность файлов, необходимых для установки средства криптографической защиты информации (далее – СКЗИ) «КриптоПро CSP» версии не ниже 4.0.
Интернет-банк - автоматизированная подсистема Системы ДБО, представляющая собой канал доступа к Системе ДБО с использованием web-приложения, состоящий из совокупности программно-аппаратных средств, позволяющий обеспечить электронный документооборот между Клиентом и Банком, в том числе подготавливать и отправлять в Банк ЭД, подписанные ЭП Клиента, получать статусы обработки ЭД Банком и принимать ЭСИД Банка.
Заявление о подключении к системе дистанционного банковского обслуживания (Заявление ДБО) – заявление по форме, установленной Банком, о дистанционном банковском обслуживании Клиента, представленное Клиентом с целью заключения Договора ДБО.
Заявление об изменениях в системе дистанционного банковского обслуживания (Заявление об изменениях ДБО) – заявление по форме Банка, предоставляемое Клиентом на бумажном носителе в целях внесения изменений в параметры подключения Системы ДБО.
Ключевой носитель – отчуждаемый носитель, предназначенный для хранения ключа электронной подписи.
Контактные данные - Номер телефона УЛ и Адрес электронной почты УЛ.
Криптографические ключи – общее название ключа электронной подписи и ключа проверки электронной подписи:

ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи;

ключ проверки электронной подписи (ключ проверки ЭП) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

Компрометация ключа ЭП - утрата доверия к тому, что используемый ключ электронной подписи недоступен посторонним лицам. К событиям, связанным с компрометацией ключа ЭП, относятся следующие:
-утрата Ключевых носителей;
-утрата Ключевых носителей с последующим их обнаружением;
-увольнение сотрудников Клиента, имевших доступ к ключу ЭП;
-утрата ключей от сейфа в момент нахождения в нем Ключевых носителей;
-временный доступ посторонних лиц к ключам ЭП или Ключевому носителю;

[1] С программами, в которых реализована технология 1С:DirectBank, можно ознакомиться на сайте разработчика http://v8.1c.ru/edi/edi_app/bank/standards.htm.

-обнаружение на персональном компьютере (с использованием которого осуществляется доступ в Систему ДБО) или на Ключевом носителе постороннего (вредоносного) программного обеспечения;
-утрата либо кража МУ, на которое (-ые) установлено Мобильное приложение с возможностью подписания ЭД;
-иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к Системе ДБО третьих или неуполномоченных лиц.
Лицензия - право на использование программы «КриптоПро CSP» версии не ниже 4.0 на условиях простой (неисключительной) лицензии на 1 (Одном) рабочем месте (на 1 (Одном) ПК) Клиента для осуществления электронного документооборота с использованием электронной подписи с Банком**.**
Логин – уникальная последовательность алфавитно-цифровых символов, присваиваемых Клиенту Банком и позволяющая однозначно идентифицировать Клиента в Системе ДБО.
Мобильный банк – автоматизированная подсистема Системы ДБО, предоставляемая дополнительно к Интернет-банку и обеспечивающая, доступ Клиенту к Системе ДБО с использованием Мобильного приложения, установленного на Мобильное устройство Клиента.
Мобильное приложение – программное обеспечение Банка «СМП Бизнес», представляющее собой канал доступа к Системе ДБО, позволяющий обеспечить электронный документооборот между Клиентом и Банком, в том числе создание, подписание ЭП и отправку ЭД в Банк на исполнение, при условии наличия на МУ подключения сети Интернет. Установка Мобильного приложения на МУ возможна из авторизованных магазинов приложений (App Store или Google Play для iOS/Android соответственно).
Мобильное устройство (МУ) – мобильное устройство (телефон, смартфон и т.д.), работающее под управлением операционной системы iOS / Android и используемое Клиентом для установки Мобильного приложения.
Номер телефона Уполномоченного лица (Номер телефона УЛ) – номер мобильного телефона Уполномоченного лица, используемый для всех выбранных для Уполномоченного лица услуг/опций, предусматривающих получение SMS-сообщений. В целях услуги SMS-подтверждение Уполномоченное лицо вправе дополнительно указать не более 2-х дополнительных номеров телефона УЛ.
Операция по счету Клиента – не противоречащая Законодательству РФ операция по распоряжению денежными средствами на Счете Клиента или по предоставлению информации о состоянии и использовании Счета Клиента (в том числе об остатках денежных средств на Счете, проведенных операциях по Счету, а также выписки по Счету), исполняемая Банком на основании Поручений Клиента, передаваемых в соответствии с Договором банковского обслуживания (далее – Договор), в том числе условиями настоящего Порядка.
Пароль – уникальная последовательность алфавитно-цифровых и специальных символов, связанная с присвоенным Клиенту Логином. Пароль необходим для контроля правомочности обращения Клиента к Системе ДБО.
Персональный компьютер (ПК, рабочее место) – ноутбук или стационарный компьютер Уполномоченного лица Клиента.
Подтверждение ЭД – услуга подтверждения электронного документа с целью его отправки в Банк с использованием Интернет-банка, осуществляется посредством ввода Сеансового ключа в соответствующее поле.
Поручение – распоряжение Клиента на совершение одной или нескольких Операций по Счету Клиента, переданное Клиентом Банку с использованием Системы ДБО.
Рутокен ЭЦП 2.0 (Рутокен) – ключевой носитель, USB-устройство с поддержкой российских криптографических стандартов, предназначенный для безопасной двухфакторной аутентификации Клиента, генерации и защищенного хранения Криптографических ключей.
Сеансовый ключ – числовой код, однократно вводимый Клиентом для подтверждения авторизации в Системе ДБО, а также при отправке ЭД в Банк при подключении услуги «Подтверждение ЭД». После использования Сеансовый ключ аннулируется.
Сервис «Светофор» – сервис проверки контрагентов на базе партнерского web-сервиса проверки контрагентов «Светофор» программного обеспечения «Контур.Фокус» компании АО «ПФ «СКБ Контур» (ИНН 6663003127, официальный сайт компании в сети Интернет https://kontur.ru/).
Сертификат ключа проверки электронной подписи (Сертификат ключа подписи) - электронный документ или документ на бумажном носителе, выпущенные Удостоверяющим центром АО «СМП Банк», и выданные Удостоверяющим центром АО «СМП Банк» либо доверенным лицом Удостоверяющего центра АО «СМП Банк» и подтверждающие принадлежность ключа проверки электронной подписи владельцу Сертификата ключа подписи. Аналогом Сертификата ключа подписи на бумажном носителе является Акт признания ключа проверки электронной подписи для обмена сообщениями в Системе ДБО/Акт подтверждения идентификатора ключа для обмена сообщениями в Системе ДБО (Приложение № 2, 2а к настоящему Порядку).

Система дистанционного банковского обслуживания «Интернет-банк для бизнеса» (Система ДБО) – автоматизированная компьютерная система, представляющая собой совокупность программно-аппаратных средств, включающая подсистемы Интернет-банк и Мобильный банк, и предназначенная для передачи Клиентом в Банк ЭПД/ЭСИД и получения указанным Клиентом из Банка ЭСИД, в том числе по каналу интеграции с 1С:Предприятие при подключении услуги «Интеграция 1С:DirectBank».
Доступ к Системе ДБО предоставляется Клиентам с использованием Интернет-банка и Мобильного банка. Далее по тексту Порядка при упоминании Система ДБО имеется в виду совместное указание как на Интернет-банк, так и Мобильный банк, если иное не будет оговорено в настоящем Порядке.
СКЗИ «КриптоПро CSP» – копия программы «КриптоПро CSP» версии не ниже 4.0 для ПК, разработанная «ООО «КРИПТО-ПРО» ОГРН 10377000854444, включая документацию в электронном виде. Программный продукт входит в состав Дистрибутива.
Уполномоченное лицо – лицо, действующее от имени Клиента, обладающее правом подписи документов Клиента на основании предоставленных в Банк сведений и документов и указанное в Сертификате ключа подписи в качестве его владельца, и уполномоченное Клиентом подключать в Интернет-банке уведомления в рамках Услуги Информирования. По заявлению Клиента в рамках Системы ДБО Уполномоченному лицу может быть предоставлен доступ только в информационном режиме (без возможности подписания ЭД). Для Клиентов, у которых открыты Счета (за исключением Счетов по вкладу) Уполномоченными лицами являются лица, указанные в карточке с образцами подписей и оттиска печати.
Услуга «Интеграция 1С:DirectBank» - услуга, позволяющая обеспечить электронный документооборот ЭД между 1С:Предприятие и АБС Банка, посредством Системы ДБО.
Чат – сервис для обмена текстовыми сообщениями, в том числе файлами и фото-информацией между Клиентом и Банком по Системе ДБО. Чат предназначен для получения Клиентом ответов на интересующие вопросы, касающиеся обслуживания в Банке.
Электронный документ (ЭД) – совокупность данных, зафиксированных на электронном носителе информации и передаваемых по электронным каналам связи с реквизитами, позволяющими идентифицировать эти данные и их автора. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа или порождаться в процессе информационного взаимодействия Сторон.
Электронный платежный документ (ЭПД) – электронный документ, представляющий собой Поручение Клиента, составленный в электронном виде и содержащий все предусмотренные банковскими правилами реквизиты, подписанный корректной ЭП, и являющийся основанием для совершения операций по Счету (Счетам) Клиента, открытым в Банке. На ЭПД Клиента, распечатанном на бумажном носителе, обязательно присутствует отметка «ЭП верна».
Электронный служебно-информационный документ (ЭСИД) – электронный документ, обеспечивающий обмен информацией между Клиентом и Банком, в том числе, но не ограничиваясь, заявления Клиента, являющиеся основанием для изменения/прекращения Договора, реестры, выписки по Счету Клиента, запросы, отчеты, информационные сообщения.
Электронная подпись (ЭП) – электронный аналог собственноручной подписи Уполномоченного лица, в виде данных, добавляемых к тексту ЭД и полученных в результате ее криптографического преобразования, обеспечивающий возможность контроля целостности и подтверждения подлинности электронных документов. Электронная подпись позволяет подтвердить ее принадлежность Клиенту. В документах, действующих до вступления в силу настоящей редакции Порядка обмена электронными документами с использованием системы ДБО, Электронная подпись может именоваться Электронная цифровая подпись (ЭЦП).
eToken PASS – устройство, представляющее собой брелок с кнопкой и экраном, предназначенное для генерации Сеансовых ключей.
PayControl – мобильное приложение PayControl / PayControl Classic (программное обеспечение), разработанное ООО «СейфТек» ОГРН 1117746015144, позволяющее подписывать ЭД, создаваемые в Интернет-банке и Мобильном банке, с помощью ЭП на основе средств PayControl. Установка приложения на МУ возможна из авторизованных магазинов приложений (App Store или Google Play для iOS/Android соответственно).
PIN-код – числовой код, используемый для входа в Мобильный банк и аутентификации Банком Клиента в Мобильном банке. Аутентификация Банком Клиента с помощью PIN-кода приравнивается к аутентификации с использованием Логина и Пароля. PIN-код может быть использован как альтернатива ввода Логина и Пароля. Использование PIN-кода как альтернативного способа аутентификации возможно после первичной аутентификации Клиента с использованием Логина и Пароля.

Push-уведомление – сообщение, отправляемое Банком с использованием сети Интернет на Мобильное устройство с установленным на нем Мобильным приложением. Настройка получения Push-уведомлений осуществляется Уполномоченным лицом в Мобильном приложении. Получение Push-уведомлений возможно только при наличии у Уполномоченного лица подключения к сети Интернет на Мобильном устройстве, при отсутствии подключения к сети Интернет, направление уведомлений осуществляется с помощью SMS-сообщений.

SMS-подтверждение – услуга по отправке Сеансовых ключей на указанный в Заявлении ДБО/Заявлении об изменениях ДБО Номер телефона УЛ. В случае указания более одного Номера для получения SMS-подтверждения, отправка Сеансовых ключей осуществляется одновременно на все указанные Номера телефонов. Также для получения SMS-подтверждения отправка Сеансовых ключей осуществляется с помощью Push-уведомлений при наличии соответствующей настройки в Мобильном приложении.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий порядок определяет условия и порядок осуществления электронного документооборота, в том числе проведение операций по Счетам, с использованием Системы ДБО.

1.2. Предоставление услуги дистанционного банковского обслуживания Клиенту осуществляется после заключения Договора ДБО. Для заключения Договора ДБО Клиент представляет в Банк Заявление ДБО по форме Банка на бумажном носителе.

Банк оказывает Клиенту услуги дистанционного банковского обслуживания с использованием Системы ДБО с учетом ограничений, установленных настоящим Порядком, в отношении:

- всех Счетов, открытых в Банке согласно условиям Договора;

- иных счетов, открытых в Банке согласно условиям иных договоров, при условии установления соответствующими договорами возможности использования Системы ДБО;

- иных договоров, заключенных между Клиентом и Банком, при условии установления указанными договорами возможности использования Системы ДБО.

1.3. Договор ДБО, в том числе настоящий Порядок, регулируют отношения Сторон, возникающие в процессе оказания Банком банковских услуг с использованием Системы ДБО, в том числе с использованием Интернет-банка и Мобильного банка.

1.4. Для обеспечения безопасности Системы ДБО» используются:

- средства криптографической защиты информации (далее - СКЗИ) «Message-PRO». Распространение и использование СКЗИ «Message-PRO» осуществляется в соответствии с требованиями законодательства Российской Федерации.

При этом для обеспечения безопасности Системы ДБО используются:

- средства PayControl в соответствии с разделом 5 настоящего Порядка;

- СКЗИ «КриптоПро CSP» в соответствии с разделом 6 настоящего Порядка.

1.5. Для первоначального доступа в Систему ДБО Банк направляет Уполномоченному лицу Логин и Пароль на Контактные данные, указанные Клиентом в Заявлении ДБО/Заявлении об изменениях ДБО (Логин направляется на Адрес электронной почты УЛ, Пароль – на Номер телефона УЛ).

