Редакция действует с 25.07.2024 г.
Приложение №1
к Приказу № 107/6
от 09.07.2024

ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ЮРИДИЧЕСКИХ ЛИЦ

1. Термины и определения

1.1. **Банк** – «КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ, зарегистрированное в Сервисе, осуществляющее аккредитацию Клиентов в Сервисе, а также организующее обмен информацией с Клиентами с использованием Сервиса.

1.2. **Дистанционное Банковское Обслуживание (ДБО) –** предоставление Банком Клиенту услуг по обмену электронными документами, простыми электронными документами в системе Интернет-банк.

1.3. **Договор Дистанционного Банковского Обслуживания (Договор ДБО)** – Правила Дистанционного Банковского обслуживания юридических лиц, Заявление о присоединении к Договору Дистанционного Банковского Обслуживания, заявление на обслуживание по системе Интернет-банк с предоставлением доступа по ключу электронной подписи, заявление на обслуживание по системе Интернет-банк с предоставлением доступа по Логин Паролю, надлежащим образом заполненные и подписанные Клиентом, и Тарифы на услуги Банка, предоставляемые юридическим лицам (кроме кредитных организаций), в совокупности являющиеся заключенным между Клиентом и Банком Договором ДБО.

1.4. **Зарегистрированный номер** – номер мобильного телефона, указанный в соответствующем заявлении Клиента.

1.5. **Заявление о присоединении** – заявление о присоединении к Договору ДБО, составленное по форме, установленной Банком.

1.6. **Интернет-банк для клиентов (система Интернет-банк)** – услуга в рамках Сервиса «FAKTURA.RU», заключающаяся в обеспечении информационного и технологического взаимодействия между Банком и Клиентами Банка

1.7. **Клиент** - юридическое лицо, иностранная структура без образования юридического лица, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством РФ порядке частной практикой, присоединившиеся к системе Интернет-банк, в соответствии настоящими Правилами.

1.8. **Оператор Сервиса (Оператор)** –ЗАО «Биллинговый центр» (ИНН 5401152049), осуществляющее информационное и технологическое обслуживание Банка и Клиента в рамках Сервиса.

1.9. **Операционное время -** часть рабочего времени, в течение которого производится расчетно-кассовое обслуживание Клиентов, совершаются банковские операции и другие сделки.

1.10. **Операционный день -** включает в себя операционное время, а также период документооборота и обработки учетной информации, обеспечивающей оформление и отражение в бухгалтерском учете операций, совершенных в течение операционного времени, календарной датой соответствующего операционного дня, и составление ежедневного баланса в установленные сроки.

1.11. **Персональные данные (ПДн)**- как определено Федеральным законом от 27.07.2006 года №152-ФЗ "О персональных данных».

1.12. **Электронный документ (далее по тексту - ЭД)** – электронное сообщение, подписанное электронной подписью, в котором информация представлена в электронно-цифровой форме и соответствует установленному Оператором или Организатором сервиса формату. Электронный документ может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

1.13. **Простой электронный документ (по тексту – ПЭД)** - электронное сообщение, подписанное Простой электронной подписью, в котором информация представлена в

электронно-цифровой форме и соответствует установленному Организатором сервиса формату. Простой электронный документ может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

1.14. **Несанкционированный ЭД/ПЭД** – ЭД/ПЭД, соответствующий одному или нескольким признакам осуществления перевода денежных средств без добровольного согласия Клиента, установленным Банком России и размещенным на его официальном сайте в сети Интернет по адресу: https://cbr.ru/.

1.15. **Рисковый ЭД/ПЭД** – ЭД/ПЭД, соответствующий одному или нескольким признакам мошеннических операций, зафиксированным во FRAMOS, за исключением признаков несанкционированных операций.

1.16. **Сервис «FAKTURA.RU» (Сервис)** – информационно-технологический Сервис, позволяющий сторонам организовать обмен электронными документами, простыми электронными документами, sms-сообщениями, push-сообщениями, e-mail-сообщениями и прочей информацией, имеющей значение для сторон (далее - все вышеперечисленное именуется Информация).

1.17. **Система «BeSafe»** (система) – корпоративная информационная система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в соответствии с Правилами электронного документооборота Корпоративной информационной системы **«BeSafe» (далее Правила КИС «BeSafe»).**

1.18. **Смарт-карта** (USB – ключ / ключевой носитель) – компактное программно-аппаратное устройство, предназначенное для хранения ключа электронной подписи, ключа проверки электронной подписи, Сертификата, а также другой электронно-цифровой информации.

1.19. **Тарифы** – тарифы на услуги Банка, предоставляемые Клиентам.

1.20. **Удостоверяющий Центр «Authority»** (удостоверяющий центр**)** – удостоверяющий центр создан Закрытым акционерным обществом «Центр Цифровых Сертификатов», осуществляет изготовление Сертификатов ключей проверки электронных подписей для юридических и физических лиц для возможности осуществления электронного документооборота в рамках КИС «BeSafe». Удостоверяющий центр осуществляет изготовление цифровых Сертификатов в соответствии с «Правилами работы Удостоверяющего Центра (AUTHORITY)».

1.21. **Услуга «Альтернативный фактор подтверждения F.Business»** – услуга по обеспечению информационного и технологического взаимодействия между Банком и Клиентом, позволяющая Банку получать от Клиента подтверждение факта отправки Клиентом Банку ЭД/ПЭД, которые на основании Правил FRAMOS относятся к Рисковым и Несанкционированным ЭД/ПЭД, и подтверждение возобновления исполнения ЭД/ПЭД (далее – «подтверждение альтернативным фактором»).

1.22. **FRAMOS (FRAud MOnitoring System**) – технологическая платформа, которая обеспечивает анализ ИНФОРМАЦИИ, в том числе ПЭД/ЭД, на предмет отнесения их к ПЭД/ЭД с признаками рисковых операций и ПЭД/ЭД с признаками несанкционированных операций.

Все остальные термины и определения, встречающиеся в тексте настоящих Правил, толкуются Сторонами в соответствии с законодательством Российской Федерации, действующими Правилами электронного документооборота корпоративной информационной системы «BeSafe», которые расположены в Интернете по адресу www.besafe.ru, Правилами Сервиса «FAKTURA.RU» (https://cft.group/contracts), Правилами работы Удостоверяющего Центра (AUTHORITY (www.authority.ru). При отсутствии однозначного толкования термина, Стороны руководствуются обычаями делового оборота, в том числе сложившимися в сети Интернет.

2. ПРЕДМЕТ ДОГОВОРА, ПОРЯДОК ЗАКЛЮЧЕНИЯ, ИЗМЕНЕНИЯ

2.1. Предметом настоящего Договора является:

- предоставление Банком возможности Клиенту использовать Сервис «FAKTURA.RU» для обмена между Банком и Клиентом ЭД, ПЭД, электронными сообщениями (sms-сообщения, push-сообщения, e-mail-сообщения и прочее);

- оказание Банком услуг Клиенту с использованием Сервиса «FAKTURA.RU».

2.2. По системе Интернет-банк оказываются следующие услуги:

2.2.1. предоставление информации о состоянии Счета/Счетов Клиента, открытых в Банке, включая прием/ передачу выписок;

2.2.2. прием к исполнению от Клиента ЭД/ПЭД, содержащих в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций, просмотр информации о состоянии указанных ЭД/ПЭД;

2.2.3. прием/передача ЭД/ПЭД, связанных с выполнением Банком функций агента валютного контроля;

2.2.4. прием/передача иных ЭД, ПЭД, связанных с использованием Клиентом услуг Банка, включая, но не ограничиваясь, запросы о предоставлении информации и документов, касающихся операций по Счету/ Счетам Клиента, направление согласия на получение кредитного отчета в любом БКИ, реестров на выплаты физическим лицам;

2.2.5. обмен информацией о банковских услугах и продуктах.

2.3. Настоящий Договор является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

2.4. Заключение настоящего Договора между Сторонами осуществляется путем подачи Клиентом в Банк надлежащим образом оформленного заявления о присоединении к Договору Дистанционного Банковского Обслуживания (***Приложение №1***) на бумажном носителе в 2-х экземплярах и предоставлении документов, предусмотренных настоящим Договором, законодательством РФ и необходимых для подключения к системе Интернет-банк.

2.5. Настоящий Договор опубликован на официальном сайте Банка: www.sibsoc.ru и распространяется на всех Клиентов, присоединившихся к нему в той части, которая относится к Клиенту и в отношении тех услуг, которыми Клиент выразил намерение воспользоваться в порядке, предусмотренном настоящим Договором.

2.6. Акцептом *з*аявления о присоединении*,* моментом присоединения к настоящему Договору является дата принятия Банком заявления о присоединении к настоящему Договору.

2.7. Внесение изменений и дополнений в Договор ДБО осуществляется Банком в одностороннем порядке. Изменения доводятся Банком до сведения Клиента посредством уведомления не позднее, чем за 15 (пятнадцать) календарных дней до даты вступления в силу таких изменений. Уведомление осуществляется путем опубликования на официальном сайте Банка: www.sibsoc.ru.

2.8. Клиент, заключая настоящий Договор, присоединяется к Правилам электронного документооборота корпоративной информационной системы «BeSafe», которые расположены в сети Интернет по адресу www.besafe.ru, а также соглашается для обмена ЭД, ПЭД, иной информацией и предоставления услуг Банком использовать Сервис «FAKTURA.RU» на условиях Правил Сервиса «FAKTURA.RU», расположенных в сети Интернет по адресу https://cft.group/contracts.

2.9. Дополнительные соглашения к Договорам банковского счета по обслуживанию в системе Интернет-банк, соглашения об обслуживании в системе Интернет-банк, заключенные до вступления настоящих Правил, действуют на условиях настоящих Правил. Заключение дополнительных договоров/соглашений не требуется.

3. ОБЩИЕ УСЛОВИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

3.1. Электронный документооборот между Банком и Клиентом осуществляется посредством Сервиса «FAKTURA.RU» в порядке и на условиях, определенных Правилами электронного документооборота корпоративной информационной системы «BeSafe».

3.2. Передаваемые в системе Интернет-банк документы заверяются электронной подписью (далее - ЭП) или аналогом собственноручной подписи (далее –АСП) уполномоченного лица Клиента, уполномоченного распоряжаться денежными средствами, которые гарантируют подлинность, целостность и авторство документов, предаваемых в электронной форме. При этом поврежденные в результате помех в линиях связи, либо других воздействий документы не будут приняты Банком к исполнению.

3.3. Банк, используя программно-технические средства, проверяет подлинность ЭП/ АСП входящего ЭД/ПЭД. В случае положительного результата проверки ЭД/ПЭД данный ЭД/ ПЭД признается полученным. В противном случае данный ЭД/ПЭД считается не полученным.

Проверка ЭП/АСП в системе Интернет-банк осуществляется в соответствии с Правилами КИС «BeSafe».

