Публичное акционерное общество «Западно-Сибирский коммерческий банк»
(ПАО «Запсибкомбанк»)

УТВЕРЖДЕНЫ
Приказом Президента ПАО «Запсибкомбанк»

"29" апреля 2016 г. N 21/1045_R4

Правила

обслуживания Клиентов с использованием Интернет-технологий (система «ЗапСиб iNet»)

Редакция №4
(с Изменениями №1, утвержденными Приказом от 21.10.2016. № 476,
с Изменениями №2, утвержденными Приказом от 13.02.2017г. № 59,
с Изменениями №3, утвержденными Приказом от 07.08.2017г. №360,
с Изменениями №4, утвержденными Приказом от 05.12.2017г. №591)

г. Тюмень, 2016 г.

Оглавление

1. Общие положения

1.1. «Правила обслуживания Клиентов с использованием Интернет-технологий (система «ЗапСиб iNet») (далее – Правила) определяют порядок обслуживания Клиентов с использованием системы «ЗапСиб iNet».

1.2. Правила являются неотъемлемой частью Договора о дистанционном банковском обслуживании с использованием Интернет-технологий (система «ЗапСиб iNet») (далее – Договор по «ЗапСиб iNet»).

1.3. Все Приложения к настоящим Правилам являются неотъемлемой их частью и обязательны для исполнения Банком и Клиентом.

1.4. Правила регламентируют требования и принципы работы Клиентов в системе дистанционного банковского обслуживания «ЗапСиб iNet» (далее – система «ЗапСиб iNet»/ система ДБО).

Полный функционал системы «ЗапСиб iNet» представлен в Инструкции по работе с системой, размещенной на официальном сайте Банка – www.zapsibkombank.ru.

Банк предоставляет Клиентам право использования системы «ЗапСиб iNet» по назначению в рамках систем дистанционного банковского обслуживания, осуществлять установку, наладку системы «ЗапСиб iNet» безвозмездно по сублицензионному договору (простая (неисключительная) лицензия на использование принадлежит Банку на основании лицензионного договора).

1.5. Подключение Клиентов осуществляется к системе «ЗапСиб iNet» с Пакетом безопасности.

1.6. Все Клиенты, обслуживающиеся по системе «ЗапСиб iNet» без Пакета безопасности, при очередной плановой либо внеплановой смене ключа ЭП переводятся Банком на обслуживание по системе «ЗапСиб iNet» с Пакетом безопасности в соответствии с п. 3.1.5. настоящих Правил (если иное не предусмотрено соглашением между Банком и Клиентом).

2. Термины и обозначения

Администратор Сертификационного Центра Банка – работник Банка, в обязанности которого входит выпуск и отзыв сертификатов ключей проверки электронной подписи.

Банк – Публичное акционерное общество «Западно-Сибирский коммерческий банк» (ПАО «Запсибкомбанк»), его филиалы, дополнительные офисы, операционные офисы и иные внутренние структурные подразделения.

Банковский счет – расчетные, текущие, транзитные счета, в том числе бюджетные счета, открытые на основании Договоров банковского счета (счетов) в рублях и иностранной валюте, на которые зачисляются и с которых могут расходоваться денежные средства организаций, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой (нотариусы, адвокаты), корпоративные счета, открытые для учета операций Клиентов по международным расчетным корпоративным банковским картам VISA Business, VISA Business Gold, а также счета, открываемые Клиенту для учета денежных средств, размещаемых в Банке с целью получения процентного дохода по вкладу по договорам банковского вклада (депозитные счета).

«Белый список» или Список доверенных получателей платежей (далее – «Белый список») – это список контрагентов (физических и юридических лиц, индивидуальных предпринимателей), в пользу которых Клиентом Банка регулярно совершаются платежи по определенным параметрам (реквизитам) ЭД, устанавливаемым с согласия Клиента.

Владелец сертификата ключа проверки электронной подписи – лицо, на имя которого Сертификационным Центром Банка выдан сертификат ключа проверки электронной подписи и которому принадлежат соответствующие ключи электронной подписи, позволяющие с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы электронной подписью).

Внеплановая смена ключа электронной подписи – смена ключа электронной подписи в случае, когда уполномоченное лицо Клиента меняет существующий ключевой носитель на Rutoken ЭЦП до момента истечения срока действия сертификата ключа проверки электронной подписи, в том числе при компрометации ключа проверки электронной подписи, смене уполномоченного лица Клиента, поломке ключевого носителя.

Вредоносное программное обеспечение (ПО) – программное обеспечение, которое разрабатывается для получения несанкционированного доступа к персональному компьютеру, а также к данным, которые на нем хранятся. Программы предназначены для нанесения ущерба владельцу информации или ПК, путем копирования, искажения, удаления или подмены информации.

Договор банковского вклада юридического лица (индивидуального предпринимателя, адвоката, нотариуса) (далее – Договор банковского вклада) **–** договор между Банком и Вкладчиком, заключенный путем присоединения Вкладчика к Правилам организации работы по

привлечению средств юридических лиц, индивидуальных предпринимателей, адвокатов, нотариусов по Договорам банковского вклада Банка (действующая редакция), согласно которому Банк, принявший от Вкладчика на депозитный счет денежные средства, обязуется возвратить сумму вклада и выплатить проценты на условиях и в порядке, предусмотренных договором и Правилами организации работы по привлечению средств юридических лиц, индивидуальных предпринимателей, адвокатов, нотариусов по Договорам банковского вклада Банка (действующая редакция).

Доставка электронного документа – физический процесс перемещения электронного документа от отправителя к получателю.

Заявка на размещение вклада – это электронный документ, который содержит условия размещения денежных средств в депозит, формируемый и направляемый пользователем в системе «ЗапСиб iNet» в разделе «Депозиты».

Информационный посредник – это лицо, осуществляющее передачу материала в информационно-телекоммуникационной сети, в том числе в сети Интернет, лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети, лицо, предоставляющее возможность доступа к материалу в этой сети.

Клиент (владелец сертификата ключа проверки электронной подписи) – юридическое лицо, индивидуальный предприниматель без образования юридического лица, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, заключившее (-ий) с Банком Договор банковского счета в рублях и/или иностранной валюте и Договор «ЗапСиб iNet», которому выдан сертификат ключа проверки электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, известная владельцу сертификата ключа проверки электронной подписи и предназначенная для создания электронной подписи и шифрования электронного документа с использованием средств электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи, доступная Банку и Клиенту и предназначенная для проверки подлинности электронной подписи в электронном документе.

Ключевой носитель – информационный носитель, содержащий криптографические ключи.

Компрометация ключа электронной подписи – нарушение конфиденциальности, угроза доступа неуполномоченных лиц (лиц, не наделенных правом распоряжения денежными средствами, находящимися на счете, с использованием электронной подписи (аналога собственноручной подписи)). К событиям, связанным с нарушением конфиденциальности, компрометацией ключа электронной подписи, относятся следующие события:

- утрата ключевых носителей;
- утрата ключевых носителей с их последующим обнаружением;

- увольнение работников, имевших доступ к ключевой информации;
- нарушение правил хранения ключа электронной подписи;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате чьих-либо несанкционированных действий).

Корректная электронная подпись Клиента – электронная подпись электронного документа, проверка которой с использованием соответствующего ключа проверки электронной подписи дает положительный результат, которая соответственно обладает свойствами:

- уникальна для подписанного документа при использовании ключа электронной подписи;
- подлинность ее может быть удостоверена Банком и Клиентом;
- она неразрывно связана с конкретным документом и только с ним.

Отправитель электронного документа – юридическое лицо, индивидуальный предприниматель без образования юридического лица, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, которое (-ый) непосредственно направляет или от имени которого направляется электронный документ, за исключением лиц, действующих в качестве информационных посредников в отношении этого документа.

Пакет безопасности – сервис, предоставляемый Банком и включающий комплекс мер, предназначенных для защиты денежных средств Клиента от удаленных атак на систему «ЗапСиб iNet». Пакет безопасности включает в себя устройство визуализации подписываемых в системе ДБО электронных документов SafeTouch с подключенной услугой «Белый список».

Перевод денежных средств – действия Банка в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика.

Плановая смена ключа электронной подписи – смена ключа электронной подписи, вызванная окончанием срока действия сертификата ключа проверки электронной подписи, по истечению 1 (одного) года 3 (трех) месяцев с момента выдачи Банком сертификата ключа проверки электронной подписи.

Получатель электронного документа – физическое, юридическое лицо, индивидуальный предприниматель без образования юридического лица, которому электронный документ отправлен самим отправителем или от имени отправителя за исключением лиц, действующих в качестве информационных посредников в отношении этого документа.

Пользователь – лицо, которое по решению Клиента наделено правом осуществлять работу в системе «ЗапСиб iNet».

Разрешительная комиссия – группа лиц из состава Клиента и Банка, действующая на основании доверенности уполномоченного лица Клиента и распорядительного документа уполномоченного лица Банка, соответственно, в задачи которой входит урегулирование конфликтной ситуации между сторонами в досудебном порядке с привлечением экспертов в областях информационных технологий и информационной безопасности.

Сервис визуального подтверждения платежа - возможность проверки и подтверждения реквизитов электронного документа на дисплее SafeTouch .

Сертификат ключа проверки электронной подписи – документ на бумажном носителе с собственноручной подписью или электронный документ с электронной подписью администратора Сертификационного Центра Банка, который включает в себя ключ проверки электронной подписи и который выдается администратором Сертификационного Центра Банка уполномоченному лицу Клиента для подтверждения принадлежности электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификационный Центр Банка – подразделение Департамента информационных технологий Банка, в обязанности которого входит создание и выдача сертификатов ключей проверки электронных подписей (удостоверяющий центр).

Средства криптографической защиты информации (далее по тексту - СКЗИ) – совокупность программно-технических средств, обеспечивающих применение электронной подписи и шифрования при организации электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Средства электронной подписи (далее по тексту - СЭП) – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной подписи в электронном документе с использованием ключа электронной подписи, подтверждение с использованием сертификата ключа проверки электронной подписи подлинности электронной подписи в электронном документе, создание ключей проверки электронной подписи и ключей электронной подписи. СЭП могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Система «ЗапСиб iNet» – автоматизированная компьютерная система, устанавливается на любое рабочее место или несколько рабочих мест, соответствующих требованиям настоящих Правил, имеющих доступ к сети Интернет. Пользователь входит в систему через Интернет браузер. При использовании данной системы все электронные документы хранятся на сервере системы «ЗапСиб iNet». Система позволяет Клиенту осуществлять передачу электронных документов в Банк по сети Интернет. Действия по подготовке электронных документов Клиент производит на сайте Банка, являющемся составной частью комплекса обслуживания Клиента с использованием системы «ЗапСиб iNet».

Система «ЗапСиб iNet» является информационной, коммуникационной и операционной, поскольку предоставляет Клиенту возможность совершать расходные операции по его счету путем оформления распоряжений о переводе денежных средств и направления их в Банк, а также получать выписки по счету, обмениваться официальными письмами с Банком и распечатывать платежные поручения, согласно которым Банком осуществляется зачисление средств на счет Клиента. В системе «ЗапСиб iNet» также возможно просматривать и распечатывать иные расчетные документы, согласно которым Банком осуществляется списание денежных средств со счета Клиента и зачисление денежных средств на счет Клиента, просматривать информацию об ограничениях к расчетному счету, предъявленных к счету в соответствии с нормами действующего законодательства РФ.

Трансграничный перевод денежных средств – перевод денежных средств, при осуществлении которого плательщик либо получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого плательщика или получателя средств обслуживает иностранный центральный (национальный) банк или иностранный банк.

Уполномоченные лица Клиента – лица, наделенные правом распоряжения денежными средствами, находящимися на счете Клиента в пределах срока полномочий лиц, указанных в карточке с образцами подписей и оттиска печати.

Уполномоченное лицо Клиента с уровнем подписи А – единоличный исполнительный орган Клиента и/или иной представитель Клиента, действующий от имени Клиента в силу закона, доверенности, договора либо по иному основанию, имеющий полномочия на заключение договора о дистанционном банковском обслуживании с использованием Интернет-технологий (система «ЗапСиб iNet»), распределение прав пользователям системы «ЗапСиб iNet», распоряжение денежными средствами на банковском(их) счете(ах) без ограничений, заключение договоров банковского вклада в системе «ЗапСиб iNet» от имени Клиента в соответствии с представленными в Банк документами.

Услуга «Белый список» – услуга, предоставляемая Клиенту Банком, в рамках которой Клиент самостоятельно определяет Список доверенных получателей платежей. При отправке платежных документов контрагентам из Белого списка, не превышающим установленный лимит, не требуется дополнительный контроль Банка, при этом платежи иным получателям, не относящимся к Списку доверенных получателей платежей, и платежи, не проходящие по лимиту, дополнительно подтверждаются Клиентом.

Устройства обеспечения безопасности - совокупность устройств, предназначенных для защиты денежных средств Клиента от удаленных атак на систему «ЗапСиб iNet» (Rutoken ЭЦП и SafeTouch).

Формат электронного документа – перечень реквизитов (полей) документа и правил их заполнения.

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

Электронная подпись (далее - ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В настоящих Правилах под ЭП понимается усиленная неквалифицированная электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа ЭП;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с помощью средств ЭП.

Электронный документ (далее по тексту – ЭД) – информация, подписанная ЭП и представленная в электронно-цифровой форме, пригодной для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронный документооборот – это система ведения документации, при которой весь массив создаваемых, передаваемых и хранимых документов поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сетевую структуру, предусматривающую возможность формирования и ведения распределенной базы данных, в которой ЭД признается приоритетным над бумажным документом, создается, корректируется и хранится в компьютере. Обмен ЭД включает в себя:

- формирование ЭД в формате, установленном для данного ЭД;
- регистрацию ЭД;
- проверку ЭД на соответствие установленному формату, а также на предмет подлинности всех ЭП ЭД;
- подтверждение получения ЭД;
- отзыв ЭД;
- учет ЭД (регистрацию входящих и исходящих ЭД);
- хранение ЭД (ведение архивов ЭД);
- создание дополнительных экземпляров ЭД;
- создание бумажных копий ЭД.

Электронное средство платежа – это средство и (или) способ, позволяющие Клиенту составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-

коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Rutoken ЭЦП – физический носитель, предназначенный для хранения ключа ЭП и ключа проверки ЭП, являющийся персональным средством аутентификации пользователей системы «ЗапСиб iNet», имеющих право подписи, и обеспечивающий доступ к распоряжению счетом и обмену ЭД по системе «ЗапСиб iNet».

SafeTouch – внешнее устройство визуализации подписываемых в системе «ЗапСиб iNet» ЭД, позволяющее защитить денежные средства Клиентов от удаленных атак на систему «ЗапСиб iNet» при помощи дополнительного подтверждения реквизитов ЭД на данном устройстве. При использовании SafeTouch перед отправкой ЭД в Банк информация об ЭД (основные реквизиты) поступает в SafeTouch и отображается на экране устройства, при этом информационный обмен с Rutoken ЭЦП заблокирован до момента нажатия на кнопку подтверждения. При нажатии Клиентом на кнопку подтверждения ЭД успешно отправляется в Банк, при нажатии на кнопку отказа документ в Банк не отправляется, происходит отмена операции. Устройство SafeTouch может использоваться Клиентом только при работе в системе «ЗапСиб iNet».

3. Общие положения об обеспечении Клиенту доступа к системе «ЗапСиб iNet».

3.1. Порядок ввода системы «ЗапСиб iNet» в эксплуатацию.

3.1.1. Основанием ввода системы «ЗапСиб iNet» в эксплуатацию является заключенный между Банком и Клиентом Договор «ЗапСиб iNet» при условии предварительного оформления Заявления на подключение системы ДБО (Приложение 1 к настоящим Правилам).

3.1.2. В согласованные с Клиентом сроки, но не позднее 3 (трех) рабочих дней с момента оформления и передачи в Банк Заявления на подключение системы ДБО (Приложение 1 к настоящим Правилам), при условии обязательного заполнения раздела 3 Заявления на подключение системы ДБО (Приложение 1 к настоящим Правилам) Банк предоставляет Клиенту:

– Установочный пакет, включающий Рутокен Плагин, JCWebClients – плагины для работы с электронной подписью, Драйвер Rutoken (Клиент самостоятельно скачивает с официального сайта Банка – www.zapsibkombank.ru).