Далее Уполномоченное лицо формирует запрос на выпуск Сертификата ключа проверки в соответствии с п. 1.10 настоящего Порядка.

Для доступа к Системе ДБО посредством Интернет-банка и получения Сеансовых ключей Клиент подключает услугу SMS-подтверждение и/или приобретает eToken PASS. Также для доступа к Системе ДБО посредством Интернет-банка в дополнение к одному из вышеперечисленных средств Клиент может использовать PayControl [2].

При необходимости работать в Системе ДБО на операционной системе macOS или с целью повышения безопасности хранения ключа ЭП Клиенту необходимо приобрести Рутокен в соответствии с Тарифами. Рутокен выдается Клиенту на основании Заявления ДБО/ Заявления об изменениях ДБО и по Акту приема-передачи (Приложение № 5 к настоящему Порядку).

[2] Использование PayControl для доступа к Системе ДБО посредством Интернет-банка/Мобильного банка возможно при подключении Уполномоченному лицу Мобильного банка с возможностью подписания ЭД.

В случае необходимости получения eToken PASS / Рутокена, формирование запроса на выпуск Сертификата ключа проверки электронной подписи возможно только после получения eToken PASS / Рутокена в офисе Банка.

1.6. Для доступа к Системе ДБО посредством Мобильного банка и получения Сеансовых ключей Клиент подключает услугу SMS-подтверждение, либо приобретает eToken Pass. При подключении услуги SMS-подтверждение Банк направляет SMS-сообщения/Push-уведомления, содержащие Сеансовый ключ, на Номер телефона УЛ/на Мобильное устройство.

Также для доступа к Системе ДБО посредством Мобильного банка в дополнение к одному из вышеперечисленных средств Клиент может использовать PayControl[3].

1.7. Для идентификации Банком Уполномоченных лиц, указанных в Заявлении ДБО/Заявлении об изменениях ДБО и подключении к Системе ДБО, Клиентом должны быть представлены в Банк документы, удостоверяющие личность указанных лиц и иные документы, в том числе подтверждающие право иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации (при наличии) (оригиналы, заверенные Банком копии с предоставленных Клиентом оригиналов документов или нотариально заверенные копии), если данные документы не предоставлялись в Банк ранее.

1.8. Настоящим Клиент на основании и во исполнение статьи 431.2 Гражданского кодекса Российской Федерации заверяет Банк в наличии у Уполномоченных лиц полномочий распоряжаться денежными средствами на счете Клиента, используя аналог собственноручной подписи.

Клиент подтверждает, что ему известны правовые последствия недостоверности данных выше гарантий и заверений, предусмотренные пунктами 1 и 2 статьи 431.2 Гражданского кодекса Российской Федерации.»

1.9. Присоединением к Правилам Клиент поручает, а Банк принимает на себя обязательства по обслуживанию Клиента с использованием Системы ДБО, позволяющей обеспечить доставку ЭСИД/ЭПД между Клиентом и Банком (в т.ч. проведение расчетных операций по Счету (Счетам) Клиента, открытым в Банке, на основании ЭПД, и обработку реестров, запросов и т.п. на основании ЭСИД). Обмен ЭД осуществляется дистанционно по сети Интернет.

1.10. Для подтверждения авторизации в Системе ДБО посредством Интернет-банка, а также для Подтверждения ЭД (в случае подключения услуги «Подтверждение ЭД») Клиент использует eToken PASS и/или подключает услугу SMS-подтверждение. Выбор способов получения Сеансовых ключей фиксируется Клиентом в Заявлении ДБО.

Также для подтверждения авторизации в Системе ДБО посредством Интернет-банка, Мобильного банка Клиент в дополнение к вышеперечисленным средствам может использовать PayControl[3].

1.11. При первоначальном доступе в Систему ДБО посредством Интернет-банка Клиент самостоятельно генерирует Криптографические ключи и, посредством Интернет-банка, направляет в Банк запросы на сертификацию ключей проверки ЭП, при наличии Рутокена, Клиент самостоятельно осуществляет генерацию и запись на Рутокен Криптографических ключей. Далее Клиент самостоятельно из Интернет-банка распечатывает Акты признания ключа проверки электронной подписи для обмена сообщениями в Системе ДБО/ Акты подтверждения идентификатора ключа для обмена сообщениями в Системе ДБО (по форме Приложения № 2, 2а к настоящему Порядку) (далее - Акт) для каждой ЭП в 2 (Двух) экземплярах и предоставляет все экземпляры подписанных и заверенных печатью Клиента (при наличии) Актов в Банк. Банк осуществляет сертификацию ключей проверки ЭП Клиента не позднее рабочего дня, следующего за днем получения Банком корректно оформленных и подписанных Клиентом Актов. В случае успешной сертификации ключей проверки ЭП Клиент получает возможность пользоваться Интернет-банком.

1.12. Банк имеет право отказать в сертификации ключей проверки ЭП в следующих случаях:

- в случае обнаружения несоответствия информации в запросе на сертификацию, поданного в электронном виде, информации, содержащейся в Акте;
- в случае сертификации ключа проверки ЭП, соответствующего скомпрометированному ключу ЭП;
- в случае несоответствия данных запроса на сертификацию ключей проверки ЭП информации, содержащейся в карточке с образцами подписей и оттиска печати;
- в случае отсутствия запроса на сертификацию в электронном виде в Системе ДБО.

1.13. В случае осуществления Банком резервирования номера Счета в соответствии с условиями, указанными в Правилах, Клиент имеет право самостоятельно пройти процедуру регистрации в Системе ДБО и сформировать запрос на выпуск сертификата ключа проверки электронной подписи, следуя инструкциям в Системе ДБО. При этом Сертификат ключа проверки электронной подписи будет действителен после заключения Договора банковского счета и Договора ДБО и с момента сертификации ключа.

1.14. Клиент обязан хранить у себя ключи ЭП на Ключевом носителе, в соответствии с Правилами информационной безопасности при работе в системе дистанционного банковского обслуживания (Приложение №3 к настоящему Порядку).

1.15. Все приложения и дополнения к настоящему Порядку являются неотъемлемой частью Договора ДБО.

2. ЗАВЕРЕНИЯ И ПОДТВЕРЖДЕНИЯ СТОРОН

2.1. Клиент и Банк признают, что ЭД в Системе ДБО имеют юридическую силу документов, составленных на бумажных носителях и подписанных Уполномоченными лицами, и являются основанием для осуществления операций по Счету Клиента (в части ЭПД) при выполнении следующих условий:

- ЭД оформлены в соответствии с требованиями Законодательства РФ и переданы в защищенном виде с использованием программного обеспечения Системы ДБО;
- ЭД подписаны ЭП Клиента;
- ЭД подтверждены при отправке в Банк Сеансовым ключом (при подключении Клиенту услуги «Подтверждение ЭД»);
- ЭД успешно получены Банком;
- проверка ЭП, которыми заверены ЭД, дала положительный результат.

Клиент предоставляет право Банку использовать ЭД, отвечающие вышеперечисленным условиям, наравне с документами, составленными на бумажных носителях.

2.2. Стороны признают, что:

2.2.1. программные средства, обеспечивающие изготовление Криптографических ключей, формирование и проверку ЭП, предоставляемые Клиенту, выполнены в соответствии с требованиями Законодательства РФ;

2.2.2. ЭСИД, заверенные ЭП Клиента, имеют юридическую силу, равную соответствующим документам на бумажном носителе, подписанным Уполномоченным лицом и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами, при условии соблюдения условий, изложенных в п. 2.1 настоящего Порядка. ЭД без ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются;

2.2.3. ЭСИД может содержать несколько связанных между собой ЭСИД (пакет ЭСИД). При подписании электронной подписью сопровождающего пакет документов ЭСИД каждый из ЭСИД, входящих в этот пакет, считается подписанным той электронной подписью, которой подписан ЭСИД, сопровождающий пакет документов. Пакет электронных документов в целом и каждый вложенный документ (файл), переданный в Банк, в составе пакета ЭСИД, являются неизменными, обладающими юридической силой, и соответствующим документам на бумажном носителе, подписанным Уполномоченным лицом и имеющим оттиск печати Клиента, при условии, что ЭСИД, заверен ЭП Клиента;

2.2.4. ЭД с ЭП Клиента, создаваемые в электронной форме с использованием Системы ДБО, являются письменными доказательствами при разрешении спорных вопросов. ЭД, не подписанные корректной ЭП, при наличии спорных вопросов, доказательствами не являются;

2.2.5. ключ проверки ЭП, указанный в соответствующем Сертификате ключа подписи, принадлежит Клиенту;

2.2.6. в качестве единой шкалы времени при работе с Системой ДБО принято московское время. Контрольным является время системных часов аппаратных средств Банка;

2.2.7. Записи в электронных журналах Системы ДБО относительно действий, совершаемых от имени Клиента, имеют доказательную силу при рассмотрении спорных ситуаций.

2.3. Каждая Сторона несет ответственность за сохранность своих ключей ЭП и за правомерность

действий при обмене ЭД.

2.4. Клиент вправе установить в отношении каждого Уполномоченного лица необходимость подтверждения ЭД, отправляемого соответствующим Уполномоченным лицом, с целью отправки их в Банк Сеансовым ключом, подключив в отношении соответствующего Уполномоченного лица услугу «Подтверждение ЭД». Услуга подключается на основании Заявления ДБО/Заявления об изменениях ДБО для всех или выбранных Уполномоченных лиц Клиента. При подключении услуги «Подтверждение ЭД» для Уполномоченного лица подтверждение ЭД Сеансовым ключом распространяется на все ЭД, которые отправляет в Банк указанное Уполномоченное лицо.

3. ПОРЯДОК ОБСЛУЖИВАНИЯ КЛИЕНТА В СИСТЕМЕ ДБО

3.1. Поручения Клиента на осуществление Операций по счету Клиента передаются Клиентом Банку по Системе ДБО в виде ЭПД с заполнением соответствующих экранных форм Системы ДБО.

3.2. ЭПД передаются и принимаются с использованием Системы ДБО без их последующего предоставления на бумажном носителе.

3.3. Прием ЭПД и ЭСИД от Клиента в Банке производится в автоматическом режиме круглосуточно. При этом поручения Клиента, поступившие в Банк в операционное время Банка (по месту ведения Счета Клиента, указанного в ЭПД) считаются поступившими текущим операционным днем, а поступившие после окончания операционного дня – считаются поступившими следующим операционным днем.

3.4. Банк информирует Клиента о результатах приема, исполнения ЭПД, ЭСИД Клиента путем присвоения ЭПД, ЭСИД в Системе ДБО соответствующего статуса, статусы ЭПД, ЭСИД доступны для просмотра в Системе ДБО. Исполненные ЭПД также отражаются в выписке из Счета. Статусы, присвоенные Банком ЭПД, указаны в Порядке приема, исполнения, отзыва и возврата (аннулирования) распоряжений о переводе денежных средств со счетов/на счета юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в АО «СМП Банк» (Приложение № 4 к Правилам).

3.5. Для информирования Клиента о результатах приема ЭСИД в Системе ДБО используются следующие статусы:

- «Не принят»/ «Отказано» - (с указанием причины) - документ не принят Банком,
- «Обработан» - документ принят и обработан Банком.

3.6. Банк имеет право запросить у Клиента дополнительное подтверждение ЭПД/ЭСИД в порядке и случаях, установленных Законодательством РФ и внутренними нормативными документами Банка.

3.7. Банк имеет право отказать Клиенту в принятии ЭПД/ЭСИД в соответствии с Законодательством РФ и внутренними нормативными документами Банка.

Об отказе в приеме ЭПД/ЭСИД по указанной причине Банк уведомляет Клиента письмом по Системе ДБО.

3.8. При необходимости отозвать ранее отосланный ЭПД/ЭСИД Клиент присылает в Банк ЭСИД об отзыве ранее направленного ЭПД/ЭСИД. Отзыв ЭПД/ЭСИД возможен при условии, что на момент получения Банком ЭСИД Клиента об отзыве переданного ранее ЭПД/ЭСИД не были совершены действия по исполнению ЭПД/ЭСИД, делающие отзыв невозможным.

3.9. С использованием Системы ДБО, Клиент имеет возможность получить выписку по своему Счету (Счетам). Приложения к выписке подписанные ЭП Банка имеют равную юридическую силу с приложением на бумажном носителе и могут не создаваться Банком на бумажном носителе. В случае обнаружения расхождений между документами Клиента и полученной выпиской, Клиент, связавшись по телефону с подразделением Банка, обслуживающего Счет (Счета), выясняет причины расхождений.

3.10. Прием Клиентом сформированных Банком и предназначенных Клиенту ЭД производится с использованием Системы ДБО, передача Банку созданных Клиентом ЭПД и ЭСИД производится исключительно по инициативе Клиента путем организации им сеанса электронной связи с Банком с использованием Системы ДБО.

3.11. Номер телефона УЛ, Адрес электронной почты УЛ (далее совместно – Контактные данные) указываются Клиентом в разделе «Контактные данные» Заявления ДБО/ Заявления об изменениях ДБО/Заявлении о назначении Контактных данных/заявления о подключении

услуг в рамках Системы ДБО в целях получение SMS-сообщений, электронных сообщений, предусмотренных услугами/опциями в рамках Системы ДБО.

Для изменения Контактных данных УЛ Клиент предоставляет в Банк Заявление об изменениях ДБО на бумажном носителе, Банк осуществляет изменение Контактных данных не позднее 3 (Трех) рабочих дней с даты принятия от Клиента соответствующего заявления.

Для назначение Контактных данных Клиент может предоставить Заявление о назначении Контактных данных посредством Интернет-банка. Банк осуществляет назначение Контактных данных не позднее 3 (Трех) рабочих дней с даты принятия от Клиента заявления.

При предоставлении Клиентом каждого последующего заявления, содержащего Контактные данные, Банк изменяет Контактные данные в соответствии с данными, указанными в заявлении с более поздней датой.