3.4. Электронные документы, простые электронные документы передаются и применяются сторонами без их последующего предоставления на бумажном носителе.

Выписка по счету может быть сформирована Клиентом в системе Интернет-банк самостоятельно за любой период, начиная со дня подключения к системе Интернет-банк.

3.5. Клиент может направлять ЭД/ПЭД в Банк по системе Интернет-банк круглосуточно.

3.6. Прием Банком ЭД/ПЭД осуществляется в течение установленного в Банке операционного времени в соответствии с режимом работы Банка. ЭД/ПЭД, направленный в Банк после завершения операционного времени, официально установленного Банком, считается принятым к исполнению Банком на следующий рабочий день в течение следующего операционного времени.

3.7. Исполнение ЭД/ПЭД, содержащих в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций, осуществляется Банком не позднее рабочего дня, следующего за днем поступления в Банк данного ЭД/ПЭД.

3.8. Банк и Клиент признают, что уведомление об изменении состояния ЭД/ПЭД, содержащих в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций, доступное Клиенту для просмотра в системе Интернет-банк, является основным способом уведомления Клиента об исполнении ЭД/ПЭД, содержащих в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций. Использование иных способов уведомления Клиента (sms/e-mail/push–уведомлений) осуществляется по заявлению Клиента на подключение уведомлений (при предоставлении доступа по ключу электронной подписи (***Приложение № 3***)) в соответствии с тарифами Банка, за исключением уведомлений при выявлении несанкционированного ЭД/ПЭД и рискового ЭД/ПЭД. Способы уведомления Клиента в случае выявления Несанкционированного ЭД/ПЭД и Рискового ЭД/ПЭД обозначены в п. 3.9 настоящих Правил.

3.9. Банк и Клиент признают, что основными способами уведомлений Клиента при выявлении Несанкционированного ЭД/ПЭД и Рискового ЭД/ПЭД являются по усмотрению Банка: уведомление путем телефонного звонка, отправки письма на электронный адрес Клиента, sms/push-уведомлений по системе Интернет-банк либо путем вручения письменного уведомления.

3.10. Банк и Клиент признают, что:

- используемые ими по настоящему Договору ЭП/АСП, метод шифрования информации, подсистемы обработки, хранения, защиты и передачи информации достаточны для обеспечения надежной, эффективной и безопасной работы, и система шифрования гарантирует защиту от несанкционированного доступа к передаваемой информации в ходе сеансов связи;

- отправленные Клиентом и полученные Банком ЭД/ПЭД, электронное сообщение (далее ЭС), заверенные ЭП/АСП Клиента, юридически равнозначны документам на бумажном носителе, заверенным собственноручными подписями и оттиском печати Клиента (при наличии) из «Карточки с образцами подписей и оттиска печати», хранящейся в Банке, являются основанием для осуществления операций по банковскому счету Клиента. Исполнение ЭД/ПЭД Клиента, подписанных его ЭП/АСП, считается надлежащим исполнением Банком обязательством по настоящему Договору;

- используемые в Сервисе «FAKTURA.RU» способы защиты информации, которые обеспечивают формирование и проверку ЭП/АСП, достаточны для подтверждения авторства и подлинности ЭД/ПЭД;

- подделка ЭП, то есть создание ЭП ЭД, успешно проходящей проверку, невозможно без знания Ключа электронной подписи отправителя документа (доступа к ключу электронной подписи);

- подделка АСП, то есть создание АСП, успешно проходящей проверку невозможно без знания пароля и разового секретного пароля.

Положения, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Сертификат и Аналог собственноручной подписи Клиента созданы с использованием технологии КИС «BeSafe».

3.11. Банк и Клиент признают электронную выписку по счету, сформированную и полученную с помощью системы Интернет-банк, равнозначной выписке, распечатанной на бумажном носителе и полученной Клиентом.

3.12. Банк и Клиент признают, что датой представления Клиентом в Банк документов валютного контроля в электронном виде является дата, указанная в штампе «Дата представления» ЭД/ПЭД.

3.13. Банк и Клиент признают, что датой получения Клиентом от Банка документов валютного контроля в электронном виде после положительного результата их проверки является дата, указанная в штампе «Дата принятия банком» ЭД/ПЭД, проставляемом при подписании документов ЭП/АСП уполномоченного лица Банка. При отрицательном результате проверки документов валютного контроля в электронном виде Банк отказывает Клиенту в принятии документов и информации/проведении операции и направляет Клиенту информацию о причинах отказа с указанием даты отказа, дата отказа является также датой возврата представленных документов и информации.

3.14. В случае выявления Несанкционированного/Рискового ЭД/ПЭД Сервис приостанавливает отправку ЭД/ПЭД, а в совершении операции с использованием сервиса быстрых платежей отказывает.

3.15. В случае, когда Клиенту подключена услуга «Альтернативный фактор подтверждения F.Business» и Сервисом выявлен Несанкционированный/Рисковый ЭД/ПЭД, то для возобновления отправки ЭД/ПЭД Клиенту необходимо подтвердить ЭД/ПЭД альтернативным фактором в течение настроенного периода времени (в течение часа).

4. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ ИНТЕРНЕТ-БАНК

4.1. К системе Интернет-банк подключаются Клиенты, которые заключили Договор банковского счета, а также Клиенты, имеющие иные договорные отношения с Банком для обмена документами в электронной форме, в том числе при зачислении денежных средств на счета физических лиц.

4.2. Подключение и допуск к системе Интернет-банк осуществляется в соответствии с «Правилами Сервиса «FAKTURA.RU».

4.3. Процедура аккредитации осуществляется Банком в соответствии с «Правилами Сервиса «FAKTURA.RU».

4.4. Подключение Клиента к системе Интернет-банк осуществляется одним из способов:

- с помощью ключа ЭП;
- с помощью Логина и Пароля.

4.5. Для подключения к системе Интернет-банк с помощью ключа ЭП уполномоченное лицо Клиента представляет в Банк:

- заявление на присоединение к Правилам ДБО в 2-х экземплярах (***Приложение №1***);
- заявление на обслуживание по системе Интернет-банк с предоставлением доступа по ключу электронной подписи (***Приложение № 4***) (возможен вариант наличия у клиента смарт карты);
- согласие на обработку Персональных данных (***Приложение № 5***);
- заявление на выдачу Сертификата ключа проверки электронной подписи (***Приложение № 6***);
- акт приема передачи смарт-карты (***Приложение № 7***).

4.5.1. Для хранения Ключей ЭП Банк передает Клиенту необходимое количество ключевых носителей по акту приема-передачи (***Приложение № 7***), который подписывается Банком и Клиентом.

4.5.2. Банк регистрирует Клиента, уполномоченное лицо Клиента, Сертификаты ключей проверки электронной подписи в Сервисе «FAKTURA.RU», о чем составляется акт регистрации (***Приложение № 8*** либо ***Приложение № 9***) .

4.5.3. Подключение Клиента к системе Интернет-банк с помощью ключа ЭП осуществляется Банком в течение 2 (двух) рабочих дней с момента представления в Банк Клиентом подписанных актов регистрации (***Приложение № 8*** либо ***Приложение № 9***), актов приема-передачи Сертификата ключа проверки электронной подписи (***Приложение № 10***), оформленных в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY», выданных на лиц, наделенных правом подписи согласно выбранным Клиентом сочетаниям подписей и указанных в карточке образцов подписей и оттиска печати.

4.5.4. Заявление на выдачу Сертификата ключа проверки электронной подписи ***(Приложение №6),*** акт приема-передачи Сертификата ключа проверки электронной подписи

(***Приложение № 10***) и соответствующие заявление на выдачу Сертификата ключа проверки электронной подписи, акт приема-передачи Сертификата ключа проверки электронной подписи, утвержденные Правилами работы Удостоверяющего центра «AUTHORITY» имеют для Сторон одинаковую юридическую силу и могут быть использованы в работе.

4.5.5. Создание Ключей электронной подписи и Ключей проверки электронной подписи, изготовление Сертификата ключа проверки электронной подписи осуществляется Клиентом в соответствии с Правилами электронного документооборота КИС «BeSafe».

4.5.6. Срок действия Сертификата составляет один календарный год с даты начала действия Сертификата. Сертификат действует в пределах срока должностных полномочий Владельца Сертификата ключа проверки электронной подписи.

4.5.7. Продление срока действия Сертификата на новый срок оформляется обязательной сменой Ключей не позднее 15 календарных дней до момента окончания срока действия Сертификата. Клиент отправляет в Банк запрос на обновление Сертификата через Интернет-банк Faktura.ru, сохраняет обновленный Сертификат, предоставляет в Банк подписанные заявление на выдачу Сертификата ключа проверки электронной подписи ***(Приложение № 4)*** , акты приема-передачи Сертификата ключа проверки электронной подписи (***Приложение № 10***).

4.6. Для подключения к системе Интернет-банк с помощью Логина и Пароля уполномоченное лицо Клиента представляет в Банк:

- заявление на присоединение к Правилам ДБО в 2-х экземплярах (***Приложение №1***);
- заявление на обслуживание по системе Интернет-банк с предоставлением доступа по Логину и Паролю ***Приложение № 11***);
- согласие на обработку Персональных данных (***Приложение № 5***).

4.6.1. Подключение Клиента к системе Интернет-банк с помощью Логина и Пароля осуществляется Банком в следующем порядке:

- создание Логина, первичного Пароля Клиента и Пароля осуществляется в соответствии с требованиями Правил КИС «BeSafe», Правилами Сервиса «FAKTURA.RU»;
- Клиент получает на адрес электронной почты Логин для входа в систему Интернет-банк. Логин направляется на электронную почту уполномоченного лица Клиента, которому предоставлен доступ к системе Интернет-банк в соответствии с заявлением на обслуживание по системе Интернет-банк с предоставлением доступа по Логину и Паролю ***(Приложение № 11***).
- Банк регистрирует Клиента, уполномоченное лицо Клиента, Логин в сервисе «FAKTURA.RU», о чем составляется акт приема-передачи Логина (***Приложение № 12***), акт регистрации (***Приложение № 13*** либо ***Приложение № 14***).
- Подключение Клиента к системе Интернет-банк с помощью Логина осуществляется Банком в течение 2(двух) рабочих дней с момента представления в Банк Клиентом подписанных актов приема-передачи Логина (***Приложение № 12***), выданного на лиц, наделенных правом подписи согласно выбранным Клиентом сочетаниям подписей и указанных в карточке образцов подписей и оттиска печати, актов регистрации (***Приложение № 13***) либо ***Приложение № 14***);
- Клиент получает на номер мобильного телефона sms-сообщение с Первичным паролем для входа в систему. Первичный пароль направляется на номер телефона уполномоченного лица Клиента, которому предоставлен доступ в систему Интернет-банк в соответствии с заявлением на обслуживание по системе Интернет-банк с предоставлением доступа по Логину и Паролю. Срок действия Первичного пароля составляет 14 календарных дней;
- на странице входа в систему Интернет-банк Клиент вводит Логин и Первичный пароль Клиента, который Клиент обязан поменять на пароль, который будет использовать в дальнейшем для входа в систему Интернет-банк, следуя подсказкам на странице системы Интернет-банк;
- процедура подключения к системе Интернет-банк считается завершенной после подтверждения на странице системы Интернет-банк успешной регистрации Пароля.
- после получения доступа и завершения процедуры подключения к системе Интернет-банк Клиент может осуществлять вход в систему Интернет-банк в любое время после ввода Логина и Пароля.