  Предусмотрена проверка целостности установочного пакета, размещенного на официальном сайте Банка. Контрольная сумма для проверки целостности указывается на странице со ссылкой на установочный пакет. Порядок проверки целостности указан в Инструкции по настройке системы;

– Первичный пароль для Rutoken ЭЦП, который в дальнейшем должен быть заменен на уникальный пароль в соответствии с Инструкцией по настройке системы «ЗапСиб iNet»;Код пользователя (логин) и первичный пароль для входа в Систему «ЗапСиб iNet», который в дальнейшем должен быть заменен на уникальный пароль в соответствии с Инструкцией для клиентов по работе в системе «ЗапСиб iNet»;

– Ключевой носитель Rutoken ЭЦП. Количество, получаемых Клиентом Rutoken ЭЦП, определяется Заявлением о подключении системы ДБО (Приложение 1 к настоящим Правилам) и оплачивается согласно Тарифам Банка;

– Пакет безопасности. Количество получаемых Клиентом пакетов безопасности определяется Заявлением о подключении системы ДБО (Приложение 1 к настоящим Правилам) и оплачивается согласно Тарифам Банка.

Инструкции для клиентов по работе в системе «ЗапСиб iNet» (Клиент самостоятельно скачивает с официального сайта Банка – www.zapsibkombank.ru).

3.1.3. Рабочее место Клиента, на которое устанавливается система «ЗапСиб iNet», должно соответствовать следующим требованиям:

- Компьютер с установленной лицензионной операционной системой MS Windows 7/8;
- Лицензионное антивирусное программное обеспечение с актуальными базами;
- Монитор, поддерживающий разрешение экрана не менее 1280x720 точек, параметры цветности не менее 16 бит;
- Канал доступа в сеть Интернет со скоростью приема/передачи данных не ниже 512 кБит/с;
- Открытые порты TCP 443, 448;

- Открытый доступ к USB-порту;
- Работоспособный принтер, подключенный к компьютеру автоматизированного рабочего места.

3.1.4. При открытии Клиенту нового счета (расчетного, текущего, корпоративного) отображение данного счета у пользователей Клиента в системе «ЗапСиб iNet» и наделение указанных пользователей Клиента соответствующими полномочиями осуществляется на основании представленного Клиентом надлежаще заполненного Заявления на подключение системы ДБО (Приложение 1 к настоящим Правилам). Оформленное Клиентом Заявление на подключение системы ДБО должно быть подписано уполномоченным лицом Клиента с уровнем подписи А и заверено печатью (при наличии). Данное Заявление передается в Банк на бумажном носителе либо в виде сканированного документа, отправленного в Банк с использованием системы «ЗапСиб iNet».

Пользователю Клиента, который на 21.10.2016г. является единственным уполномоченным лицом Клиента с уровнем подписи А, по которому у Банка отсутствует информация по ограничениям в части распоряжения счетами от единоличного исполнительного органа/не имеющему лимитов на распоряжение денежными средствами на депозитных счетах, на которого выпущен сертификат ключа проверки электронной подписи в системе «ЗапСиб iNet», отображаются в системе «ЗапСиб iNet» все открытые Клиенту депозитные счета. Вновь открываемые Клиенту депозитные счета также подлежат отображению в системе «ЗапСиб iNet» для данного пользователя при наличии соответствующих полномочий.

Для получения возможности отображения всех открытых и вновь открываемых депозитных счетов у пользователя Клиента, не указанного в абзаце втором настоящего пункта Правил, и наделения указанного пользователя Клиента соответствующими полномочиями необходимо предоставить Заявление на подключение системы ДБО (Приложение 1 к настоящим Правилам). Оформленное Клиентом Заявление на подключение системы ДБО должно быть подписано уполномоченным лицом Клиента с уровнем подписи А и заверено печатью (при наличии). Данное Заявление передается в Банк на бумажном носителе либо в виде сканированного документа, отправленного в Банк с использованием системы «ЗапСиб iNet».

Полномочия пользователя Клиента, указанного в первом и третьем абзацах настоящего пункта Правил, подтверждаются представленными в Банк документами либо их надлежаще заверенными копиями, содержащими необходимые полномочия и позволяющими произвести идентификацию пользователя Клиента в соответствии с требованиями Федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

При необходимости пользователю/пользователям Клиента может быть ограничен доступ к просмотру и управлению счетом/счетами по выбору Клиента. Для этого Клиенту необходимо

предоставить в Банк Заявление на подключение системы ДБО, заполненное в соответствующей части.

Заявление на подключение системы ДБО должно быть подписано уполномоченным лицом Клиента с уровнем подписи А и заверено печатью (при наличии). Данное Заявление передается в Банк на бумажном носителе либо в виде сканированного документа, отправленного в Банк с использованием системы «ЗапСиб iNet».

3.1.5. Пользователю Клиента, который на «05» декабря 2017г. является единственным уполномоченным лицом Клиента с уровнем подписи А, по которому у Банка отсутствует информация по ограничениям в части полномочий на просмотр информации в модуле «Кредиты» системы «ЗапСиб iNet» от единоличного исполнительного органа, в указанном модуле отображается информация по всем действующим договорам кредитования, заключенным между Банком и Клиентом, а также по договорам кредитования, обязательства по которым были полностью исполнены Клиентом в течение 3 (трех) лет до даты первого входа пользователя Клиента в модуль «Кредиты» системы «ЗапСиб iNet». Информация по вновь заключаемым между Банком и Клиентом договорам кредитования также подлежит отображению в системе «ЗапСиб iNet» для данного пользователя при наличии полномочий на просмотр информации в модуле «Кредиты» системы «ЗапСиб iNet».

Для получения возможности отображения информации в модуле «Кредиты» системы «ЗапСиб iNet» у пользователя Клиента, не указанного в абзаце первом настоящего подпункта Правил, и наделения данного пользователя Клиента соответствующими полномочиями необходимо предоставить в Банк Заявление на подключение системы ДБО (Приложение 1 к настоящим Правилам). Заявление на подключение системы ДБО должно быть подписано уполномоченным лицом Клиента с уровнем подписи А и заверено печатью (при наличии). Данное Заявление передается в Банк на бумажном носителе либо в виде сканированного документа, отправленного в Банк с использованием системы «ЗапСиб iNet».

При необходимости пользователю/пользователям Клиента может быть ограничен доступ к информации, отображаемой в модуле «Кредиты» системы «ЗапСиб iNet». Для этого Клиенту необходимо предоставить в Банк Заявление на подключение системы ДБО (Приложение 1 к настоящим Правилам), заполненное в соответствующей части.

Полномочия пользователя Клиента, указанного в первом и втором абзацах настоящего подпункта Правил, подтверждаются представленными в Банк документами либо их надлежаще заверенными копиями, содержащими необходимые полномочия и позволяющими произвести идентификацию пользователя Клиента в соответствии с требованиями Федерального закона от 07.08.2001г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

3.1.6. При переходе/переводе Клиента с обслуживания по системе «ЗапСиб iNet» без Пакета безопасности на обслуживание по системе «ЗапСиб iNet» с Пакетом безопасности Клиенту

необходимо оформить Заявление на подключение системы ДБО (Приложение 1 к настоящим Правилам).

В случае, если Клиент при плановой либо внеплановой смене ключа ЭП не подключил Пакет безопасности, Банк вправе приостановить работу системы «ЗапСиб iNet» до момента подключения сервиса. Если Клиент в дальнейшем отказывается от подключения Пакета безопасности, то Договор «ЗапСиб iNet» прекращает свое действие по истечение десяти дней с даты смены ключа ЭП.

3.2. Порядок предоставления Банком Rutoken ЭЦП.

3.2.1. В качестве ключевого носителя Клиент в обязательном порядке использует Rutoken ЭЦП.

3.2.2. Rutoken ЭЦП предоставляется в количестве, равном количеству подписей в карточке с образцами подписей и оттиска печати, но не менее количества, равного одной подписи каждого уровня. Количество получаемых Клиентом Rutoken ЭЦП определяется заявлением о подключении системы ДБО (Приложение 1 к настоящим Правилам) и оплачивается согласно Тарифам Банка.

3.2.3. Банк передает Клиенту Rutoken ЭЦП:

- после проверки работоспособности ключевого носителя (выполняется работником Банка);
- после подписания обеими сторонами Акта приема-передачи Rutoken ЭЦП (Приложение 2 к настоящим Правилам).

Акт приема-передачи Rutoken ЭЦП оформляется в двух экземплярах. Один экземпляр Акта приема-передачи Rutoken ЭЦП остается у Клиента, второй экземпляр хранится в Банке и прилагается к Договору ДБО.

3.2.4. Передача Rutoken ЭЦП осуществляется Банком руководителю Клиента либо уполномоченному лицу на основании доверенности, оформленной по форме Приложения 3 к настоящим Правилам или нотариально удостоверенной.

3.2.5. Использование в качестве ключевых носителей Rutoken ЭЦП, полученных Клиентом не в Банке, запрещается.

3.3. Порядок предоставления Банком Пакета безопасности.

3.3.1. Пакет безопасности включает в себя устройство визуализации подписываемых в системе «ЗапСиб iNet» электронных документов SafeTouch с подключенной услугой «Белый список».

3.3.2. В качестве основных средств защиты отправляемых в Банк ЭД Клиент в обязательном порядке использует SafeTouch.

3.3.3. Для получения SafeTouch уполномоченное лицо Клиента предварительно оформляет Заявление на подключение системы ДБО (Приложение 1 к настоящим Правилам) и передает его в Банк.

3.3.4. Банк передает Клиенту SafeTouch:

- после проверки работоспособности SafeTouch (выполняется работником Банка);

- после оплаты Клиентом комиссионного вознаграждения согласно Тарифам Банка, если иной размер не установлен соглашением сторон;
- после подписания обеими сторонами Акта приема-передачи SafeTouch (Приложение 4 к настоящим Правилам).

3.3.5. Акт приема-передачи SafeTouch оформляется в двух экземплярах. Один экземпляр Акта приема-передачи SafeTouch остается у Клиента, второй экземпляр хранится в Банке и прилагается к Договору ДБО.

3.3.6. Передача SafeTouch осуществляется Банком руководителю Клиента либо уполномоченному лицу на основании доверенности, оформленной по форме Приложения 3 к настоящим Правилам или нотариально удостоверенной.

3.3.7. Использование устройства SafeTouch , полученного Клиентом не в Банке, запрещается.

3.4. Порядок оказания услуги «Белый список».

3.4.1. Услуга «Белый список» подключается только Клиентам, обсуживающимся по системе «ЗапСиб iNet» в составе Пакета безопасности.

3.4.2. Для подключения услуги «Белый список» и определения первичного перечня доверенных контрагентов руководителю Клиента либо уполномоченному лицу на основании доверенности необходимо оформить Заявление на подключение к системе ДБО Банка (Приложение 1 к настоящим Правилам).

3.4.3. В последующем Клиент самостоятельно редактирует перечень доверенных контрагентов путем добавления/удаления и корректировки лимитов платежа в рублях/иностранной валюте по контрагенту в рамках услуги «Белый список» с использованием отдельного раздела системы «ЗапСиб iNet».

3.4.4. Запрос Клиента на внесение изменений в «Белый список» подлежит обязательному подписанию Rutoken ЭЦП и подтверждается дополнительным средством защиты SafeTouch.

3.4.5. Основными параметрами «Белого списка» являются:

- наименование контрагента – обязательное к заполнению поле;
- БИК обслуживающего контрагента Банка – обязательное к заполнению поле;
- счет контрагента – обязательное к заполнению поле;
- ИНН контрагента – обязательное к заполнению поле;
- лимит платежа в рублях/иностранной валюте – предусматривает лимит в рамках одного платежного документа.

Поле не является обязательным к заполнению, в случае отсутствия необходимости установления лимита проставляется значение «не лимитировано».

3.5. Порядок подключения SMS-оповещений пользователям системы «ЗапСиб iNet».

3.5.1. К SMS-оповещениям системы «ЗапСиб iNet» относятся:

- дополнительный уровень авторизации пользователя системы «ЗапСиб iNet», путем ввода одноразового пароля для входа в систему, который направляется Банком Клиенту посредством SMS на номер сотового телефона, указанный в Заявлении на подключение системы ДБО (Приложение 1 к настоящим Правилам);
- информирование об успешной аутентификации пользователя в системе «ЗапСиб iNet» с помощью SMS на номер сотового телефона, указанный в Заявлении на подключение системы ДБО (Приложение 1 к настоящим Правилам);
- информирование о входе пользователя в систему «ЗапСиб iNet» с помощью SMS на номер сотового телефона, указанный в Заявлении на подключение системы ДБО (Приложение 1 к настоящим Правилам);
- SMS-информирование Клиента об успешном проведении платежного поручения, отправленного по системе «ЗапСиб iNet»;
- SMS-информирование Клиента о создании платежного поручения в системе «ЗапСиб iNet».

С другими сервисами Клиент может ознакомиться, зайдя в раздел «*Настройки» – «Оповещения» – «Настройка оповещений»* в системе «ЗапСиб iNet».

3.5.2. Для подключения SMS-оповещений по системе «ЗапСиб iNet» Клиенту необходимо в заявлении на подключение системы ДБО указать телефонный номер и контактное лицо (Приложение 1 к настоящим Правилам).

3.5.3. В случае отказа Клиентов от подключения SMS-оповещений по системе «ЗапСиб iNet», указанных в п. 3.5.1. настоящих Правил, Клиенту необходимо оформить Заявление на отказ от подключения SMS-оповещений (Приложение 6 к настоящим Правилам). В случае если Банку стали известны признаки/факты, указывающие на смену получателя SMS-сообщений от Банка, смену SIM-карты, прекращение обслуживания либо изменение номера телефона получателя SMS-сообщений, указанного в Заявлении на подключение системы ДБО (Приложение 1 к настоящим Правилам), Банк приостанавливает пересылку Клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации с уведомлением об этом Клиента любым доступным способом. Для возобновления отправки SMS-сообщений Банком Клиенту необходимо предоставить в Банк оформленное надлежащим образом и подписанное уполномоченным лицом Клиента новое Заявление на подключение системы ДБО (в случае смены пользователя системы ДБО)/Заявление о дополнении/изменении номеров телефонов в рамках SMS-оповещений (в случае смены номера телефона)/Заявление на разблокирование номера телефона (в случае если данные Клиента не изменились) (Приложение 19 к настоящим Правилам), которое может быть передано в Банк лично/ по системе ДБО.

3.6. Порядок формирования ключа ЭП и получения сертификата ключа проверки ЭП, а также порядок смены ключей ЭП и их аннулирования (отзыва).

3.6.1. Изготовление пользователем ключа ЭП и получение сертификата ключа проверки ЭП.

3.6.1.1. После передачи Банком Клиенту всех необходимых устройств, программного обеспечения, инструкций, указанных в п.3.2.-3.3. настоящих Правил, пользователь самостоятельно генерирует ключи ЭП на Rutoken ЭЦП. В результате генерации ключей ЭП создается ключ ЭП и ключ проверки ЭП. Ключ проверки ЭП создается путем направления запроса на изготовление сертификата ключа проверки ЭП в Сертификационный центр Банка. При возникновении трудностей и вопросов по генерации ключа ЭП Клиенту необходимо обратиться за консультацией в службу технической поддержки Банка.

3.6.1.2. Сертификат ключа проверки ЭП для пользователя с правом подписи может быть выпущен только на уполномоченное лицо Клиента, указанное в карточке с образцами подписи и оттиска печати и только в соответствии с карточкой с образцами подписей и оттиска печати, т.е.:

- если у Клиента имеется несколько уполномоченных лиц, обладающих равнозначным правом подписи, то Банком принимаются к исполнению распоряжения Клиента, содержащие подпись одного из нескольких уполномоченных лиц. На каждое лицо, которое будет подписывать документ в системе «ЗапСиб iNet», должен быть выпущен отдельный сертификат ключа проверки ЭП;
- если у Клиента имеется несколько уполномоченных лиц, обладающих неравнозначным правом подписи, то ЭД должен содержать одновременно подпись двух и более уполномоченных лиц. На каждое уполномоченное лицо, которое будет подписывать документ в системе «ЗапСиб iNet», должен быть выпущен отдельный сертификат ключа проверки ЭП. При этом в системе «ЗапСиб iNet» задается многоуровневая система подписи документов, т.е. отправка документов в Банк возможна только после подписания их двумя и более уполномоченными лицами Клиента.
- сертификат ключа проверки ЭП для пользователей системы «ЗапСиб iNet», не имеющих право подписи, не выпускается Банком.

3.6.1.3. Запрос на изготовление сертификата ключа проверки ЭП направляется пользователем по системе «ЗапСиб iNet» в Сертификационный центр Банка.

