ИНВЕСТИЦИОННЫЙ КОММЕРЧЕСКИЙ БАНК РАЗВИТИЯ «ЯРИНТЕРБАНК»
(ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ)
ИКБР «ЯРИНТЕРБАНК» (ООО)

УТВЕРЖДЕНЫ
Приказом Председателя Правления
ИКБР «ЯРИНТЕРБАНК» (ООО)
от 25.07.2024

Правила системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Ярославль, 2024

1. **Определения.**

Агент — уполномоченный представитель Удостоверяющего центра, заключивший с Удостоверяющим центром договор, в соответствии с которым Агент осуществляет от имени Удостоверяющего центра проверку Клиентов, документов Клиентов, предшествующую изготовлению Удостоверяющим центром Сертификатов.

Банк НВЕСТИЦИОННЫЙ КОММЕРЧЕСКИЙ БАНК РАЗВИТИЯ "ЯРИНТЕРБАНК" (ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ) (сокращенное наименование — *ИКБР «ЯРИНТЕРБАНК» (ООО)*), являющийся участником системы дистанционного банковского обслуживания на основании заключенного с Оператором Системы договора, а также осуществляющий функции Агента Удостоверяющего центра.

Безотзывность Платежного ЭД — характеристика Платежного ЭД, обозначающая отсутствие или прекращение возможности отзыва Клиентом Платежного ЭД в определенный момент времени. Безотзывность Платежного ЭД наступает в момент списания денежных средств со Счета Клиента в соответствии с условиями, изложенными в заключенных с Клиентом договорах банковского счета, банковского вклада (депозита), в том числе заключаемых в рамках Соглашений/Генеральных соглашений об общих условиях привлечения денежных средств (далее по тексту по-отдельности - Договор Счета или Договор Депозита, а в совокупности - Договор Счета/Депозита).

Владелец ключа шифрования (Владелец сертификата ключа шифрования) — физическое лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа шифрования и который обладает соответствующим Закрытым ключом шифрования.

Владелец сертификата — общее название Владельцев сертификатов ключей проверки ЭП и (или) Владельцев ключей шифрования.

Владелец сертификата ключа проверки ЭП (Владелец сертификата ключа подписи) —

физическое лицо, на имя которого Удостоверяющим центром выдан Сертификат ключа проверки ЭП и которое владеет соответствующим Ключом ЭП, позволяющим с помощью Средств ЭП создавать ЭП в ЭД (подписывать ЭД).

Владелец квалифицированного сертификата КЭП ФНС – юридическое лицо или индивидуальный предприниматель, которому Удостоверяющим центром ФНС РФ выдан квалифицированный сертификат ключа проверки квалифицированной электронной подписи ФНС и которое владеет соответствующим ключом КЭП ФНС, позволяющим с помощью средств криптографической защиты информации, сертифицированных ФСБ РФ, создавать квалифицированную электронную подпись в Электронных документах (подписывать Электронные документы), а также расшифровывать Электронные документы, адресованные Владельцу сертификата КЭП ФНС.

Гибернация — энергосберегающий режим операционной системы компьютера, позволяющий сохранять содержимое оперативной памяти на энергонезависимое устройство хранения данных (жёсткий диск или твердотельный накопитель) перед выключением питания.

Журнал системы — журнал работы Клиентов в Системе, фиксирующий доступ Клиентов, отправку ЭД, прием и подтверждение запросов (поручений, распоряжений, иных документов), прочие события. Журнал Системы ведется Оператором Системы в рабочем порядке регулярно автоматически в соответствии с утвержденным Оператором Системы Правилами, исключающим модификацию и удаление записей о протоколируемых действиях, а также внесение записей способами, не предусмотренными технологией Системы. Целями ведения Журнала системы являются выявление ситуаций, связанных с несанкционированными действиями, мониторинг событий для осуществления контроля, разрешение спорных и конфликтных ситуаций, связанных с работой в Системе.

Закрытый (секретный) ключ — Ключ ЭП и (или) Закрытый (секретный) ключ шифрования.

Закрытый (секретный) ключ шифрования — последовательность символов, известная Владельцу ключа шифрования и предназначенная для расшифровывания Электронных документов.

Зарегистрированный номер телефона — номер мобильного телефона Клиента (Уполномоченного лица Клиента), предоставленный данному лицу оператором сотовой связи и указанный в запросе на предоставления Логина для работы через Мобильное приложение.

Защищенный носитель —ключевой носитель «Рутокен ЭЦП», являющийся одновременно и ключевым носителем, и аппаратным СКЗИ.

Карточка с образцами подписей — банковская карточка с образцами подписей и оттиска печати Клиента.

Квалифицированный сертификат ключа проверки КЭП ФНС (КС КЭП ФНС, Квалифицированный сертификат КЭП ФНС) – КС КЭП ФНС, соответствующий требованиям, установленным Законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный Удостоверяющим центром ФНС России.

КИС «BeSafe» — корпоративная информационная система (https://besafe.ru/), организованная Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ИНН 5407187087, ОГРН 1025403189602).

Клиент — юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, присоединившееся к Правилам.

Ключ проверки ЭП (Открытый ключ ЭП) — последовательность символов, соответствующая Ключу ЭП, предназначенная для Проверки ЭП в ЭД.

Ключ ЭП (Закрытый (секретный) ключ электронной подписи) — последовательность символов, известная Владельцу сертификата ключа проверки ЭП и предназначенная для создания в ЭД ЭП с использованием Средств ЭП.