4.7. В соответствии с настоящим Договором и на основании Заявления Клиента на доступ к системе Интернет-банк (***Приложение № 4***, ***Приложение № 11***) Банк предоставляет следующие варианты доступа в систему Интернет-банк по счету:

4.7.1. С правом распоряжаться денежными средствами, находящимися на счете, используя ЭП/ АСП;

4.7.2. Без права распоряжаться денежными средствами, находящимися на счете, используя ЭП/ АСП:

- просмотр движения денежных средств по счету;
- запрос выписки по счету;
- создание Распоряжений;
- просмотр информации
- другое (указывается конкретный вид ограниченного доступа).

4.8. Для подключения услуги «Альтернативный фактор подтверждения F. Business» уполномоченное лицо Клиента представляет в Банк заявление установленной формы (Приложение 4 либо Приложение 17).

Заявление может быть представлено Клиентом в Банк на бумажном носителе либо по системе ДБО.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. ПРАВА И ОБЯЗАННОСТИ БАНКА:

5.1.1. Банк обеспечивает доступ Клиента в систему Интернет-банк через сайт https://www.faktura.ru, https://ib.sibsoc.ru.

5.1.2. Банк обязуется исполнять распоряжения Клиента, переданные в электронных документах, только при их правильном оформлении и если получен положительный результат проверки ЭП/АСП Клиента.

5.1.3. Банк обязуется исполнять ЭД/ПЭД Клиента о переводе денежных средств с его счета не позднее рабочего дня, следующего за днем поступления в Банк соответствующего ЭД/ПЭД.

5.1.4. Банк имеет право изменять тарифы за эксплуатацию, техническое обслуживание системы Интернет-банк и дополнительные услуги.

5.1.5. Банк в течение каждого месяца имеет право списывать с банковского счета Клиента плату за использование системы Интернет-банк в соответствии с действующими Тарифами Банка.

5.1.6. В соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» Банк и оператор Сервиса «FAKTURA.RU» обязаны осуществлять проверку наличия признаков осуществления перевода денежных средств без добровольного согласия Клиента до момента списания денежных средств Клиента.

5.1.7. В случае если проводимые Клиентом операции согласно нормам действующего законодательства, вызывают у работников Банка подозрения, что операции совершаются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, Банк вправе не исполнять ЭД/ПЭД Клиента, содержащие в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций.

5.1.8. Банк вправе отказать в приеме к исполнению ЭД/ПЭД, содержащих в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций, в случае если на счете Клиента недостаточно денежных средств для оплаты услуг Банка.

5.1.9. В целях снижения риска мошеннических операций Банк включил автоматический контроль за ЭД/ПЭД Клиента, содержащих в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций.

5.1.10. В случае выявления операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента (за исключением операции с использованием платежных карт, перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России), с момента выявления такой операции:

- приостановить прием к исполнению распоряжения Клиента на два рабочих дня;

- незамедлительно направить Клиенту уведомление о приостановлении одним из следующих способов на усмотрение Банка: путем телефонного звонка, отправки письма на электронный адрес Клиента, sms/push-уведомлений, по системе Интернет-банк либо путем вручения письменного уведомления.

5.1.11. В случае выявления перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России, соответствующих признакам

осуществления перевода денежных средств без добровольного согласия Клиента отказать в совершении операции (перевода) и незамедлительно направить Клиенту уведомление об отказе в совершении операции в порядке, установленном в соответствии с п.5.1.10 настоящих Правил.

5.1.12. При получении от Клиента подтверждения распоряжения, в случаях предусмотренных п.5.1.10 Правил или осуществление Клиентом действий по совершению повторной операции (т.е. операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода, далее - повторная операция) и (или) получения Банком от Клиента информации о том, что перевод денежных средств не является переводом денежных средств без добровольного согласия Клиента, в случаях предусмотренных п.5.1.11 Правил, незамедлительно принять к исполнению подтвержденное распоряжение (поручение) Клиента или совершить повторную операцию, в порядке предусмотренном договором, при отсутствии иных установленных законодательством Российской Федерации оснований не принимать распоряжение Клиента к исполнению.

5.1.13. При неполучении от Клиента подтверждения распоряжения в порядке, предусмотренном настоящим договором, указанное распоряжение считается не принятым к исполнению, а при осуществлении действий по совершению Клиентом повторной операции способом, не предусмотренным договором, повторная операция считается несовершенной.

5.1.14. В случае, если, после получения Банком от Клиента подтверждения распоряжения или осуществление Клиентом действий по совершению повторной операции, Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, Банк обязан:

- приостановить прием к исполнению подтвержденного распоряжения Клиента на два рабочих дня со дня направления Клиентом подтверждения распоряжения или отказать в совершении клиентом повторной операции;
- незамедлительно в порядке, предусмотренном настоящим договором, уведомить клиента о приостановлении приема к исполнению подтвержденного распоряжения клиента или об отказе в совершении клиентом повторной операции с указанием причины такого приостановления (отказа) и срока такого приостановления, а также о возможности совершения клиентом последующей повторной операции.

5.1.15. В случае приостановления приема к исполнению подтвержденного распоряжения Клиента в соответствии с п.5.1.14 настоящих Правил по истечении двух рабочих дней со дня направления Клиентом подтверждения распоряжения в соответствии с п.5.2.11 настоящих Правил Банк обязан незамедлительно принять к исполнению подтвержденное распоряжение клиента при отсутствии иных установленных законодательством Российской Федерации оснований не принимать подтвержденное распоряжение клиента к исполнению.

5.1.16. В случае отказа в совершении Клиентом повторной операции в соответствии с п.5.1.14 настоящих Правил по истечении двух рабочих дней со дня осуществления действий по совершению клиентом повторной операции Банк обязан совершить последующую повторную операцию Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не совершать последующую повторную операцию клиента.

5.1.17. В случае, если Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к клиенту и (или) его электронному средству платежа, Банк вправе приостановить использование клиентом электронного средства платежа на период нахождения сведений, относящихся к такому клиенту и (или) его электронному средству платежа, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.

5.1.18. Банк обязан приостановить использование клиентом электронного средства платежа, если от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к клиенту и (или) его электронному средству платежа, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемые в соответствии с частью 8 статьи 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» на период нахождения указанных сведений в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.

5.1.19. Банк обязуется информировать Клиента о рисках использования системы Интернет-банк и о соблюдении мер информационной безопасности, необходимых для обеспечения безопасности работы в системе Интернет-банк, изложенных в ***Приложение № 2***. Информирование осуществляется в системе Интернет-банк, в подразделениях Банка.

5.2. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА:

5.2.1. Клиент обязуется использовать систему Интернет-банк на технически исправном оборудовании, характеристики которого должны соответствовать требованиям системы Интернет-банк, изложенным на сайте http://www.faktura.ru.

5.2.2. Клиент обязуется заполнять реквизиты ЭД/ПЭД, содержащих в электронной форме распоряжение Клиента на совершение операций по счетам Клиента или иных операций, в соответствии с требованиями законодательства и нормативных актов ЦБ РФ.

5.2.3. Клиент обязуется контролировать доставку ЭД/ПЭД и результаты их обработки. Для этого связь с Банком должна повторяться по прошествии времени, достаточного для обработки Банком пришедших ЭД/ПЭД.

5.2.4. Клиент обязуется ознакомиться и соблюдать меры информационной безопасности «О рисках использования системы Интернет-банк и о соблюдении мер информационной безопасности, необходимых для обеспечения безопасности работы в системе Интернет-банк» ***Приложение № 2***).

5.2.5. Клиент обязуется самостоятельно обеспечивать сохранность информации путем своевременного создания резервных копий.

5.2.6. Клиент признает, что обмен ЭД/ПЭД, осуществляемый с использованием Сервиса «FAKTURA.RU», не является нарушением банковской тайны.

5.2.7. Клиент обязуется предоставить Банку достоверную информацию о номере мобильного телефона и электронном адресе для направления уведомлений Банка об операциях, совершаемых с помощью системы Интернет-банк, а в случае его изменения или утери Мобильного устройства/смены адреса электронной почты незамедлительно предоставить Банку обновленную информацию путем письменного обращения в Банк.

5.2.8. Клиент обязуется для получения sms/push–уведомлений самостоятельно обеспечить на своем Мобильном устройстве поддержку функций приема sms/push–уведомлений, а также подключение Мобильного устройства к любым операторам связи, поддерживающим стандарт GSM, работоспособность Мобильного устройства.

5.2.9. Клиент обязуется для получения e-mail-уведомлений на адрес электронной почты, обеспечить доступ к сети Интернет, а также необходимый размер почтового ящика, указанного Банку электронного адреса, для беспрепятственного получения входящих электронных сообщений.

5.2.10. Клиент обязуется немедленно информировать (по телефону с использованием кодового слова с последующим письменным подтверждением) Банк (телефоны Банка – 8 (3852) 370-230, 8(3852)370-241, 8(3852)370-213) о возникновении угрозы компрометации Ключа электронной подписи/ Логина и Пароля, а также незамедлительно но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции в порядке п.3.8. настоящего Соглашения, уведомить Банк о такой компрометации.

Под компрометацией понимается:

- утрата ключевых носителей Ключа электронной подписи (в том числе, с последующим их обнаружением);
- обнаружение факта использования системы Интернет-банк без добровольного согласия Клиента;
- увольнение сотрудников – Владельцев Сертификата, имевших доступ к Ключам электронной подписи, увольнение сотрудников – Владельцев Логина и Пароля;
- утрата ключей от сейфа, хранилища в момент нахождения в нем ключевых носителей Ключа электронной подписи;
- нарушение конфиденциальности Ключа электронной подписи/ Логина и Пароля, констатация их владельцем обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование Ключа электронной подписи/ Логина и Пароля;
- утеря/передача Мобильного устройства с Зарегистрированным номером неуполномоченным лицам, замена/утеря SIM-карты Зарегистрированного номера;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к Ключу электронной подписи/ Логину и Паролю третьих неуполномоченных лиц.

5.2.11. В случаях, предусмотренных законом или настоящими Правилами, или Договором банковского счета не позднее одного рабочего дня, следующего за днем приостановления Банком приема к исполнению распоряжения, направить в Банк запрашиваемую информацию и (или) подтверждение о приеме к исполнению распоряжения, одним из следующих способов:

- путем отправки ответа по системе Интернет-банк с обязательным подтверждением информации по телефонному звонку представителя Банка о том, что перевод денежных средств не является переводом денежных средств без добровольного согласия клиента;

- либо путем направления письменного уведомления в Банк.