3.6.1.4. Сертификационный Центр Банка имеет право отказать пользователю в выпуске сертификата ключа проверки ЭП, если информация, указанная в запросе на выпуск сертификата ключа проверки ЭП, отличается от информации, указанной в Заявлении на подключение системы ДБО (Приложение 1 к настоящим Правилам). В этом случае Сертификационный Центр Банка уведомляет пользователя об отказе в выпуске сертификата ключа проверки ЭП с указанием причин любым способом (по телефону, электронной почте и пр.) не позднее рабочего дня, следующего за днем поступления запроса на выпуск сертификата ключа проверки подписи.

3.6.1.5. Если причин для отказа в выпуске сертификата ключа проверки ЭП не выявлено, администратор Сертификационного Центра Банка подписывает своей ЭП и направляет по системе ДБО сертификат ключа проверки ЭП пользователю не позднее рабочего дня, следующего за днем получения вышеуказанного запроса.

3.6.1.6. Пользователь, получив сертификат ключа проверки ЭП, на своих технических средствах с помощью программной среды, предоставляемой системой «ЗапСиб iNet», производит регистрацию сертификата ключа проверки ЭП согласно Инструкциям, размещенным на официальном сайте Банка (www.zapsibkombank.ru).

3.6.1.7. После регистрации сертификата ключа проверки ЭП пользователю необходимо распечатать 3 (три) экземпляра Сертификата ключа проверки ЭП на бумажном носителе.

3.6.1.8. Каждый экземпляр сертификата ключа проверки ЭП заверяется:

- собственноручной подписью пользователя, проходящего процедуру регистрации;
- собственноручной подписью руководителя и печатью Клиента;
- собственноручной подписью администратора Сертификационного Центра Банка и печатью Сертификационного Центра Банка, либо работником филиала Банка, уполномоченным на основании доверенности заверять собственноручной подписью и специально предусмотренной для этих целей печатью.

Два экземпляра Сертификата ключа проверки ЭП пользователя хранятся в Банке. Третий экземпляр находится у Клиента.

До момента предоставления трех экземпляров Сертификата ключа проверки ЭП пользователя в Банк возможность отправки ЭД в системе «ЗапСиб iNet» для пользователя заблокирована.

3.6.2. Порядок смены ключей ЭП пользователем.

3.6.2.1. При плановой и внеплановой смене ключа ЭП осуществляется изготовление нового ключа и сертификата ключа проверки ЭП.

3.6.2.2. При внеплановой смене ключа ЭП, в случае, если срок действия сертификата ключа проверки ЭП не истек и данные текущего пользователя системы «ЗапСиб iNet» не изменились, для изготовления нового ключа и сертификата ключа проверки ЭП пользователю необходимо выполнить указания, прописанные в пункте «Перевыпуск сертификата ключа проверки ЭП» «Инструкции для клиентов по работе в системе «ЗапСиб iNet», размещенной на официальном сайте Банка (www.zapsibkombank.ru). Процесс формирования ключа проверки ЭП и сертификата ключа проверки ЭП осуществляется аналогично процедуре, описанной в пп. 3.6.1.1.-3.6.1.8. настоящих Правил. При внеплановой смене ключа проверки ЭП в системе «ЗапСиб iNet» запрос на сертификат подписывается через систему с использованием действующего сертификата ключа проверки ЭП, за исключением случаев, описанных в пп 3.6.1. настоящих Правил. После выпуска нового сертификата на основании запроса, подписанного с использованием действующего сертификата ключа проверки ЭП, новому сертификату в системе автоматически устанавливается статус «Активен». Сертификату, действовавшему до момента выпуска нового сертификата, устанавливается статус «Заблокирован». Предоставление Сертификата ключа проверки ЭП на бумажном носителе в Банк не требуется.

3.6.2.3. При плановой смене ключа ЭП, когда срок действия сертификата истек, и при внеплановой смене ключа ЭП (поломка ключевого носителя, смена уполномоченного лица, ключ скомпрометирован), для изготовления нового ключа и сертификата ключа проверки ЭП необходимо предоставить в Банк Заявление на подключение системы ДБО (Приложение 1 к настоящим Правилам). Далее формирование ключа проверки ЭП и сертификата ключа проверки ЭП осуществляется аналогично процедуре, описанной в пп.3.6.1. настоящих Правил.

3.6.2.4. При смене Клиентом карточки с образцами подписей и оттиска печати в случае изменения уполномоченного лица, на имя которого изготовлен сертификат ключа проверки ЭП, необходимо предоставить в Банк письменное Заявление на подключение системы «ЗапСиб iNet» (Приложение 1 к настоящим Правилам). До момента смены сертификата ключа проверки ЭП прием и исполнение документов с использованием системы «ЗапСиб iNet» приостанавливаются Банком и осуществляются на бумажных носителях.

3.6.3. Аннулирование (отзыв) сертификата ключа проверки ЭП.

3.6.3.1. При внеплановой смене ключа ЭП, в случае, если срок действия сертификат ключа проверки ЭП не истек и данные текущего пользователя системы «ЗапСиб iNet» не изменились, предыдущий сертификат ключа проверки ЭП считается недействительным и аннулируется с момента выпуска нового сертификата ключа проверки ЭП на основании запроса, подписанного с использованием действующего сертификата ключа проверки ЭП.

3.6.3.2. При плановой смене ключа ЭП, когда срок действия сертификата ключа проверки ЭП истек, и при внеплановой смене ключа ЭП (поломка ключевого носителя, смена уполномоченного лица, ключ скомпрометирован), предыдущий сертификат ключа проверки ЭП считается недействительным и аннулируется с момента получения Банком заявления на подключение системы «ЗапСиб iNet» (Приложение 1 к настоящим Правилам). Клиент не сможет воспользоваться системой «ЗапСиб iNet» до момента завершения процедуры выпуска нового сертификата ключа проверки ЭП.

3.6.3.3. Клиент при увольнении работника, который является владельцем сертификата ключа проверки ЭП, обязан не позднее дня увольнения работника предоставить в Банк Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи (Приложение 8 к настоящим Правилам).

Аннулирование (отзыв) сертификата ключа проверки ЭП осуществляется не позднее рабочего дня с момента получения Банком Заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи (Приложение 8 к настоящим Правилам).

В случае предоставления Клиентом Заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи (Приложение 8 к настоящим Правилам) работа с сертификатом ключа проверки ЭП заканчивается.

3.6.3.4. Банк вправе аннулировать сертификаты ключей проверки ЭП пользователей в одностороннем порядке в случае, если Клиент находится в стадии банкротства/ликвидации.

3.7. Порядок заключения Договора банковского вклада посредством системы «ЗапСиб iNet».

3.7.1. Договор банковского вклада может быть заключен посредством системы «ЗапСиб iNet» в соответствии с параметрами, предусмотренными системой «ЗапСиб iNet» в разделе «Депозиты».

Договор банковского вклада заключается путем направления Клиентом Заявки на размещение вклада посредством системы «ЗапСиб iNet» (оферта) и принятия Банком суммы вклада на депозитный счет (акцепт). Заявка на размещение вклада должна быть подписана ЭП уполномоченного лица/уполномоченными лицами Клиента в соответствии с требованиями п. 4.3.1. настоящих Правил. Предоставление пользователю прав на формирование и подписание Заявки на размещение вклада в системе «ЗапСиб iNet» осуществляется в соответствии с порядком, установленным п. 3.1.4. настоящих Правил. Акцепт считается принятым Банком в момент зачисления суммы вклада на депозитный счет Клиента.

Сохранение сформированной пользователем Заявки на размещение вклада в перечне заявок в разделе «Депозиты» системы «ЗапСиб iNet» подтверждается присвоением указанной Заявке статуса «Подготовлен».

Факт подписания пользователем Заявки на размещение вклада подтверждается присвоением указанной Заявке статуса «Подписан» в перечне заявок в разделе «Депозиты» системы «ЗапСиб iNet».

По отправленной пользователем в Банк Заявке на размещение вклада в перечне заявок в разделе «Депозиты» системы «ЗапСиб iNet» отображается статус «Выгружен».

Прием Банком Заявки на размещение вклада подтверждается присвоением указанной Заявке в перечне заявок в разделе «Депозиты» системы «ЗапСиб iNet» статуса «Получен».

В случае отказа Банком в приеме Заявки на размещение вклада по причине отсутствия полномочий у пользователя прав на заключение Договора банковского вклада и подписание электронного документа, Заявке на размещение вклада в перечне заявок в разделе «Депозиты» системы «ЗапСиб iNet» присваивается статус «Отказано. Полномочия не подтверждены.».

В случае отказа Банком в приеме Заявки на размещение вклада по причине наличия действующих решений Федеральной налоговой службы (ФНС) о приостановлении операций по счетам Клиента, Заявке на размещение вклада в перечне заявок в разделе «Депозиты» системы «ЗапСиб iNet» присваивается статус «Отказано. Имеются приостановления ФНС по счетам налогоплательщика».

После получения Банком Заявки на размещение вклада от Клиента при отсутствии ограничений, препятствующих заключению Договора банковского вклада и открытию депозитного счета, указанных в настоящем пункте Правил, Банком открывается депозитный счет, отображаемый в перечне депозитов Клиента в разделе «Депозиты» системы «ЗапСиб iNet». До зачисления суммы депозита на депозитный счет в перечне депозитов Клиента в разделе «Депозиты» системы «ЗапСиб iNet» депозитный счет имеет статус «Ожидает пополнения до

ДД.ММ.ГГГГ», где ДД – день, ММ – месяц, ГГГГ – год. При этом Заявке на размещение вклада присваивается статус «Исполнен».

3.7.2. После пополнения Клиентом в установленный срок депозитного счета и зачисления Банком суммы депозита на депозитный счет (акцепт) в перечне депозитов Клиента в разделе «Депозиты» системы «ЗапСиб iNet» отображается открытый депозитный счет со статусом «Открыт».

Договор банковского вклада вступает в силу (считается заключенным) с момента зачисления Клиентом на депозитный счет в Банке суммы вклада в размере, установленном Договором банковского вклада.

Условия Договора банковского вклада указываются в Подтверждении о заключении договора банковского вклада, размещенного посредством системы «ЗапСиб iNet», (далее - Подтверждение). Указанный документ подписывается сотрудником Банка, уполномоченным на заключение договоров банковского вклада. Подтверждение вручается уполномоченному представителю Клиента под роспись, либо при неполучении уполномоченным представителем Клиента данного документа в течение одного рабочего дня с даты заключения Договора банковского вклада, направляется Клиенту заказным письмом по адресу, указанному в выписке из Единого государственного реестра юридических лиц/Единого государственного реестра индивидуальных предпринимателей. Документ, подтверждающий отправку Подтверждения Клиенту Банком, помещается в юридическое дело Клиента. Вместе с Подтверждением Банком выдается Вкладчику выписка по депозитному счету о зачислении суммы вклада, подписанная лицом, уполномоченным на заключение договоров банковского вклада.

Второй экземпляр Подтверждения формируется Банком и помещается в юридическое дело Клиента не позднее 3-х рабочих дней с момента заключения Договора банковского вклада.

По письменному запросу Клиента (в произвольной форме) Банком может дополнительно выдаваться (не позднее 3-х рабочих дней с момента получения обращения Клиента) Подтверждение, заверенное сотрудником Банка, уполномоченным на заключение Договоров банковского вклада, содержащее информацию об условиях вклада, заключенного посредством системы «ЗапСиб iNet».

Письменная форма Договора банковского вклада, заключенного посредством системы «ЗапСиб iNet», удостоверяется выданным/направленным Банком Клиенту Подтверждением, выпиской по депозитному счету, и Правилами организации работы по привлечению средств юридических лиц, индивидуальных предпринимателей, адвокатов, нотариусов по договорам банковского вклада Публичного акционерного общества «Западно-Сибирский коммерческий банк» (ПАО «Запсибкомбанк») от «12» апреля 2013 года № 21/1212/Едиными правилами банковского обслуживания для корпоративных клиентов от «04» февраля 2014 года № 21/1236.

В случае невозможности зачисления денежных средств Банком на депозитный счет Клиента по причине наличия действующих решений ФНС о приостановлении операций по счетам

Клиента, депозитному счету в перечне депозитов Клиента в разделе «Депозиты» системы «ЗапСиб iNet» присваивается статус «Счет не пополнен. Имеются ограничения, обратитесь в офис Банка.».

В случае неперечисления в течение 3 (трех) рабочих дней с даты, следующей за днем присвоения Заявке на размещение вклада статуса «Исполнен суммы вклада в размере, установленном Договором банковского вклада, Договор банковского вклада считается не заключенным, после окончания операционного времени Банка третьего рабочего дня депозитному счету в перечне депозитов Клиента в разделе «Депозиты» системы «ЗапСиб iNet» присваивается статус «Не заключен. Период ожидания истек».

3.7.3. Порядок заключения Договора банковского вклада посредством системы «ЗапСиб iNet», предусмотренный настоящим пунктом Правил, считается согласованным на основании соглашения Сторон в соответствии с требованиями п.2 ст.160 ГК РФ при присоединении Клиента к настоящим Правилам при заключении Договора по «ЗапСиб iNet».

4. Требования, предъявляемые к ЭД системы «ЗапСиб iNet».

4.1. ЭД, сформированный в системе «ЗапСиб iNet», имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия.

4.2. ЭД, используемый в системе «ЗапСиб iNet», считается надлежащим образом оформленным при условии его соответствия законодательству Российской Федерации, соответствующим нормативным документам Банка, а также договорам, заключаемым между Клиентом и Банком.

4.3. Использование ЭП в электронном документообороте.

4.3.1. ЭД считается подписанным пользователем, если он подписан тем ключом ЭП, для которого Сертификационный Центр Банка изготовил сертификат ключа проверки ЭП для пользователя.

В случае если в системе «ЗапСиб iNet» задана многоуровневая система подписи документов, ЭД считается подписанным, если он подписан всеми требуемыми подписями.

ЭД, подписанный ЭП, признается равнозначным документу на бумажном носителе в следующих случаях:

– Сертификат ключа проверки ЭП не утратил силу (действующий), информация о прекращении действия или аннулировании сертификата ключа проверки ЭП в момент подписания ЭД и/или на момент проверки и принятия ЭД не поступала в Сертификационный Центр Банка.

– ЭП Клиента является корректной, подтверждена подлинность ЭП в ЭД.

– ЭП используется в соответствии со сведениями, указанными в сертификате ключа проверки ЭП.

– Фактов внесения изменений в ЭД после момента его подписания при осуществлении проверки в момент принятия ЭД не обнаружено.

4.3.2. Замена ключей ЭП не влияет на юридическую силу ЭД, если он был подписан действующим на момент подписания ключом ЭП.

4.3.3. У каждого уполномоченного лица Клиента, являющегося пользователем системы «ЗапСиб iNet», имеются индивидуальные ключи ЭП, при помощи которых они подписывают ЭД своей ЭП.

4.3.4. Одной ЭП могут быть подписаны несколько связанных между собой ЭД (пакет ЭД). При подписании ЭП пакета ЭД каждый из ЭД, входящих в этот пакет, считается подписанным ЭП.

4.3.5. Предусмотренные для данного ЭД правовые последствия могут наступить только если получен положительный результат проверки ЭП и реквизитов ЭД.

4.3.6. С целью уменьшения объемов передаваемой информации при транспортировке ЭД могут использоваться специальные алгоритмы сжатия информации. В случае необходимости может выполняться подпись и шифрование сжатого ЭД.

4.4. ЭД вступает в силу с момента его регистрации в системе «ЗапСиб iNet». Внесение каких-либо изменений в ЭД, зарегистрированный в системе «ЗапСиб iNet», не допускается.

4.5. Все экземпляры ЭД являются подлинниками данного ЭД. ЭД не может иметь копий в электронном виде.

4.6. Копии ЭД могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью лица, уполномоченного Банком. ЭД и его копии на бумажном носителе должны быть идентичными.

4.7. Программные средства, осуществляющие преобразование ЭД для изготовления (распечатки) в виде бумажного документа, являются составной частью программного обеспечения, используемого в подсистемах системы «ЗапСиб iNet».

5. Порядок совершения операций по системе «ЗапСиб iNet».

5.1. Формирование ЭД осуществляется в следующем порядке:

- формирование ЭД в формате, установленном для данного ЭД;
- в процессе формирования ЭД система «ЗапСиб iNet» контролирует правильность заполнения отдельных реквизитов документа;
- подписание сформированного электронного сообщения ЭП.

Регистрация ЭД в системе «ЗапСиб iNet» происходит автоматически после завершения его формирования.

Проверка ЭД включает:

- проверку ЭД на соответствие установленному для него формату;
- проверку подлинности всех ЭП ЭД.

При получении ЭД, подписанного отозванным (недействительным) ключом ЭП, данный ЭД отклоняется системой «ЗапСиб iNet» и к исполнению не принимается.