Ключ КЭП ФНС – уникальная последовательность символов, предназначенная для создания КЭП ФНС.

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

Ключевой носитель — информационный (материальный) носитель, на который могут быть записаны Криптографические ключи. В Системе допускается использование только Ключевых носителей, совместимых со СКЗИ, разрешенных к использованию в Системе.

Компрометация ЭСП— нарушение конфиденциальности Закрытого ключа, Логина и Постоянного пароля, констатация Владельцем обстоятельств или наступление обстоятельств, при которых возможно несанкционированное использование Закрытого ключа и/или Логина и Постоянного пароля неуполномоченными лицами. Утрата ЭСП, использование ЭСП без согласия Клиента являются частными случаями Компрометации Закрытого ключа.

Компрометация ключа КЭП ФНС – нарушение конфиденциальности Ключа КЭП ФНС, констатация Владельцем сертификата ключа проверки КЭП ФНС обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование Ключа КЭП ФНС неуполномоченными лицами. Действия при компрометации КЭП ФНС регламентируются нормативными и инструктивными документами ФНС России.

Криптографические ключи – общее название Ключей электронной подписи и Ключей проверки электронной подписи, Ключей КЭП ФНС и Ключей проверки КЭП ФНС.

Квалифицированная электронная подпись ФНС (КЭП ФНС) – квалифицированная электронная подпись, квалифицированный сертификат которой выдан юридическому лицу или индивидуальному предпринимателю Удостоверяющим центром ФНС России – реквизит Электронного документа, предназначенный для защиты Электронного документа с использованием средств криптографической защиты информации (СКЗИ), сертифицированных ФСБ РФ, позволяющий идентифицировать Владельца квалифицированного сертификата КЭП ФНС, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в Электронном документе информации после момента его подписания.

Мобильное приложение — программное обеспечение для мобильных устройств с операционными системами iOS или Android, позволяющее Клиентам управлять своими счетами, получать выписки, совершать операции по переводам денежных средств и платежи при помощи Мобильного устройства. Мобильное приложение ЯРИНТЕРБАНК Business устанавливается бесплатно из авторизованных магазинов App Store и Google Play. Доступ к работе через Мобильное приложение предоставляется Клиенту (Уполномоченному лицу Клиента), являющемуся Владельцем сертификата.

Мобильное устройство — Электронное устройство (телефон, смартфон, планшетный компьютер и т.п.), которое используется для доступа в Систему через Мобильное приложение и (или) для получения Разовых секретных паролей.

Неплатежный ЭД — любой ЭД, не представляющий собой распоряжение Клиента на совершение операции по Счету, содержащий все реквизиты, предусмотренные действующим законодательством Российской Федерации, нормативными актами Банка России и установленными Банком правилами. Неплатежный документ может содержать как документы, сформированные в электронном виде, так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажном носителе.

Ограниченный доступ в Систему — доступ к Счету на просмотр получаемой из Банка информации, запрос выписки, создание электронного сообщения, прием электронного документа.

Оператор Системы — Процессинговый центр Faktura.ru (www.faktura.ru), созданный Закрытым акционерным обществом «Биллинговый центр» (ИНН 5401152049, ОГРН 1025400512400), осуществляющий информационное и технологическое обслуживание Системы.

Открытый ключ — Ключ проверки ЭП и (или) Открытый ключ шифрования.

Открытый ключ шифрования — последовательность символов, предназначенная для зашифровывания Электронных документов, предназначенных Владельцу ключа шифрования.

Офис банка — подразделение Банка, в котором осуществляется обслуживание Счета Клиента.

Платежный ЭД — ЭД, представляющий собой распоряжение Клиента на совершение операций по Счету, содержащий все предусмотренные законодательством Российской Федерации реквизиты.

Подозрительная операция — сомнительная операция, по которой, в результате реализации мер внутреннего контроля, у Банка возникает подозрение в том, что такая операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путём, или финансирования терроризма.

Подтверждение подлинности Электронной подписи в Электронном документе (Проверка ЭП в ЭД) - положительный результат проверки принадлежности ЭП в ЭД Владельцу сертификата ключа проверки ЭП и отсутствия искажений в данном ЭД. Проверка ЭП в ЭД должна осуществляться соответствующим Средством ЭП с использованием Сертификата ключа проверки ЭП. При обмене ЭД с использованием одноразовых паролей, ЭП считается принадлежащей Клиенту (Уполномоченному лицу Клиента), если отправленный Банком Разовый секретный пароль совпадает с введенным Клиентом (Уполномоченным лицом Клиента) Разовым секретным паролем.

Подтверждение подлинности КЭП ФНС в Электронном документе (проверка КЭП ФНС документа) – положительный результат проверки принадлежности Электронной подписи в Электронном документе Владельцу сертификата и отсутствия искажений в данном Электронном документе. Подтверждение подлинности КЭП ФНС должно осуществляться соответствующим средством Электронной подписи с использованием КС КЭП ФНС.

Постоянный пароль — секретная последовательность символов, которая известна только Клиенту (Уполномоченному лицу Клиента). Использование в совокупности Логина и Постоянного пароля являются подтверждением того, что вход и действия в Системе совершаются Клиентом (Уполномоченным лицом Клиента). Передача Постоянного пароля третьим лицам, включая работников Банка или Клиента, запрещена.