При неполучении от клиента подтверждения распоряжения и (или) информации, запрошенной в соответствии с настоящим пунктом, указанное распоряжение считается не принятым Банком к исполнению, а при осуществлении действий по совершению Клиентом повторной операции способом, не предусмотренным настоящим договором и (или) при неполучении информации, запрошенной Банком, повторная операция считается несовершенной.

5.2.12. При получении от Банка уведомления о приостановлении совершения операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, в срок не позднее одного рабочего дня, следующего за днем приостановления Банком операции (приема к исполнению распоряжения):

- направить в Банк подтверждение в совершении операции (перевода) в порядке, предусмотренном п.5.2.11 настоящих Правил, в случаях, предусмотренных п. 5.1.10 настоящих Правил;

- предоставить Банку информацию о том, что перевод денежных средств не является переводом денежных средств без добровольного согласия, в порядке, предусмотренном п. 5.2.11 настоящих Правил, и совершить повторную операцию в случаях, предусмотренных п.5.1.11 настоящих Правил;

- совершить последующую повторную операцию по истечении двух дней со дня осуществления действий по совершению Клиентом повторной операции в соответствии с настоящим пунктом.

5.2.13. Клиент обязуется оплачивать услуги, предоставленные Банком в рамках настоящего Договора в соответствии с действующими тарифами Банка.

Абонентская плата за месяц, в котором подключена система Интернет-банк, взимается за полный рабочий месяц независимо от даты подключения.

5.2.14. Клиент обязуется в случае досрочного расторжения настоящего Договора оплачивать абонентскую плату за последний месяц в полном объеме независимо от того, сколько дней обслуживался с начала этого месяца.

5.2.15. Клиент имеет право устанавливать ограничения на проведение операций с использованием системы ДБО (ограничение на осуществление операций по переводу денежных средств и/или ограничение операций по переводу денежных средств за календарные сутки по часовому поясу МСК для организаций) посредством предоставления в Банк уполномоченному лицу Банка Заявления на изменение условий использования Системы ДБО ***(Приложение №16).***

Заявление может быть представлено Клиентом в Банк как на бумажном носителе, так и по системе ДБО.

Обработка заявления Банком осуществляется не ранее следующего рабочего дня за днем подачи заявления Клиентом.

6. ПОРЯДОК ВЗАИМОДЕЙСВИЯ БАНКА И КЛИЕНТА В СЛУЧАЕ ЗАМЕНЫ СЕРТИФИКАТА, ЛОГИНА И ПАРОЛЯ

6.1. Замена Сертификата может осуществляться по инициативе одной из сторон, либо в случае компрометации ключа ЭП и проводится в следующем порядке:

- Клиент подает заявление на отмену действия ключей ЭП Клиента (***Приложение № 15***)

- Банк блокирует полученные, но не проведенные электронные документы, заверенные «старой» ЭП Клиента с момента получения соответствующей информации (через телефонный звонок с использованием кодового слова) от Клиента, либо из собственных источников;

- Банк и Клиент проверяют, что все электронные документы (принятые и проведенные, принятые, но не проведенные Банком), за период с момента возникновения необходимости замены Сертификата по момент замены, заверенные «старой» ЭП верны и не вызывают сомнений;

- Клиент подает заявление на выдачу Сертификата ключа проверки электронной подписи (***Приложение № 6***);

- Банк направляет на адрес электронной почты Клиента ссылку для сохранения Сертификата;

- Клиент подписывает акты регистрации (***Приложение № 8*** либо ***Приложение № 9***), акты приема-передачи Сертификата (***Приложение № 10***);

- Банк возобновляет прием электронных документов по системе Интернет-банк.

6.2. Замена Логина и Пароля может осуществляться по инициативе одной из сторон, либо в случае компрометации Логина и Пароля и проводится в следующем порядке:

- Клиент подает заявление на отмену действия Логина и Пароля (***Приложение № 15***);

- Банк блокирует полученные, но не проведенные электронные документы, заверенные «старой» АСП Клиента с момента получения соответствующей информации (через телефонный звонок с использованием кодового слова) от Клиента, либо из собственных источников;

- Банк и Клиент проверяют, что все электронные документы (принятые и проведенные, принятые, но не проведенные Банком), за период с момента возникновения необходимости замены Логина по момент замены, заверенные «старой» АСП верны и не вызывают сомнений;

- Клиент подает заявление на обслуживание по системе Интернет-банк с предоставлением доступа по Логину и Паролю (***Приложение № 11)***;

- Банк направляет на адрес электронной почты Клиента Логин и на номер телефона Клиента первичный Пароль;

- Факт передачи Банком Клиенту Логина оформляется актом приема-передачи Логина (***Приложение № 12***).

- Клиент подписывает акт регистрации (***Приложение № 13*** либо ***Приложение № 14***).

- Банк возобновляет прием электронных документов по системе Интернет-банк.

7. СРОК ДЕЙСТВИЯ ДОГОВОРА

7.1. Настоящий Договор вступает в силу с даты принятия Банком заявления о присоединении к Договору и действует один год.

7.2. Настоящий Договор считается пролонгированным на очередной год, если до истечения срока его действия ни одна из Сторон не уведомила другую о его расторжении. Количество пролонгаций срока действия настоящего Договора не ограничено.

7.3. Банк вправе в одностороннем порядке расторгнуть Договор:

- при расторжении с Клиентом договора банковского счета, не использовании Клиентом услуг, предоставляемых в рамках Договора Дистанционного Банковского Обслуживания в течение 10 (десяти) календарных дней (для Клиентов, с которыми не заключен Договор банковского счета).

- не ранее чем через 10 (десяти) календарных дней после уведомления (в том числе через систему Интернет-банк) Клиента;

- в случае неоплаты Клиентом услуг Банка, предоставленных в текущем месяце, при этом Договор Банком расторгается в последний рабочий день месяца.

7.4. Клиент вправе в любой момент расторгнуть настоящий Договор, уведомив о данном намерении Банк путем подачи в Банк заявления о расторжении Договора.

8. СТОИМОСТЬ УСЛУГИ

8.1. Услуги Банка оплачиваются Клиентом согласно действующим тарифам в Банке до совершения операции.

8.2. Клиент с тарифами Банка, действующими на момент заключения настоящего Договора, ознакомлен и согласен.

8.3. В течение действия Договора Банк в одностороннем порядке может изменять тарифы, исключать или вводить новые платные услуги, размещая информацию для Клиентов на официальном сайте Банка в сети Интернет, в помещении Банка за 10 календарных дней до изменения действующих или введения новых тарифов.

8.4. Услуги Банка оплачиваются Клиентом любыми возможными способами, установленными законодательством РФ, либо оплата за услуги списывается Банком с банковского счета Клиента на основании права, предоставленного договором банковского счета.

9. ОТВЕСТВЕННОСТЬ СТОРОН

9.1. Банк и Клиент несут ответственность за сохранение в тайне своих ключей электронной подписи, Логинов и Паролей, за правильность заполнения и оформления электронных документов, простых электронных документов и за действия своего персонала при работе с системой Интернет-банк в рамках исполнения обязательств по настоящему Договору.

9.2. За невыполнение либо ненадлежащее выполнение своих обязательств по Договору Стороны несут ответственность, предусмотренную законодательством РФ.

9.3. Стороны не несут ответственности за срывы и помехи в работе линий связи, приводящих к невозможности передачи информации.

9.4. Стороны не несут ответственности за прекращение использования системы Интернет-банк, возникшее вследствие действия непреодолимой силы, существенно влияющей на функционирование системы, в виде стихийных бедствий, отключения электроэнергии, повреждения линий связи, общественных явлений, а также решений органов власти, обязательных для исполнения.

9.5. Банк не несёт ответственности за ущерб, возникший вследствие неправильного оформления Клиентом ЭД, ПЭД, за срывы и помехи в работе используемой Клиентом линии связи, приводящих к невозможности направления в Банк документов, в случае воздействия на программно-аппаратные комплексы Клиента вредоносных программ, неправомерный доступ третьих лиц к программно-аппаратным комплексам/Мобильному устройству и/или Ключам электронной подписи Клиента.

9.6. Банк не несет ответственности за исполнение распоряжений Клиента, в случае, если полномочия уполномоченного лица Клиента, уполномоченного распоряжаться денежными средствами с использованием ЭП/АСП, были прекращены либо изменены по каким-либо основаниям, но Банк не был об этом своевременно извещен.

9.7. Банк не несёт ответственность в случаях финансовых потерь, понесенных Клиентом в связи с нарушением и (или) ненадлежащим исполнением им требований по защите от вредоносного кода рабочего места, с которого осуществляется вход в систему Интернет-банк, Мобильного устройства.

9.8. Банк не несет ответственности за несвоевременное получение или неполучение Клиентом уведомлений по факту совершения операций с использованием системы Интернет-банк по причинам, находящимся вне сферы контроля Банка, в частности:

- за отсутствие доступа к сети Интернет вследствие ненадлежащих действий Клиента (отключение связи Интернет, ненадлежащей связи Интернет и т.д.), сбои в работе сетей, обеспечивающих связь Интернет, и т.п.;
- за неполучение Клиентом sms-сообщений по вине оператора сотовой связи, а также вследствие ненадлежащих действий Клиента (отключение от услуг «sms» у соответствующего оператора сотовой связи, отключение Мобильного устройства или нахождение его вне зоны покрытия/ в роуминге, при блокировке номера телефона мобильной связи, утрате Мобильного устройства и/или SIM карты, возникновении технических проблем с Мобильным устройством);

- в случае непредставления Клиентом достоверной информации для связи с Клиентом, а в случае ее изменения, непредставления обновленной информации о номере телефона Мобильной связи, электронного почтового адреса Клиента.

9.9. Банк не несет ответственности за достоверность сведений (в т.ч. номера телефона мобильной связи, электронного почтового адреса), представленных Клиентом.

9.10. Банк не несет ответственности за использование ключа электронной подписи, а также Логина и пароля уполномоченного лица Клиента неуполномоченными лицами, а также за

любые убытки Клиента, третьих лиц, связанные с использованием ключей электронной подписи, Логина и пароля и не связанные с нарушением Банком своих обязательств.

9.11. Банк не несет ответственность за сохранность программного обеспечения и архивов электронных документов, размещаемых на оборудовании Клиента.

9.12. Ответственность Банка за виновное неисполнение (ненадлежащее исполнение) своих обязательств по настоящему Договору, повлекшее возникновение убытков у Клиента, ограничена суммой не более 50 000 рублей.

10. ИНЫЕ УСЛОВИЯ

10.1. Все споры, возникающие по исполнению настоящего Договора ДБО, решаются сторонами путем переговоров и в случае необходимости с привлечением оператора Сервиса «FAKTURA.RU.