5.2. ЭД, зарегистрированные в системе «ЗапСиб iNet» в течение операционного времени Банка, принимаются к исполнению текущим операционным днем. Если у Банка есть сомнения в том, что ЭД инициирован Клиентом, и Банк не может связаться с Клиентом для подтверждения ЭД, документ, поступивший в течение операционного времени Банка, может быть проведен позднее по факту подтверждения платежа уполномоченным представителем Клиента, но не позднее следующего операционного дня. В случае задержки исполнения ЭД до следующего операционного дня в связи с отсутствием подтверждения его инициации, санкционированности Клиентом, факт задержки подтверждается Актом выезда (Приложение 18 к настоящим Правилам), составленным уполномоченным работником Точки продаж по результатам выезда по адресу юридического лица в пределах места нахождения Клиента.

ЭД, зарегистрированные в послеоперационное время Банка, принимаются к исполнению следующим рабочим днем Банка.

Списание денежных средств со счета Клиента на основании зарегистрированного ЭД осуществляется программным способом при достаточности средств на счете в соответствии со значениями реквизитов, указанных в ЭД.

Операционное время Банка размещено на стендах в операционных залах Банка в местах, доступных для всеобщего обозрения, и на официальном сайте Банка – www.zapsibkombank.ru. Контрольным временем является время системных часов аппаратных средств Банка.

Прием ЭД Клиента к исполнению подтверждается Банком присвоением статуса ЭД в перечне документов в разделе «Документы» – «Получен» системы «ЗапСиб iNet».

Исполнение ЭД Клиента подтверждается Банком присвоением статуса ЭД в перечне документов в разделе «Документы» – «Проведен» системы «ЗапСиб iNet».

В случае отказа от исполнения ЭД Банк уведомляет Клиента посредством присвоения статуса ЭД в перечне документов в разделе «Документы» системы «ЗапСиб iNet» – «Отказан» с указанием причины отказа.

В случае помещения документа в очередь не исполненных в срок распоряжений (при отсутствии достаточности денежных средств на расчетном счете Клиента для полной оплаты платежного поручения), Банк уведомляет Клиента посредством помещения ЭД в раздел «Счета» подраздел – «Картотека» системы «ЗапСиб iNet». Исполнение документов, переведенных в очередь не исполненных в срок распоряжений, контролируется Клиентом самостоятельно по состоянию документа в разделе «Счета» подраздел – «Картотека» системы «ЗапСиб iNet».

В случае частичной оплаты документа, находящегося в разделе «Счета» подраздел – «Картотека» системы «ЗапСиб iNet», документу будет присвоен статус «Частично оплачен».

5.3. Уполномоченное лицо Клиента, являющееся пользователем системы «ЗапСиб iNet», может отозвать созданный ЭД, находящийся на исполнении в Банке, путем направления в Банк официального письма в электронном виде с обязательным указанием в письме номера счета, номера документа, суммы, даты ЭД.

Отзыв электронного распоряжения Клиента осуществляется до наступления безотзывности перевода денежных средств. Безотзывность перевода денежных средств наступает с момента списания денежных средств с банковского счета Клиента. В случае поступления в Банк заявления об отзыве распоряжения, отправленного в целях осуществления перевода денежных средств, после наступления безотзывности перевода денежных средств Банк оставляет вышеуказанное заявление об отзыве распоряжения без исполнения. ЭД со статусами «Проведен», «Отказан», «Оплачен в полном объеме», «Удален из картотеки» не могут быть отозваны пользователем. ЭД со статусом «Частично оплачен» может быть отозван пользователем в сумме неоплаченного остатка.

Все ЭД, зарегистрированные в системе «ЗапСиб iNet», хранятся бессрочно в электронных архивах. При хранении ЭД обеспечивается привязка (синхронизация) ЭД и соответствующих сертификатов ключей проверки ЭД для проведения процедуры разрешения конфликтных ситуаций.

5.4. При невозможности передачи информации в Банк с использованием системы «ЗапСиб iNet» документы могут поступить от Клиента в виде подлинника на бумажном носителе. При этом Банком взимается комиссия за обработку документов на бумажном носителе в соответствии с Тарифами Банка, если невозможность передачи информации в Банк с использованием системы «ЗапСиб iNet» возникла не по вине Банка, в период, когда производится выяснение причин несанкционированного доступа к счету Клиента, отказа в дистанционном доступе к счету в результате реализации правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем. Комиссия за обработку документов на

бумажном носителе может не взиматься Банком в случаях, отличных от вышеуказанных, на основании письменного заявления Клиента.

5.5. Банк вправе отклонять поступившие от Клиента ЭД, оформленные с нарушением действующего законодательства РФ.

5.6. Банк информирует Клиента о совершении каждой операции с использованием системы «ЗапСиб iNet» путем направления Клиенту соответствующего уведомления в порядке, установленном настоящими Правилами.

5.7. В качестве надлежащего уведомления Клиента о совершении каждой операции с использованием системы «ЗапСиб iNet» применяются следующие способы:

5.7.1. Предоставление информации в рамках автоматически подключенного SMS-информирования об успешном проведении платежного поручения, отправленного системой «ЗапСиб iNet», на указанный Клиентом номер мобильного телефона. Моментом исполнения Банком обязанности уведомления Клиента о совершении каждой операции с использованием системы «ЗапСиб iNet» является момент отправки SMS–сообщения на указанный Клиентом номер мобильного телефона. При информировании Банком о совершении каждой операции с использованием системы «ЗапСиб iNet» указанным способом Клиент принимает на себя риски, связанные с использованием мобильной связи. Банк не несет ответственности за доставку отправленных им SMS-сообщений Клиентам.

5.7.2. Предоставление ежедневной выписки по счету в офисе Банка при отсутствии доступа к системе «ЗапСиб iNet». В данном случае выписки предоставляются Клиентам уполномоченными работниками Банка на бумажном носителе при личном обращении Клиента в Банк либо при письменном запросе не позднее следующего рабочего дня после исполнения распоряжений о переводе денежных средств. Клиенту необходимо обратиться в Банк не позднее следующего рабочего дня со дня совершения операции в операционное время Банка. Если Клиент своевременно не обратился в офис Банка за получением выписки на бумажном носителе, в этом случае Клиент принимает на себя все риски совершения операций с использованием системы «ЗапСиб iNet» без его согласия, и Банк не несет ответственности за последствия исполнения таких операций.

5.8. Дополнительными способами получения информации о совершении каждой операции с использованием системы «ЗапСиб iNet» либо неуспешности прохождения операции для Клиента являются:

5.8.1. Предоставление информации в рамках оказания услуги «GSM-Банк» посредством направления Клиенту по каждой операции, совершенной с использованием системы «ЗапСиб iNet», SMS-сообщения на указанный им номер мобильного телефона в порядке, установленном Договором «GSM-Банк» и Правилами «GSM-Банк», являющимися неотъемлемой часть Договора «GSM-Банк» и размещенными на официальном сайте Банка.

5.8.2. Статусы платежных документов и сервисные сообщения, отображаемые Клиенту в системе «ЗапСиб iNet» по факту совершения операции;

5.8.3. Электронная выписка, содержащая информацию обо всех движениях по счету и сформированная Клиентом самостоятельно с использованием системы «ЗапСиб iNet».

5.8.4. Моментом исполнения Банком обязанности уведомления Клиентов с использованием дополнительных способов уведомлений, указанных в п. 5.8.2., 5.8.3. настоящих Правил, является момент непосредственного отображения информации Клиенту в системе «ЗапСиб iNet».

5.8.5. Банк обязан предоставлять Клиенту документы и информацию, которые связаны с использованием Клиентом системы «ЗапСиб iNet», по письменному запросу Клиента в срок не более 30 календарных дней либо 60 календарных дней для трансграничных переводов с момента получения запроса Банком.

5.8.6. Все ЭД, зарегистрированные в системе «ЗапСиб iNet», хранятся в электронных архивах. При хранении ЭД обеспечивается привязка (синхронизация) ЭД и соответствующих сертификатов ключей проверки ЭП для проведения процедуры разрешения конфликтных ситуаций.

6. Оплата услуг Банка по обслуживанию Клиентов с использованием системы «ЗапСиб iNet».

6.1. Услуги Банка по обслуживанию Клиентов с использованием системы «ЗапСиб iNet», а также предоставленный Банком Rutoken ЭЦП, Пакет безопасности оплачиваются Клиентом согласно Тарифам, утвержденным Банком, если иной размер не установлен соглашением сторон.

6.2. Оплата услуг Банка по Договору «ЗапСиб iNet», а также предоставленного Банком Rutoken ЭЦП, Пакета безопасности осуществляется Клиентом со счета, указанного в разделе 4 Договора «ЗапСиб iNet», либо с иного счета самостоятельно или списывается Банком на основании заявления Клиента о заранее данном акцепте (Приложение 6 к Правилам расчетно-кассового обслуживания/Приложение 8 к Единым правилам банковского обслуживания для корпоративных клиентов).

6.3. Банк в одностороннем порядке устанавливает (в том числе вводит новые), изменяет, дополняет Тарифы, порядок и условия оплаты за услуги по обслуживанию Клиентов с использованием системы «ЗапСиб iNet». Обо всех изменениях, дополнениях, нововведениях Тарифов, порядка и условий оплаты за услуги, Банк не позднее, чем за 5 (пять) календарных дней до вступления в силу соответствующих изменений, дополнений, нововведений извещает Клиентов путем размещения соответствующей информации на официальном сайте Банка – www.zapsibkombank.ru, в операционных залах Банка в местах, доступных для всеобщего обозрения и посредством системы ДБО.

Если после установления, изменения, дополнения, нововведения Тарифов, а также порядка и условий оплаты за услуги Клиент продолжает пользоваться услугами, считается, что Клиент согласен с указанными изменениями. Оплата услуг Банка по обслуживанию Клиентов с использованием системы «ЗапСиб iNet» осуществляется в соответствии с Тарифами, действующими на дату предоставления услуг.

7. Порядок эксплуатации и обеспечения безопасности конфиденциальной банковской информации клиентской части системы «ЗапСиб iNet».

В целях обеспечения безопасности работы с системой «ЗапСиб iNet» Клиенту необходимо строго и точно соблюдать нижеперечисленные требования.

7.1. Организационные меры информационной безопасности системы «ЗапСиб iNet».

7.1.1. Клиенту необходимо ежедневно контролировать состояние счета любым из способов, перечисленных в пунктах 5.7., 5.8 настоящих Правил. При обнаружении подозрительных операций, а также в случае утраты электронного средства платежа и (или) его использования без согласия Клиента незамедлительно обратиться в Банк для информирования о несанкционированном доступе к системе «ЗапСиб iNet» и объявления ключей ЭП скомпрометированными.

7.1.2. На рабочей станции, на которой установлена система «ЗапСиб iNet», запрещается открытие и исполнение файлов, не требующихся при работе с системой «ЗапСиб iNet», в том числе полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них вредоносного ПО.

7.1.3. Двери помещения во время осуществления действий доступа и других манипуляций в системе «ЗапСиб iNet» должны быть закрыты, присутствие посторонних лиц, не имеющих доступа к ключевой информации, должно быть исключено.

7.1.4. Размещение, охрана и специальное оборудование помещения, в котором установлена клиентская часть системы «ЗапСиб iNet», должны обеспечивать сохранность информации, невозможность неконтролируемого проникновения в это помещение. Для этого необходимо:

- установить систему «ЗапСиб iNet» и сейфы (металлические шкафы) с ключами ЭП в помещении с ограниченным доступом, входная дверь которого снабжена кодовым замком или опечатывается;
- выделить отдельный компьютер для инсталляции системы «ЗапСиб iNet» (данная мера носит рекомендательный, а не императивный характер);
- установить видеокамеру в поле наблюдения за доступом к системе «ЗапСиб iNet» (данная мера носит рекомендательный, а не императивный характер).

7.1.5. Все оборудование, входящее в состав рабочего места, с которого осуществляется работа в системе «ЗапСиб iNet», должно быть технически исправным.

7.1.6. При эксплуатации системы «ЗапСиб iNet» запрещается:

- вносить изменения в исполняемые и конфигурационные файлы программного и информационного обеспечения системы;
- вносить изменения или удалять программное обеспечение, используемое для работы с Rutoken ЭЦП в системе.

7.1.7. В случае возникновения технических неисправностей системы «ЗапСиб iNet» и ее элементов, а также в случае неисправности работы Rutoken ЭЦП, SafeTouch Банк должен быть незамедлительно проинформирован о невозможности использования системы «ЗапСиб iNet» и/или Rutoken ЭЦП, SafeTouch в системе «ЗапСиб iNet» по телефонам, указанным в Приложении 9 к настоящим Правилам.

7.1.8. В случае утраты электронного средства платежа и (или) его использования без согласия пользователя, а также в случае возникновения подозрений в нарушении безопасности системы «ЗапСиб iNet», выявления признаков или фактов возможности таких нарушений, а также в случаях компрометации ключа ЭП, передача платежных поручений должна быть приостановлена, а Банк уведомлен Клиентом по телефонам, указанным в Приложении 9 к настоящим Правилам. При этом Клиент должен уведомить Банк незамедлительно, но не позднее дня, следующего за днем получения Клиентом от Банка уведомления о совершенной операции. Уполномоченный работник Банка перед приостановлением работы системы «ЗапСиб iNet» перезванивает Клиенту для его идентификации не позднее 30 минут с момента обращения Клиента. Идентификация Клиента производится посредством запроса ФИО, кодового слова (при использовании системы «ЗапСиб iNet»), паспортных данных работника Клиента, обратившегося по вопросу приостановления работы системы «ЗапСиб iNet», проверки наличия права обратившегося работника распоряжаться счетом организации). Удостоверившись в личности Клиента и получив подтверждение приостановления работы системы «ЗапСиб iNet», работник Банка блокирует систему.

После уведомления Банка о приостановлении использования системы «ЗапСиб iNet» посредством телефонной связи, Клиент в течение текущего рабочего дня, но не позднее одного рабочего дня со дня обращения в Банк по телефону, обязан направить в Банк письменное подтверждение с подробным описанием произошедшего случая. Система «ЗапСиб iNet» блокируется Банком с момента подтверждения Клиентом приостановления работы системы при его идентификации посредством телефонной связи до устранения признаков небезопасной работы с системой «ЗапСиб iNet», при этом Клиент считается уведомленным о приостановлении работы системы «ЗапСиб iNet»с момента его идентификации.

7.1.9. Клиенту необходимо извещать Банк обо всех случаях увольнения или смены работников Клиента, являющихся пользователями системы «ЗапСиб iNet».

В случае увольнения работника, являющегося владельцем сертификата ключа проверки ЭП, Клиенту необходимо предоставить Заявление на аннулирование сертификата ключа проверки электронной подписи (Приложение 8 к настоящим Правилам) в Банк не позднее дня увольнения работника Клиента.

7.1.10. Клиенту необходимо извещать Банк обо всех случаях увольнения или смены работников Клиента, являющихся пользователями системы «ЗапСиб iNet».

В случае увольнения работника, являющегося владельцем сертификата ключа проверки ЭП, Клиенту необходимо предоставить Заявление на аннулирование сертификата ключа проверки электронной подписи (Приложение 8 к настоящим Правилам) в Банк не позднее дня увольнения работника Клиента.

В случае увольнения работника, являющегося пользователем системы «ЗапСиб iNet», но не имеющего сертификат ключа проверки ЭП (пользователи системы «ЗапСиб iNet» без права подписи), Клиенту необходимо предоставить в Банк Заявление на блокировку системы «ЗапСиб iNet» указанному пользователю (Приложение 10 к настоящим Правилам) не позднее дня увольнения работника Клиента.

В случае смены работника Клиента, являющегося владельцем сертификата ключа проверки ЭП, а также в случае изменения фамилии, имени, отчества, должности, паспортных данных пользователя, имеющего сертификат ключа проверки ЭП, либо наименования Клиента, необходимо получить новый сертификат ключа проверки ЭП согласно п. 3.6. настоящих Правил не позднее дня смены работника/личных данных работника Клиента/наименования Клиента. С момента подачи Заявления на подключение системы «ЗапСиб iNet» (Приложение 1 к настоящим Правилам) с актуальными данными по пользователю, предыдущий сертификат ключа проверки ЭП считается недействительным и аннулируется. Клиент не сможет воспользоваться системой «ЗапСиб iNet»до момента завершения процедуры выпуска нового сертификата ключа проверки ЭП.

7.2. Меры по обеспечению безопасности персонального компьютера, с которого осуществляется работа с системой «ЗапСиб iNet».

7.2.1. К работе с системой «ЗапСиб iNet» допускаются только пользователи системы «ЗапСиб iNet».