Потенциально опасные файлы - исполняемые файлы, файлы с активным содержимым (программным кодом в виде макросов или скриптов), а также другие файлы, повышающие риски Банка при их обработке.

Правила КИС «BeSafe» — Правила электронного документооборота корпоративной информационной системы «BeSafe», которые расположены в Интернете по адресу https://besafe.ru/.

Правила сервиса «Faktura.ru» — Правила работы сервиса «Faktura.ru», которые расположены в Интернете по адресу http://service.cft.ru/Pages/agreements.aspx.

Простая электронная подпись (Простая ЭП) — реквизит Простого электронного документа, посредством использования кодов, паролей или иных средств позволяющий подтвердить факт формирования электронной подписи определенным лицом.

Рабочее время Службы технической поддержки клиентов — рабочие будние дни (с понедельника по четверг) с 8:30 до 17:30 по Московскому времени, пятница и предпраздничные дни — с 8:30 до 16:30 по Московскому времени.

Разовый секретный пароль — уникальный набор символов, предоставляемый Клиенту на Номер мобильного телефона в виде SMS/PUSH-сообщения. Разовый секретный пароль используется в качестве дополнительной меры защиты для Подтверждения ЭД / группы ЭД, совершения иных действий и признается ключом Простой электронной подписи при обмене документами через Мобильное приложение.

Регистрация квалифицированного сертификата ключа проверки КЭП ФНС (Регистрация КС КЭП ФНС) – процедура регистрации Идентификатора владельца квалифицированного сертификата ключа проверки КЭП ФНС, позволяющая предоставить Владельцу сертификата КЭП ФНС права на осуществление действий в рамках Системы.

Правила — настоящие правила системы дистанционного банковского обслуживания «Интернет Банк-Клиент», утвержденные Правлением Банка и содержащие условия оказания услуг по дистанционному банковскому обслуживанию «Интернет Банк-Клиент», требования к техническому и информационному обеспечению процессов формирования, обработки и хранения ЭД. Правила в соответствии со статьей 428 Гражданского кодекса Российской Федерации являются соглашением о присоединении (далее по тексту — Соглашение).

Сайт Банка — официальный сайт Банка в сети Интернет по адресу www.yarinterbank.ru

Сервис «Faktura.ru» — информационно-технологический сервис, позволяющий организовать обмен ЭД (www.faktura.ru), реализованный на платформе КИС «BeSafe».

Сертификат — общее название Сертификатов ключей проверки ЭП и (или) Сертификатов ключей шифрования, использование которых регулируется настоящими Правилами, Правилами КИС «BeSafe» и Правилами сервиса «Faktura.ru».

Сертификат ключа проверки ЭП (Сертификат ключа подписи) — ЭД с ЭП Удостоверяющего центра, доступный Сторонам, включающий в себя Ключ проверки ЭП Владельца сертификата ключа проверки ЭП. Сертификаты ключей проверки ЭП выдаются Удостоверяющим центром Сторонам для подтверждения подлинности ЭП и идентификации Владельца сертификата ключа проверки ЭП. Сертификат ключа проверки ЭП уникален в рамках выдавшего его Удостоверяющего центра.

Сертификат ключа шифрования — документ на бумажном носителе или ЭД с ЭП Удостоверяющего центра, доступный Сторонам, включающий Открытый ключ шифрования Владельца ключа шифрования. Сертификат ключа шифрования создаётся Удостоверяющим центром для обеспечения возможности шифрования предназначенных Владельцу ключа шифрования ЭД. Сертификат ключа шифрования уникален в рамках выдавшего его Удостоверяющего центра.

Система дистанционного банковского обслуживания «Интернет Банк-Клиент» (Система) — реализованная на основе Сервиса «Faktura.ru» система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, включая программный комплекс, состоящий из средств формирования, обработки, хранения, передачи ЭД, реализующая обмен ЭД между Клиентом и Банком в соответствии с Правилами.

Служба технической поддержки клиентов — подразделение Банка, позволяющее Клиенту обратиться по Телефонам Службы технической поддержки клиентов в Рабочее время Службы технической поддержки клиентов за получением консультаций и иной помощи при возникновении вопросов при использовании Системы.

Соглашение — Соглашение о присоединении к системе дистанционного банковского обслуживания **«Интернет Банк-Клиент»**

Сомнительная операция — это операция, осуществляемая Клиентом, имеющая необычный характер
и признаки отсутствия явного экономического смысла и очевидных законных целей, которая может проводиться для вывода капитала из страны, финансирования "серого" импорта, перевода денежных средств из безналичной в наличную форму и последующего ухода от налогообложения, а также для финансовой поддержки коррупции и других противозаконных целей; операция, относящаяся к отдельным видам операций, в отношении которых Банком России даны рекомендации о повышении к ним внимания кредитными организациями, а также любая иная операция, которая, по мнению Банка,

может осуществляться с целью отмывания доходов, полученных преступным путем, и/или финансирования терроризма.

Средства криптографической защиты информации (СКЗИ) — аппаратные и (или) программные средства, обеспечивающие применение ЭП и шифрования при организации обмена ЭД. В Системе допускается использование только средств криптографической защиты информации, разрешённых к использованию в КИС «BeSafe».