3.12. Банк при выявлении им операции с использованием Системы ДБО, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, обязан до осуществления списания денежных средств со Счета Клиента на срок не более 2 (Двух) рабочих дней приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, а также приостановить использование Клиентом Системы ДБО согласно требованиям Федерального закона от 27.06.2011г. N 161-ФЗ «О национальной платежной системе», уведомив об этом Клиента способом, выбранным по усмотрению Банка.

4. ИНТЕРНЕТ-БАНК

4.1. Подключение Клиенту Интернет-банка осуществляется путем предоставления Клиентом Заявления ДБО с соответствующими отметками.

4.2. Клиент при подготовке ЭПД или ЭСИД, в Интернет-банке выполняет следующие операции:

- осуществляет вход в Интернет-банк;
- авторизуется при входе в Интернет-банк с помощью Сеансового ключа или PayControl (при указании Клиентом в Заявлении ДБО/Заявлении об изменениях ДБО дополнительного средства авторизации PayControl);
- вводит документ в Интернет-банк и формирует ЭД (возможен ручной ввод или импорт из какой-либо программы);
- проверяет правильность ввода документа;
- подписывает ЭД ЭП;
- подтверждает ЭД Сеансовым ключом (в случае подключения услуги «Подтверждение ЭД»),;
- отправляет подписанный ЭД в Банк.

4.3. В процессе проведения сеанса электронной связи с использованием Интернет-банка Клиент имеет возможность:

- передавать в Банк созданные им ЭПД и/или ЭСИД (при использовании Сеансового ключа);
- получать информацию о совершенных операциях по его Счету (Счетам) (выписки по Счетам Клиента) с приложением ЭПД, являющихся основанием для совершения соответствующих операций;
- получать информацию о текущих остатках средств на его Счете (Счетах) в Банке;
- получать информацию о статусах отправленных ЭПД/ЭСИД;
- получать созданные Банком и предназначенные Клиенту ЭД;
- до передачи в Банк ЭПД осуществить проверку своих контрагентов с использованием Сервиса «Светофор» при наличии информации о соответствующем контрагенте в базе данных партнерского web-сервиса «Светофор».

4.4. Также подписание ЭД в Интернет-банке возможно с помощью PayControl при подключении Уполномоченному лицу Мобильного банка с возможностью подписания ЭД и выпуска ЭП PayControl. Подписание ЭД в Интернет-банке с помощью PayControl осуществляется в онлайн режиме (при наличии подключения к сети оператора на МУ) или оффлайн режиме (в случае если МУ находится в оффлайн режиме/ отсутствует подключение к сети оператора).

5. МОБИЛЬНЫЙ БАНК

5.1. Мобильный банк подключается в дополнение к Интернет-банку. Для подключения Мобильного банка Клиент предоставляет в Банк Заявление ДБО/Заявление об изменениях

ДБО на бумажном носителе либо Заявление о подключении/отключении Мобильного банка посредством Интернет-банка. Возможность доступа к Мобильному банку предоставляется Клиенту не позднее 3 (Третьего) рабочего дня, следующего за днем принятия Банком соответствующего заявления. Принятие Банком заявления подтверждается соответствующими отметками (заявление на бумажном носителе) или изменением статуса заявления в Системе ДБО в соответствии с п.3.5 настоящего Порядка (в случае если заявление предоставлено в Банк посредством Системы ДБО). Мобильный банк может быть подключен с возможностью подписания ЭД или без возможности подписания ЭД, выбор параметров подключения осуществляется Клиентом в Заявлении ДБО/Заявлении об изменениях ДБО/Заявлении о подключении/отключении Мобильного банка.

5.2. Мобильный банк позволяет:

- получать информацию о текущих остатках средств на Счете/Счетах Клиента;

- отправлять реквизиты Счета контрагентам по заданному каналу (электронная почта, SMS, мессенджеры и иные каналы);

- получать информацию о движении денежных средств по Счету/Счетам Клиента за период времени, выбранный Клиентом;

- просматривать информацию о динамике средств на Счетах в виде графиков, обороты движения денежных средств по Счету (-ам);

- осуществлять экспорт и отправку выписки по Счету (-ам) в различных форматах (XLS, PDF, XML и иные) на адрес электронный почты Клиента, указанный при экспорте;

- создавать ЭД (платежные поручения, запросы на отзыв платежного поручения, письма) и направлять подписанные ЭП ЭД на исполнение в Банк;

- подписывать ЭД (платежные поручения, запросы на отзыв платежного поручения, письма), в т.ч. созданные посредством Интернет-Банка);

- просматривать статусы направленных в Банк ЭД (платежные поручения, запросы на отзыв платежного поручения, письма и др.);

- отправлять экземпляры исполненных ЭПД со штампом Банка об исполнении в различных форматах (RTF, XLS, PDF) по заданному каналу (электронная почта, SMS, мессенджеры и иные каналы);

- осуществлять проверку контрагентов с использованием сервиса «Светофор»;

- просматривать ЭСИД (письма), направленные Клиентом в Банк/Банком Клиенту;

- просматривать новости Банка;

- просматривать курсы валют Банка;

- осуществлять поиск офисов/банкоматов Банка.

5.3. Для использования Мобильного банка без возможности подписания ЭД Клиенту необходимо установить на МУ Мобильное приложение.

Для входа в Мобильный банк Клиенту необходимо на странице авторизации в Мобильном приложении ввести Логин и Пароль. В дальнейшем Клиент вправе использовать иные способы авторизации, предусмотренные Мобильным приложением, которые поддерживает Мобильное устройство, в том числе PIN-код/Touch ID (сканер отпечатков пальцев)/Face ID (сканер объемно-пространственной формы лица человека).

5.4. Для использования Мобильного банка с возможностью подписания ЭД Клиенту необходимо:

- установить на МУ Мобильное приложение;
- установить на МУ PayControl (установка не требуется при наличии встроенного PayControl в Мобильном приложении);
- сформировать криптографические ключи на основе средств PayControl[3];
- в Интернет-банке распечатать в 2-х экземплярах Акта подтверждения идентификатора ключа для обмена сообщениями в Системе ДБО (по форме Приложения № 2а к настоящему Порядку) для каждой ЭП в 2 (Двух) экземплярах и предоставить все экземпляры подписанных и заверенных печатью Клиента (при наличии) Актов в Банк.

Банк осуществляет сертификацию ключей проверки ЭП Клиента не позднее рабочего дня, следующего за днем получения Банком корректно оформленных и подписанных Клиентом

[3] Количество ЭП PayControl соответствует количеству МУ, с которых Уполномоченное лицо планирует работать в Мобильном банке с возможностью подписания ЭД, на каждое МУ должна быть выпущена отдельная ЭП PayControl.

Актов. В случае успешной сертификации ключей проверки ЭП Клиент получает возможность подписывать ЭД ЭП PayControl в Мобильном банке[4].

5.5. Для отключения Мобильного банка Клиент предоставляет в Банк Заявление об изменениях ДБО на бумажном носителе или Заявление о подключении/отключении Мобильного банка по Интернет-банку, отключение Банк осуществляет не позднее 3 (Третьего) рабочего дня, следующего за днем принятия Банком соответствующего заявления.

После отключения Мобильного банка Клиент удаляет Мобильное приложение с Мобильного устройства.

5.6. Банк вправе отключить Мобильный банк Клиенту в случае неиспользования Клиентом Мобильного банка в течение более чем 180 (Ста восьмидесяти) календарных дней с даты подключения Клиенту Мобильного банка/последнего случая использования Мобильного банка.

5.7. Банк вправе внедрять обновленные версии Мобильного банка в течение действия Договора. В случае невозможности использования в обновленной версии Мобильного банка действующих Криптографических ключей ЭП PayControl, Банк предварительно извещает об этом Клиента не менее чем за 20 рабочих дней в порядке, установленном Договором, в том числе, но, не ограничиваясь посредством SMS-извещения. Выпуск новых Криптографических ключей ЭП PayControl для подписания ЭД в обновленной версии Мобильного банка осуществляется на основании предоставленного Уполномоченным лицом в Банк Заявления об изменениях ДБО на бумажном носителе или Заявления о подключении/отключении Мобильного банка по Системе ДБО. При этом ранее действовавший Криптографический ключ ЭП PayControl в случае, когда на имя указанного Уполномоченного лица был выпущен единственный Криптографический ключ ЭП PayControl, аннулируется с даты сертификации нового Криптографического ключа ЭП PayControl. В случае, когда на имя Уполномоченного лица ранее выпущены несколько Криптографических ключей ЭП PayControl, Уполномоченное лицо для аннулирования таких Криптографических ключей ЭП PayControl предоставляет в Банк Заявление об изменениях ДБО с указанием аннулируемых Криптографических ключей ЭП PayControl.

6. УСЛУГА «ИНТЕГРАЦИЯ 1С:DIRECTBANK»

6.1. Услуга «Интеграция 1С:DirectBank» предоставляется при наличии одновременно у Клиента:

- подключенной Системы ДБО;
- подключенной услуги SMS-подтверждение для подтверждения авторизации при входе в Систему ДБО;
- СКЗИ «КриптоПро CSP»;
- Лицензии;
- программного обеспечения «1С:Предприятие» с поддержкой технологии 1С:DirectBank[5];
- открытого в Банке Счета в валюте Российской Федерации (далее - валюта РФ), подключенного к Системе ДБО.

6.2. Услуга «Интеграция 1С:DirectBank» позволяет в электронном виде:

- направлять в Банк сформированные и подписанные ЭП в 1С:Предприятие ЭПД по счету в валюте РФ;
- направлять запрос на отзыв ранее направленного ЭПД, сформированного в 1С:Предприятие[6];
- направлять запросы[8], подписанные ЭП, на получение выписок по операциям по счету в валюте РФ, сформированные в 1С:Предприятие, и получать с использованием 1С:Предприятие выписки по операциям по Счету в валюте РФ с приложением экземпляров исполненных документов по каждой операции, указанной в выписке.

6.3. Клиент вправе подключиться к Услуге «Интеграция 1С:DirectBank» в течение срока действия Договора ДБО.

---

[4] При заключении Договора ДБО с одновременным подключением Мобильного банка с возможностью подписания ЭД для обеспечения безопасности Системы ДБО используются средства PayControl, при необходимости Клиент может выпустить ЭП СКЗИ «Message-PRO», путем предоставления в Банк заявления по форме Приложения №2 к Заявлению об изменениях ДБО.

[5] С программами, в которых реализована технология 1С:DirectBank, можно ознакомиться на сайте разработчика - http://v8.1c.ru/edi/edi_app/bank/standards.htm.

[6] В случае если у Клиента для подписания ЭД используется одновременно более 1 (Одной) ЭП и/или установлено сочетание подписей соответствующим заявлением, запрос на отзыв ранее направленного ЭПД/запрос на получение выписок, сформированного в 1С:Предприятие достаточно подписать одной из ЭП Уполномоченных лиц.

6.4. Для подключения услуги Клиенту необходимо:

- приобрести у правообладателя программное обеспечение «1С:Предприятие» с правами на его использование и оборудовать рабочее место Клиента (ПК) в соответствии с эксплуатационной документацией данного программного обеспечения;

- скачать (при необходимости) с сайта производителя (https://www.cryptopro.ru/products/csp/downloads) Дистрибутив СКЗИ «КриптоПро CSP» и установить его на рабочее место;

- для установки и эксплуатации СКЗИ «КриптоПро CSP» приобрести Лицензию»[7]. Лицензия приобретается Клиентом самостоятельно либо Клиент может получить Лицензию у Банка на условиях простой (неисключительной) лицензии по Сублицензионному соглашению (Приложение №7 к настоящему Порядку), заключенному с Банком.

Способ приобретения Лицензии указывается Клиентом в Заявлении ДБО/Заявлении об изменениях ДБО/Заявлении на подключение/отключение услуги «Интеграция 1С:DirectBank».

- предоставить в Банк Заявление ДБО/Заявление об изменениях ДБО на бумажном носителе или Заявление на подключение/отключение услуги «Интеграция 1С:DirectBank» посредством Системы ДБО.

6.5. Подключение Услуги «Интеграция 1С:DirectBank» осуществляется не позднее 3 (Трех) рабочих дней с даты принятия Банком от Клиента соответствующего заявления. Принятие Банком заявления подтверждается соответствующими отметками (заявление на бумажном носителе) или изменением статуса заявления в Системе ДБО в соответствии с п.3.5 настоящего Порядка (в случае если заявление предоставлено в Банк посредством Системы ДБО). После предоставления заявления Клиенту необходимо:

- самостоятельно осуществить генерацию ЭП в Системе ДБО с использованием СКЗИ «КриптоПро» и предоставить Акты признания ключа проверки электронной подписи для всех Уполномоченных лиц по аналогии с п. 1.10 настоящего Порядка[8];

- осуществить настройки в соответствии с Руководством по настройке услуги «Интеграция 1С:DirectBank». Руководство по настройке услуги «Интеграция 1С:DirectBank» размещено в разделе «Поддержка» на странице входа в Систему ДБО.

После выполнения настроек Клиент получает возможность пользоваться Услугой «Интеграция 1С:DirectBank».

6.6. Банк информирует Клиента о совершении Операций по счету Клиента путем присвоения соответствующего статуса распоряжению с указанием даты его присвоения, отображаемом в 1С:Предпритятие.

Датой получения Клиентом уведомления о совершении Операции по счету Клиента считается дата присвоения распоряжению Клиента соответствующего статуса.

6.7. Стороны признают, что передаваемые Клиентом в Банк посредством 1С:Предпритятие распоряжения, заверенные надлежащим образом ЭП Клиента, идентичны распоряжениям о переводе денежных средств (платежным поручениям) на бумажном носителе, подписанным уполномоченными от имени Клиента представителями и скрепленным оттиском печати Клиента (при ее наличии).

6.8. За пользование услугой «Интеграция 1С:DirectBank» взимается ежемесячная комиссия согласно Тарифам.

6.9. Для отключения Услуги «Интеграция 1С:DirectBank» Клиенту необходимо предоставить в Банк Заявление об изменениях ДБО на бумажном носителе или Заявление на подключение/отключение услуги «Интеграция 1С:DirectBank» посредством Системы ДБО.