10.2. В случае возникновения спорной ситуации, не описанной в настоящем Договоре и связанной с работой системы Интернет-банк, повлекшей за собой потерю электронного документа или вызывающей сомнения в подлинности электронного документа, стороны образуют экспертную комиссию для рассмотрения создавшейся ситуации с использованием процедуры подтверждения достоверности документов, предусмотренной Правилами Сервиса «FAKTURA.RU».

10.3. При несогласии одной из сторон с решением экспертной комиссии, спор передается на рассмотрение в Арбитражный суд Алтайского края. Выводы экспертной комиссии имеют доказательное значение при рассмотрении дела в суде.

10.4. Все изменения к настоящему Договору размещаются на сайте Банка www.sibsoc.ru.

10.5. Во всем, что не урегулировано условиями настоящего Договора, стороны руководствуются:

- Правилами электронного документооборота корпоративной информационной системы «BeSafe», которые расположены в Интернете по адресу www.besafe.ru.
- Правилами Сервиса «FAKTURA.RU», которые расположены в Интернете по адресу https://cft.group/contracts.
- Правилами работы Удостоверяющего Центра (AUTHORITY), которые расположены в Интернете по адресу www.authority.ru.
- Инструкцией по созданию Ключа ЭП, инструкцией по подключению Интернет-банка технология Логин Пароль, инструкцией по обновлению Сертификата ЭП, размещенных на сайте Банка по адресу www.sibsoc.ru.

Приложение №1

ЗАЯВЛЕНИЕ
о присоединении к Договору Дистанционного Банковского Обслуживания

« » _____20__

_____
(Наименование Клиента)
в лице _____
(должность, Ф.И.О. уполномоченного лица Клиента)
действующего (ей) на основании _____
(наименование документа, подтверждающего полномочия лица, подписавшего заявление)
именуемый в дальнейшем «Клиент», настоящим в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью присоединяюсь к Договору Дистанционного Банковского Обслуживания, условия которого мне известны и имеют обязательную юридическую силу.

Клиент, заключая настоящий Договор, обязуется соблюдать меры информационной безопасности, необходимые для обеспечения безопасной работы в системе Интернет-банк (Приложение № 2).

Клиент, заключая настоящий Договор, дает согласие «СИБСОЦБАНК» ООО, ЗАО «Биллинговый центр» (ИНН 5401152049) на осуществление записи телефонного разговора с Клиентом и ее хранение.

Настоящим Клиент подтверждает, что ознакомился с Тарифами (www.sibsoc.ru) и Договором (www.sibsoc.ru), Правилами электронного документооборота корпоративной информационной системы «BeSafe» (www.BeSafe.ru), Правилами работы Сервиса «FAKTURA.RU» (www.faktura.ru), Правилами работы Удостоверяющего Центра «AUTHORITY» (www.authority.ru.). Понимает текст данных документов, выражает свое согласие с ним и обязуется их выполнять.

_____ / _____
(подпись) (должность, ФИО)

М.П.

Отметка Банка о приеме:

«____»_____202__г.

_____ / _____
(подпись) (должность, ФИО)

М.П.

Приложение № 2

О рисках использования системы Интернет-банк и о соблюдении мер информационной безопасности, необходимых для обеспечения безопасной работы в системе Интернет-банк

Основным риском при использовании системы Интернет-банк является риск получения злоумышленником несанкционированного доступа к управлению счетом Клиента и к документам Клиента, передаваемым в Банк через систему Интернет-банк. Последствиями несанкционированного доступа могут быть списание денежных средств со счета Клиента или утечка конфиденциальной информации о совершаемых Клиентом операциях.

Способы несанкционированного доступа к системе Интернет-банк

Основными способами получения несанкционированного доступа к системе Интернет-банк являются:

– перехват злоумышленником управления компьютером клиента;

– кража Логина и Пароля Клиента для входа в систему Интернет-банк, а также закрытой части ключа электронной подписи Клиента;

– перехват данных, передаваемых Клиентом в Банк и получаемых Клиентом из Банка.

Получение несанкционированного доступа может быть осуществлено:

– штатными сотрудниками организации Клиента;

– нештатными сотрудниками, приходящими по вызову для обслуживания компьютеров организации Клиента;

– злоумышленниками, получившими доступ к компьютерам организации Клиента через сеть Интернет или иные каналы связи;

- в результате утраты (потри, хищения) устройства, с использованием которого клиентом осуществляются действия в целях осуществления банковских операций.

Признаки несанкционированного использования клиентского рабочего места системы Интернет-банк:

– наличие в системе нелегитимного платёжного поручения (платёжное поручение сформировано злоумышленником);

– наличие в системе не заказанных выписок, или иных документов (документы заказаны злоумышленником);

– «самостоятельная» (независимая от действий пользователя) работа компьютера: перемещение курсора, открытие и закрытие окон программ, заполнение форм и документов и пр. (управление компьютером захвачено злоумышленником);

– отсутствие доступа к системе Интернет-банк по причине неверного пароля (пароль изменен злоумышленником);

– нестабильная работа компьютера или полная его неработоспособность (последствия деятельности злоумышленника по уничтожению следов вторжения);

– не работает ключевой носитель (возможные последствия деятельности злоумышленника).

Данный перечень признаков несанкционированного использования системы Интернет-банк не является исчерпывающим. В зависимости от новых видов атак список может дополняться и корректироваться.

Компрометация закрытой части ключа электронной подписи (ключевого носителя).

К событиям, на основании которых принимается решение о компрометации, относятся, включая, но, не ограничиваясь, следующие события:

– потеря ключевых носителей (даже с их последующим обнаружением);

– увольнение сотрудников, имевших доступ к ключевым носителям;

– нарушение печати на сейфе с ключевыми носителями;

– 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 несанкционированных действий злоумышленника);

- заражение компьютера вредоносным программным обеспечением.

Меры, необходимые для обеспечения безопасной работы в системе Интернет-банк

Клиенту, в целях снижения возможного риска несанкционированного использования рабочего места системы Интернет-банк и списания третьими лицами денежных средств со счета Клиента, необходимо выполнять следующие меры информационной безопасности:

1.Меры сетевой безопасности:

1.1. На компьютере должна быть установлена парольная защита на вход в BIOS и в операционную систему. Рекомендуется использовать в качестве пароля комбинацию знаков, смысл и последовательности которых трудно определить. При использовании смартфона или планшета необходимо настроить блокировку экрана способом, исключающих доступ к нему посторонних (PIN-код, графический ключ, отпечаток пальца и т.п.).

1.2. Перед установкой системы Интернет-банк на устройство, используемое для осуществления операций, необходимо проверить его на отсутствие вредоносного программного обеспечения и программ удаленного доступа (BeTwin, RAdmin и др.). Использование подобных программ несет большие риски, решение об их использовании организация принимает на свой страх и риск.

1.3. Не привлекать для администрирования и обслуживания компьютера, планшета, смартфона сотрудников посредством предоставления удаленного доступа.

1.4. Если компьютер установлен внутри локальной сети организации, провести мероприятия по защите локальной сети от зловредных воздействий со стороны сети Интернет. При выходе в Интернет рекомендуется использовать сетевые экраны, разрешив доступ только к доверенным ресурсам сети.

1.5. Включите систему фильтрации ложных web-узлов (антифишинг) в своем браузере либо в антивирусном программном обеспечении, если браузер ее не имеет —обновите браузер.

1.6. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам. Наилучшей практикой является отказ от использования электронной почты на устройствах с установленными рабочими местами системы Интернет-банк.

1.7. При вводе личной информации, ПОМНИТЕ, что любой веб-адрес в адресной строке Интернет- банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить конфиденциальные данные нельзя.

Удостоверьтесь, что адрес сайта введён правильно и вы не зашли на мошеннический сайт с похожим адресом. Например, вместо окончания «ru» злоумышленник может зарегистрировать ложный сайт «faktura.ру» или вместо «faktura.ru» сделать ложный сайт «factura.ru» и узнать ваш пароль, для доступа к системе «Интернет-банк», когда он будет там введён.

1.8. Не давайте разрешения неизвестным программам выходить в интернет.

1.9. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.

1.10. Не используйте компьютер, планшет, смартфон, на котором установлено рабочее место системы Интернет-банк, не по назначению, например, для игр, просмотра фильмов и т.п.

1.11. Для повышения степени безопасности эксплуатации системы Интернет-банк можно сообщить в Банк список доверенных IP-адресов, с которых возможен вход в систему. Возможность входа в систему с IP-адресов, не входящих в список доверенных в этом случае будут полностью исключены.

2. Меры по защите от вредоносного программного обеспечения:

2.1. Установить на компьютере, планшете, смартфоне антивирусное программное обеспечение. Обновление баз данных антивирусного программного обеспечения должно осуществляться ежедневно, либо по мере выхода новых официальных версий баз данных.

2.2. Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки устройства. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов.

2.3. Должны быть установлены последние пакеты обновлений (Service Packs), актуальные патчи безопасности, критичных обновлений операционной системы и браузеров, обновление которых должно проводиться регулярно.

2.4. Необходимо своевременно обновлять, используемое для работы с системой Интернет-банк программное обеспечение. Установку обновлений необходимо производить только с официальных сайтов разработчиков соответствующего программного обеспечения.

2.5. В операционной системе должна быть отключена функция AutoRun.

2.6. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.

2.7. Необходимо исключить установку на компьютер, планшет, смартфон нелицензионного и полученного из не заслуживающих доверия источников программного обеспечения.

2.8. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки.

2.9. Контролируйте конфигурацию устройства, чтобы вовремя обнаружить его несанкционированное использование или изменения. Например, появление в списке нового программного обеспечения, которое было установлено без вашего ведома.

3. Меры, направленные на защиту от копирования (хищения) ключевой и парольной информации:

3.1. Храните носители ключей (смарт-карты, дискеты, флэш-карты и другие носители с записанными ключами) в месте, недоступном посторонним лицам (сейфе и т.д.). Исключите хранение ключей на жестком диске, в сетевых каталогах и прочих общедоступных ресурсах.

3.2. Храните в тайне пароль доступа к ключу, а также Логин и Пароль для доступа в систему Интернет-банк, исключите их запись на стикерах, носителях ключей и т.п.

3.3. Не передавайте ключи электронной подписи и не сообщайте Логин и Пароль доступа к системе Интернет-банк кому-либо.

3.4. Извлекайте ключевой носитель сразу после окончания сеанса работы с системой Интернет-банк.

3.5. Юридические лица во всех случаях увольнения или смены лиц, допущенных к ключам электронной подписи, Логину и Паролю, а также руководителей юридического лица, которые подписывали доверенности о допуске пользователей к ключам электронной подписи, логинам и паролям, должны заменить карточку с образцами подписей и оттиска печати, ключи электронной подписи, Логин и Пароль.