Средства криптографической защиты информации КЭП ФНС (СКЗИ КЭП ФНС) аппаратные, программные или аппаратно-программные средства, сертифицированные ФСБ РФ, осуществляющие криптографические преобразования информации для обеспечения ее безопасности
Средства электронной подписи (Средства ЭП) — аппаратные и (или) программные средства, являющиеся частью средств криптографической защиты информации и реализующие хотя бы одну из следующих функций при организации обмена ЭД: создание ЭП в ЭД с использованием Ключа ЭП; Подтверждение подлинности ЭП, содержащейся в ЭД, с использованием Ключа проверки ЭП; создание Ключей ЭП и Ключей проверки ЭП.

Сторона — Клиент или Банк.

Счет — банковский счет, открытый Клиенту Банком, в соответствии с Договором Счета/Депозита распоряжение которым Клиент осуществляет, в том числе, посредством Системы. В рамках Системы Клиент может распоряжаться несколькими Счетами, подключенными к Системе.

Тарифы — Тарифы на расчетно-кассовое обслуживание корпоративных Клиентов ИКБР «ЯРИНТЕРБАНК» (ООО) в валюте РФ, Тарифы на расчетно-кассовое обслуживание корпоративных Клиентов ИКБР «ЯРИНТЕРБАНК» (ООО) в иностранных валютах, утверждаемые Правлением Банка и размещаемые в помещениях Банка в общедоступном месте и на Сайте Банка. Тарифы являются неотъемлемой частью Правил.

Телефоны Службы технической поддержки клиентов — 8 (4852) 205-195.

Удостоверяющий центр — Удостоверяющий Центр «AUTHORITY», созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ИНН 5407187087, ОГРН 1025403189602) (www.authority.ru), который для обеспечения обмена ЭД в рамках Системы осуществляет следующие функции:

- ведет реестр Сертификатов ключей проверки ЭП (ключей шифрования), обеспечивает его актуальность и возможность доступа к нему Сторон;
- осуществляет проверку на уникальность идентификатора Владельца сертификата ключа проверки ЭП (ключа шифрования) в реестре Сертификатов ключей проверки ЭП (ключей шифрования);
- удостоверяет Сертификаты ключей проверки ЭП и ключей шифрования;
- выдает Сертификаты ключей проверки ЭП и сертификаты ключей шифрования в электронной форме и (или) в форме документов на бумажных носителях с информацией об их действии;
- приостанавливает и возобновляет действие Сертификатов ключей проверки ЭП (ключей шифрования), а также аннулирует их;
- осуществляет по обращениям Сторон подтверждение подлинности ЭП в ЭД в отношении выданных им Сертификатов ключей проверки ЭП.

Удостоверяющий центр ФНС России (далее – «УЦ ФНС») – Федеральная налоговая служба Российской Федерации (далее также «ФНС РФ»), осуществляющая функции аккредитованного удостоверяющего центра. В соответствии с Законом «Об электронной подписи» с 01.01.2022 сертификаты квалифицированной электронной подписи выдаются юридическим лицам (с указанием в качестве владельца сертификата квалифицированной электронной подписи также лица, уполномоченного действовать без доверенности), за исключением юридических лиц, указанных в 2 ст. 17.2 этого закона, и индивидуальным предпринимателям. УЦ ФНС работает согласно Регламенту Удостоверяющего центра Федеральной налоговой службы, утвержденного Приказом ФНС РФ (далее – «Регламент УЦ ФНС»). На момент вступления в силу текущей редакции Правил действует Приказ ФНС РФ от «25» апреля 2022 г. № ЕД-7-24/340.

Уполномоченное лицо Банка — работник Банка, уполномоченный от имени Банка взаимодействовать с Клиентом в рамках Системы, в том числе вести переписку, отправлять документы, а также осуществлять иные полномочия.

Уполномоченное лицо Клиента — лицо, наделенное правом подписания расчетных документов по распоряжению денежными средствами на Счете (-ах) (правом подписания распоряжений об осуществлении перевода денежных средств) и создания Неплатежных ЭД, либо обладающее только Ограниченными правами доступа в Систему, действующее в соответствии с учредительными документами Клиента или на основании доверенности и имеющее доступ к Счету (-ам) согласно Заявления на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Интернет Банк-Клиент» (Приложение № 2 к Правилам) или Заявления на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в систему дистанционного банковского обслуживания «Банк-клиент» (Приложение № 2а к Правилам).

Усиленная неквалифицированная электронная подпись (Электронная подпись, ЭП) — реквизит ЭД, предназначенный для защиты ЭД от подделки, полученный в результате криптографического преобразования информации с использованием Ключа ЭП и позволяющий идентифицировать Владельца сертификата ключа проверки ЭП, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в ЭД информации.

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

Электронное сообщение (ЭС) — логически целостная совокупность структурированных данных, имеющих смысл для Сторон. Информация в ЭС представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

Электронное средство платежа (ЭСП) — Электронное устройство, Ключевой носитель, Закрытый ключ и Сертификат Уполномоченного лица Клиента в совокупности, позволяющие Уполномоченному лицу Клиента в рамках Системы составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в соответствии с Договором Счета/Депозита.

Электронное устройство (ЭУ) — персональный компьютер, ноутбук и иное рабочее место, используемое Уполномоченным лицом Клиента для дистанционного управления Счетом в рамках Системы.

Электронный документ (ЭД) – Электронное сообщение, подписанное Электронной подписью или Квалифицированной электронной подписью ФНС, в котором информация представлена в электронно-цифровой форме и соответствует установленному формату. Электронный документ может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

Иные определения, используемые в Правилах, применяются в значениях, определенных Правилами КИС «BeSafe» и Правилами сервиса «Faktura.ru».