7.2.2. Запрещается передавать в какой-либо ремонт или на обслуживание за пределы организации рабочие станции с установленной системой «ЗапСиб iNet» и также приглашать сторонних специалистов без уведомления Банка.

7.2.3. Использовать только лицензионное программное обеспечение (операционные системы, офисные пакеты, антивирусные программы и пр.), обеспечивая при этом регулярное их обновление (не реже 1 раза в неделю).

7.2.4. Необходимо исключить непрофильное использование сети Интернет (например, посещение развлекательных ресурсов, социальных сетей и т.д.).

7.2.5. Запрещается устанавливать на компьютер развлекательные и игровые программы.

7.2.6. Необходимо осуществлять проверку компьютера на наличие вредоносного ПО перед началом работы с системой «ЗапСиб iNet», а также в следующих случаях:

- при увольнении штатного системного администратора, осуществляющего обслуживание компьютера, с которого ведется работа с системой «ЗапСиб iNet»;

- после доступа к компьютеру внештатных системных администраторов или любых других работников, выполнивших работу по установке, обновлению и поддержке различных бухгалтерских, правовых, информационных и других программ.

Заражение компьютера вредоносным ПО представляет собой серьезный риск для безопасности, так как позволяет отслеживать нажатия клавиш и похищать конфиденциальную банковскую информацию (например, номера счетов, пароли).

Необходимо незамедлительно удалять обнаруженное вредоносное ПО (вирусы, шпионское программное обеспечение и т.п.). Клиент должен незамедлительно проинформировать Банк (по телефону, указанному в Приложении 9 к настоящим Правилам, либо путем направления по системе «ЗапСиб iNet» письма в свободной форме) об обнаруженном и удаленном вредоносном программном обеспечении для дальнейшего осуществления действий по внеплановой смене ключа ЭП.

7.3. Меры по обеспечению информационной безопасности ключей ЭП.

7.3.1. Использовать Rutoken ЭЦП 64 Кб только для доступа к системе «ЗапСиб iNet». Запрещается использовать Rutoken ЭЦП 64 Кб flash 8Gb для любой другой цели, например, для переноса документов или фотографий с одного компьютера на другой.

7.3.2. Rutoken ЭЦП должен быть подключен к компьютеру (если Клиент еще не переведен на обслуживание по системе «ЗапСиб iNet» с «Пакетом безопасности»)/SafeTouch (если клиент обслуживается с «Пакетом безопасности») только на время подписания ЭД в системе «ЗапСиб iNet». В остальное время Rutoken ЭЦП должен храниться в месте, где доступ посторонних лиц к нему исключен (сейф, металлический шкаф и т.д.).

7.3.3. Не подвергать носители электронных ключей воздействию сильных магнитных полей и высокого напряжения.

7.3.4. Генерация ЭП осуществляется клиентом самостоятельно.

7.3.5. Не принимать от кого-либо, включая работников Банка, ЭП, сгенерированную не самостоятельно.

7.3.6. Ни под каким предлогом не передавать носитель ЭП другому лицу, включая системных администраторов или работников Банка, даже для проверки работы системы «ЗапСиб iNet», настроек взаимодействия с Банком и т.п. При необходимости таких проверок, владелец ЭП обязан лично подключать носитель с ключами ЭП к компьютеру и производить необходимые настройки/проверки самостоятельно под наблюдением системных администраторов или работников Банка.

7.3.7. Незамедлительно осуществлять перегенерацию ключей ЭП в следующих случаях:

- при возникновении любых подозрений на компрометацию (копирование) ключей ЭП;
- при проведении ремонтных работ, устранения технических сбоев и т.п. на компьютере, с которого осуществляется работа с системой «ЗапСиб iNet»;

– в случае обнаружения каких-либо вредоносных программ на компьютере, используемом для работы в системе «ЗапСиб iNet».

7.4. Меры по обеспечению безопасности при работе с SafeTouch.

7.4.1. Запрещается подключать Rutoken ЭЦП напрямую к персональному компьютеру (при использовании в работе устройства SafeTouch). В случае нарушения работы устройства SafeTouch необходимо обратиться в Банк.

7.4.2. Запрещается использовать один SafeTouch несколькими (более одного) Клиентами Банка.

7.4.3. Необходимо произвести сверку реквизитов ЭД, отображаемых на экране устройства (при работе с SafeTouch), с реквизитами исходного документа, сформированного в системе «ЗапСиб iNet», на идентичность.

7.4.4. Произвести подтверждение реквизитов ЭД допускается только после их проверки на экране SafeTouch на соответствие исходному документу, сформированному в системе «ЗапСиб iNet».

7.4.5. В случае если реквизиты на экране SafeTouch отличаются от реквизитов, указанных в исходном документе, сформированном в системе «ЗапСиб iNet», необходимо отказаться от совершения операции, изъять Rutoken ЭЦП из SafeTouch и незамедлительно проинформировать Банк о происшествии по телефонам, указанным в Приложении 9 к настоящим Правилам.

7.5. Меры по обеспечению безопасности средств доступа, используемых в системе «ЗапСиб iNet».

7.5.1. Не допускается использование простых паролей, например: 123456, qwerty. Необходимо использовать различные сложные комбинации из букв (желательно сочетание заглавных и строчных букв) и цифр, не расположенных подряд на клавиатуре, в количестве не менее 8 символов.

7.5.2. Осуществлять регулярно (минимум – 1 раз в месяц) смену паролей, используемых в системе «ЗапСиб iNet».

7.5.3. Логины и первичные пароли для входа в систему «ЗапСиб iNet» передаются работником Банка лично в руки руководителю Клиента либо уполномоченному лицу на основании доверенности.

7.5.4. Пароли, используемые в системе «ЗапСиб iNet», запрещается записывать и хранить в местах, доступных посторонним лицам.

7.5.5. Не сообщать пароли, используемые в системе «ЗапСиб iNet», кому-либо, в том числе системным администраторам или работникам Банка для проверки работы Системы «ЗапСиб iNet», настроек взаимодействия с Банком и пр. При необходимости таких проверок владелец средств доступа обязан сам лично вводить свои логин и пароль в системе «ЗапСиб iNet».

7.5.6. Не назначать пароли, используемые в системе «ЗапСиб iNet», в любых других системах и сервисах.

7.5.7. Ни при каких обстоятельствах не вводить пароль доступа в систему «ЗапСиб iNet» на сайтах в сети Интернет.

7.5.8. Первоочередные меры информационной безопасности при работе с системой «ЗапСиб iNet» изложены в Приложении 9 к настоящим Правилам в форме уведомления-памятки, которая размещена на официальном сайте Банка – www.zapsibkombank.ru.

8. Ответственность сторон.

8.1. Совместная ответственность Банка и Клиента.

8.1.1. За невыполнение или ненадлежащее исполнение обязательств по Договору «ЗапСиб iNet» стороны несут ответственность в соответствии с законодательством Российской Федерации.

8.1.2. Банк и Клиент несут ответственность за сохранность, обеспечивают конфиденциальность своих ключей ЭП и отвечают за действия своего персонала.

8.1.3. Банк и Клиент несут ответственность за несвоевременное информирование друг друга обо всех случаях компрометации ключей ЭП и устройств обеспечения безопасности, их утраты, хищения, несанкционированного использования, а также повреждения программно-технических средств подсистем обработки, хранения, защиты и передачи информации.

8.1.4. Банк и Клиент не несут ответственность за сбои в обмене информацией, возникшие в результате неисправности линий связи, отключения или перебоев в линиях электропитания, неисправности аппаратных средств.

8.2. Ответственность Клиента.

8.2.1. Клиенты в полном объеме несут ответственность за последствия, вызванные нарушением ими порядка эксплуатации и обеспечения безопасности конфиденциальной банковской информации клиентской части системы «ЗапСиб iNet», описанного в разделе 8 настоящих Правил.

8.2.2. Клиент в полном объеме несет ответственность за последствия несанкционированного доступа к ключам ЭП и устройствам обеспечения безопасности.

8.2.3. Клиент в полном объеме несет ответственность за последствия, вызванные отправкой Банком сообщений на неактуальный (-ые) номер (-а) сотового (-ых) телефона (-ов) в рамках сервисов безопасности системы «ЗапСиб iNet», указанных в п. 3.5.1. настоящих Правил, в следующих случаях:

а) если Клиент сообщил ошибочный номер телефона (номер, не принадлежащий Клиенту);

б) своевременно не оформил Заявление о дополнении/изменении номеров телефонов в рамках SMS-оповещений (Приложение 11 к настоящим Правилам). Заявление о дополнении/изменении номеров телефонов в рамках SMS-оповещений оформляется Клиентом не позднее дня смены номера (-ов) телефона (-ов), подписывается ЭП и предоставляется в Банк посредством системы «ЗапСиб iNet» либо подписывается и предоставляется в Банк лично.

8.2.4. Клиент несет ответственность за содержание реквизитов ЭД.

8.2.5. Банк информирует Клиента о совершении операций способами, указанными в п. 5.6.-5.7. настоящих Правил. Клиент в полном объеме несет ответственность за последствия совершения операций, по которым им не предприняты действия по получению информации о совершении операций способами, указанными в п. 5.6-5.7. настоящих Правил, в следующих случаях:

а) Клиент, обслуживающийся по системе «ЗапСиб iNet», отказался от подключения SMS-информирования об успешном проведении платежного поручения в системе «ЗапСиб iNet»,

предоставив соответствующее заявление по форме, установленной в Приложении 6 настоящих Правил;

б) Клиент, обслуживающийся по системе «ЗапСиб iNet», не обратился в офис Банка за получением выписки на бумажном носителе.

Клиент принимает на себя все риски по операциям, совершенным с использованием системы «ЗапСиб iNet» без его согласия, в случае отказа от информирования и Банк не несет ответственности за последствия исполнения таких операций.

8.2.6. Прекращение (приостановление) использования системы «ЗапСиб iNet» не прекращает обязательств Клиента и Банка, возникших до момента прекращения (приостановления) использования системы «ЗапСиб iNet».

8.2.7. В рамках услуги «Белый список» Клиент в полном объеме несет ответственность за:

- достоверность информации, предоставленной в Заявлении на смену номеров телефонов в рамках услуги «Белый список» (Приложение 16 к настоящим Правилам), Заявлении на изменение Списка доверенных получателей платежей (Приложение 17 к настоящим Правилам);
- подтверждение платежного документа, отправленного на контрагента (получателя), не включенного в Список доверенных получателей платежей.

8.3. Ответственность Банка.

8.3.1. Банк после принятия ЭД от Клиента несет ответственность за его неизменность в процессе исполнения.

8.3.2. Банк несет ответственность за несоблюдение сроков проведения расчетных операций по счету Клиента на основании надлежащим образом оформленных и своевременно доставленных ЭД Клиента в соответствии с действующим законодательством Российской Федерации и п.5.2. настоящих Правил.

8.3.3. Банк несет ответственность за убытки Клиента:

- при использовании ключа ЭП и сертификата ключа проверки ЭП пользователями только в случае, если данные убытки возникли при компрометации ключа подписи администратора Сертификационного Центра Банка;
- при проведении операции, о которой Клиент не был проинформирован способами, указанными в п. 5.6.-5.7 настоящих Правил (за исключением случаев, описанных в п. 8.2. настоящих Правил).

8.3.4. Банк не несет ответственности за:

- последствия исполнения поручений, выданных неуполномоченными лицами, в тех случаях, когда с использованием процедур, предусмотренных настоящими Правилами и Договором «ЗапСиб iNet», Банк не мог установить факта выдачи распоряжения неуполномоченными

лицами или Клиент своими действиями или бездействием способствовал поступлению в Банк указанных распоряжений;

- за работоспособность системы «ЗапСиб iNet», если работа с системой «ЗапСиб iNet» осуществлялась на компьютере, не соответствующем требованиям, указанным в п. 3.1.3. настоящих Правил;
- ущерб Клиента, возникший вследствие принятия к исполнению ЭД с недействительной или скомпрометированной ЭП Клиента, поступившей до получения от Клиента информации о признании ее недействительной или о ее компрометации;
- ущерб Клиента, возникший вследствие:

a) неправильного заполнения Клиентом реквизитов ЭД в системе «ЗапСиб iNet»;

b) нарушение Клиентом порядка эксплуатации и обеспечения безопасности конфиденциальной банковской информации клиентской части системы «ЗапСиб iNet», указанного в разделе 7 настоящих Правил;

c) несанкционированного доступа к системе «ЗапСиб iNet» по причинам, указанным в пп. 8.2.2., 8.2.3. настоящих Правил, в том числе в рамках услуги «Белый список» при наступлении событий, указанных в пп. 3.5. настоящих Правил;

d) совершения операций без согласия Клиента, если Банком исполнена обязанность и соблюден порядок информирования Клиента, установленный п. 5.6.-5.7. настоящих Правил, а Клиентом не предприняты действия по получению информации о совершении операций способами, указанными в п. 5.6.-5.7. настоящих Правил, в случаях указанных в п. 7.2. настоящих Правил, или Клиент не направил Банку уведомление в соответствии с п. 7.1.8. настоящих Правил. Банк не обязан возмещать Клиенту сумму операции, совершенной без согласия Клиента в указанных случаях.

9. Порядок разрешения конфликтов между Банком и Клиентом.

9.1. Возникновение конфликтных ситуаций в системе «ЗапСиб iNet» **возможно в следующих случаях:**

9.1.1. При осуществлении электронного документооборота, связанного с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭП.

Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- неподтверждение подлинности ЭД средствами ЭП принимающей стороны;
- оспаривание факта формирования ЭД;
- оспаривание факта идентификации владельца сертификата ключа проверки ЭП, подписавшего документ;
- заявление Банка либо Клиента об искажении ЭД;
- оспаривание факта отправления и/или доставки ЭД;
- оспаривание времени отправления и/или доставки ЭД;
- оспаривание аутентичности экземпляров ЭД и/или подлинника и копии ЭД на бумажном носителе;
- оспаривание факта отправки Банком уведомления о совершенной операции в соответствии с п. 5.6.-5.7. настоящих Правил;
- иные случаи возникновения конфликтных ситуаций, связанных с функционированием системы «ЗапСиб iNet».

9.1.2. При возникновении у Банка недоверия относительно используемого Клиентом программного обеспечения.

9.2. Уведомление о конфликтной ситуации.

9.2.1. В случае возникновения конфликтной ситуации Банк и/или Клиент должен незамедлительно, в течение не более чем одного рабочего дня со дня получения информации о таком нарушении, направить заявление о конфликтной ситуации противоположной стороне.

9.2.2. Заявление о предполагаемом наличии конфликтной ситуации оформляется в произвольной письменной форме, отправляется электронно, по почте или нарочно. Заявление должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. В заявлении должны быть перечислены основные реквизиты оспариваемого ЭД, фамилия, имя и отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

9.2.3. Сторона, которой направлено заявление, обязана незамедлительно, но не позднее следующего рабочего дня со дня получения заявления, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и не позднее двух рабочих дней с

момента поступления заявления о предполагаемом наличии конфликтной ситуации, устно (по телефону) либо письменно предоставить заявителю предварительную информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

9.2.4. Банк рассматривает обращение Клиента, в том числе при возникновении споров, связанных с использованием Клиентом системы «ЗапСиб iNet», и предоставляет Клиенту итоговое заключение в срок не более 30 календарных дней со дня получения Банком заявления, а также не более 60 календарных дней со дня получения заявления в случае использования системы «ЗапСиб iNet» для осуществления трансграничного перевода денежных средств. Клиенту также предоставляется возможность получать информацию о результатах рассмотрения заявления, в том числе в письменной форме по требованию Клиента в сроки указанные в данном пункте настоящих правил.

9.3. Разрешение конфликтной ситуации в рабочем порядке.

9.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от противоположной стороны.

9.3.2. На время разрешения конфликтной ситуации Банк имеет право приостановить действие систем «ЗапСиб iNet», уведомив об этом Клиента любым доступным для Банка способом.

9.3.3. В случае если уведомитель не удовлетворен информацией, полученной от противоположной стороны, он обязан сообщить об этом противоположной стороне в срок не позднее 3х рабочих дней со дня получения информации от противоположной стороны, в противном случае конфликт считается урегулированным в рабочем порядке.

9.4. Формирование разрешительной комиссии (далее по тексту – Комиссия), ее состав.

9.4.1. В случае если Клиент принимает предложение о формирования Комиссии, Клиенту необходимо предоставить в Банк Согласие (Приложение 12 к настоящим Правилам) не позднее 5 (пяти) рабочих дней с момента получения предложения от Банка о проведении Комиссии.