6.10. Банк имеет право отказать Клиенту в предоставлении услуги «Интеграция 1С:DirectBank» при невозможности осуществить электронный документооборот с Банком из 1С:Предприятие, установленной на ПК Клиента, в Систему ДБО по техническим причинам.

7. УСЛУГА ИНФОРМИРОВАНИЯ

[7] Лицензия приобретается Клиентом на каждое рабочее место, с которого осуществляется электронный документооборот с использованием ЭП в рамках Услуги «Интеграция 1С:DirectBank».

[8] После установки Сертификата ключа проверки ЭП с использованием СКЗИ «КриптоПро CSP» Клиент может обратиться в Банк для аннулирования/приостановления действия Сертификата ключа проверки ЭП с использованием СКЗИ «Message-PRO», используемого в Системе ДБО, путем предоставления в Банк заявления по форме Приложения №2 к Заявлению об изменениях ДБО.

Банк оказывает Клиенту услугу «SMS-информирование об изменении остатка на счете и действиях, совершенных Клиентом в Системе ДБО» (далее – Услуга Информирования), с помощью которой Клиент получает информацию об изменении остатка на Счете (-ах), действиях, совершенных Клиентом в Системе ДБО, мини-выписку в виде SMS-сообщения /Push-уведомления. Оказание услуги осуществляется путем направления SMS-сообщения на Номер телефона УЛ/ Push-уведомления на Мобильное устройство. Дополнительно к информированию посредством SMS-сообщений/Push-уведомлений, Клиент может подключить информирование путем направления электронного сообщения на Адрес электронной почты УЛ. Услуга Информирования оказывается только при наличии не менее одного действующего банковского счета, открытого в Банке.

7.1. В случае если Клиентом ранее была подключена иная услуга по информированию в рамках настоящего Порядка, указанная услуга считается соответствующим образом измененной и изложенной в редакции настоящего Порядка. Возможность управления уведомлениями предоставляется всем Уполномоченным лицам в объеме Услуги Информирования на Контактные данные[9]. Клиент соглашается, что Банк рассматривает Уполномоченных лиц, как лиц, наделенных полномочиями на управление в Интернет-банке уведомлениями и получение уведомлений Услуги Информирования. Клиент несет все риски, связанные с доступом лиц, не имеющим соответствующих полномочий к указанным функциям. Номера телефонов/адреса электронной почты, используемые для получения уведомлений, рассматриваются Банком как номера телефонов/ адреса электронной почты лиц, уполномоченных Клиентом на получение уведомлений в рамках Услуги Информирования.

7.2. Услуга Информирования включает в себя следующие виды уведомлений:

7.2.1. об изменении остатка на Счете (-ах). Уведомление об изменении остатка на Счете (-ах) в рублях РФ направляется Уполномоченному лицу в случае изменения остатка денежных средств на Счете (-ах), но не реже одного раза в час. SMS-сообщение/Push-уведомление/ электронное сообщение содержит следующую информацию: номер Счета, событие по Счету (увеличение/уменьшение остатка денежных средств на Счете), сумму события (в случае наступления нескольких событий, изменяющих сумму остатка на Счете в рамках одного интервала информирования, направляется 1 (Одно) SMS-сообщение/Push-уведомление с суммарным результатом), остаток на Счете на момент отправки сообщения;

7.2.2. Мини-выписка по Счету в рублях РФ. Данное уведомление содержит следующую информацию: сумму входящего остатка, сумму исходящего остатка, сумму оборотов по дебету и по кредиту, и направляется ежедневно 1 (Один) раз в календарный день в установленное Клиентом время;

7.2.3. о действиях, совершенных Клиентом в Системе ДБО, таких как:

- об изменении настроек уведомлений. Уведомление направляется в случае изменения настроек информирования, таких как:

  - изменение способа информирования (SMS-сообщение/Push-уведомление/электронное сообщение) или отмены информирования;
  - изменение временных параметров информирования (допустимый период).

- об изменении Номера телефона УЛ. Данный вид уведомления направляется в случае изменения Номера телефона УЛ;
- о попытке входа в Систему ДБО. Данный вид уведомления направляется при попытке авторизации и входа в Систему ДБО под логином Уполномоченного лица;
- о входе в Систему ДБО (о каждом входе в Систему ДБО (дата и время входа). Данный вид уведомления подключается Банком в виде SMS-сообщения автоматически при подключении Услуги Информирования и может быть отключен по усмотрению Клиента самостоятельно в Системе ДБО;
- о результатах обработки ЭД. Выбор ЭД и статуса ЭД (принят, отозван и т.п.), необходимых для информирования, осуществляется Клиентом в Системе ДБО самостоятельно, при этом уведомление о поступлении ЭПД в Банк на обработку (изменение статуса ЭПД на «Принят») в Банк подключается Банком в виде SMS-сообщения автоматически при подключении Услуги Информирования и может быть отключено по усмотрению Клиента самостоятельно в

[9] В случае отсутствия Контактных данных, Банк направляет уведомления на номер телефона/адрес электронной почты, используемые для ранее подключенной услуги по информированию. В случае если номер телефона/адрес электронной почты ранее не предоставлялись в Банк, для направления уведомлений необходимо предоставить заявление по форме Банке.

Системе ДБО.

7.3. Информирование о действиях, совершенных Клиентом в Системе ДБО, осуществляется по мере наступления событий, указанных в п. 7.2.3 настоящего Порядка, в виде SMS-сообщений/Push-уведомление на Номер телефона УЛ/Мобильное устройство и электронных сообщений на Адрес электронной почты УЛ.

7.4. Для уведомлений, указанных в п.7.2 настоящего Порядка, Уполномоченное лицо имеет возможность установить допустимый период направления уведомлений, в который Банком будут направляться уведомления в рамках Услуги Информирования в часовом поясе адреса местонахождения филиала Банка, в котором Клиент обслуживается. Для своевременного получения уведомлений рекомендуется установить допустимый период направления уведомлений кратным часу. В случае если Клиентом установлен допустимый период информирования, то информирование произойдет при наступлении такого периода. При установлении отметки об отправке уведомления «в любое время» уведомления будет отправляться в момент наступления события.

7.5. Клиент/Уполномоченное лицо самостоятельно в Интернет-банке подключает необходимые ему виды уведомлений и устанавливает параметры уведомлений. Подключение уведомлений осуществляется Клиентом/Уполномоченным лицом путем указания способа информирования посредством SMS-сообщений/Push-уведомлений в Интернет-банке. Также Клиент/Уполномоченное лицо может указать дополнительный способ информирования в виде направления электронных сообщений на Адрес электронной почты УЛ. Клиент, подключая уведомления в Интернет-банке, подтверждает, что ознакомлен и согласен с условиями предоставления Услуги Информирования, Тарифами, а также с тем, что указанные действия будут рассматриваться Банком в качестве оферты, направленной Клиентом с целью подключения уведомлений Услуги Информирования, а акцептом – действия Банка по отправке первого сообщения, предусмотренного Услугой Информирования. При наличии технической возможности Клиент/Уполномоченное лицо может в Интернет-банк самостоятельно установить дополнительный номер телефона для получения уведомлений.

Для получения уведомлений с помощью Push-уведомлений Уполномоченное лицо самостоятельно осуществляет настройку в Мобильном приложении. Push-уведомления направляются Банком по тем видам уведомлений, которые подключены Уполномоченным лицом в Интернет-банке со способом уведомления посредством SMS-сообщений.

В случае если Клиент подключил Push-уведомления на несколько Мобильных устройств, то при отключении Push-уведомлений на одном из Мобильных устройств, направление Push-уведомлений и Sms-сообщений на данное Мобильное устройство прекращается, на иные Мобильные устройства Push-уведомления и Sms-сообщения продолжают направляться. Для повторного подключения Sms-сообщений/Push-уведомлений Клиент выполняет действия, указанные в настоящем пункте Порядка.

7.6. В соответствии со ст. 160 Гражданского кодекса Российской Федерации Стороны договорились о возможности подключения уведомлений Услуги Информирования в интерфейсе Интернет-банка путем совершения Клиентом действий, предусмотренных Интернет-банком и с которыми связано начало оказание соответствующей услуги. Клиент принимает в связи с этим на себя всю ответственность за действия Уполномоченных лиц, имеющих доступ к Системе ДБО. Все Уполномоченные лица, управляющие уведомлениями в Интернет-банке и получающие уведомления, рассматриваются со стороны Банка как лица, наделенные такими полномочиями со стороны Клиента, ответственность за управление уведомлениями лицами, не наделенными такими полномочиями, возлагается на Клиента. Клиент соглашается, что действия в Интернет-банке любых Уполномоченных лиц, направленные на подключение уведомлений в Системе ДБО, которые хотя и не уполномочены надлежащим образом, однако действуют так, что из их действий и обстановки следует наличие у таких лиц необходимых полномочий, рассматриваются Банком как лица, уполномоченные на подключение соответствующих уведомлений. К числу обстоятельств, свидетельствующих о наличии у лица необходимых полномочий, относится, в т.ч. право доступа в Систему ДБО.

7.7. Клиент оплачивает Банку абонентскую ежемесячную плату за оказание Услуги Информирования в порядке и размере, установленном Тарифами. В случае если Клиент в Интернет-банке выбирает уведомления, которые предоставляются Банком на платной основе, Клиент, выбирая такие уведомления, подтверждает и выражает свое согласие на оплату Услуги Информирования в соответствии с Тарифами и объемом передаваемой

информации. Размер платы не зависит от способа оказания Услуги Информирования Банком посредством SMS-сообщений или Push-уведомлений.

7.8. Банк оставляет за собой право изменять содержание SMS-сообщения/Push-уведомления /электронного сообщения, в порядке, установленном Договором банковского обслуживания, для внесения изменений в Договор банковского обслуживания.

7.9. Услуга считается оказанной с момента отправки SMS-сообщения на Номер телефона УЛ, Push-уведомления на Мобильное устройство или электронного сообщения на Адрес электронной почты УЛ с момента доставки сообщения оператору, предоставляющему соответствующую услугу доставки сообщения Клиенту.

7.10. Для подключения Услуги Информирования Клиент предоставляет в Банк Заявление ДБО/Заявление об изменениях ДБО на бумажном носителе или Заявление о подключении/изменении/отключении Услуги Информирования с использованием Интернет-банка.

7.11. Оказание Услуги Информирования начинается не позднее 3 (Трех) рабочих дней с даты принятия Банком от Клиента соответствующего заявления, указанного в п.7.10 настоящего Порядка. Принятие Банком заявления подтверждается соответствующими отметками (заявление на бумажном носителе) или изменением статуса заявления в Интернет-банке в соответствии с п.3.5 настоящего Порядка (в случае если заявление предоставлено в Банк посредством Интернет-банка).

Предоставление Клиентом заявления означает волеизъявление, согласие Клиента с тем, что используемые Банком при оказании Услуги Информирования способы доставки сообщения являются открытыми и не гарантируют защиту передаваемой информации. Клиент дает поручение Банку совершать все действия, необходимые для оказания Услуги Информирования, и подтверждает, что Услуга Информирования предоставляются ему исходя из его поручения и в его интересах.

Клиент гарантирует наличие полномочий Уполномоченных лиц, управляющих уведомлениями в Интернет-банке, на получение и управление уведомлениями Услуги Информирования.

Клиент предоставляет Банку безусловное право на направление в адрес Уполномоченных лиц SMS-сообщений/Push-уведомлений/электронных сообщений, содержащих информацию в объеме, определенном Услугой Информирования.

7.12. Банк вправе в одностороннем порядке вводить в действие иные способы информирования Клиента в рамках Услуги Информирования, а также изменять основания, при наступлении которых Банком оказывается Услуга Информирования, в порядке, установленном Договором банковского обслуживания для внесения изменений в Договор банковского обслуживания.

7.13. Банк не контролирует подтверждение Клиентом принятия SMS-сообщений/Push-уведомлений/электронных сообщений и осуществляет обслуживание Клиента с использованием Системы ДБО вне зависимости от получения/неполучения Клиентом данных сообщений.

7.14. До даты уведомления Клиентом Банка о случаях, указанных в п. 13.13 настоящего Порядка, информация, переданная по указанным в заявлении Номеру телефона УЛ и/или Адресу электронной почты УЛ, считается переданной Банком надлежащим образом.

7.15. Для отключения Услуги Информирования Клиент предоставляет в Банк Заявление об изменениях ДБО на бумажном носителе или Заявление о подключении/изменении/отключении Услуги Информирования и использованием Интернет-банка.

Отключение Услуги Информирования в порядке, предусмотренном настоящим пунктом, осуществляется не позднее 3 (Трех) рабочих дней с даты принятия Банком от Клиента соответствующего заявления.

8. ЧАТ

В целях получения ответов на интересующие вопросы, в том числе информации по Счетам, Уполномоченное лицо может задать вопрос с помощью Чата в Системе ДБО. Информация предоставляется по Счетам, открытым у Клиента в рамках Правил банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «СМП Банк».

Клиент предоставляет Банку безусловное право на консультирование Уполномоченных лиц по всем открытым Клиенту Счетам с использованием Чата. Клиент соглашается, что любые

Уполномоченные лица, обращающиеся за консультированием в Чат, которые хотя и не уполномочены надлежащим образом, однако действуют так, что из их действий и обстановки следует наличие у таких лиц необходимых полномочий, рассматриваются Банком как лица, наделенные правом получения информации от Банка по всем Счетам с использованием Чата. К числу обстоятельств, свидетельствующих о наличии у лица необходимых полномочий, относится, в т.ч. право доступа в Систему ДБО.

Клиент на основании и во исполнение статьи 431.2 Гражданского кодекса Российской Федерации подтверждает, что ему известны правовые последствия недостоверности данных выше гарантий и заверений, предусмотренные пунктами 1 и 2 статьи 431.2 Гражданского кодекса Российской Федерации.

8.1. Чат доступен всем Клиентам, подключенным к Системе ДБО. Для получения консультации необходимо зайти в Систему ДБО и нажать на значок диалогового окна.