2. Общие положения.

2.1. Правила устанавливают порядок организации обмена ЭД между Клиентом и Банком в рамках Системы, реализованной на основе сервиса «Faktura.ru» на платформе КИС «BeSafe». Присоединение к Правилам и подключение Клиента к Системе осуществляется путем подписания между Клиентом и Банком Соглашения по форме Приложения №10 к Правилам.

2.2. Присоединяясь к настоящим Правилам, Участник принимает их условия целиком в порядке, предусмотренном ст. 428 Гражданского Кодекса Российской Федерации, и обязуется их выполнять.

2.3. Правила КИС «BeSafe» и Правила сервиса «Faktura.ru» являются неотъемлемой частью настоящих Правил. Стороны присоединяются к Правилам КИС «BeSafe» и Правилам сервиса «Faktura.ru» и обязуются их исполнять.

2.4. Положения настоящих Правила применяются, если иное не предусмотрено Правилами КИС «BeSafe», Правилами сервиса «Faktura.ru», законодательными или иными правовыми актами Российской Федерации, включая нормативные акты Банка России. При исполнении Договора Счета/Депозита, положения настоящих Правил применяются в той мере, в которой они не противоречат условиям данных договоров.

2.5. Стороны признают, что:

2.5.1. получение ЭД/Простого ЭД, подписанного в соответствии с настоящими Правилами ЭП/КЭП ФНС/Простой ЭП Участника, юридически эквивалентно получению документа на бумажном носителе, подписанного собственноручными подписями Участника/уполномоченных лиц Участника и заверенному печатью, если документ на бумажном носителе должен быть заверен печатью (для ЭП, КЭП ФНС) Участника. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что Ключ ЭП, ЭП, Простая ЭП и Сертификат Участника созданы с использованием и в соответствии с настоящими Правилами, Правилами КИС «BeSafe», а ключ КЭП ФНС, КЭП ФНС, КС КЭП ФНС созданы в соответствии с Регламентом УЦ ФНС;

2.5.2. используемые в Системе способы защиты информации, которые обеспечивают формирование и проверку ЭП/КЭП ФНС/Простой ЭП, достаточны для подтверждения авторства и подлинности ЭД;

2.5.3. подделка ЭП/КЭП ФНС/Простой ЭП, то есть создание корректной ЭП/КЭП ФНС/Простой ЭП ЭД, невозможна без знания Закрытого ключа Стороны (доступа к Закрытому ключу Стороны);

2.5.4. ЭП/КЭП ФНС/Простой ЭП ЭД является аналогом собственноручной подписи Уполномоченного лица Стороны.

3. Порядок вступления в действие и внесения изменений в Правила.

3.1. Правила могут быть изменены по инициативе Банка в одностороннем порядке путем утверждения новой редакции Правил, в порядке, установленном настоящим разделом Правил

3.2. В случае изменения законодательства Российской Федерации Правила, до момента их изменения Банком, применяются в части, не противоречащей требованиям законодательства Российской Федерации.

3.3. Новая редакция Правил утверждается Приказом Председателя Правления Банка и вступает в силу в сроки, определяемые таким приказом.

3.4. Действующая редакция Правил размещается на Сайте Банка.

3.5. Новая редакция Правил, а также информация о сроках вступления его в силу доводится Банком до сведения Клиентов посредством уведомления. Уведомление осуществляется путем размещения новой редакции Правил на Сайте Банка либо иным способом извещения в соответствии с п.7.6 Правил, обеспечивающим возможность получения Клиентом указанных изменений.

3.6. В случае несогласия Клиента с условиями новой редакции Правил или новой редакции Правил КИС «BeSafe», или новой редакции Правил сервиса «Faktura.ru» Клиент вправе расторгнуть Соглашение в порядке, предусмотренном разделом 12 Правил.

3.7. С момента вступления в силу новой редакции Правил, новой редакции Правил КИС «BeSafe» или новой редакции Правил сервиса «Faktura.ru» Стороны при работе в Системе руководствуются новой редакцией Правил, новой редакцией Правил КИС «BeSafe» или новой редакцией Правил сервиса «Faktura.ru». Начало работы Клиента на условиях, предусмотренных новой редакцией Правил или новой редакцией Правил КИС «BeSafe» или новой редакцией Правил сервиса «Faktura.ru» со дня вступления их в силу автоматически означает полное согласие с условиями, а также принятие всех обязательств, предусмотренных таким Правилами, Правилами КИС «BeSafe» или Правилами сервиса «Faktura.ru».

3.8. Банк не несет ответственности, если информация об утверждении новой редакции Правил, опубликованная в порядке и в сроки, установленные Правилами, не была получена и/или изучена, и/или правильно истолкована Клиентом.

4. Порядок и особенности организации технического доступа к Системе. Обеспечение информационной безопасности работы в Системе.

4.1. Банк до заключения Соглашения информирует Клиента об условиях использования ЭСП путем размещения соответствующей информации на Сайте Банка.

4.2. Клиент до подключения к Системе обязан оценить риски, связанные с использованием Системы,

в соответствии с п.7.1 и других положений настоящего Правил, размещаемых на Сайте Банка, и, основываясь на проведенной оценке рисков, принять решение об использовании Системы или отказе от работы с ней.