9.4.2. По истечении 5 (пяти) рабочих дней с момента получения Согласия о формировании Комиссии (Приложение 12 к настоящим Правилам), из состава работников Банка и Клиента должна быть сформирована Комиссия. При необходимости в состав Комиссии включаются независимые эксперты. Оплату услуг независимых экспертов осуществляет та сторона, которая ходатайствовала об участии данных экспертов.

9.4.3. Представление членов Комиссии со стороны Клиента осуществляется Клиентом самостоятельно.

В состав Комиссии со стороны Банка входят (представители и их функции):

- Представители филиала/дополнительного офиса/операционного офисы/иного внутреннего структурного подразделения Банка, где обслуживается Клиент (руководитель филиала/заместитель руководителя филиала/дополнительного офиса/операционного

офиса/иного структурного подразделения Банка) – выполняет функции взаимодействия с Клиентом и является модератором Комиссии;

- Департамента корпоративного бизнеса:
  - заместитель начальника Департамента – эксперт от бизнес-подразделения;
  - сотрудник, ответственный за методологию системы «ЗапСиб iNet» – выполняет функции организатора разрешительной комиссии (место и время), координации участников Комиссии, а также является секретарем Комиссии и формирует протокол по результатам проведения Комиссии;
- Департамента экономической безопасности (начальник/заместитель начальника Департамента) – эксперт по вопросам безопасности систем дистанционного банковского обслуживания;
- Департамента информационных технологий (руководитель подразделения Департамента, ответственного за техническое сопровождение и работу с клиентами в системе –«ЗапСиб iNet») – эксперт по техническим вопросам функционирования систем дистанционного банковского обслуживания, выполняют функции организации записи и технического обеспечения проведения заседания Комиссии;
- Юридического управления (юрист Головного офиса/филиала/дополнительного офиса/операционного офиса/иного структурного подразделения Банка, в зависимости от того, где обслуживается Клиент) – выполняет функции по изложению правовой позиции Банка;
- а также (при необходимости) представители других профильных служб Банка.

Сотрудники Головного офиса в случае проведения Комиссии в территориально удаленном филиале/дополнительном офисе/операционном офисе участвуют в проведении Комиссии посредством видео-конференц связи.

9.4.4. Право представлять в Комиссии сторону Клиента должно подтверждаться доверенностью, выданной каждому представителю на срок работы Комиссии.

Право представлять в Комиссии сторону Банка должно подтверждаться Распоряжением за подписью курирующего корпоративный бизнес Вице-президента Банка.

9.5. Компетенция и полномочия Комиссии.

9.5.1. Сформированная Комиссия при рассмотрении конфликтной ситуации устанавливает:

- на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки ЭД, его подлинности, а также о подписании ЭД конкретной ЭП, аутентичности отправленного документа полученному (ответственные – руководитель подразделения Департамента информационных технологий, ответственного за техническое сопровождение и работу с клиентами в системе «ЗапСиб iNet»);

- причины возникновения конфликтной ситуации и причастность сотрудников Банка к инциденту (ответственные - начальник/заместитель начальника Департамента экономической безопасности).

9.5.2. Комиссия вправе рассматривать иные вопросы, необходимые, по мнению Комиссии, для выяснения причин и последствий возникновения конфликтной ситуации.

9.5.3. Для проведения необходимых проверок и документирования данных, используемых при указанных проверках, может применяться специальное программное обеспечение.

9.5.4. Результатом рассмотрения конфликта Комиссией является озвучивание каждой стороной позиции о полноте совершенных действий для предотвращения возникновения конфликтной ситуации на основании вывода:

- об истинности подписи под приложенным ЭД;
- о соответствии реквизитов ЭД требованиям нормативных документов РФ;
- о подтверждении реквизитов ЭД посредством сервиса визуального подтверждения платежа.

9.5.5. Все споры и разногласия, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, стороны будут стремиться разрешить, используя механизмы согласительного урегулирования споров и разногласий.

9.5.6. Если по итогам проведения согласительной процедуры конфликтная ситуация остается полностью или частично неурегулированной, стороны вправе передать неурегулированный спор и разногласия в Арбитражный суд по месту нахождения истца.

9.6. Протокол работы Комиссии.

9.6.1. Все действия, предпринимаемые Комиссией для выяснения фактических обстоятельств, а также выводы, сделанные Комиссией, заносятся в Протокол работы Комиссии. Протокол работы Комиссии должен содержать следующие данные:

- состав Комиссии с указанием должности каждого из членов Комиссии;
- краткое изложение обстоятельств возникшей конфликтной ситуации;
- информация, изложенная и обсуждаемая в рамках заседания Комиссии;
- мероприятия, проводимые Комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты и времени, места их проведения;
- выводы, к которым пришла Комиссия в результате проведенных мероприятий;
- подписи всех членов Комиссии.

9.6.2. В случае если мнение члена (или членов) Комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов Комиссии, об этом в Протоколе составляется соответствующая запись, которая подписывается членом (или членами Комиссии), чье особое мнение отражает соответствующая запись.

9.6.3. Протокол должен быть подписан всеми участниками Комиссии со стороны Банка в течение 5 календарных дней с момента получения Протокола.

9.6.4. Протокол составляется в двух экземплярах на бумажном носителе, один из них остается в Банке, другой передается Клиенту. По требованию любой из сторон конфликтной ситуации, или любого из членов Комиссии, им может быть выдана заверенная Банком копия Протокола.

9.6.5. Протокол (в двух экземплярах), подписанный со стороны Банка, направляется Банком Клиенту. В течение трех рабочих дней после получения от Банка Протокола, Клиенту необходимо рассмотреть его и подписать всеми членами Комиссии со стороны Клиента и отправить в Банк 1 экземпляр подписанного Протокола. В случае если Клиент не согласен с какой-либо информацией, изложенной в Протоколе, необходимо составить Акт разногласий к Протоколу заседания разрешительной комиссии (Приложение 13 к настоящим Правилам).

10. Порядок прекращения (приостановления) использования системы «ЗапСиб iNet».

10.1. Любая из сторон вправе в одностороннем порядке расторгнуть Договор ДБО, письменно предупредив об этом другую сторону за 10 (десять) календарных дней до предполагаемой даты расторжения Договора ДБО.

Расторжение Договора ДБО по инициативе Банка осуществляется на основании письменного Уведомления, отправленного Клиенту заказным письмом или иным способом, позволяющим подтвердить факт уведомления Клиента. При этом датой передачи Уведомления Клиенту признается дата принятия Уведомления отделением почтовой связи, вручения курьеру, передача на руки и пр. Договор ДБО считается расторгнутым по инициативе Банка с даты, указанной в Уведомлении.

Расторжение Договора ДБО по инициативе Клиента осуществляется на основании предоставленного в Банк надлежащим образом оформленного и подписанного Клиентом Заявления на блокировку системы ДБО (Приложение 10 к настоящим Правилам). Договор ДБО считается расторгнутым по инициативе Клиента в срок, указанный в абзаце первом настоящего пункта Правил, если больший срок не установлен в заявлении Клиента. Банк считается уведомленным Клиентом с даты передачи вышеуказанного заявления в Банк.

10.2. В случае расторжения Договора «ЗапСиб iNet» или прекращения его действия Банк закрывает доступ Клиенту к системе «ЗапСиб iNet», при этом Клиент обязан удалить программное обеспечение, предоставленное Банком. Банк закрывает доступ Клиенту в систему «ЗапСиб iNet» не позднее рабочего дня, следующего за днем получения Банком надлежащим образом оформленного и подписанного Клиентом Заявления на блокировку системы «ЗапСиб iNet» (Приложение 10 к настоящим Правилам).

10.3. Клиент вправе временно приостановить и возобновить действие Договора «ЗапСиб iNet», письменно уведомив об этом Банк по форме Приложения 15 к настоящим Правилам.

10.4. Банк имеет право в одностороннем порядке приостановить использование системы «ЗапСиб iNet» в следующих случаях:

10.4.1. получения от Клиента сведений о нарушении безопасности системы «ЗапСиб iNet», выявления признаков, фактов или возможности таких нарушений;

10.4.2. возникновения технических неисправностей элементов системы «ЗапСиб iNet», до устранения обстоятельств, препятствующих использованию системы «ЗапСиб iNet»;

10.4.3. при нарушении Клиентом порядка использования системы «ЗапСиб iNet»;

10.4.4. в соответствии с п.3.1.5. настоящих Правил.

10.5. Банк вправе отказать Клиенту в дистанционном доступе к счету, распоряжение по которому производится с использованием аналога собственноручной подписи, в следующих случаях:

– совершения по счету сомнительных операций, то есть операций, в отношении которых есть основания полагать, что они имеют необычный характер и не имеют экономического смысла или очевидной законной цели;

– в случае если в результате реализации правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее – ПВК ПОД/ФТ), у работников Банка возникают подозрения, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, в том числе появление в Банке информации, выявленной при обновлении сведений в анкете Клиента, включая проверку сведений, поступивших из контролирующих органов о том, что Клиент, его постоянно действующий исполнительный орган, а в случае отсутствия постоянно действующего исполнительного органа – иной орган или лицо, уполномоченные выступать от имени юридического лица, в силу закона, иного правового акта или учредительного документа, отсутствует по адресу юридического лица в пределах места нахождения юридического лица, указанному в данных ЕГРЮЛ, и/или в Банке отсутствуют актуальные документы, устанавливающие адрес юридического лица в пределах места нахождения юридического лица;

– непредставления Клиентом документов/сведений, предусмотренных Федеральным закон от 07.08.2001 №115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее - Закон №115-ФЗ), Положением Банка России об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма от 15.10.2015 № 499-П (далее - Положение №499-П), ПВК ПОД/ФТ и Правилами расчетно-кассового обслуживания Банка, и необходимых для идентификации Клиента/Представителей клиента/Выгодоприобретателей/Бенефициарных владельцев, в том числе при обновлении сведений о Клиенте/Представителях клиента/Выгодоприобретателях/Бенефициарных владельцах.

В указанных случаях, Банк направляет Клиенту по системе «ЗапСиб iNet» – в тот же день, а также по почте заказным письмом – в течение трех рабочих дней, Уведомление о том, что дистанционный доступ к счету прекращен полностью до предоставления Клиентом в Банк запрашиваемой информации:

- документов, поясняющих экономический смысл или очевидную законную цель проводимых по счету операций, подтверждающих легальность источника происхождения денежных средств и(или) иного имущества Клиента;
- документов, подтверждающих адрес юридического лица в пределах места нахождения юридического лица;
- документов/сведений, необходимых для идентификации Клиента/ Представителей клиента/ Выгодоприобретателей/ Бенефициарных владельцев в целях противодействия легализации

(отмыванию) доходов, полученных преступным путем, и финансированию терроризма, предусмотренных Законом № 115-ФЗ, Положением № 499-П, ПВК ПОД/ФТ и Правилами расчетно-кассового обслуживания Банка, в том числе при обновлении сведений о Клиенте/ Представителях клиента/Выгодоприобретателях/ Бенефициарных владельцах

К документам, поясняющим экономический смысл или очевидную законную цель проводимых по счету операций, подтверждающих легальность источника происхождения денежных средств и (или) иного имущества Клиента, включая, но, не ограничиваясь, относятся: документы, касающиеся целей, характера сделки, документы, относящиеся к исполнению и/или подтверждающие факт исполнения сделки, а также документы о стороне по сделке.

К документам, подтверждающим адрес юридического лица в пределах места нахождения Клиента относятся: выписка из Единого государственного реестра юридических лиц и прочие документы, установленные Правилами расчетно-кассового обслуживания Банка (договор аренды/субаренды, свидетельство о праве собственности на недвижимое имущество т.д.).

Требования и перечень документов и сведений, необходимых для идентификации Клиентов/ Представителей клиента/Выгодоприобретателей /Бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма установлены в соответствии с Законом №115-ФЗ, Положением №499-П, ПВК ПОД/ФТ, Правилами расчетно-кассового обслуживания Банка.

В условиях прекращения дистанционного доступа к счету и невозможности совершения Клиентом операций по счету с использованием системы «ЗапСиб iNet» – Клиент вправе в дальнейшем совершать операции при предоставлении в Банк распоряжений о переводе денежных средств на бумажном носителе, оформленных надлежащим образом в соответствии с порядком, установленным законодательством Российской Федерации и Правилами расчетно-кассового обслуживания Банка и документов по запросу Банка, подтверждающих экономический смысл или очевидную законную цель проводимой операции, оплачивая услуги Банка в соответствии с Тарифами, утвержденными уполномоченными лицами Банка, если иные Тарифы не предусмотрены соглашением сторон.

Распоряжения Клиента на выполнение операций, за исключением операций по зачислению денежных средств, поступивших на счет Клиента, на бумажном носителе не выполняются Банком в случае не предоставления Клиентом документов, указанных в настоящем пункте Правил, либо при наличии у Банка информации о недостоверных данных, предоставленных Клиентом, а также в случае, если в результате реализации ПВК ПОД/ФТ у работников Банка возникают подозрения, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

В случае если запрашиваемые документы не представлены Клиентом в срок, указанный в Уведомлении, Банк в одностороннем порядке вправе отказаться от исполнения Договора «ЗапСиб iNet». Договор «ЗапСиб iNet» считается расторгнутым с даты направления Банком Клиенту

соответствующего Уведомления, направленного с использованием системы «ЗапСиб iNet», а также по почте заказным письмом по адресу юридического лица в пределах местонахождения юридического лица.

Срок предоставления Клиентом документов по запросу Банка устанавливается в соответствии с действующей редакцией Правил расчетно-кассового обслуживания Банка, если иной срок не установлен Уведомлением Банка.

Банк вправе в одностороннем порядке отказаться от исполнения Договора «ЗапСиб iNet» в случае, если запрашиваемые документы представлены Клиентом в срок, определённый в Уведомлении, но из них не следует, что:

- проводимая операция имеет экономический смысл или очевидную законную цель, Клиентом подтверждена легальность источника происхождения денежных средств и (или) иного имущества;
- подтвержден адрес юридического лица в пределах места нахождения юридического лица;
- документы содержат сведения, достаточные для идентификации Клиента/Представителей клиента/ Выгодоприобретателей/Бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в соответствии с Законом № 115-ФЗ, Положением № 499-П, ПВК ПОД/ФТ и Правилами расчетно-кассового обслуживания Банка.

Клиенту, предоставившему в установленный срок все запрашиваемые Банком документы, восстанавливается дистанционный доступ к счету при условии, что из представленных документов следует, что совершенная(ые) операция(и) имеет(ют) экономический смысл и очевидную законную цель и(или) подтверждена легальность источника происхождения денежных средств и (или) иного имущества Клиента, и(или) подтвержден адрес юридического лица в пределах места нахождения юридического лица, и/или документы позволяют идентифицировать Клиента/ Представителей клиента/Выгодоприобретателей/Бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в соответствии с Законом № 115-ФЗ, Положением № 499-П, ПВК по ПОД/ФТ и Правилами расчетно-кассового обслуживания Банка.

Клиент обязуется предоставлять Банку по первому требованию документы и сведения, подтверждающие экономический смысл или очевидную законную цель проводимых операций по счету, и/или документы, подтверждающие источник происхождения денежных средств и(или) иного имущества Клиента и(или) документы, подтверждающие адрес юридического лица в пределах места нахождения юридического лица, и/или документы/сведения, необходимые для идентификации Клиента/Представителей клиента/Выгодоприобретателей/Бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, предусмотренные Законом № 115-ФЗ, Положением № 499-П, ПВК по ПОД/ФТ и Правилами расчетно-кассового обслуживания Банка, в том числе при

обновлении сведений о Клиенте/Представителей клиента/Выгодоприобретателей/Бенефициарных владельцев.

11. Внесение изменений в Правила

11.1. Настоящие Правила могут быть изменены (дополнены) Банком в одностороннем порядке. Любые изменения (дополнения) настоящих Правил размещаются Банком на официальном сайте Банка – www.zapsibkombank.ru, в операционных залах Банка в местах, доступных для всеобщего обозрения, не менее чем за 1 (один) рабочий день до даты вступления изменений в силу (за исключением случаев, когда внесение изменений в Правила связано с изменением действующего законодательства РФ). Если после изменений (дополнений) настоящих Правил Клиент продолжает пользоваться услугами, то считается, что Клиент уведомлен надлежащим образом об указанных изменениях (дополнениях) в Правила, согласен с ними, и считает их для себя обязательными.

В случае несогласия Клиента с изменениями (дополнениями), указанными в настоящих Правилах, Клиент может расторгнуть Договор по «ЗапСиб iNet».