3.6. Минимизируйте количество пользователей, которые имеют право доступа к компьютеру, планшету, смартфону с установленным рабочим местом системы Интернет-банк, ограничив его кругом лиц, непосредственно использующих систему Интернет-банк.

3.7. Не используйте функцию автозаполнения (пароль пользователя, имя пользователя, пароль на токен и др.) это предотвратит использование данных сторонними лицами.

3.8. Сотрудники Банка никогда не запрашивают по телефону, электронной почте или через SMS сообщения никакой конфиденциальной информации (ключи, пароли и пр.)! Не выполняйте никаких рекомендаций, особенно связанных с вводом каких-либо данных на любых страницах, открытых вашим браузером. Работники банка не обращаются к Клиентам по телефону с предложениями попытаться войти в систему еще раз или ввести еще один код подтверждения, не пытаются узнать у Клиентов пароли или код подтверждения. Ни при каких обстоятельствах не сообщать данную информацию!

4. Меры по контролю несанкционированных списаний:

4.1. Необходимо контролировать доставку пакета электронных документов и результаты его обработки. Для этого связь с Банком должна повторяться по прошествии времени, достаточного для обработки Банком пришедших пакетов документов.

4.2. Следует регулярно контролировать состояние своих счетов и незамедлительно информировать обслуживающее подразделение Банка обо всех подозрительных или несанкционированных операциях, но не позднее дня, следующего за днём получения от Банка уведомления о совершённой операции, об их использовании без добровольного согласия Клиента.

4.3. В случае неожиданного выхода из строя компьютера (планшета, смартфона), либо пропадания на нём программного обеспечения системы Интернет-банк, необходимо прекратить работу на нём, отключив его от всех видов сетей, включая локальную корпоративную сеть, и модемов, срочно запросить в Банке выписку по счету. При обнаружении несанкционированных платежных операций написать заявление в Банк, а также обратиться с соответствующим заявлением в правоохранительные органы. устройства не восстанавливайте до проведения технической экспертизы.

4.4. В случае обнаружения несанкционированного доступа к компьютеру с установленным рабочим местом системы Интернет-банк, подозрительных операций, установлении фактов компрометации закрытой части ключа электронной подписи, утрате (потери, хищения) устройства, применяемого для осуществления банковских операций:

- срочно связаться с Банком и проинформировать об имеющихся подозрениях или фактах;
- проверить легитимность всех выполненных за последнее время платежей;
- направить в Банк заявление о блокировке операций в системе Интернет-банк;
- произвести смену ключей электронной подписи.

4.5. Необходимо выполнять незамедлительную блокировку и смену ключей электронной подписи, паролей для доступа в случаях их компрометации, а также по истечении срока действия ключей с периодичностью, установленной договорами и документацией.

4.6. Необходимо заменять ключи электронной подписи, Логины и Пароли во всех случаях увольнения или смены руководителей Клиента, подписывавших распоряжения (доверенности) о предоставлении сотрудникам Клиента, полномочий подписания электронной подписью, аналогом собственноручной подписи электронных документов.

4.7. Подключите sms-информирование, чтобы оперативно узнать о несанкционированном переводе и своевременно сообщить о мошеннической операции (компрометации ключа электронной подписи или Логина и Пароля). Используйте разные устройства для работы в Интернет-банке и получения уведомлений о совершённых операциях. Например, если доступ в систему Интернет-банк осуществляется с планшета и на него же придёт SMS о переводе, то в случае заражения его вредоносным программным обеспечением SMS-сообщение может быть удалено и вы о переводе не узнаете.

5. Меры по поддержанию уровня информационной безопасности:

5.1. Для обеспечения высокого уровня информационной безопасности при эксплуатации системы Интернет-банк у Клиента должен быть назначен ответственный, который осуществляет:

- постоянный контроль соблюдения мер информационной безопасности, предусмотренных настоящей памяткой, документацией на систему и средства защиты;
- выявление, устранение и информирование руководства Клиента обо всех выявленных нарушениях;
- контроль над устранением выявленных нарушений;
- документирование результатов проведенных работ и проверок.

Для работы с ПРОСТОЙ ЭП / АСП:

1. Запомните, что для входа в Интернет-банк вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона, номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в Интернет-банке.
2. Никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в Интернет- банк или для подтверждения платежей, а также номера ваших карт и CVV2/CVC2 коды.
3. Обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS указан пароль для платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему счету платеж, ни в коем случае не вводите его в Интернет-банке и не называйте его, в том числе сотрудникам банка.
4. В случае утери мобильного телефона, на который приходят разовые пароли, немедленно заблокируйте SIM-карту / войдите в Интернет-банк и удалите телефон из списка зарегистрированных устройств для получения PUSH-сообщений.
5. Запишите контактный телефон вашего банка в адресную книгу или запомните его. В случае если в личном кабинете Интернет-банка вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в банк по ранее записанному вами телефону. Также для этих целей подойдет телефон, указанный на вашей банковской карте.
6. Устанавливайте мобильные приложения Faktura.ru только из авторизованных магазинов приложений App Store и Google Play. Используйте антивирусное программное обеспечение, в случае, если оно доступно для вашего телефона/смартфона.
7. Избегайте регистрации номера вашего мобильного телефона, на который приходят SMScообщения с разовым паролем, в социальных сетях и других открытых источниках.

Приложение № 3

ЗАЯВЛЕНИЕ НА ПОДКЛЮЧЕНИЕ УВЕДОМЛЕНИЙ
(при предоставлении доступа по ключу электронной подписи)

_____
(Наименование Клиента)

1.	В рамках Договора Дистанционного Банковского Обслуживания в системе Интернет-банк просим осуществлять уведомления по следующему номеру телефона/ адресу электронной почты сотрудника: Внимание! Указываются только уполномоченные лица Клиента, имеющие право электронной подписи документов

1) ФИО уполномоченного лица Клиента	Зарегистрированный номер мобильного телефона	Электронная почта (e-mail)
	+7__ __ __ __ __ __ __ __ __ __	

Отметить нужное:

☐ Уведомлять о входе в систему Интернет-банк; ☐ Уведомлять об отправке платежей;
☐ Уведомлять об исполнении платежей;
Отказ от подтверждения входа в Систему Интернет-банк одноразовыми паролями повлечет снижение уровня безопасности при работе с системой Интернет-банк, что может привести к реализации мошеннических действий в отношении Клиента.

2) ФИО уполномоченного лица Клиента	Зарегистрированный номер мобильного телефона	Электронная почта (e-mail)
	+7__ __ __ __ __ __ __ __ __ __	

Отметить нужное:

☐ Уведомлять о входе в систему Интернет-банк; ☐ Уведомлять об отправке платежей;
☐ Уведомлять об исполнении платежей;
Отказ от подтверждения входа в Систему Интернет-банк одноразовыми паролями повлечет снижение уровня безопасности при работе с системой Интернет-банк, что может привести к реализации мошеннических действий в отношении Клиента.

2.	Руководитель Клиента

Обязуюсь своевременно сообщать Банку об изменении номера сотового телефона для получения sms-уведомлений, об изменении адреса электронной почты (e-mail).

Разрешаю Банку в одностороннем порядке принимать дополнительные меры обеспечения безопасности и надлежащего обслуживания в системе Интернет-банк. С Тарифами за предоставление услуги ознакомлен и согласен.

Признаю, что получение уведомлений от Банка посредством sms/ e-mail/push -уведомлений не является нарушением банковской тайны.

Признаю, что Банк не несет ответственность за несвоевременную доставку sms/push -уведомлений оператором сотовой связи, e-mail –уведомлений.

Дата подачи заявления «____» _____ г.
ФИО:_____ / _____
(уполномоченное лицо Клиента)

м.п.

Отметка Банка о приеме:
«____»_____202__г.
_____ / _____
(подпись) (должность, ФИО)

М.П.

Приложение № 4

Заявление на обслуживание по системе Интернет-банк
с предоставление доступа по ключу электронной подписи

_____
(Наименование Клиента)

в лице _____
(должность, Ф.И.О. уполномоченного лица Клиента)

действующего (ей) на основании _____
(наименование документа, подтверждающего полномочия лица, подписавшего заявление)

поручает Банку произвести:

1. Подключение к системе дистанционного банковского обслуживания Интернет-банк и осуществлять облуживание следующих банковских счетов:

Дата договора банковского счета	Номер договора банковского счета	Номер расчетного счета

2. Предоставить доступ к системе Интернет-банк с выдачей смарт-карты (USB-ключа/ключевого носителя), произвести регистрацию Клиента, Сертификата ключа проверки электронной подписи следующему лицу[1]:

Уполномоченное лицо Клиента	должность, Ф.И.О. уполномоченного лица Клиента
Документ, удостоверяющий личность:	Вид, серия, номер, орган, выдавший документ, удостоверяющий личность, дата выдачи
Электронная почта (E-mail):	
Право доступа, вид подписи:	**С правом подписи**: ☐ единоличная подпись, ☐ первая подпись (одновременно со второй подписью)*, ☐ вторая подпись (одновременно с первой подписью)* **Без права подписи** ☐ (просмотр движения денежных средств по счету, ☐ запрос выписки по счету, ☐ создание Распоряжений, ☐просмотр информации), ☐ другое (указать конкретный вид ограниченного доступа)_____ **Иное:_____**
☐ **Подключить услугу «Альтернативный фактор подтверждения F. Business»**	**Номер мобильного телефона для отправки sms-сообщений** +7__ __ __ __ __ __ __ __ __ __

*Заполняется при предоставлении доступа Владельцу Сертификата ключа проверки электронной подписи в случае наличия в карточке с образцами подписей и оттиска печати более одной подписи.

Клиент обязуется немедленно информировать (по телефону с использованием кодового слова_____с последующим письменным подтверждением) Банк (телефоны Банка – 8 (3852) 370-230, 8(3852)370-241, 8(3852)370-213) о возникновении угрозы несанкционированного доступа к ключам электронной подписи уполномоченного лица Клиента (в том числе утраты), а также незамедлительно, но не позднее дня, следующего за днём получения от Банка уведомления о совершённой операции, об их использовании без добровольного согласия Клиента.

_____ _____
(подпись) (должность, ФИО)

«___»_____202__г. М.П.

[1] Указанные данные принимаются Банком в качестве сведений о контактных лицах Клиента и используются для связи с Клиентом в случае выявления операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента в соответствии с положениями Федерального закона Российской Федерации №161-ФЗ от 27.06.2011 г. «О национальной платежной системе».

Клиент обязуется в течение срока действия настоящего Договора незамедлительно информировать Банк об изменении указанных в настоящем Заявлении реквизитов/сведений, в том числе о прекращении либо изменении объема полномочий представителей Клиента, указанных в настоящем Заявлении.