8.2. История переписки сохраняется в Чате по всем организациям, к которым Уполномоченное лицо имело доступ. Банк не контролирует информацию, размещаемую, передаваемую, используемую Уполномоченным лицом в Чат

8.3. Для отключения Чата Клиент предоставляет в Банк Заявление об изменениях ДБО на бумажном носителе.

Отключение Чата осуществляется не позднее 3 (Трех) рабочих дней с даты принятия Банком от Клиента заявления.

В случае необходимости Клиент может повторно подключить Чат, подав Заявление об изменениях ДБО на бумажном носителе. Подключение Чата осуществляется не позднее 3 (Трех) рабочих дней с даты принятия Банком от Клиента заявления.

9. ПРАВА И ОБЯЗАННОСТИ СТОРОН

9.1. При исполнении условий Договора ДБО Стороны обязаны руководствоваться требованиями Законодательства РФ, регулирующего использование ЭП, а также положениями договоров и соглашений, заключенных Сторонами, в рамках которых Стороны используют Систему ДБО.

9.2. Стороны имеют право запрашивать друг у друга копии ЭПД/ЭСИД, составленные на бумажном носителе и заверенные собственноручными подписями уполномоченных лиц и оттиском печати Стороны, создавшей ЭПД.

9.3. В случае возникновении конфликтных ситуаций между Клиентом и Банком при использовании Системы ДБО Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций» (Приложение № 1 к настоящему Порядку), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации.

10. БАНК ОБЯЗУЕТСЯ:

10.1. Выдать Клиенту eToken PASS/Рутокен/подключить услугу SMS-подтверждение в срок не позднее 3 (Трех) рабочих дней от даты принятия Банком подписанного Заявления ДБО/Заявления об изменениях ДБО. Формы Заявлений размещаются на официальном сайте Банка, либо предоставляются в подразделении Банка по устному запросу Клиента.

10.2. Обеспечить Клиенту возможность в режиме реального времени получать информацию о статусах состояния ЭПД/ЭСИД, переданных Клиентом в Банк.

10.3. Своевременно обрабатывать ЭПД/ЭСИД, полученные в процессе сеансов электронной связи с использованием Системы ДБО.

10.4. Вести электронные журналы протоколов сеансов связи Сторон с использованием Системы ДБО, результатов проверки подлинности и авторства ЭД, архив принятых и отправленных ЭД в рамках Договора ДБО в течение 5 (пяти) лет со дня проведения сеанса связи.

10.5. Заблаговременно информировать Клиента по системе ДБО о блокировке ключей ЭП в связи с истечением срока полномочий Уполномоченных лиц и необходимости предоставления в Банк документов, подтверждающих продление полномочий.

10.6. Не разглашать и не передавать другим лицам (обеспечивать конфиденциальность) информацию, связанную с использованием Системы ДБО, за исключением случаев, предусмотренных Законодательством РФ.

10.7. Оказывать консультационные услуги Клиенту по вопросам функционирования Системы ДБО

круглосуточно и без выходных. Консультации предоставляются по телефону, указанному на официальном сайте Банка www.smpbank.ru.

11. БАНК ИМЕЕТ ПРАВО:

11.1. Отказать Клиенту в заключении Договора ДБО в соответствии с Законодательством РФ и внутренними нормативными документами Банка.

11.2. В одностороннем порядке досрочно расторгнуть Договор ДБО в случае нарушения Клиентом своих обязательств, принятых в рамках Договора банковского обслуживания.

11.3. В случае возникновения у Банка претензий по выполнению Клиентом условий Договора ДБО требовать от Клиента проведения технической экспертизы в соответствии с Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций (Приложение № 1 к настоящему Порядку).

11.4. Требовать от Клиента замены Криптографических ключей:

- при проведении периодической плановой их замены, в течение 30 дней до окончания срока действия ключа ЭП (срок действия ключа ЭП – 24 месяца);
- при внеплановой замене: увольнении Уполномоченных лиц, компрометации или подозрении на компрометацию ключей ЭП, нарушении правил эксплуатации Системы ДБО.

11.5. Требовать от Клиента замены Криптографических ключей при смене Уполномоченного лица либо при окончании срока его полномочий в соответствии с карточкой с образцами подписей и оттиска печати, предоставленной в Банк. Криптографические ключи подлежат замене в порядке, предусмотренном для их оформления при подключении к Системе ДБО.

11.6. При возникновении подозрений в нарушении безопасности Системы ДБО, выявлении признаков или фактов, а также возможности таких нарушений, немедленно приостановить использование Системы ДБО и оповестить об этом Клиента для принятия мер.

11.7. При истечении срока полномочий Уполномоченного лица Клиента блокировать ЭП указанного лица до момента предоставления Клиентом документов, необходимых для продления срока полномочий Уполномоченного лица Клиента.

11.8. Приостанавливать оказание услуг:

- при их неоплате;
- при совершении сомнительных на усмотрение Банка операций;
- в случае непредставления Клиентом запрошенных сведений и документов;
- при истечении срока полномочий всех Уполномоченных лиц,;
- при наличии подозрений о компрометации ключей ЭП;
- в иных случаях.

11.9. Информировать Клиента способом, выбранным по усмотрению Банка, о факте:

- осуществления операций по Счету (Счетам) Клиента с использованием Системы ДБО;
- наличия подозрений в нарушении Правил информационной Безопасности Клиентом, и (или) подозрений в осуществлении попыток хищения денежных средств со Счета (Счетов) Клиента и (или) попыток хищения аутентификационной информации Клиента с использованием Системы ДБО.

11.10. Самостоятельно определять набор услуг, предоставляемых Клиенту посредством Интернет-банка, внедрять новые версии Системы ДБО, новые форматы, и порядок оформления и проверки ЭПД и ЭСИД, изменять и дополнять перечень видов документов, которые могут направляться Клиентом с использованием Системы ДБО.

11.11. Самостоятельно определять объем дистанционного банковского обслуживания с применением Мобильного банка, вносить изменения в Мобильное приложение и обновлять.

11.12. Без объяснения причин приостановить/прекратить доступ Клиента к проверке контрагентов Клиента с использованием Сервиса «Светофор» либо изменить поставщика соответствующей услуги.

11.13. Прекратить обслуживание Клиента с использованием Системы ДБО в случае неиспользования Клиентом Системы ДБО (отсутствия сеансов связи) в течение более чем 180 (Ста восьмидесяти) календарных дней с даты подключения Клиенту Системы ДБО (даты последнего сеанса связи).

12. БАНК НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ:

12.1. за задержки и сбои, возникающие в сетях операторов сотовой связи и сервисах провайдеров, которые могут повлечь за собой задержку или недоставку SMS-сообщений Клиенту;

12.2. за недоставленные, либо доставленные не полностью SMS–сообщения/Push-уведомления//электронные сообщения Клиенту по причинам, не зависящим от Банка;

12.3. за возможное раскрытие информации в случае утраты Клиентом мобильных телефонов и/или SIM-карт с зарегистрированными Номерами телефонов УЛ для SMS-сообщений;

12.4. за возможное раскрытие/непредставление информации в случае несвоевременного сообщения Клиентом об изменении Контактных данных для получения SMS-сообщений/электронных сообщений;

12.5. за недоставку Push-уведомлений на Мобильное устройство Уполномоченного лица, возникающие с отсутствием сети Интернет;

12.6. за возможное разглашение Клиентом третьим лицам Логина, Пароля, PIN-кода, используемых Клиентом при работе с Мобильным Банком, и возникшие в связи с этим финансовые последствия и репутационные риски;

12.7. за сбои, возникающие в сетях операторов сотовой связи и сервисах провайдеров, которые могут привести к невозможности доступа к Системе ДБО посредством Мобильного приложения;

12.8. за ущерб, причиненный Клиенту, в случае, если прекращение полномочий лиц, утративших право распоряжаться Счетом, не было своевременно документально подтверждено Клиентом;

12.9. за искажение/несвоевременное получение Клиентом сведений/информации, передаваемой с использованием Мобильного банка, по не зависящим от Банка причинам, в том числе в случаях, когда имел место сбой в работе операторов сотовой связи и сервисах провайдеров;

12.10. за сбои в работе Мобильного банка, обусловленные неисправностью Мобильного устройства Клиента, внесением Клиентом самостоятельно в Мобильное приложение изменений или иными внешними факторами;

12.11. за возможное раскрытие информации в случае компрометации соответствующего канала связи (электронная почта, SMS, мессенджеры и иные каналы) при направлении Клиентом реквизитов Счета контрагентам с использованием Мобильного банка;

12.12. за несвоевременное получение контрагентом Клиента информации о реквизитах Счета, передаваемой с использованием Мобильного банка, по не зависящим от Банка причинам, в том числе в случаях, когда имел место сбой в работе операторов сотовой связи и сервисах провайдеров;

12.13. за задержки и сбои исполнения ЭД Банком в случае, если указанные задержки и сбои связаны с нарушениями работоспособности PayControl, а также за негативные последствия, в т.ч. в виде убытков, связанные с неправомерным доступом третьего лица к МУ Уполномоченного лица, в том числе с целью изменения (редактирования), подмены ЭПД Клиента, составляемых для направления в Банк;

12.14. за задержки и сбои передачи ЭД из 1С:Предприятие в Банк в случае, если указанные задержки и сбои связаны с нарушениями работоспособности 1С:Предприятие и/или 1С:DirectBank, а также за негативные последствия, в т.ч. в виде убытков, связанные с неправомерным доступом злоумышленников в 1С:Предприятие, в том числе с целью изменения (редактирования), подмены ЭПД Клиента, составляемых для направления в Банк;

12.15. за убытки Клиента, которые могут возникнуть в силу приостановления предоставления услуги из-за неработоспособности 1С:Предприятие и/или 1С:DirectBank или несвоевременной обработки ЭД Уполномоченным лицом до момента отправки ЭД в Банк;

12.16. за неисполнение, несвоевременное исполнение ЭД Клиента, созданных в 1С:Предприятие, в случае если указанные ЭД не поступили/несвоевременно поступили в Банк по причине сбоя в работе 1С:Предприятие и/или 1С:DirectBank;

12.17. за возможные последствия, связанные с переходом Клиента на сайт партнерского web-сервиса «Светофор», в случае его компрометации (взлома). Банк освобождается от ответственности с момента подтверждения Клиентом факта ознакомления с уведомлением о рисках, указанных в пунктах 12.16 и 12.17 настоящего Порядка, независимо от фактического ознакомления (прочтения) Клиента с ним. Уведомление доводится до Клиента Банком при первом использовании Сервиса «Светофор». Клиент гарантирует ознакомление всех

Уполномоченных лиц, с уведомлением и несет ответственность за возникшие риски, вызванные несоблюдением Уполномоченными лицами соответствующих мер;

12.18. за корректность данных, получаемых от партнерского web-сервиса «Светофор», и достоверность источников их получения. Банк освобождается от ответственности с момента подтверждения Клиентом факта ознакомления с уведомлением, указанным в п. 12.15 настоящего Порядка;

12.19. за возможное отсутствие в Системе ДБО информации о результатах проверки контрагентов в случае сбоя в работе партнерского web-сервиса «Светофор»;

12.20. за возможное раскрытие информации в случае утраты Клиентом МУ и/или SIM-карт с Номерами телефонов УЛ, указанных в предоставленных в Банк заявлениях;

12.21. за возможное раскрытие/непредоставление информации в случае несвоевременного сообщения Клиентом об изменении Номеров телефонов УЛ и/или Адресов электронной почты УЛ, указанных в переданном в Банк заявлении;

12.22. за возможное раскрытие информации в связи с несанкционированным доступом третьих лиц к электронному почтовому ящику Клиента или перехватом электронных сообщений, произошедших не по вине Банка;

12.23. за неисполнение или просрочку исполнения ЭД Клиента, если таковые произошли из-за отсутствия инициативы Клиента в установлении сеанса связи с Банком в соответствии с п.13.5 настоящего Порядка;

12.24. за ошибочное перечисление (неперечисление) денежных средств, связанное с неправильным указанием Клиентом в расчетных документах реквизитов получателя средств;

12.25. за неисполнение или несвоевременное исполнение распоряжений Клиента, в случае если электронный документ оформлен ненадлежащим образом и/или результаты проверки ЭП электронного документа некорректны, а также при возникновении у Банка обоснованного подозрения о компрометации ключа ЭП Клиента;

12.26. за убытки, понесенные Клиентом в связи с указанием Клиентом неверных Контактных данных в соответствии в п. 3.11 настоящего Порядка;

12.27. за убытки, понесенные Клиентом в связи с указанием Клиентом/Уполномоченным лицом в Интернет-банке неверного дополнительного номера телефона для Услуги Информирования.

13. КЛИЕНТ ОБЯЗУЕТСЯ:

13.1. Обеспечить конфиденциальность информации, связанной с использованием Системы ДБО, за исключением случаев, предусмотренных Законодательством РФ.

13.2. При возникновении подозрений в нарушении безопасности Системы ДБО, несанкционированного доступа к Системе ДБО, выявлении признаков, фактов или возможности таких нарушений:

- немедленно приостановить использование Системы ДБО до даты устранения обстоятельств, их повлекших;
- проинформировать о наличии подозрений в нарушении безопасности Системы ДБО, выявлении признаков, фактов или возможности таких нарушений службу технической поддержки Банка по телефону, указанному на официальном сайте Банка/ на сайте Системы ДБО с целью временной блокировки учетной записи Клиента/Уполномоченного лица в Системе ДБО;
- передать письменное сообщение о данном факте в Банк в течение одного рабочего дня;
- осуществить генерацию новых ключей ЭП.

13.3. Производить замену Криптографических ключей при смене Уполномоченного лица, а также в любое время по требованию Банка. Предоставлять заявление в письменном виде в порядке и по форме, утвержденной Банком.

13.4. За собственный счет поддерживать в рабочем состоянии аппаратные и программные технические средства, обеспечивающие функционирование Системы ДБО, в том числе Мобильное устройство.