Приложение 1

к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Директору/начальнику филиала/ДО/ОО/ДпРК

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ СИСТЕМЫ ДБО

1. Наименование Клиента:

_____

_____

(полное наименование ЮЛ в соответствии с учредительными документами;
ФИО ИП /ФЛ, занимающегося в установленном законодательством РФ порядке частной практикой)

ИНН:												

в лице_____

(должность и ФИО представителя Клиента)

действующего на основании _____

(наименование документа: Устав, доверенность, свидетельство, иной документ)

юридический адрес Клиента_____

_____

2. Клиент просит подключить счета:

1																				
2																				
3																				
4																				
5																				

☐ все открытые и открываемые в дальнейшем депозитные счета

к системе «ЗапСиб iNet» с подключенным «Пакетом безопасности»

3. Клиент просит:

3.1. зарегистрировать организацию в Реестре пользователей Сертификационного Центра информационной сети ПАО «Запсибкомбанк»

№	ФИО, должность пользователя	Кодовое слово	С правом подписи (да/нет)	Группа подписи (А/В)	Доступные счета (указать номер счета/номера счетов/все открытые и открываемые в дальнейшем депозитные счета)	Доступ к модулю «Кредиты» (да/нет)
1						
2						
3						
4						
5						

3.2. изготовить на данного(ых) пользователя(ей) сертификат(ы)* ключа(ей) проверки электронной подписи в количестве (Rutoken ЭЦП)**

☐

3.3. подключить Пакет безопасности в количестве *** ☐

**Срок действия сертификата ключа проверки электронной подписи уполномоченного лица Клиента – 1 год 3 месяца.*
***Rutoken ЭЦП предоставляется Клиенту в количестве, равном количеству подписей в карточке с образцами подписей и оттиска печати, но не менее количества, равного одной подписи каждого уровня.*
****Пакет безопасности предоставляется Клиенту в количестве, равном количеству подписей в карточке с образцами подписей и оттиска печати, но не менее количества, равного одной подписи каждого уровня.*

Области использования сертификата, при которых электронный документ с электронной подписью уполномоченного лица будет иметь юридическое значение, ограничиваются рамками Договора на дистанционное банковское обслуживание, а также Договора банковского вклада, заключенного между ПАО «Запсибкомбанк» и Клиентом.

4. Клиент просит подключить услугу «Белый список» и закрепить следующий Список доверенных получателей платежей:

Наименование контрагента	БИК	Счет	ИНН	Лимит платежа, руб./ин.валюта
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

При подтверждении платежного документа в адрес контрагента, не входящего в Список доверенных получателей платежей, необходимо обращаться по следующим номерам телефонов:

___8-_____-_____-_____ _____
(номер телефона) (Ф.И.О. контактного лица**)
___8-____ - _____-_____ _____
(номер телефона) (Ф.И.О. контактного лица**)

***может быть указано ТОЛЬКО лицо, включенное в карточку образцов подписей и оттиска печати*.

5. Клиент просит подключить следующие SMS-оповещения:

V	Успешная аутентификация пользователя										
на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*
V	Пользователь вошел в систему										
на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*
V	Платежное поручение проведено банком										
на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*

V	Одноразовый пароль при входе в систему

на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*

V	Создано платежное поручение в системе

на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*

6. Клиент просит направить обучающие материалы по системе «ЗапСиб iNet» на e-mail:

на e-mail:	*Ф.И.О. пользователя, должность*

7. Клиент просит ограничить доступ к счетам следующим пользователям системы:

№	ФИО, должность	Расчетный счет/депозитный счет/иной банковский счет (указать)
1		
2		
3		

8. Стоимость услуг, необходимых для подключения к системе «ЗапСиб iNet»:

Услуга	Количество	Сумма за 1 ед. (руб)	Итоговая сумма (руб)
Rutoken ЭЦП*			
Подключение первого Пакета безопасности*			
Подключение второго и последующего Пакета безопасности			
Итоговая стоимость			

заполняется сотрудником Банка

** При подключении Клиентом Сервиса «Оптом дешевле!» один Rutoken ЭЦП и один «Пакет безопасности» предоставляется в рамках перечня услуг, входящих в Сервис «Оптом дешевле!». Дополнительные Rutoken ЭЦП и «Пакет безопасности» предоставляются Клиенту в соответствии с Тарифами Банка на услуги, оказываемые юридическим лицам.*

Заполняя настоящее Заявление на подключение системы ДБО, Клиент соглашается и дает Банку заранее данный акцепт (согласие) на списание Банком платы за услуги Банка, предоставленные по системам ДБО, со своих счетов, открытых в Банке, без дополнительных распоряжений для списания денежных средств на основании платежного требования/банковского ордера либо иного документа, установленного законодательными актами и нормативными документами Банка России.

Руководитель _____/_____ **Дата** | | | / | | | / | | | | |
(подпись) *(Ф.И.О.)*

Заявление о регистрации принял _____ / _____ **Дата** | | | / | | | / | | | | |
(*подпись)* *(должность, Ф.И.О. работника Банка)*

Приложение 2
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Акт приема-передачи

Rutoken ЭЦП

«____»_____ _____ год

Публичное акционерное общество «Западно-Сибирский коммерческий банк» (ПАО «Запсибкомбанк»), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, при совместном упоминании именуемые «Стороны», заключили настоящий Акт о нижеследующем:

1. По настоящему Акту Банк передал, а Клиент принял для использования в системе «ЗапСиб iNet» Rutoken ЭЦП в следующем количестве:

№ п/п	Серийный номер Rutoken ЭЦП	Данные об уполномоченном лице Клиента, которое будет хранить ключ ЭП на Rutoken ЭЦП
1	…	Фамилия, имя, отчество, должность
2	…	Фамилия, имя, отчество, должность

2. Клиент подтверждает, что корпус (-а) переданного (-ых) Rutoken ЭЦП не имеет (-ют) видимых признаков повреждения или взлома.
3. Клиент подтверждает, что проинформирован о размещении на сайте Банка:
   - Драйвера для Rutoken ЭЦП;
   - Рутокен Плагин, JCWebClients – плагины для работы с электронной подписью.
4. Клиентом подтверждается обязанность:

4.1. организовать инсталляцию необходимого драйвера для Rutoken ЭЦП, а также программного обеспечения для генерации ключей ЭП, на компьютере, на котором будет эксплуатироваться вышеуказанное устройство и система «ЗапСиб iNet»;

4.2. обеспечить генерацию с помощью Rutoken ЭЦП ключей ЭП уполномоченным лицом Клиента – ключ ЭП и ключ проверки ЭП – и предоставление в Банк сертификата ключа проверки ЭП уполномоченного лица Клиента.

5. Клиент гарантирует использование Rutoken ЭЦП только для работы в системе «ЗапСиб iNet», а также обязуется не передавать их (его) третьим лицам.

К настоящему Акту прилагается Приложение 1 «Правила и требования по работе с Rutoken ЭЦП».

Настоящий Акт и Приложение 1 к настоящему Акту составлены в 2 (Двух) экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

Дата, время передачи Rutoken ЭЦП Клиенту: «____»_____ _____ год _____:_____
(час. : мин.)

От БАНКА передал	**От КЛИЕНТА получил**
(должность)	(должность)
(подпись)	(подпись)
М.П. (Ф.И.О.)	М.П. (Ф.И.О.)

Приложение 1
к Акту приема-передачи Rutoken ЭЦП
от «19» апреля 2016 года

Правила и требования по работе с Rutoken ЭЦП.

Общие сведения о Rutoken ЭЦП.

Электронный идентификатор Rutoken ЭЦП – физический носитель, предназначенный для хранения ключа ЭП и ключа проверки ЭП, являющийся персональным средством аутентификации уполномоченного лица Клиента и обеспечивающий доступ к распоряжению счетом и обмену электронными документами по системе «ЗапСиб iNet».

Основные преимущества использования Rutoken ЭЦП для Клиентов Банка:

1. *Безопасность применения* – воспользоваться Rutoken ЭЦП может только его владелец, знающий PIN-код устройства.

Rutoken ЭЦП гарантирует Клиентам Банка сохранность ключей ЭП от копирования как наиболее распространенного способа хищения ключевой информации, так как при подписании электронного документа ключом ЭП, находящимся на Rutoken ЭЦП, такой ключ не извлекается из памяти устройства, и весь процесс визирования электронного документа происходит внутри Rutoken ЭЦП.

Таким образом, ключ ЭП генерируется внутри Rutoken ЭЦП, хранится в защищенной памяти Rutoken ЭЦП и не может быть из Rutoken ЭЦП считан. А неизвлекаемость ключа ЭП из памяти ключевого носителя – залог надежного обеспечения секретности ключа ЭП.

2. *Надежность хранения информации* – качественная микросхема и прочный герметичный корпус существенно уменьшают риск выхода устройства из строя.

3. *Мобильность* – минимальные требования к рабочему месту для обеспечения использования Rutoken ЭЦП в системе ДБО.

Rutoken ЭЦП работает под управлением операционных систем MS Windows начиная с Windows XP.

Для того, чтобы Клиент мог воспользоваться USB-ключом в системе «ЗапСиб iNet», необходимо на рабочую станцию установить драйвер Rutoken ЭЦП, а также программное обеспечение для генерации ключей ЭП (AdminPKI)/Рутокен Плагин, JCWebClients – плагины для работы с электронной подписью). Драйвер и программное обеспечение для генерации ключей ЭП предоставляется Банком.

4. *Удобство работы* – Rutoken ЭЦП выполнен в виде брелока со световой индикацией, напрямую подключается к компьютеру через USB-порт.

Функциональные возможности Rutoken ЭЦП .

Rutoken ЭЦП обеспечивает:

- генерацию ключевых пар ЭП;
- формирование и проверку ЭП по ГОСТ Р34.10-2001;
- генерацию ключей шифрования;
- шифрование информации по ГОСТ 28147-89;
- формирование и проверку имитовставки по ГОСТ 28147-89;
- вычисление хэш-функции по ГОСТ 34.11-97.

Правила использования Rutoken ЭЦП.

Rutoken ЭЦП необходимо оберегать от воздействия влаги и агрессивных сред сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.), воздействия высоких и низких температур. При

резкой смене температуры (перемещение охлажденного ключевого носителя с мороза в теплое помещение) не рекомендуется использовать Rutoken ЭЦП в течение 3 часов во избежание повреждения ключевого носителя из-за сконденсированной на его электронной схеме влаги. Необходимо оберегать Rutoken ЭЦП от попадания на него прямых солнечных лучей.

Недопустимо воздействие на Rutoken ЭЦП сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.

При засорении разъема Rutoken ЭЦП нужно применять меры для его очистки. Для очистки корпуса и разъема необходимо использовать сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.

В случае неисправности или неправильного функционирования Rutoken ЭЦП необходимо обращаться в Банк по следующим телефонам:

8 (3452) 522-000;

8-800-100-5005 (звонок бесплатный как с городского, так и с мобильного телефона).

Подготовка Rutoken ЭЦП к работе

Перед началом роботы с Rutoken ЭЦП на рабочее место пользователя системы «ЗапСиб iNet» необходимо предварительно установить:

1. *Драйвер Rutoken ЭЦП.* Драйвер Rutoken ЭЦП необходимо установить до подключения устройства.
2. Рутокен Плагин, JCWebClients – *плагины для работы с электронной подписью*.

Во время установки драйвера и программного обеспечения для генерации ключей ЭП все приложения должны быть закрыты.

Важно!

Не передавайте Rutoken ЭЦП третьим лицам! Не сообщайте третьим лицам PIN-код доступа к ключу ЭП. В случае утери (хищения) Rutoken ЭЦП немедленно свяжитесь с Банком по следующим телефонам:

- 8 (3452) 522-000;
- 8-800-100-5005 (звонок бесплатный как с городского, так и с мобильного телефона).

Обращаем особое внимание!

Rutoken ЭЦП должен быть подключен к компьютеру (если клиент не переведен на обслуживание по системе «ЗапСиб iNet» с «Пакетом безопасности»)/SafeTouch (если клиент обслуживается с «Пакетом безопасности») только на время работы в системе «ЗапСиб iNet». **Недопустимо** постоянное подключение Rutoken ЭЦП к компьютеру /SafeTouch.

Приложение 3
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Доверенность оформляется на фирменном бланке организации и подписывается руководителем Клиента.

ДОВЕРЕННОСТЬ

Город _____ Дата выдачи: «____» _____ год

Настоящим _____, в лице_____
(наименование Клиента) (должность, фамилия, имя, отчество)
_____(далее по тексту – «Доверитель»),
действующего на основании_____
(название документа, на основании которого действует указанное лицо)

предоставляет право _____
(фамилия, имя, отчество)
паспорт серии_____ № _____ выдан_____
(серия паспорта) (номер паспорта) (кем и когда выдан, код подразделения)
_____
совершать от имени Доверителя следующие действия:
1. Получать Rutoken ЭЦП в количестве _____ штук.
2. Подписывать Акт приема-передачи Rutoken ЭЦП.
3. Прочие действия, связанные с получением Rutoken ЭЦП.

Подпись _____ _____ удостоверяю
(фамилия, имя, отчество)

Доверенность выдана сроком на _____
(не более 3-х лет)

_____ _____ _____
(должность руководителя Клиента) (подпись) М.П. (фамилия, имя, отчество)

Приложение 4
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(Система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Акт приема-передачи SafeTouch

(населенный пункт) «____»_____ _____ год

Публичное акционерное общество «Западно-Сибирский коммерческий банк» (ПАО «Запсибкомбанк»), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, при совместном упоминании именуемые «Стороны», заключили настоящий Акт о нижеследующем:

1. По настоящему Акту Банк передал, а Клиент принял для использования в системе «ЗапСиб iNet» устройство SafeTouch в следующем количестве:

п/п	Серийный номер устройства	Данные об уполномоченном лице Клиента, которое будет использовать устройство
	…	Фамилия, имя, отчество, должность
	…	Фамилия, имя, отчество, должность

2. Гарантийный срок на передаваемое устройство составляет 6 (шесть) месяцев с даты передачи устройства, путем подписания настоящего Акта.

3. При обнаружении недостатков устройства Клиент письменно уведомляет об этом Банк.

4. При наличии претензий Банк производит проверку качества устройства в течение 10 (десяти) рабочих дней с момента передачи устройства Клиентом.

При наличии заключения о том, что устройство имеет неустранимые недостатки и они возникли в процессе эксплуатации в связи с ненадлежащим качеством устройства, Банк обязуется заменить некачественное устройство на аналогичное в течение 10 (десяти) рабочих дней с момента вручения указанного заключения Клиенту (при наличии аналогичного устройства у Банка). При отсутствии аналогичного устройства Сторонами по договоренности решается вопрос о возможности его замены другим или возврате суммы стоимости устройства Клиенту.

При наличии заключения о том, что недостатки устройства возникли в процессе эксплуатации в связи с действиями Клиента (неаккуратное (нецелевое) использование, вызвавшее нарушение целостности устройства, его поломку), обязательства Банка по устранению недостатков, предусмотренные вторым абзацем настоящего пункта Акта, не возникают и Клиент самостоятельно несет все риски, связанные с выходом устройства из строя.

5. Требования, связанные с недостатками устройства, могут быть предъявлены Клиентом, если недостатки обнаружены в течение гарантийного срока. По истечении указанного выше срока никакие рекламации не принимаются.

Банк отвечает за недостатки устройства, если не докажет, что недостатки устройства возникли после его передачи Клиенту вследствие нарушения Клиентом инструкции по эксплуатации и хранению устройства либо действий третьих лиц, либо непреодолимой силы.

6. Гарантия не распространяется на неисправности, связанные с нештатным использованием поставляемого устройства или несоблюдением условий эксплуатации. Гарантия не распространяется на механические повреждения, а также на случаи, когда устранение неисправностей осуществлялось Клиентом или третьими лицами самостоятельно без письменного обращения к Банку.

7. Гарантийный срок на устройство начинает исчисляться с момента подписания настоящего Акта.

Клиент подтверждает, что корпус (-а) переданного (-ых) SafeTouch не имеет (-ют) видимых признаков повреждения или взлома.

Дата, время передачи устройства Клиенту: «____»_____ _____ год _____:_____
(час. : мин.)

От БАНКА передал		**От КЛИЕНТА получил**
(должность)		(должность)
(подпись)		(подпись)
(Ф.И.О.) М.П.		(Ф.И.О.) М.П.

Приложение 5
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Доверенность оформляется на фирменном бланке организации и подписывается руководителем Клиента.