Приложение № 5

Согласие на обработку Персональных данных

Настоящим я, _____
(ФИО собственноручно)
паспорт: серия_____ номер_____ дата выдачи _____
кем выдан _____
адрес регистрации_____
являющийся (аяся) также _____
(наименование единоличного исполнительного органа/представителя)
_____ (далее — Клиент),
(наименование общества/ИП/КФХ) (ИНН)
действующий(ая) на основании _____
(наименование документа: устав/доверенность, а также реквизиты документа)

с целью получения услуг дистанционного банковского обслуживания, регистрации/аккредитации Клиента и осуществления иных действий, предусмотренных Правилами работы сервиса «FAKTURA.RU» (https://faktura.ru) и Правилами сервиса КИС «BeSafe» (https://besafe.ru/), **ДАЮ СОГЛАСИЕ** «СИБСОЦБАНК» ООО (ИНН 2224009042, юридический адрес: 656049, Алтайский край, г. Барнаул, пр-кт Ленина, д.61а) (далее - Банк) на обработку, передачу и поручение обработки (включая запись, систематизацию, накопление, хранение, блокирование, извлечение, обезличивание, уничтожение и предоставление) оператору сервиса КИС «BeSafe» ЗАО «ЦЦС» (ИНН 5407187087, адрес: 630055, г.Новосибирск, ул. Мусы Джалиля, д.11), оператору сервиса «FAKTURA.RU» ЗАО «Биллинговый центр» (ИНН 5401152049, адрес: 630055, г.Новосибирск, ул. Мусы Джалиля, д.11) и его технологическим партнерам, перечисленным в Правилах сервиса «Faktura.ru» , моих персональных данных и иных сведений, определенных следующим перечнем:
- ФИО;
- ИНН;
- данные основного документа, удостоверяющего личность;
- адрес регистрации;
- контактные данные (адрес, телефон, адрес электронной почты);
- информация о Компании (занимаемая должность, сведения из ЕГРЮЛ/ЕГРИП).

Согласие действует в течении срока действия Договора ДБО Клиента с Банком. По истечению указанного срока персональные данные подлежат уничтожению или обезличиванию, если иное не предусмотрено законодательством РФ. Банк принимает меры по обеспечению уничтожения персональных данных, предусмотренные правилами работы сервиса «FAKTURA.RU» (https://faktura.ru). Обработка персональных данных регулируется между Клиентом и сервисами ЗАО «ЦЦС» в соответствии с Правилами УЦ «Authority» и/или Правилами КИС «BeSafe» (https://besafe.ru/).
Согласие может быть отозвано путём направления письменного заявления в Банк. В этом случае Банк прекращает обработку моих персональных данных, а персональные данные подлежат уничтожению, если отсутствуют иные правовые основания для обработки, установленные законодательством РФ. Заявление может быть оформлено в письменном виде при личном посещении Банка, либо может быть отправлено почтой по адресу: 656049, г. Барнаул, Алтайский край, пр-кт Ленина, д.61а, «СИБСОЦБАНК» ООО. Заявление, вне зависимости от формы подачи, должно содержать обязательную информацию, предусмотренную действующим законодательством.

«___» _____ 20___ г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 6

Агенту Удостоверяющего центра "AUTHORITY"
"КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ
СОЦИАЛЬНЫЙ БАНК"
ОБЩЕСТВО С ОГРАНИЧЕННОЙ
ОТВЕТСТВЕННОСТЬЮ

Заявление на выдачу Сертификата ключа проверки электронной подписи

Прошу Удостоверяющий центр "AUTHORITY" создать и выдать уполномоченному лицу организации _____ (наименование организации), действующ(-ему)(-ей) на основании_____, Сертификат ключа проверки электронной подписи (Класс 2 Сертификата) с параметром Идентификатора владельца Сертификата: _____ (ФИО \ псевдоним уполномоченного лица организации/ наименование\ псевдоним организации).
Уникальный номер запроса: _____.

С Правилами Электронного документооборота корпоративной информационной Системы "BeSafe" (далее - Система "BeSafe"), которые размещены в сети Интернет на сайте www.besafe.ru ознакомлены, согласны и обязуемся соблюдать и выполнять.

Признаем, что получение документа, подписанного Электронной подписью Участника Системы "BeSafe" (далее - "Участник") юридически эквивалентно получению документа на бумажном носителе, подписанного собственноручными подписями уполномоченных лиц Участника и заверенного печатью Участника, если документ на бумажном носителе должен быть заверен печатью. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки электронной подписи Участника созданы и используются в соответствии с Правилами работы Удостоверяющего центра "AUTHORITY".

Реквизиты Клиента:

ФИО уполномоченного лица организации	
Наименование организации	
Контактный номер телефона	
E-mail	

Настоящим соглашаюсь с обработкой своих персональных данных, в том числе с использованием технических средств, Закрытым акционерным обществом «Центр Цифровых сертификатов», а также Агентом (Доверенным лицом) Удостоверяющего центра «AUTHORITY».

Признаю, что мои персональные данные, включенные в Сертификат, будут внесены Удостоверяющим центром в реестр Сертификатов. Реестр Сертификатов доступен в сети Интернет на сайте www.authority.ru.

Понимаю, что Удостоверяющий центр обрабатывает мои персональные данные, включенные в Сертификат и размещенные в реестре Сертификатов, для выполнения обязанностей по ведению реестра Сертификатов, включению содержащихся в Сертификатах персональных данных в реестр Сертификатов и обеспечению доступа лиц к информации, содержащейся в реестре Сертификатов с использованием сети Интернет, которые возложены на Удостоверяющий центр частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Понимаю, что в соответствии с пунктом 2 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» выполнение Удостоверяющим центром обязанностей, возложенных на него частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», является правовым основанием обработки моих персональных данных, включенных в Сертификат.

_____ _____
(подпись уполномоченного лица организации) (ФИО уполномоченного лица организации)

М.П.

принято Агентом Удостоверяющего центра:
«КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ
СОЦИАЛЬНЫЙ БАНК»
ОБЩЕСТВО С ОГРАНИЧЕННОЙ
ОТВЕТСТВЕННОСТЬЮ
«____» _____ 20__ г.

_____
(подпись уполномоченного лица)

_____
(ФИО уполномоченного лица)

Приложение № 7

Акт приема-передачи

г. Барнаул «___»_____20___г.

_____,
(Ф.И.О.)

работник _____
(Наименование Клиента)

действующий (ая) на основании _____,
именуемый (ая) в дальнейшем **«Клиент»**, с одной стороны, и **«КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ**, именуемое в дальнейшем «**Банк»** в лице _____, действующей (его) на основании _____ _____от «____»_____20__г., с другой стороны, далее именуемые **«Стороны»,** составили настоящий акт о нижеследующем:

1. С целью подключения (продолжения работы) к системе Интернет-банк Банк передал, а Клиент принял смарт-карту серийный номер _____ .
2. Обязательства Банка перед Клиентом выполнены в полном объеме, претензий у клиента не имеется.

БАНК:
«СИБСОЦБАНК» ООО
Адрес_____
реквизиты _____
_____
_____
ИНН_____
тел/факс _____
e-mail: info@sibsoc.ru

_____
(должность, подпись, ФИО)

КЛИЕНТ:
_____
Адрес_____
_____
_____
тел/факс _____
ИНН_____

_____
(должность, подпись, ФИО)

Подтвердил полномочия работника Клиента: М.П.

_____
(должность, подпись, ФИО)

М.П.

Приложение № 8

Акт регистрации

_____ «___» _____ 20___г.

_____
(Наименование Клиента)

далее именуемое Клиент, в лице _____

_____
(должность, Ф.И.О. уполномоченного лица Клиента)

действующего на основании _____
(наименование документа, подтверждающего полномочия лица подписавшего акт)

и «КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ (далее - Банк) в лице _____, действующего(ей) на основании_____, совместно именуемые Стороны, действуя в рамках Договора ДБО, составили настоящий акт о нижеследующем:

1. Банк осуществил регистрацию Клиента, уполномоченного лица Клиента и его Сертификат ключа проверки электронной подписи в Сервисе «FAKTURA.RU»:

Клиент	
Уполномоченное лицо Клиента	
Контакты (тел., факс, e-mail)	
Эмитент Сертификата	
Владелец Сертификата	

2. Клиент признаёт юридическую силу всех электронных документов, направленных Клиентом с использованием Сервиса «FAKTURA.RU» и подписанных уполномоченным лицом Клиента – владельцем Сертификата ключа проверки электронной подписи.
3. Стороны признают, что электронные документы, подписанные уполномоченным лицом Клиента – владельцем Сертификата ключа проверки электронной подписи, юридически равнозначны документам на бумажном носителе, заверенным собственноручными подписями и оттиском печати Клиента из «Карточки с образцами подписей и оттиска печати».

Подписи сторон:

от Клиента

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

от Банка

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

Приложение № 9

Акт регистрации

_____ «___» _____ 20___г.

_____
(Наименование Клиента)

далее именуемое Клиент, в лице _____
_____
(должность, Ф.И.О. уполномоченного лица Клиента)

действующего на основании _____
(наименование документа, подтверждающего полномочия лица подписавшего акт)

и «КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ (далее - Банк) в лице _____, действующего(ей) на основании_____, совместно именуемые Стороны, действуя в рамках Договора ДБО, составили настоящий акт о нижеследующем:

1. Банк осуществил регистрацию Клиента, уполномоченного лица Клиента и его Сертификат ключа проверки электронной подписи в Сервисе «FAKTURA.RU»:

Клиент	
Уполномоченное лицо Клиента	
Контакты (тел., факс, e-mail)	
Эмитент Сертификата	
Владелец Сертификата	

2. Клиент признает, что предоставил уполномоченному лицу Клиента право доступа к

	да/нет
Просмотру движения денежных средств по счету	
Запросу выписки по счету	
Созданию Распоряжений	
Просмотр информации	
Другое (указать конкретный вид ограниченного доступа)	

получаемых с использованием Сервиса «FAKTURA.RU», а передача указанных сведений с использованием Сервиса «FAKTURA.RU» уполномоченному лицу Клиента не является нарушением банковской тайны.

Подписи сторон:

от Клиента

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

от Банка

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

Приложение № 10

Акт приема—передачи Сертификата ключа проверки электронной подписи

г. Барнаул «____» _____ 20___г.

Юридическое лицо <наименование организации, на имя которой создан и выдан Сертификат>, именуемое в дальнейшем “Клиент”, представленное своим уполномоченным лицом <ФИО уполномоченного лица, оформившего Заявление на выдачу сертификата>, действующим от имени организации на основании _____, с одной стороны, и «КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ, именуемое в дальнейшем «Агент», в лице <должность и ФИО администратора ключей либо иного уполномоченного сотрудника Агента>, действующ (его) (-ей) на основании <документ>, с другой стороны, в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY» составили настоящий Акт приема - передачи о следующем.