13.5. В целях обеспечения оперативности обработки Клиентом информации, передаваемой ему в виде ЭД в рамках организованного информационного обмена, связанного с обслуживанием Клиента в Банке, и поддержания ее актуальности, осуществлять не менее одного сеанса электронной связи с Банком посредством Системы ДБО в каждый рабочий день Банка.

13.6. Представить в Банк сведения, информацию и документы, необходимые Банку в связи с осуществлением обслуживания Клиента с использованием Системы ДБО, в том числе, сведения и документы, позволяющие идентифицировать лиц (лицо), имеющих право подписывать ЭД ЭП, а также сведения, информацию и документы, необходимые Банку для выполнения требований Законодательства РФ.

13.7. При смене Уполномоченного лица либо окончании срока его полномочий в соответствии с карточкой с образцами подписей и оттиска печати, предоставленной в Банк, внесении изменений в иные сведения, подлежащие установлению Банком при заключении Договора ДБО, изменении реквизитов, уведомить о данном обстоятельстве Банк и представить в Банк новые документы, содержащие сведения об указанных изменениях, в порядке и по форме, установленным в Банке.

13.8. Организовать внутренний режим функционирования рабочего места Уполномоченного лица таким образом, чтобы исключить возможность доступа к Системе ДБО лиц, не имеющих таких полномочий.

13.9. Исключить возможность использования паролей доступа, ключей ЭП, Сеансовых ключей не уполномоченными лицами. Не допускать при использовании ключевых носителей следующих ситуаций:

- несанкционированного копирования ключевых носителей;
- вывода ключей ЭП на дисплей (монитор) ПК или принтер;
- установки ключевых носителей в считывающее устройство ПК в непредусмотренных Системой ДБО режимах, а также в другие ПК;
- записи на Ключевые носители посторонней информации.

13.10. Осуществлять смену Логина и/или Пароля, кода доступа (PIN-кода) к Мобильному приложению по требованию Банка, а также, в случае выявления их компрометации.

13.11. Использовать предоставленные Банком средства Системы ДБО только для целей, определенных Правилами.

13.12. Соблюдать Правила информационной безопасности при работе в системе дистанционного банковского обслуживания (Приложение №3 к настоящему Порядку).

13.13. Немедленно сообщать в Банк:

- в случае подозрения о компрометации ключа ЭП (или подозрения на компрометацию ключа ЭП) и необходимости аннулирования Сертификата ключа проверки ЭП скомпрометированного ключа ЭП, в том числе в случае подозрения о компрометации ключа ЭП при утрате либо краже МУ, на которое (-ые) установлено Мобильное приложение с возможностью подписания ЭД;

- об исключении Уполномоченных лиц, имеющих право доступа к Системе ДБО, в том числе в связи с увольнением, а также об изменении состава лиц – владельцев ЭП и/или их прав и т.д.

Извещение Банка может осуществляться при личном посещении подразделения Банка путем предоставления на бумажном носителе Заявления об изменениях ДБО с соответствующими отметками или по телефону службы технической поддержки Банка, указанному на официальном сайте Банка/ на сайте Системы ДБО, с последующим предоставлением на бумажном носителе Заявление об изменениях ДБО с соответствующими отметками не позднее 2 (Второго) рабочего дня, следующего за днем обращения в службу технической поддержки Банка. При этом возобновление работы Системы ДБО осуществляется путем предоставления Клиентом в Банк Заявления об изменениях ДБО с соответствующими отметками на бумажном носителе, в том числе генерации ключа ЭП;

- о случаях утраты либо кражи МУ и/или SIM-карт с Номерами телефонов УЛ, указанных в переданном в Банк заявлении Клиента, в соответствии с п.7.4 настоящего Порядка, выявлении факта несанкционированного доступа третьих лиц к электронному почтовому ящику, указанному в заявлении Клиента, Клиент обязан незамедлительно уведомить об этом службу технической поддержки Банка по телефону, указанному на официальном сайте Банка/ на сайте Системы ДБО, для отключения Номера(-ов) телефона(-ов) УЛ и Адреса(-ов) электронной почты УЛ от Услуги Информирования, с последующим предоставлением в течение 2 (двух) рабочих дней с даты соответствующего информирования Банка Заявления об изменениях ДБО Клиента. При этом возобновление предоставления Услуги Информирования осуществляется путем предоставления Клиентом в Банк Заявления в порядке, определенном п.7.10 настоящего Порядка.

13.14. Предоставить в Банк и своевременно актуализировать контактную информацию (номера мобильного и городского телефонов, адрес электронной почты) для экстренной связи с Клиентом, путем представления в Банк соответствующего письменного заявления в порядке и по форме, утвержденным в Банке.

13.15. Обеспечить предоставление в Банк и своевременную актуализацию контактной информации (номера мобильного и городского телефонов, адрес электронной почты) для экстренной связи с Уполномоченными лицами.

13.16. Обеспечить допуск к работе в Мобильном приложении только Уполномоченным лицам, указанным Клиентом в Заявлении ДБО/Заявлении об изменениях ДБО.

13.17. Передавать по требованию Банка распоряжения без использования Системы ДБО в случае невозможности их передачи с использованием Системы ДБО по техническим причинам, возникновения у Банка сомнений в подлинности переданных от имени Клиента электронных документов и в иных случаях, предусмотренных п. 11.7 настоящего Порядка, а также при нарушении Клиентом его обязанностей, предусмотренных Договором ДБО, до устранения причин невозможности передачи документов и/или опасных последствий допущенных нарушений.

14. КЛИЕНТ ИМЕЕТ ПРАВО:

14.1. Получать выписки по Счету (Счетом) Клиента и иную информацию, имеющую отношение к расчетно-кассовому обслуживанию Клиента, в виде ЭСИД.

14.2. Передавать в Банк и получать от Банка расчетные и иные документы, имеющие отношение к обслуживанию в Банке, не только в электронном виде, но и иными способами, установленными Договором.

14.3. В любое время по своему усмотрению подключить/отключить свои Счета к/от Системы ДБО, прекратить (в т.ч. временно)/возобновить свою работу в Системе ДБО, представив в Банк письменное заявление в порядке и по форме, установленным Банком.

14.4. В любое время, по своему усмотрению осуществлять смену своих Криптографических ключей.

В любое время по своему усмотрению заявить о смене способа получения Сеансовых ключей, Номера телефона УЛ, о выдаче нового eToken PASS/Рутокена, подключения нового Номера телефона УЛ путем представления в Банк соответствующего письменного заявления в порядке и по форме, утвержденным в Банке.

14.5. В любое время по своему усмотрению сменить Логин и/или Пароль в Интернет-банке. Восстановить Пароль для доступа в Систему ДБО с использованием функционала Интернет-банка. Для этого необходимо заранее установить контрольный вопрос (вопрос, используемый для восстановления Пароля) в Интернет-банке и предоставить в Банк сведения о Контактных данных Клиента/Уполномоченного лица, в случае если Контактные данные ранее не предоставлялись. Контактные данные можно предоставить путем подачи в Банк Заявления ДБО/Заявления об изменениях ДБО на бумажном носителе или Заявления о назначении Контактных данных посредством Системы ДБО.

В процессе восстановления Пароля, после успешного ввода необходимых данных и верного ответа на контрольный вопрос, Банк направляет Клиенту/Уполномоченному лицу временный пароль на Номер телефона УЛ. Действие временного пароля ограничено, далее Клиенту/Уполномоченному лицу необходимо изменить временный пароль на постоянный в Интернет-банке.

Для восстановления Логина Клиенту необходимо предоставить в Банк Заявление об изменениях ДБО с соответствующими отметками. Далее Банк направляет Уполномоченному лицу Логин и Пароль на Номер телефона УЛ, указанный Клиентом в Заявлении об изменениях ДБО.

14.6. В случае возникновения у Клиента претензий, связанных с предоставлением или не предоставлением и/или исполнением ЭД, требовать от Банка проведения технической экспертизы в соответствии с порядком, установленным Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций (Приложение № 1 к настоящему Порядку).

14.7. Предъявлять претензии по услугам, оказанным с использованием Системы ДБО, в течение 10 (Десяти) рабочих дней с даты осуществления операции. По каждой операции оформляется отдельная претензия.

14.8. Осуществлять проверку своих контрагентов с использованием Сервиса «Светофор» при наличии информации о соответствующем контрагенте в базе данных партнерского web-сервиса «Светофор» в порядке, установленном Правилами осуществления проверки Клиентом своих контрагентов с использованием Сервиса «Светофор» (Приложение № 6 к настоящему Порядку).

15. СРОК ДЕЙСТВИЯ ДОГОВОРА ДБО И ПОРЯДОК ЕГО РАСТОРЖЕНИЯ

15.1. Договор ДБО действует одновременно с заключенным(ими) между Клиентом и Банком Договором банковского счета, иными договорами, соглашениями и т.п. между Сторонами по предоставлению/оказанию Банком Клиенту банковских услуг, в рамках которого(ых) возможно осуществление дистанционного банковского обслуживания и информационного обмена ЭД между Сторонами посредством Системы ДБО.

15.2. Каждая из Сторон вправе отказаться от исполнения Договора ДБО в одностороннем порядке, письменно уведомив об этом противоположную сторону не позднее, чем за 10 (Десять) рабочих дней до даты расторжения в следующем порядке:

15.2.1. В случае расторжения Договора ДБО по инициативе Банка, в том числе в соответствии с п. 11.2 настоящего Порядка, Банк письменно уведомляет об этом Клиента не позднее, чем за 10 (десять) рабочих дней до даты предполагаемого расторжения Договора ДБО посредством направления уведомления о расторжении Договора ДБО по Системе ДБО и/или посредством почтовой связи по почтовому адресу, имеющемуся в Банке. Обязательства Банка по приему и исполнению ЭД с использованием Системы ДБО считаются прекращенными с даты, указанной в уведомлении о расторжении Договора ДБО.

15.2.2. В случае расторжения Договора ДБО по инициативе Клиента, последний обязан передать в Банк (в т.ч. с использованием Системы ДБО) Заявление о расторжении Договора ДБО, составленное по форме установленной Банком.

Все надлежащим образом оформленные ЭД Клиента, направленные Клиентом в Банк до даты расторжения Договора ДБО, указанной в Заявлении о расторжении Договора ДБО, подлежат исполнению Банком в соответствии с условиями Договора ДБО. С даты расторжения Договора ДБО, указанной в Заявлении о расторжении Договора ДБО, Банк прекращает прием ЭД Клиента.

15.2.3. При расторжении Договора ДБО, Клиент обязуется уничтожить все Ключевые носители, содержащие Криптографические ключи, удалить СКЗИ, использовавшихся для формирования и проверки ЭП, Лицензии, переданные Банком, и прочие компоненты средств ЭП.

15.3. В случае невыполнения Клиентом своих обязательств по Договору ДБО, а также в случае возникновения задолженности Клиента по оплате услуг в рамках Договора ДБО, Банк вправе в одностороннем порядке приостановить действие Договора ДБО до устранения выявленных нарушений/задолженности, о чем Клиенту сообщается с использованием Системы ДБО. Возобновление действия Договора ДБО производится после устранения указанных нарушений/задолженности. В случае невыполнения Клиентом требования Банка об устранении нарушений или допущения нарушений, устранение которых не представляется возможным, обслуживание Клиента по Системе ДБО прекращается, а Договор ДБО расторгается в порядке, определенном настоящими документом.

15.4. В случае прекращения или временного отключения Клиента от обслуживания с использованием Системы ДБО Клиент доставляет в Банк документы на бумажном носителе в установленном в Банке порядке.

ПОЛОЖЕНИЕ
о порядке проведения технической экспертизы при возникновении спорных ситуаций

1. В настоящем Положении под спорной ситуацией понимается существование претензий у одной из Сторон, справедливость которых может быть однозначно установлена по результатам проверки обмена документами с помощью Системы ДБО.
2. Сторона, заявляющая о наличии разногласий, (инициатор спора) обязана направить другой Стороне заявление о разногласиях, подписанное уполномоченным лицом Стороны, с подробным изложением причин разногласий и предложением создать разрешительную комиссию. Заявление должно содержать фамилии представителей Стороны – инициатора спора, которые будут участвовать в работе комиссии, место, время и дату сбора комиссии.
3. В состав комиссии должно входить равное количество представителей от каждой из Сторон. При необходимости, с письменного согласия каждой из Сторон, в состав комиссии могут быть дополнительно введены эксперты третьей стороны.
4. Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке.
5. Срок работы комиссии устанавливается не более 5 (Пяти) рабочих дней с даты сбора комиссии. В исключительных ситуациях этот срок может быть увеличен по взаимной договоренности Сторон.
6. Стороны способствуют работе комиссии и не допускают отказа от предоставления необходимых документов. При необходимости Стороны обязаны предоставить комиссии возможность ознакомиться с условиями и порядком работы Системы ДБО. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы ДБО. Информация, содержащаяся в данном журнале, может быть использована при разрешении спорных ситуаций разрешительной комиссией.
7. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение стороны, несущей ответственность согласно выводу об истинности ЭД, содержащего информацию об операциях, совершенных по счетам.
8. Разрешительная комиссия в течение 5 (Пяти) дней проводит рассмотрение заявления, которое включает в себя техническую экспертизу ЭД, на основании которого выполнены оспариваемые действия, техническую экспертизу ключа проверки ЭП, которым подписан этот ЭД и техническую экспертизу корректности ЭП в ЭД.
9. По итогам работы комиссии составляется акт, в котором в обязательном порядке отражаются: состав комиссии, действия членов комиссии, установленные обстоятельства, выводы, влияющие на возможность установления подлинности оспариваемого ЭД и основания, которые послужили для формирования выводов.
10. Банк несет ответственность перед Клиентом в случае, когда имело место хотя бы одна из следующих ситуаций:

    – Банк не предъявляет ЭД, переданного Клиентом, на основании которого Банк выполнил операции по счету Клиента;

    – ЭП Клиента в ЭД оказалась некорректной.
11. Банк не несет перед Клиентом ответственности по выполненным операциям со счетов Клиента в случае, когда одновременно выполнены следующие условия: Банк предъявляет ЭД, корректность ЭП Клиента признана разрешительной комиссией, принадлежность Клиенту ключа проверки ЭП Клиента подтверждена.
12. Если предложение о создании комиссии оставлено другой Стороной без ответа, либо Сторона отказывается от участия в комиссии, либо в работе комиссии были учинены препятствия, которые не позволили комиссии оформить надлежащий акт, заинтересованная Сторона в одностороннем порядке составляет акт с указанием причины его составления. В указанном акте фиксируются обстоятельства, позволяющие сделать вывод о том, что оспариваемый документ, произведенный в рамках Договора о дистанционном банковском обслуживании с использованием Системы ДБО, является надлежащим, либо формулируется вывод об обратном. Указанный акт направляется другой Стороне для сведения.