4.3. Клиент до подключения к Системе определяет способ доступа к Системе:

- с помощью Сертификата ключа подписи;
- с помощью Логина и Постоянного пароля;
- квалифицированного сертификата КЭП ФНС

4.4. Клиент до подключения к Системе, а затем на постоянной основе обязан обеспечить выполнение следующих требований информационной безопасности при использовании Системы:

4.4.1. Ключевой носитель и/или Логин и Постоянный пароль использовать только Уполномоченным лицом Клиента, которому они принадлежат, не передавать Ключевой носитель и/или Логин и Постоянный пароль одного Уполномоченного лица другому Уполномоченному лицу Клиента и иным лицам;

4.4.2. Хранить Ключевые носители раздельно, в защищенном от несанкционированного доступа месте;

4.4.3. Хранить и использовать Логин и Постоянный пароль способами, обеспечивающими невозможность их несанкционированного использования;

4.4.4. Не передавать в пользование третьим лицам Зарегистрированный номер телефона (SIM-карту) и незамедлительно уведомлять Банк о Компрометации Логина и Постоянного пароля или ЭУ;

4.4.5. Избегать регистрации Зарегистрированного номера телефона, на который приходят SMS/PUSH-сообщения с Разовым секретным паролем, в социальных сетях и других открытых источниках;

4.4.6. При работе в сети Интернет не устанавливать каких-либо дополнительных программ от недоверенных издателей;

4.4.7. Не устанавливать Ключевые носители в компьютеры, ноутбуки и иные устройства, не используемые для работы в Системе;

4.4.8. Не оставлять Ключевые носители установленными в ЭУ после завершения сеанса работы в Системе;

4.4.9. Не оставлять ЭУ с Мобильным приложением без присмотра;

4.4.10. Не использовать вход в Мобильное приложение по отпечатку пальца или с помощью распознавания лица, если в Устройстве зарегистрированы отпечатки пальцев или лица других людей;

4.4.11. Использовать ЭУ в помещениях с малой проходимостью или ограниченным доступом во избежание хищения Ключевых носителей, используемых для работы с Системой;

4.4.12. Не осуществлять доступ в систему с использованием мобильных устройств в местах с общедоступными сетями Internet (свободный WiFi в кафе, парках, гостиницах и т.п.);

4.4.13. Размещать ЭУ способом, не позволяющим производить визуальное наблюдение за экраном ЭУ и его клавиатурой, в том числе посредством системы видеонаблюдения и через оконные проемы;

4.4.14. Использовать ЭУ с установленной лицензионной операционной системой;

4.4.15. Незамедлительно после публикации обновлений — обновлять операционную систему (устанавливать критичные обновления и обновления безопасности) и иное программное обеспечение, установленное на ЭУ;

4.4.16. Не использовать установленные на ЭУ операционную систему и иное программное обеспечение, для которых прекращен предусмотренный разработчиком выпуск обновлений безопасности;

4.4.17. Использовать ЭУ с установленным лицензионным антивирусным программным

обеспечением;

4.4.18. Производить проверку наличия обновлений антивирусных баз у разработчика антивирусного программного обеспечения не реже раза в сутки и в случае наличия обновлений производить их своевременное обновление;

4.4.19. Не использовать установленное на ЭУ антивирусное программное обеспечение, для которого прекращен выпуск обновлений антивирусных баз;

4.4.20. Производить не реже раза в неделю полное антивирусное сканирование машинных носителей информации ЭУ;

4.4.21. Осуществлять работу на ЭУ с использованием учетной записи с ограниченными правами, доступ к учетной записи с полными правами (администратора) защищать надежным паролем;

4.4.22. Устанавливать длинные и сложные пароли для доступа в Систему с соблюдением следующих требований:

- для входа с помощью Логина и Постоянного пароля, пароль должен содержать от 8 до 25 символов;

- для доступа к Защищенному носителю, пароль должен содержать от 6 до 8 символов;

Независимо от способа доступа в Систему, пароль должен состоять из букв латинского алфавита, содержать хотя бы одну строчную букву, заглавную букву (например, «Q» и «q»), цифры и спецсимволы ((@, #, $, %, <, ^, &, *, _). Пароль не может содержать пробел, состоять из идущих подряд символов или содержать несколько идущих подряд повторяющихся символов;

4.4.23. Производить регулярную смену паролей не реже одного раза в месяц;

4.4.24. Максимально ограничить работу с отчуждаемыми носителями информации (флэш-накопители, дискеты, диски и т.п.) за исключением Ключевых носителей, перед использованием первых осуществлять их полное сканирование антивирусным программным обеспечением на наличие вредоносного кода;

4.4.25. Посредством Системы регулярно проверять список IP-адресов, с которых осуществлялись подключения к Системе;

4.4.26. Выполнять иные меры по обеспечению информационной безопасности, указанные на www.faktura.ru и Сайте Банка www.yarinterbank.ru.

4.4.27. Обязательным условием допуска для работы в Системе Уполномоченного лица Клиента, наделенного правом подписания расчетных документов по распоряжению денежными средствами на Счете(-ах) (правом подписания распоряжений об осуществлении перевода денежных средств) и создания Платежных ЭД, является предоставление Банку его номера(-ов) телефона(-ов) для направления и запроса информации по вопросам использования Системы и обработки ЭД. Номера телефонов предоставляются в форме Неплатежного ЭД, Приложения №10 или Приложения №2 к настоящему Регламенту, либо любым другим письменным способом. С момента получения такого документа и регистрации его в АБС Банка, номер телефона становится Зарегистрированным номером телефона. Клиент обязан незамедлительно направлять в Банк новые номера телефонов в случае их изменения.