1. Агент произвел идентификацию Клиента при личном присутствии (за исключением случаев идентификации клиента самим Удостоверяющим центром с использованием ПЭП ЕСИА), проверку данных Клиента и полномочий уполномоченного лица Клиента, Удостоверяющий центр осуществил создание Сертификата ключа проверки электронной подписи (далее – «Сертификат») и передал ДД.ММ.ГГГГ Сертификат Клиенту, а Клиент принял оригинал следующего Сертификата на Ключевой носитель:

Идентификатор Владельца сертификата

Номер Сертификата:

Алгоритм подписи

Заверен

Годен с

Годен до

Алгоритм Ключа проверки электронной подписи

Ключ проверки электронной подписи

Алгоритм отпечатка

Отпечаток

2. Обязательства Агента и Удостоверяющего центра перед Клиентом выполнены в точном соответствии с Правилами работы Удостоверяющего центра «AUTHORITY», претензий у Клиента не имеется.

Агент:
«СИБСОЦБАНК» ООО
Адрес_____
Реквизиты_____
_____
ИНН _____
тел/факс _____
e-mail: info@sibsoc.ru

_____
(подпись) (ФИО)

_____
(Дата подписи)

М.П.

Клиент:
Наименование _____
Адрес _____
тел/факс _____
ИНН _____

_____
(подпись) (ФИО)

_____
(Дата подписи)

М.П.

Приложение № 11

Заявление на обслуживание по системе Интернет-банк
с предоставление доступа по Логину и Паролю

_____
(Наименование Клиента)

в лице _____
(должность, Ф.И.О. уполномоченного лица Клиента)

действующего (ей) на основании _____
(наименование документа, подтверждающего полномочия лица подписавшего документы)

поручает Банку произвести:

1. Подключение к системе дистанционного банковского обслуживания Интернет-банк и осуществлять облуживание следующих банковских счетов:

Дата договора банковского счета	Номер договора банковского счета	Номер расчетного счета

2. Предоставить доступ к системе Интернет-банк с выдачей Логина и Пароля (без выдачи смарт-карты) следующему лицу[1]:

Владелец Логина и Пароля, должность	ФИО, должность
Документ, удостоверяющий личность:	Вид, серия, номер, орган, выдавший документ, удостоверяющий личность, дата выдачи
Зарегистрированный номер мобильного телефона	+7_ _ _ _ _ _ _ _ _ _
Электронная почта (E-mail):	
Право доступа, вид подписи:	**С правом подписи**: ☐ единоличная подпись, ☐ первая подпись (одновременно со второй подписью)*, ☐ вторая подпись (одновременно с первой подписью)* **Без права подписи:** ☐ (просмотр движения денежных средств по счету, ☐ запрос выписки по счету, ☐ создание Распоряжений, ☐ просмотр информации**,** ☐ другое (указать конкретный вид ограниченного доступа)_____ **Иное:**_____

* Заполняется при предоставлении доступа Владельцу Логина и Пароля в случае наличия в карточке с образцами подписей и оттиска печати более одной подписи.

- Логин прошу направить посредством электронного сообщения на адрес электронной почты, указанный в разделе «Электронная почта (E-mail)» настоящего Заявления.
- Первичный пароль Клиента прошу направить посредством sms-сообщения на Зарегистрированный номер, указанный в разделе «Зарегистрированный номер мобильного телефона» настоящего Заявления.
- Я уведомлен, что предоставление Сертификата ключа проверки электронной подписи лицу, являющемуся Владельцем Логина и Пароля, не осуществляется.
- Я уведомлен об обязанности сменить Первичный пароль Клиента на Пароль при первом входе в систему Интернет-банк.
- Для получения sms/push-уведомлений Клиент самостоятельно обеспечивает на своем Мобильном устройстве поддержку функций приема и отправки sms/push-сообщения, а также подключение Мобильного устройства к любым операторам связи, поддерживающим стандарт GSM, работоспособность Мобильного устройства.
- Я обязуюсь немедленно информировать (по телефону с использованием кодового слова_____с последующим письменным подтверждением) Банк (телефоны Банка – 8 (3852) 370-230, 8(3852)370-241, 8(3852)370-213) о возникновении угрозы компрометации Логина и Пароля уполномоченного лица Клиента (в том числе утраты), а также незамедлительно, но не позднее дня, следующего за днём получения от Банка уведомления о совершённой операции, об их использовании без добровольного согласия Клиента.

_____ _____
(подпись) (должность, ФИО)
«___»_____202__г. М.П.

[1] Указанные данные принимаются Банком в качестве сведений о контактных лицах Клиента и используются для связи с Клиентом в случае выявления операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента в соответствии с положениями Федерального закона Российской Федерации №161-ФЗ от 27.06.2011 г. «О национальной платежной системе».

Клиент обязуется в течение срока действия настоящего Договора незамедлительно информировать Банк об изменении указанных в настоящем Заявлении реквизитов/сведений, в том числе о прекращении либо изменении объема полномочий представителей Клиента, указанных в настоящем Заявлении.

Приложение № 12

Акт приема-передачи Логина

г. Барнаул «___»_____20___г.

_____
(Наименование Клиента)

далее именуемое Клиент, в лице _____
_____
(должность, Ф.И.О. уполномоченного лица Клиента)

действующего на основании _____
(наименование документа, подтверждающего полномочия лица подписавшего акт)

и «КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ (далее - Банк) в лице _____, действующего(ей) на основании_____, совместно именуемые Стороны, действуя в рамках Договора ДБО, составили настоящий акт о нижеследующем:

1. С целью подключения (продолжения работы) к системе Интернет-банк с предоставлением доступа по Логину и Паролю Банк передал, а Клиент получил следующий уникальный Логин_____.

2. Обязательства Банка перед Клиентом выполнены в полном объеме, претензий у клиента не имеется.

Подписи сторон:

от Клиента

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

от Банка

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

Приложение № 13

Акт регистрации

_____ «___» _____ 20___г.

_____
(Наименование Клиента)

далее именуемое Клиент, в лице _____

_____
(должность, Ф.И.О. уполномоченного лица Клиента)

действующего на основании _____
(наименование документа, подтверждающего полномочия лица подписавшего акт)

и «КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ (далее - Банк) в лице _____, действующего(ей) на основании_____, совместно именуемые Стороны, действуя в рамках Договора ДБО, составили настоящий акт о нижеследующем:

1. Банк осуществил регистрацию Клиента, уполномоченного лица Клиента и его Логина в Сервисе «FAKTURA.RU»:

Клиент	
Уполномоченное лицо Клиента-держателя Логина	
Контакты (тел., факс, e-mail)	
Эмитент Сертификата	
Владелец Сертификата	
Логин	

2. Клиент признаёт юридическую силу всех простых электронных документов, направленных Клиентом с использованием Сервиса «FAKTURA.RU» и подписанных уполномоченным лицом Клиента – держателем Логина.
3. Стороны признают, что простые электронные документы, подписанные уполномоченным лицом Клиента – держателем Логина, юридически равнозначны документам на бумажном носителе, заверенным собственноручными подписями и оттиском печати Клиента из «Карточки с образцами подписей и оттиска печати».

Подписи сторон:

от Клиента

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

от Банка

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

Приложение № 14

Акт регистрации

_____ «___» _____ 20___г.

_____
(Наименование Клиента)

далее именуемое Клиент, в лице _____
_____
(должность, Ф.И.О. уполномоченного лица Клиента)

действующего на основании _____
(наименование документа, подтверждающего полномочия лица подписавшего акт)

и «КРАЕВОЙ КОММЕРЧЕСКИЙ СИБИРСКИЙ СОЦИАЛЬНЫЙ БАНК» ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ (далее - Банк) в лице _____, действующего(ей) на основании_____, совместно именуемые Стороны, действуя в рамках Договора ДБО, составили настоящий акт о нижеследующем:

1. Банк осуществил регистрацию Клиента, уполномоченного лица Клиента и его Логина в Сервисе «FAKTURA.RU»:

Клиент	
Уполномоченное лицо Клиента-держателя Логина	
Контакты (тел., факс, e-mail)	
Эмитент Сертификата	
Владелец Сертификата	
Логин	

2 Клиент признает, что предоставил уполномоченному лицу Клиента право доступа к

	Да/нет
Просмотру движения денежных средств по счету	
Запросу выписки по счету	
Создание Распоряжений	
Просмотр информации	
Другое (указать конкретный вид ограниченного доступа)	

получаемых с использованием Сервиса «FAKTURA.RU», а передача указанных сведений с использованием Сервиса «FAKTURA.RU» уполномоченному лицу Клиента не является нарушением банковской тайны.

Подписи сторон:

от Клиента

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

от Банка

_____
(Должность, подпись, инициалы и фамилия)

М.П. «___» _____ _____г.

Приложение № 15

«СИБСОЦБАНК» ООО

_____

_____

Заявление на отмену действия

☐ ключа ЭП

☐ Логина

☐ Пароля

В связи с _____

(указать причину)

просим отменить действие

☐ ключа ЭП

☐ Логина

следующих лиц:

ФИО_____

ФИО_____

В связи с _____

(указать причину)

просим отменить действие

☐ Пароля

и осуществить выдачу нового первичного пароля для доступа в систему Интернет-банк для следующего лица:

ФИО_____

Логин_____

Направить первичный пароль на номер телефона:_+7_____

_____ _____

(подпись) (должность, ФИО)

«___»_____202_г. М.П.

Приложение № 16
«СИБСОЦБАНК» ООО

_____

(наименование Клиента, ИНН)

ЗАЯВЛЕНИЕ
на изменение условий использования Системы ДБО

Прошу изменить следующие условия использования Системы ДБО:

Установить ограничения:
(выбрать нужное)

№1:
На осуществление операций по переводу денежных средств:

	Да/нет
Создание платежных поручений	
Подпись платежных поручений	
Создание поручений на конверсию валюты (списание)	
Подпись поручений на конверсию валюты (списание)	
Создание распоряжения на списание с транзитного счета	
Подпись распоряжения на списание с транзитного счета	
Создание документов валютного контроля	
Подпись документов валютного контроля	

№2:
на сумму операций с использованием системы ДБО: максимальная сумма всех операций в сутки (суточный лимит операций) _____.

М.П. _____/_____/
(подпись) (должность, ФИО)

«____»_____20__г.

ОТМЕТКИ БАНКА

С карточкой образцов подписей и оттиска печати сверено.

Дата «____»_____20__г.

Принял:
должность, ФИО, подпись:

_____

Приложение 17
«СИБСОЦБАНК» ООО

_____

(наименование Клиента, ИНН)

ЗАЯВЛЕНИЕ
на использование услуги «Альтернативный фактор подтверждения F. Business»

☐ Подключить услугу «Альтернативный фактор подтверждения F. Business»

Уполномоченное лицо Клиента	
Номер мобильного телефона для отправки sms-сообщений	
Владелец Сертификата	

☐ Прошу изменить номер мобильного телефона для отправки sms-сообщений:

Уполномоченное лицо Клиента	
Номер мобильного телефона для отправки sms-сообщений	
Владелец Сертификата	

М.П. _____/_____/
(подпись) (должность, ФИО)

«____»_____20__г.