13. При рассмотрении в суде споров о наличии документа, исполненного с помощью Системы ДБО и подписанного ЭП, заинтересованная Сторона обязана предоставить суду акт, составленный в соответствии с настоящей Процедурой.

Приложение №2
к Порядку обмена электронными документами
с использованием системы ДБО

КОД №ЮЛАПКПЭП

АКТ признания ключа проверки электронной подписи
для обмена сообщениями в Системе ДБО

"____"_____20_г. г._____

Настоящим Актом признается ключ проверки электронной подписи Клиента.

Сведения о Клиенте:

1. Наименование: _____

Сведения об Уполномоченном лице:

1. Фамилия, имя, отчество: _____

С Правилами информационной безопасности при работе в системе дистанционного банковского обслуживания в АО «СМП Банк» ознакомлен, согласен и обязуюсь их выполнять.

Настоящим подтверждаю, что ЭП создана лично мной без участия третьих лиц.

Для экстренной связи прошу использовать:

№ тел._____, адрес электронной почты_____.

Личная подпись Уполномоченного лица _____

Текст ключа проверки электронной подписи:

Ключ проверки электронной подписи зарегистрирован и может использоваться для обмена сообщениями.

БАНК	**КЛИЕНТ**
Акционерное общество Банк «Северный морской путь»	_____
ИНН _____	ИНН _____
Тел. _____	Тел. _____
_____ должность руководителя	_____ должность руководителя
_____/ _____ М.П. подпись ФИО	_____/ _____ М.П. подпись ФИО

**АКТ подтверждения идентификатора ключа
для обмена сообщениями в Системе ДБО**

"____"_____20_г.

Настоящим Актом АО «СМП Банк» (Банк) признает ключ проверки электронной подписи Клиента.

Сведения о Клиенте:

Наименование: _____

Сведения об Уполномоченном лице:

Фамилия, имя, отчество: _____

С Правилами информационной безопасности при работе в системе дистанционного банковского обслуживания в АО «СМП Банк» ознакомлен, согласен и обязуюсь их выполнять.
Настоящим подтверждаю, что ЭП создана лично мной без участия третьих лиц.

Личная подпись Уполномоченного лица _____

Идентификатор ключа: _____

ОТ БАНКА	**ОТ КЛИЕНТА**
_____/ _____	_____/ _____
М.П. подпись ФИО	М.П. подпись ФИО руководителя

ПРАВИЛА
информационной безопасности при работе
в системе дистанционного банковского обслуживания в АО «СМП Банк»

1. Общие положения

1.1. Термины и определения.

Защитная мера - сложившаяся практика, процедура или механизм, которые используются для уменьшения Риска нарушения Информационной безопасности в Системе.

Злоумышленник - лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

Злоумышленные действия – любые действия, совершаемые Злоумышленником в Системе.

Информационная безопасность - безопасность, связанная с Угрозами в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

Инцидент - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию Угрозы Информационной безопасности.

Обработка риска нарушения информационной безопасности - процесс выбора и осуществления Защитных мер, снижающих Риск нарушения Информационной безопасности, или мер по переносу, принятию или уходу от Риска.

Риск - мера, учитывающая вероятность реализации Угрозы и величину потерь (ущерба) от реализации этой Угрозы.

Риск нарушения информационной безопасности - Риск, связанный с Угрозой Информационной безопасности.

Угроза - опасность, предполагающая возможность потерь (ущерба).

1.2. Правила информационной безопасности при работе в системе дистанционного банковского обслуживания в АО «СМП Банк» (далее - Правила) составлены в соответствии с требованиями Законодательства Российской Федерации, СТАНДАРТОМ БАНКА РОССИИ СТО БР ИББС-1.0-2014 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» и другими нормативными документами Банка России, Международными стандартами ISO 27001:2005 и ISO 17799:2005, а также Политикой информационной безопасности АО «СМП-Банк» и являются обязательными к исполнению Клиентами, заключившими Договор ДБО.

1.3. Настоящие Правила определяют Защитные меры по Обработке Рисков нарушения Информационной безопасности при использовании Клиентами Системы ДБО. При этом Клиент обязан учитывать то, что:

- Сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- Существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- Существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из сети Интернет;
- Гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
- Меры по нейтрализации Злоумышленных действий могут быть эффективными только в течение первых часов после Инцидента;
- Расследованием Злоумышленных действий и поиском Злоумышленников занимаются правоохранительные органы. В целях проведения расследования пострадавшая сторона должна предоставить в распоряжение следственных органов компьютер, который использовался для доступа в Систему, для проведения экспертизы.

2. Ограничение ответственности Банка

2.1. В связи с тем, что для доступа к услугам дистанционного обслуживания, предоставляемым Банком через Систему ДБО, Клиент использует технические и программные средства, не принадлежащие Банку, Банк не несет ответственности за любые, в том числе Злоумышленные, действия третьих лиц в отношении и/или с использованием технических и программных средств, когда-либо использовавшихся Клиентом.

2.2. За пользование нелицензированным программным обеспечением Клиент несет уголовную ответственность в соответствии со статьей 146 УК РФ.

2.3. Срок для предъявления Банку претензий по услугам, оказанным с использованием Системы ДБО, составляет 10 календарных дней с даты осуществления операции. По каждой опротестовываемой операции оформляется отдельная претензия. Решение по претензии принимается Банком в течение 30 (тридцати) рабочих дней со дня подачи заявления в офисе Банка и предоставления Клиентом необходимого пакета документов, в соответствии с п. 3.27 настоящих Правил.

2.4. Окончательное решение об использовании предлагаемых Банком в разделе 3 Защитных мер принимает Клиент.

2.5. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы ДБО. Содержимое журнала Системы ДБО используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования Злоумышленных действий.

3. Клиент должен применять следующие защитные меры:

3.1. Не сообщать посторонним лицам, а также кому бы то ни было через сеть Интернет, логины и пароли доступа к ресурсам Банка, историю операций, контактные и учетные данные, так как эти данные могут быть перехвачены Злоумышленником и использованы для получения доступа к Вашим счетам.

3.2. Не записывать логин и пароль на бумаге, мониторе или клавиатуре.

3.3. Не использовать функцию запоминания логина и пароля в браузерах.

3.4. Не использовать одинаковые логин и пароль для доступа к различным системам.

3.5. Всегда явным образом завершать сеанс работы с Системой ДБО, используя пункт меню «Выход».

3.6. В случае если доступ к Системе ДБО осуществляется с использованием постороннего ПК, не рекомендуется сохранять на нем идентификационные данные и другую информацию, а после завершения всех операций нужно убедиться, что идентификационные данные и другая информация не сохранились. После возвращения к штатному ПК обязательно менять логин и пароль.

3.7. В случае, если доступ к Системе ДБО осуществляется посредством Мобильного банка, для получения Сеансовых ключей рекомендуется использовать мобильное устройство, отличное от МУ, или eToken PASS.

3.8. В случае получения на электронную почту письма с просьбой обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе – сайт Банка), Клиент должен перезвонить в Службу технической поддержки по телефону (495) 980-24-80 и 8-800-555-2-555 и сообщите о письме или перешлите его на адрес bk@smpbank.ru. Банк никогда не просит передать данные по электронной почте. Обновление данных осуществляется только сотрудником Банка в присутствии представителя Клиента предъявившего документ, удостоверяющего личность. Не открывать ссылки, указанные в сомнительном письме, в котором просят указать конфиденциальные данные. Не звонить по телефонам, указанным в подобных письмах и не отвечать на них.

3.9. Не открывать приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть идентификационные данные для входа в Систему ДБО и ключи ЭП.

3.10. МУ должно быть защищено паролем на использование и настроено на блокировку при отсутствии активности пользователя по истечении заданного интервала времени, например, 3-х минут.

3.11. Регулярно, не реже одного раза в месяц, производить смену пароля ПК. При составлении пароля ПК использовать прописные и строчные буквы, цифры, а также различные символы,

например: ! / { } [ ] < >. Настоятельно рекомендуется использовать специализированные программы-генераторы паролей.

3.12. Не использовать в качестве пароля имена, памятные даты, номера телефонов.

3.13. Не позволять третьим лицам производить за Вас (Клиента) генерацию Криптографических ключей.

3.14. Присоединять Ключевой носитель[10] к ПК непосредственно перед началом работы с Системой ДБО. По окончании работы извлекать Ключевой носитель из ПК.

3.15. Использовать лицензированное программное обеспечение. Необходимо ПОМНИТЬ: помимо того, что Клиент несет уголовную ответственность за пользование нелицензированным программным обеспечением в соответствии со статьей 146 УК РФ, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на ПК/МУ Клиента.

3.16. Использовать лицензионное, обновляемое не реже одного раза в сутки антивирусное ПО.

3.17. Регулярно (не реже раза в неделю) проводить проверку на наличие новых версий программного обеспечения, установленного на ПК, производить установку обновлений операционной системы.

3.18. Четко регламентировать порядок использования ПК/МУ, с которого осуществляется взаимодействие с Системой ДБО, в том числе список лиц и порядок доступа к ПК/МУ. Не рекомендуется использовать указанный ПК/МУ для доступа к посторонним сайтам.

3.19. Не устанавливать на ПК/МУ, который используется для взаимодействия с Системой ДБО, постороннее программное обеспечение, например программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Доказано, что подобные программы передают информацию о содержимом просматриваемых страниц посторонним лицам.

3.20. Не запускать на своем ПК/МУ программы, полученные из незаслуживающих доверия источников.

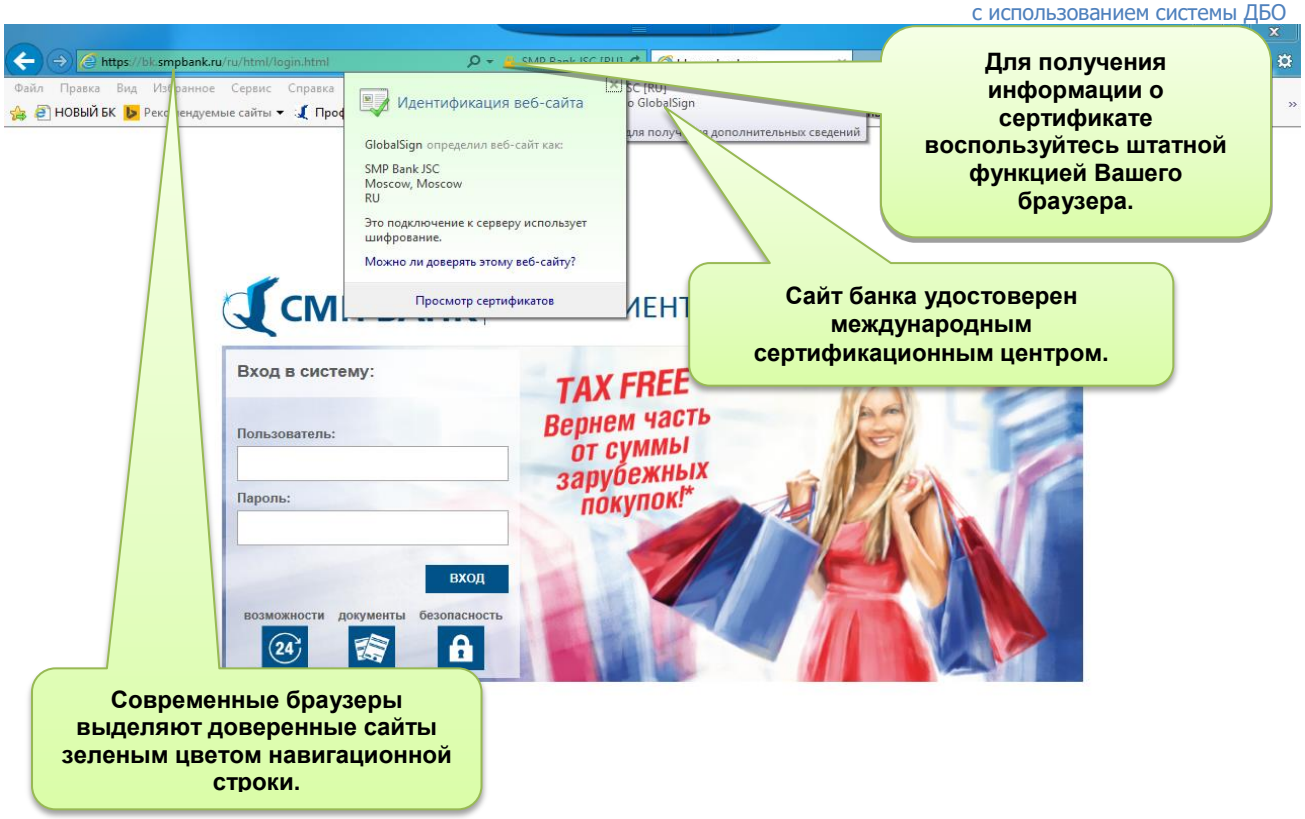
3.21. Использовать межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

3.22. Настроить браузер на использование протокола защищенной связи TLS. Использование протоколов семейства SSL не обеспечивает надлежащей защиты.

3.23. Не хранить незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к счетам Клиента.