4.5. Для существенного повышения безопасности работы в Системе Клиенту предлагается обеспечить выполнение следующих рекомендаций информационной безопасности при использовании Системы на постоянной основе:

4.5.1. настроить сетевое оборудование, обеспечивающее доступ Клиента в сеть, или специализированное программное обеспечение (брандмауэр, прокси-сервер и т.п.) на блокировку сетевых пакетов, передаваемых с ЭУ, применяемого для работы в Системе, на любые адреса, не относящиеся к Системе, системе доменных имён (Domain Name System), DHCP-серверу, службе каталогов (Active Directory и т.п.) и службам синхронизации времени, обновления установленного программного обеспечения, операционной системы и антивирусных баз;

4.5.2. настроить аудит событий, регистрирующий возникающие ошибки работы операционной системы и приложений, вход пользователей и запуск программ, периодически
просматривать журналы аудита, реагировать на ошибки и попытки несанкционированного доступа;

4.5.3. ЭУ, применяемые для работы в Системе, не использовать в других целях, в том числе рабочих;

4.5.4. использовать возможности информирования по электронной почте о расходных операциях по Счету; возможности дополнительной услуги Push-уведомлений, SMS-информирования;

4.5.5. ограничить диапазон IP-адресов, с которых будет осуществляться вход в Систему;

4.5.6. следовать иным рекомендациям информационной безопасности, размещенным на сайте Системы www.faktura.ru и Сайте Банка www.yarinterbank.ru.

4.6. Для существенного повышения безопасности работы в Системе с использованием мобильных устройств Клиенту предлагается обеспечить выполнение следующих рекомендаций информационной безопасности при использовании Системы:

4.6.1. Устанавливать мобильные приложения ЯРИНТЕРБАНК только из авторизованных магазинов App Store и Google Play.

4.6.2. Использовать антивирусное программное обеспечение, в случае, если оно доступно для мобильного устройства.

4.6.3. Избегать регистрации номера мобильного телефона, на который приходят SMS/PUSH сообщения с Разовым секретным паролем, в социальных сетях и других открытых источниках.

4.6.4. Настроить и использовать автоматическую блокировку рабочего экрана устройства

4.6.5. Обязательно сверять текст SMS/PUSH-сообщений, содержащий пароль, с деталями выполняемой операции. Если в SMS/PUSH-сообщении указан пароль для платежа, которого Клиент не совершал или третьи лица предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный платеж, ни в коем случае не вводить его в Интернет-банке и не называть его, в том числе сотрудникам Банка.

4.6.6. В случае утери мобильного телефона, на который приходят SMS/PUSH-сообщения с Разовым секретным паролем, немедленно заблокировать SIM-карту и/или сообщите об утере в Банк для осуществления блокировки Системы

4.6.7. Следовать иным рекомендациям информационной безопасности, размещенным на сайте Системы www.faktura.ru и Сайте Банка https://www.yarinterbank.ru/.

4.7. Об ошибках в работе Системы Клиенту необходимо уведомлять Службу технической поддержки клиентов.

4.8. Клиент для работы с Системой обязан использовать только технически исправное ЭУ.

4.9. Требования и рекомендации по настройке ЭУ Клиента для работы в Системе приведены в Приложении №3 к Правилам. Клиенту запрещается использовать для работы с Системой ЭУ, не настроенное в соответствии с настоящим Правилами.

5. Порядок осуществления обмена электронными документами.

5.1. Условия допуска к осуществлению обмена электронными документами в системе.

5.1.1. Клиенту для дистанционного управления в Системе могут быть подключены расчетные, депозитные, транзитные счета в национальной и иностранной валюте.

5.1.2. Клиенту дополнительно для дистанционного просмотра движения и остатков на Счете, запроса выписки по Счету в Системе могут быть подключены иные счета по усмотрению Сторон.

5.1.3. Сертификат выдается на имя Уполномоченного лица Клиента, непосредственно использующего Закрытый ключ; КЭП ФНС регистрируется в системе, в случае, если она выдана на имя Уполномоченного лица Клиента**.**

5.1.4. Право подписи ЭС может принадлежать:

- клиенту-индивидуальному предпринимателю, физическому лицу, занимающемуся в установленном законодательством Российской Федерации порядке частной практикой;
- физическим лицам на основании соответствующей доверенности, выданной в случаях и в порядке, установленных законодательством Российской Федерации,

индивидуальным предпринимателем, физическим лицом, занимающимся в установленном законодательством Российской Федерации порядке частной практикой;

- единоличному исполнительному органу клиента-юридического лица;
- иным сотрудникам (работникам), наделенным правом подписи клиентом-юридическим лицом, в том числе на основании доверенности. Право подписи может принадлежать только сотрудникам (работникам) клиента-юридического лица.

5.1.5. Доверенность от имени Клиента - юридического лица выдается в порядке, установленном законодательством Российской Федерации. Доверенности Клиентов - индивидуальных предпринимателей и лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, должны быть удостоверены нотариально.

5.1.6. Предоставляемые Банку доверенности должны содержать полномочия лиц на распоряжение денежными средствами и подписание Неплатежных ЭД с использованием ЭП.