ДОВЕРЕННОСТЬ

Город _____ Дата выдачи: «____» _____ год

Настоящим _____, в лице_____
(наименование Клиента) (должность, фамилия, имя, отчество)
_____(далее по тексту – «Доверитель»),
действующего на основании_____
(название документа, на основании которого действует указанное лицо)

предоставляет право _____
(фамилия, имя, отчество)
паспорт серии_____ № _____ выдан_____
(серия паспорта) (номер паспорта) (кем и когда выдан, код подразделения)
_____
совершать от имени Доверителя следующие действия:
1. Получать SafeTouch в количестве _____ штук.
2. Подписывать Акт приема-передачи SafeTouch .
3. Прочие действия, связанные с получением SafeTouch .

Подпись _____ _____ удостоверяю
(фамилия, имя, отчество)

Доверенность выдана сроком на _____
(не более 3-х лет)

_____ _____ _____
(должность руководителя Клиента) (подпись) М.П. (фамилия, имя, отчество)

Приложение 6
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Директору/начальнику филиала/ДО/ОО/ДпРК

Заявление на отказ от подключения SMS-оповещений

Я ознакомлен с наличием в ПАО «Запсибкомбанк» SMS-оповещений, а также с условиями предоставления данных SMS-оповещений, содержащимися в Правилах обслуживания клиентов с использованием Интернет-технологий (система «ЗапСиб iNet»).

Прошу не предоставлять мне следующие SMS-оповещения:

☐ Пользователь вошел в систему
☐ Успешная аутентификация пользователя
☐ Платежное поручение проведено Банком
☐ Одноразовый пароль при входе в систему
☐ Создано платежное поручение в системе

Я информирован о том, что:

SMS-оповещения предоставляются Банком с целью повышения безопасности использования системы «ЗапСиб iNet»;

- при отказе от использования SMS-оповещения «Пользователь вошел в систему» в системе «ЗапСиб iNet» и SMS-оповещения «Успешная аутентификация пользователя» в системе «ЗапСиб iNet», Банк не несет ответственность за неинформирование Клиента об успешной авторизации пользователя в системе «ЗапСиб iNet»;
- при отказе от использования SMS-оповещения «Платежное поручение проведено банком» и «Создано платежное поручение в системе» Банк не несет ответственность за не информирование Клиента о совершении каждой операции с использованием системы «ЗапСиб iNet», а также за последствия для Клиента в связи с совершением операций, о которых Клиент не был проинформирован Банком указанным способом. В этом случае Клиент принимает на себя все риски совершения операций с использованием системы «ЗапСиб iNet» без его согласия и Банк не несет ответственности за последствия исполнения таких операций.

Заявление исполнить «__» _____20___г.

Руководитель:_____ / _____ /_____
(должность) (подпись) (Ф.И.О.)

М.П. «__»_____20___г.

Приложение 7
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Образец письма о выпуске нового сертификата ключа проверки электронной подписи.

_____
(наименование Клиента)
в лице_____,
_____,
(*должность и ФИО представителя Клиента)*
действующего на основании_____,
(название документа, на основании которого действует указанное лицо)

Прошу выпустить новый сертификат ключа проверки электронной подписи на имя
_____
(ФИО, должность пользователя)

Руководитель _____ /_____/ _____
(подпись) *(расшифровка)* *М.П.*

Приложение 8
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4
Директору/начальнику филиала/ДО/ОО/ДпРК

ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

_____

(полное наименование ЮЛ в соответствии с учредительными документами;
ФИО ИП /ФЛ, занимающегося в установленном законодательством РФ порядке частной практикой)

в лице _____,
_____,
(*должность и ФИО представителя Клиента)*

действующего на основании _____
(наименование документа: Устав, доверенность, свидетельство, иной документ)

в связи с _____
(причина аннулирования (отзыва) сертификата: компрометация ключа, прекращение работы и т.д.)

просит аннулировать (отозвать) сертификат ключа проверки электронной подписи серийный номер_____, выданного на имя_____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан/код подразделения)

Руководитель _____ / _____ / _____
(подпись) *(Ф.И.О., должность, организация)* *М.П.*

«____» _____ _____ г.

Заявление принял _____ / _____
(подпись) *(должность, Ф.И.О. работника Банка)*

«____» _____ _____ г.

Приложение 9
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(Система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Уведомление-памятка Клиентам ПАО «Запсибкомбанк» о мерах информационной безопасности при работе с системой «ЗапСиб iNet»

1. В качестве ключевого носителя **обязательно** используйте Rutoken ЭЦП.
2. Генерацию ЭП необходимо осуществлять **только в присутствии лица уполномоченного** за эту ЭП.
3. **Запрещается принимать**, включая работников ПАО «Запсибкомбанк», **ЭП, сгенерированные без присутствия уполномоченного лица**.
4. **Запрещается передавать** Rutoken ЭЦП/SafeTouch **НЕ уполномоченному лицу**, включая бухгалтера организации, системных администраторов или работников ПАО «Запсибкомбанк».
5. Запрещается использовать один SafeTouch несколькими (более одного) Клиентами Банка.
6. Использование Rutoken ЭЦП со сгенерированным ключом проверки ЭП **должно осуществляться только уполномоченным лицом**.
7. Необходимо работать с системой ДБО **БЕЗ, подключенного** Rutoken ЭЦП, необходимо **подключать** Rutoken ЭЦП к компьютеру (если клиент не переведен на обслуживание по системе «ЗапСиб iNet» с «Пакетом безопасности»)/SafeTouch (если клиент обслуживается с «Пакетом безопасности») **только в момент подписания ЭД.**
8. Rutoken ЭЦП/SafeTouch необходимо хранить **в недоступном** для посторонних лиц **месте** (сейф, металлический шкаф и т.д.).
9. Необходимо соблюдать требования, предъявляемые к формированию пароля Rutoken ЭЦП.
10. Необходимо соблюдать требования, предъявляемые к учетным данным в системы «ЗапСиб iNet».
11. **Запрещается** использовать **учетные данные** для доступа в систему «ЗапСиб iNet» на других сайтах.
12. Запрещается непрофильное использование сети Интернет (развлекательные ресурсы, социальные сети т.д.) на компьютере с установленной системой «ЗапСиб iNet».
13. Запрещается устанавливать развлекательные и игровые программы на компьютер, на котором установлена система «ЗапСиб iNet».
14. Необходимо осуществлять работу на компьютере с установленной системой «ЗапСиб iNet» под учетной записью пользователя без наличия прав на такие задачи администрирования, как обновление операционной системы или настройка системных параметров.
15. Запрещается использовать адрес корпоративной электронной почты для регистрации на ресурсах сети Интернет (форумы, доски объявлений, Интернет-магазины и т.п.), публиковать этот адрес в СМИ и объявлениях.
16. Запрещается передавать корпоративный адрес электронной почты «недоверенным» лицам.
17. Запрещается открывать сообщения, полученные по электронной почте, без предварительной проверки на вирусы.
18. Необходимо ограничить использование отчуждаемых цифровых носителей информации (USB-накопители, CD и т.п.) на компьютере с установленной системой «ЗапСиб iNet».
19. Необходимо осуществлять проверку подключаемых носителей (USB-накопители, CD и т.п.) на вирусы до начала их использования.

Обеспечить соблюдение мер по защите компьютера, с которого осуществляется работа в системе «ЗапСиб iNet»:

- Используйте только лицензионную операционную систему MS Windows 7/8 и лицензионное антивирусное программное обеспечение с актуальными базами.
- **Постоянно обновляйте**, не реже 1 раза в неделю, установленную **антивирусную программу**.
- **Используйте специализированное программное обеспечение**, например, межсетевые экраны, для более безопасной связи.
- **Исключите** использование программ **удаленного управления** (teamviewer и др.).
- **Не передавайте в ремонт или на обслуживание** за пределы организации **компьютер** с установленной системой «ЗапСиб iNet», **без уведомления ПАО «Запсибкомбанк».**

При возникновении следующих ситуаций:

- Нарушение работы персонального компьютера: компьютер не запускается, черный экран

СРОЧНО извлекайте Rutoken ЭЦП (если клиент не переведен на обслуживание по системе «ЗапСиб iNet» с «Пакетом безопасности»)/**SafeTouch** (если клиент обслуживается с «Пакетом безопасности») **из компьютера** и **отключайте компьютер от сети Интернет,**

Если: Утерян или похищен Rutoken ЭЦП/SafeTouch или компьютер, на котором была установлена система «ЗапСиб iNet»

- Невозможно подключиться к системе «ЗапСиб iNet» по неизвестным причинам.

Необходимо незамедлительно обращаться в Банк по телефону 8-800-100-5005.

Отметка о получении Клиентом:
Данные правила мне разъяснены и понятны, обязуюсь их соблюдать при работе в системе «ЗапСиб iNet».
«___»_____201__г. _____/_____
(подпись Клиента) (расшифровка Клиента)
Инструктаж провел:
«___»_____201__г. _____/_____
(подпись Сотрудника) (расшифровка Сотрудника)

Соблюдение указанных мер и своевременное сообщение в Банк об угрозе потери конфиденциальности ключей ЭП помогут существенно снизить угрозу мошенничества с денежными средствами и предотвратить проведение несанкционированных платежей с использованием системы «ЗапСиб iNet».

Приложение 10
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Директору/начальнику филиала/ДО/ОО/ДпРК

Заявление на блокировку системы ДБО пользователю

В связи _____
(указать причину, например: увольнением работника, сменой должности работника и т.д.)
прошу заблокировать систему _____
(наименование системы)
пользователю _____
(Ф.И.О. пользователя, должность)
по клиенту _____
(наименование организации)
расчетный счет №_____

Руководитель _____ / _____ / _____ «___» _____ ____г.
(подпись) *(Ф.И.О.)* *М.П.*

Приложение 11
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Директору/начальнику филиала/ДО/ОО/ДпРК

Заявление о дополнении/изменении номеров телефонов в рамках SMS-оповещений

1. Клиент просит исключить из списка следующий (-ие) номер (-а) сотового (-ых) телефона (-ов) уполномоченных лиц:

	Успешная аутентификация пользователя											
на телефонный(е) номер(а):												*Ф.И.О. пользователя, должность*

	Пользователь вошел в систему											
на телефонный(е) номер(а):												*Ф.И.О. пользователя, должность*

	Платежное поручение проведено банком											
на телефонный(е) номер(а):												*Ф.И.О. пользователя, должность*

	Одноразовый пароль при входе в систему											
на телефонный(е) номер(а):												*Ф.И.О. пользователя, должность*

	Создано платежное поручение в системе											
на телефонный(е) номер(а):												*Ф.И.О. пользователя, должность*

2. Клиент просит включить в список следующий (-ие) номер (-а) сотового (-ых) телефона (-ов) уполномоченных лиц:

	Успешная аутентификация пользователя											
на телефонный(е) номер(а):												*Ф.И.О. пользователя, должность*

	Пользователь вошел в систему											
на телефонный(е) номер(а):												*Ф.И.О. пользователя, должность*

	Платежное поручение проведено банком

на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*

	Одноразовый пароль при входе в систему

на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*

	Создано платежное поручение в системе

на телефонный(е) номер(а):											*Ф.И.О. пользователя, должность*

Руководитель _____ / _____ / _____ «___» _____ __г.
(подпись) *(Ф.И.О.)* *М.П.*

Заявление принял _____ / _____ «___» _____ __г.
(подпись) *(должность, Ф.И.О. работника Банка)*

Приложение 12
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Директору/начальнику филиала/ДО/ОО/ДпРК

Согласие на формировании разрешительной комиссии.

_____
(наименование Клиента)
в лице_____, _____
_____,
(*должность и ФИО представителя Клиента)*
действующего на основании _____,
(наименование документа: Устав, доверенность, свидетельство, иной документ)
Дает согласие на формирование разрешительной комиссии с целью _____
_____
(указать цель формирования разрешительной комиссии, например, разрешения конфликтной ситуации по проведению платежного документа №_ на сумму ____)

Со стороны_____
(наименование Клиента)
в разрешительной комиссии будут участвовать:

№	ФИО	Должность	Основания
1	…		Доверенность (прилагается)

Руководитель _____ / _____ / _____ «___» _____ ____г.
(подпись) *(Ф.И.О.)* *М.П.*

Приложение 13
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Акт разногласий к

Протоколу заседания разрешительной комиссии

от __ _____ _____г.

№	Изложенная в Протоколе информация	Замечания
1		
2		
..		

Руководитель _____ / _____ / _____ «___» _____ ____г.
(подпись) *(Ф.И.О.)* *М.П.*

Приложение 15
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Директору/начальнику филиала/ДО/ОО/ДпРК

Образец письма по приостановлению/возобновлению работы системы ДБО

_____
(наименование Клиента)
в лице_____,_____
_____,
(*должность и ФИО представителя Клиента)*
действующего на основании _____,
(наименование документа: Устав, доверенность, свидетельство, иной документ
в связи с _____
(указать причину)
просит _____ работу в системе «ЗапСиб iNet» с _____ .
(указать: приостановить/возобновить) *(дата)*

Руководитель _____ / _____ / _____ «___» _____ ____г.
(подпись) *(Ф.И.О.)* *М.П.*

Приложение 16
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4
Директору/начальнику филиала/ДО/ОО/ДпРК

Заявление на изменение номеров телефонов в рамках услуги «Белый список»

_____
(наименование Клиента)
в лице_____,_____
(*должность и ФИО представителя Клиента)*
действующего на основании_____,
(наименование документа: Устав, доверенность, свидетельство, иной документ)
прошу:

1. не использовать следующие номера телефонов при подтверждении платежей:

___8-_____-_____-_____	_____
(номер телефона)	(Ф.И.О. контактного лица)
___8-____ - _____-_____	_____
(номер телефона)	(Ф.И.О. контактного лица)
___8-____-_____-_____	_____
(номер телефона)	(Ф.И.О. контактного лица)

2. добавить следующие номера телефонов при подтверждении платежей:

___8-_____-_____-_____	_____
(номер телефона)	(Ф.И.О. контактного лица*)
___8-____ - _____-_____	_____
(номер телефона)	(Ф.И.О. контактного лица*)
___8-____-_____-_____	_____
(номер телефона)	(Ф.И.О. контактного лица*)

* может быть указано ТОЛЬКО лицо, включенное в карточку образцов подписей и оттиска печати.

Руководитель _____ _____/ ___ __.__.____г.
(подпись) *(Ф.И.О.)* МП *дата*

Заявление принял_____ / _____ __.__.____г.
(подпись) *(должность, Ф.И.О. работника Банка)* *дата*

Приложение 17
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4
Директору/начальнику филиала/ДО/ОО/ДпРК

Заявление на изменение Списка доверенных получателей платежей

_____
(наименование Клиента)
в лице_____,_____
_____
(*должность и ФИО представителя Клиента)*
действующего на основании_____,
(наименование документа: Устав, доверенность, свидетельство, иной документ)
прошу:
1. исключить из Списка доверенных получателей платежей следующих контрагентов:

Наименование контрагента	**БИК**	**Счет**	**ИНН**

2. включить в Список доверенных получателей платежей следующих контрагентов:

Наименование контрагента	**БИК**	**Счет**	**ИНН**	**Лимит платежа*, руб./ин.валюта**

Руководитель _____/_____ __.__.____г.
(подпись) (Ф.И.О.) *МП* *дата*

Заявление принял_____/_____ __.__.____г.
(подпись) (должность, Ф.И.О. работника Банка) *дата*

*сумма лимита в рамках одного платежного документа, при отсутствии необходимости установления лимита проставляется значение «не лимитировано».

Приложение 18
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Акт выезда №
по подтверждению платежного поручения клиента
(краткое наименование клиента)

1	Цель выезда	Подтверждение инициирования отправки платежного документа №___ от __.__.____г. на сумму _____ руб. по каналам ДБО в Банк.
2	Полное наименование Клиента, к которому осуществляется выезд:	
3	Дата, время выезда	___.___._____г. с ___:___ до ___:___
4	Ф.И.О., должность работника Банка, осуществляющего выезд	
5	Адрес Клиента, по которому осуществляется выезд	
6	Результаты выезда (подкрепляется фотоотчетом с места проведения проверки)	

Проверку проводил:

___.___._____г. _____ /_____/
(*дата)* *(подпись)* *(фамилия, инициалы)*

Руководитель:

___.___._____г. _____ /_____/
(*дата)* *(подпись)* *(фамилия, инициалы)*

Приложение 19
к Правилам обслуживания Клиентов
с использованием Интернет-технологий
(система «ЗапСиб iNet»)
от «19» апреля 2016г. №21/1045_R4

Заявление на разблокирование номера телефона

Прошу разблокировать номер(а) телефона(ов):

и возобновить отправку SMS-сообщений из системы «ЗапСиб iNet».

Заявление исполнить «__» _____20___г.

Руководитель:_____ / _____ /_____
(должность) (подпись) (Ф.И.О.)

М.П. «__»_____20___г.»
(при наличии)