3.24. Перед вводом своего логина и пароля убедиться, что установлено соединение с легальным сайтом. Проверить правильность указания адреса сайта, наличие сертификата безопасности.

[10] С целью безопасной двухфакторной аутентификации, генерации и защищенного хранения Криптографических ключей рекомендуется использовать Рутокен ЭЦП 2.0



В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов АО "СМП Банк", просьба сообщить об этом по электронной почте bk@smpbank.ru.

3.25. Настроить механизм информирования о входе в Систему ДБО и совершаемых операциях на электронную почту. Регулярно проверять почтовый ящик, а также журнал операций Системы ДБО. Поддерживайте свою контактную информацию в Системе ДБО в актуальном состоянии для того, чтобы в случае необходимости с Клиентом можно было оперативно связаться. В целях оперативного реагирования на Злоумышленные действия пользоваться услугой дополнительного информирования.

3.26. В случае обнаружения подозрительных действий, совершенных от имени Клиента в Системе, незамедлительно сменить логин и пароль, сообщить об Инциденте в Службу технической поддержки и произвести смену Криптографических ключей.

3.27. В случае обнаружения несанкционированных действий со средствами, находящимися на счетах Клиента, необходимо в максимально короткий срок отозвать Сертификат ключа проверки электронной подписи и оформить заявление в операционном подразделении Банка в свободной форме, содержащее максимально подробное описание Инцидента, для инициирования расследования. Для проведения расследования необходимо по согласованию со службой технической поддержки передать в Банк файлы протоколов, подтверждающие установку обновлений операционной системы ПК и антивирусного программного обеспечения, и в течение 5 (пяти) рабочих дней представить в операционное подразделение Банка для снятия копий документы, подтверждающие факт законного приобретения операционной системы и антивирусного программного обеспечения, а также копию договора об оказании услуг по предоставлению доступа в сеть Интернет или иного удостоверяющего факт заключения подобного договора документа (квитанция, чек, счет и тому подобные) и иные документы, которые Клиент сочтет необходимыми для рассмотрения претензии по существу. В случае невозможности представления необходимых файлов и документов об этом делается соответствующая запись на заявлении с указанием причины. Необоснованный отказ в предоставлении требуемых документов может являться основанием для отказа в удовлетворении заявленных Клиентом требований. Решение об обращении в правоохранительные органы Клиент принимаете самостоятельно.

ПАМЯТКА ДЛЯ КЛИЕНТОВ
о действиях в случае обнаружения несанкционированного списания

В случае обнаружения несанкционированного списания со счета Банк рекомендует Клиенту осуществить следующие действия:

1. Максимально оперативно представить письменное заявление в Банк, заверенное печатью и подписью руководителя, по возможности, на бланке организации о факте несанкционированного списания с указанием даты, суммы платежа, других известных Клиенту обстоятельств, а также с просьбой об оказании содействия в возврате несанкционированно списанных денежных средств. Указанное заявление необходимо представить в Банк на бумажном носителе в срок не позднее 2-х рабочих дней с даты устного обращения в Банк.
2. Не использовать компьютеры, которые эксплуатировались для работы в Системе ДБО. Их необходимо отключить от корпоративной сети[11]. С высокой долей вероятности они заражены специализированным вредоносным программным обеспечением, поэтому этот шаг позволит предотвратить последующие Инциденты, а также сохранить доказательства для проведения технической экспертизы.
3. Произвести смену Криптографических ключей, используемых для работы с Системой ДБО в соответствии с действующим Договором. **До момента смены ключей работа в Системе ДБО будет прекращена в связи с компрометацией действующих средств доступа.**
4. По факту несанкционированного доступа к компьютерной информации обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по статьям 158, 159.3, 272 и 273 УК РФ в связи с созданием, использованием и распространением неустановленными лицами вредоносных компьютерных программ, повлекшим неправомерный доступ неустановленных лиц к Вашей компьютерной информации, что, в свою очередь, привело к несанкционированному Клиентом переводу денежных средств Клиента.
5. С копией указанного заявления с приложением копии талона правоохранительного органа о приеме заявления, обратиться в Арбитражный суд с исковым заявлением в отношение банка-получателя о возврате неосновательного обогащения с ходатайством об аресте похищенной суммы денежных средств на счете получателя в банке получателя и раскрытии персональных данных получателя в целях привлечения его в качестве соответчика (гл. 60 ГК РФ) Если известны полные реквизиты получателя – физического лица, указанный иск подается в суд общей юрисдикции.
6. Копии вышеуказанных обращений в правоохранительные органы и суд с отметками о приеме необходимо предоставить в Банк для того, чтобы Банк мог оказать содействие в возврате несанкционированно списанных средств.

Указанные действия произвести в течение 2-х рабочих дней с даты обнаружения несанкционированного списания в целях оперативного противодействия дальнейшему переводу и обналичиванию денежных средств.

[11] Для обеспечения возможности снятия дампа оперативной памяти скомпрометированного ПК, в случае привлечения специалистов для проведения экспертизы, электропитание ПК рекомендуется не отключать.

Акт приема-передачи
электронных идентификаторов Рутокен ЭЦП 2.0

г. Москва _____._____. 2021 г.

Настоящий Акт составлен о том, что согласно Порядку обмена электронными документами с использованием системы ДБО:

АО «СМП Банк» передал, а

Клиент_____
(наименование юридического лица или статус: индивидуальный предприниматель/адвокат/нотариус и ФИО)

ИНН _____
принял Рутокены ЭЦП 2.0 в количестве ___ шт.

_____
номер носителя

_____
номер носителя

_____
номер носителя

_____
номер носителя

Дальнейший учет и использование Рутокен ЭЦП 2.0 производится Клиентом в соответствии с Правилами информационной безопасности при работе в системе дистанционного банковского обслуживания и действующим законодательством РФ.

Настоящий Акт составлен в двух экземплярах, по одному для Банка и Клиента.

Клиент:	**АО «СМП Банк»:**
_____ / _____/	_____ / _____/
	М. П.
«_____»_____2021 г.	«_____»_____2021 г.

ПРАВИЛА
осуществления проверки Клиентом своих контрагентов с использованием Сервиса «Светофор»

1. Сервис «Светофор» предоставляет Клиенту возможность получать экспресс-отчет по контрагентам с использованием партнерского web-сервиса «Светофор». С помощью экспресс-отчета можно выявлять контрагентов, в отношении которых имеется негативная информация.
2. Экспресс-отчет по контрагенту является результатом автоматического анализа информации, собранной партнерским web-сервисом «Светофор» из открытых и общедоступных источников, в т.ч. информационных баз органов государственной власти (ЕГРЮЛ, ЕГРИП, ФССП и др.). Результаты отчета могут изменяться с течением времени в результате деятельности контрагента.
3. Клиенту доступны следующие возможности получения экспресс-отчета в Системе ДБО:
   - **Цветовой статус** контрагента представляет собой цветовое обозначение наиболее значимой категории, характеризующей факты о деятельности контрагента;
   - **Сводный экспресс-отчет** содержит информацию о категориях, обнаруженных фактов деятельности контрагента, отсортированных по уровню значимости;
   - **Полный экспресс-отчет** содержит полный список обнаруженных фактов деятельности контрагента, отсортированных по уровню значимости.
4. Получение цветового статуса доступно Клиенту при выполнении следующих операций в Системе ДБО (за исключением подсистемы Мобильный банк):
   - Формирование нового/редактирование существующего ЭПД;
   - Просмотр списка ЭПД;
   - Просмотр справочника корреспондентов (контрагентов);
   - Добавление новой/редактирование существующей записи в справочнике корреспондентов (за исключением подсистемы Мобильный банк).
5. Получение сводного экспресс-отчета доступно Клиенту из:
   - Окна формирования нового/редактирования существующего ЭПД;
   - Формы списка ЭПД;
   - Формы списка справочника корреспондентов (контрагентов);
   - Окна добавления новой/редактирования существующей записи в справочнике корреспондентов (за исключением подсистемы Мобильный банк).
6. Получить полный экспресс-отчет Клиент может перейдя по ссылке из сводного экспресс-отчета на сайт партнерского web-сервиса «Светофор». Переход на сайт партнерского web-сервиса «Светофор» означает принятие Клиентом рисков, указанных в п. 12.15 настоящего Порядка.
7. По результатам проведенной проверки Клиент самостоятельно принимает решение о проведении или не проведении платежа в отношении проверяемого получателя средств.

Сублицензионное соглашение

Настоящее сублицензионное соглашение (далее – Соглашение) в соответствии с п. 1 ст. 428 Гражданского кодекса Российской Федерации является формой, определяющей условия договора в форме присоединения, является неотъемлемой частью Порядка обмена электронными документами с использованием системы ДБО (далее – Порядок ДБО).

1. Термины и определения, используемые в настоящем Соглашении, значения которых не указаны, имеют те же значения, что и соответствующие термины и определения, содержащиеся в Порядке ДБО.
2. В рамках настоящего Соглашения под СКЗИ «КриптоПро CSP» понимается копия программы «КриптоПро CSP» версии не ниже 4.0 для ПК, разработанная «ООО «КРИПТО-ПРО» ОГРН 10377000854444 (далее - Правообладатель). Исключительное право на СКЗИ «КриптоПро CSP» принадлежит Правообладателю.
3. Клиент имеет право использовать СКЗИ «КриптоПро CSP» в соответствии с его назначением и правилами пользования, изложенными в эксплуатационной документации и иных соглашениях на сайте Правообладателя (https://www.cryptopro.ru). Клиент самостоятельно несет ответственность перед Правообладателем за свои действия в случае нарушения правил пользования, изложенных в эксплуатационной документации на сайте Правообладателя.
4. В рамках настоящего Соглашения Банк передает Клиенту право на использование СКЗИ «КриптоПро CSP» на условиях простой (неисключительной) лицензии на 1 (Одном) рабочем месте (на 1 (Одном) ПК) Клиента для осуществления электронного документооборота с использованием электронной подписи с Банком. Клиент в соответствии с настоящим Соглашением получает право на использование СКЗИ «КриптоПро CSP» на территории Российской Федерации на срок действия настоящего Соглашения.
5. Заключение Соглашения осуществляется путем присоединения Клиента к настоящему Соглашению в случае если в Заявлении на ДБО/Заявлении на изменение ДБО/Заявлении на подключение/отключение услуги «Интеграция 1С:DirectBank» в качество способа приобретения лицензии на право использования СКЗИ «КриптоПро CSP» выбрано поле по ее приобретению у Банка. Настоящие условия Соглашения, не являются публичным предложением (офертой) заключить Соглашение.
6. Сублицензионное соглашение вступает в силу с момента присоединения Клиента к соглашению, определяемого моментом списания со Счета Клиента комиссии за приобретение лицензии, установленной Тарифами Банка, и действует в течении срока действия Договора ДБО, но не более срока действия исключительных прав Правообладателя на СКЗИ «КриптоПро CSP». Настоящее Соглашение досрочно прекращает свое действие в случае прекращения действия Договора ДБО с момента прекращения действия Договора ДБО.
7. После оплаты комиссии Банк передает Клиенту право на использование СКЗИ «КриптоПро CSP» путем указания номера Лицензии по Акту приема-передачи права на использование СКЗИ «КриптоПро CSP» (Приложение № 1 к настоящему Соглашению) на 1 (Одном) рабочем месте (далее – Акт).
8. Клиент не имеет право передавать третьим лицам, тиражировать и опубликовывать номер Лицензии, переданный Банком Клиенту по Акту.
9. Банк не несет ответственность за косвенные или побочные убытки, ущерб или вред, включая упущенную прибыль, перерывы в хозяйственной деятельности, потерю деловой информации и т.п., которые могут возникнуть у Клиента в результате использования СКЗИ «КриптоПро CSP».
10. Стороны освобождаются от ответственности, за частичное или полное неисполнение принятых на себя обязательств, вследствие возникновения обстоятельств непреодолимой силы (форс-мажора).
11. Под форс-мажором понимаются обстоятельства, которые возникли после присоединения Клиента к настоящему Соглашению в результате непредвиденных и неотвратимых событий чрезвычайного характера, к числу которых относятся (но не ограничиваются): пожар, стихийное бедствие, война, какие бы то ни было военные действия, блокады, запрещение определенных коммерческих операций, акт государственного органа, в результате издания которого исполнение обязательств становится невозможным полностью или частично.

12. При наступлении форс-мажора, срок исполнения обязательств отодвигается соразмерно времени, в течение которого будут действовать такие обстоятельства и их последствия.
13. Все споры, разногласия, требования, возникающие из настоящего Соглашения или касающиеся его нарушения, прекращения, недействительности, подлежат разрешению в Арбитражном суде г. Москвы с обязательным соблюдением досудебного претензионного порядка в соответствии с действующим законодательством Российской Федерации.
14. Банк в праве в одностороннем порядке вносить изменения/дополнять в настоящее Соглашение в порядке, установленном Договором банковского обслуживания для внесения изменений в Договор банковского обслуживания.

Приложение №1
к Сублицензионному соглашению

Акт приема-передачи
права на использование СКЗИ «КриптоПро CSP»

г. Москва _____._____. 2021 г.

Настоящий Акт составлен о том, что согласно Сублицензионному соглашению, являющемуся неотъемлемой частью Порядка обмена электронными документами с использованием системы ДБО,

АО «СМП Банк» передал, а

Клиент_____
(наименование юридического лица или статус: индивидуальный предприниматель/адвокат/нотариус и ФИО)

ИНН _____

принял право на использование СКЗИ «КриптоПро CSP»:

_____
номер лицензии

на условиях и порядке, установленных Сублицензионным соглашением.

Дальнейший учет и использование лицензии производятся Клиентом в соответствии с Порядком обмена электронными документами с использованием системы ДБО, Правилами информационной безопасности при работе в системе дистанционного банковского обслуживания и действующим законодательством РФ.

Настоящий Акт составлен в двух экземплярах, по одному для АО «СМП Банк» и Клиента.

Клиент:	**АО «СМП Банк»:**
_____ / _____/	_____ / _____/
	М. П.
«_____»_____2021 г.	«_____»_____2021 г.