5.1.7. Уполномоченному лицу Клиента, не наделенному правом подписи, может быть предоставлен только Ограниченный доступ в Систему, согласно Заявления на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Интернет Банк-Клиент» (Приложение №2а к Правилам) на основании доверенности. При этом указанному лицу не может быть предоставлено право доступа на подписание ЭС и отправку ЭД. Для хранения Криптографических ключей в этом случае может использоваться Логин/пароль

5.1.8. Права доступа Уполномоченного лица Клиента могут быть дополнительно сокращены при наличии технической возможности по заявлению Клиента, оформленному в свободной форме.

5.1.9. К исполнению принимаются Платежные и Неплатежные ЭД при наличии ЭП/КЭП ФНС/Простой ЭП Уполномоченного(-ых) лица (лиц) Клиента, обладающего(-их) правом подписи, и имеющего(-их) доступ к Счету (-ам) согласно Заявления на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Интернет Банк-Клиент» (Приложение №2 к Правилам. Количество и возможные сочетания подписей, необходимых для подписания документов, содержащих распоряжение Клиента на перевод денежных средств со счета, указываются в Соглашении о выборе возможных сочетаний собственноручных подписей.

5.1.10. Обязательным условием допуска для работы в Системе Уполномоченного лица Клиента, наделенного правом подписи, является использование им:
- Защищенного носителя для web версии «Интернет Банк-Клиент»
- Логина и Постоянного пароля для доступа в Мобильное приложение ЯРИНТЕРБАНК Bissnes
- КЭП ФНС

5.2. **Порядок допуска к осуществлению обмена электронными документами в системе.**

5.2.1. В случае необходимости Клиентом подается «Заявление о направлении дополнительной информации для обеспечения информационной безопасности работы в системе дистанционного банковского обслуживания «Интернет Банк-Клиент» по форме Приложения №1 и/или Анкета о выявлении признаков осуществления перевода денежных средств без согласия Клиента по форме Приложения №1а к Правилам, если данные, предоставляемые по указанным формам, не предоставлялись ранее или требуют актуализации.

5.2.2. Для работы с Системой Клиентом на каждое Уполномоченное лицо подается «Заявление на распоряжение по счету/изменение прав доступа уполномоченного лица Клиента в системе дистанционного банковского обслуживания «Интернет Банк-Клиент» по форме Приложения №2 к Правилам или «Заявление на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в систему дистанционного банковского обслуживания

«Интернет Банк-Клиент» по форме Приложения №2а к Правилам, если данные, предоставляемые по указанному заявлению, не предоставлялись ранее или требуют актуализации. При этом для каждого Уполномоченного лица можно указать:

5.2.2.1. перечень Счетов и прав доступа к ним посредством Системы (указание хотя бы одного Счета обязательно);

5.2.2.2. на необходимость получения одноразовых паролей на вход в Систему и номер телефона для этого;

5.2.2.3. на необходимость получения сообщений на электронный адрес о входе в Систему, об отправке платежа в банк, об исполнении платежа;

5.2.2.4. IP-адрес(-а), с которого(-ых) будет осуществляться вход в Систему.

5.2.3. При подаче заявления в соответствии с п.5.2.2 по Уполномоченному лицу Клиента, не наделенному правом подписи, но обладающему ограниченными правами доступа к Счету в рамках Системы, Клиент должен предоставить доверенность, оформленную в соответствии с требованиями Банка, о наделении Уполномоченного лица Клиента такими правами, если она не была предоставлена ранее.

5.2.4. Клиентом производится подготовка безопасной работы в Системе в соответствии с требованиями раздела 4 настоящих Правил, настройка необходимого количества ЭУ в соответствии с «Требованиями и рекомендациями по настройке электронного устройства Клиента для работы в Системе», приведенными в Приложении №3 к Правилам.

5.2.5. В случае первичной выдачи Сертификата Удостоверяющим центром Уполномоченному лицу Клиента каждым Уполномоченным лицом Клиента:

5.2.5.1. с правом подписи — производится создание на Защищенном носителе Криптографических ключей и направление Удостоверяющему центру запроса на получение Сертификата в соответствии с «Инструкцией по подключению к системе «Интернет Банк-Клиент», размещенной на Сайте Банка;

5.2.5.2. не наделенным правом подписи — производится создание на Ключевом носителе Криптографических ключей и направление Удостоверяющему центру запроса на получение Сертификата в соответствии с «Инструкцией по подключению к системе», размещенной на Сайте Банка/либо Банком производится регистрация логина.

5.2.5.3. после направления Удостоверяющему центру запроса на получение Сертификата по предложенной(-ым) ссылке(-ам) производится распечатка в одном экземпляре каждого заявления на выдачу Сертификата по форме Приложения №4 к Правилам, которое подписывается Уполномоченным лицом Клиента и заверяется печатью организации.

5.2.6. Создание и выдача Сертификата с генерацией Закрытого ключа ЭП Заявителем, как при подключении Клиента к Системе, так и при плановом перевыпуске Сертификата ЭП, осуществляется в соответствии с порядком описанном в Правилах работы Удостоверяющего центра «AUTHORITY».

5.2.7. Банк вправе отказаться от подтверждения выдачи нового Сертификата Клиенту. При этом Клиенту направляется сообщение об отказе в создании и выдаче Сертификата.

5.2.8. Не позднее пяти рабочих дней до дня окончания срока действия Сертификата Уполномоченного лица Клиента (далее — в случае перевыпуска Сертификата) Уполномоченным лицом Клиента производится создание на Ключевом носителе Криптографических ключей и направление Удостоверяющему центру запроса на получение Сертификата в соответствии с «Инструкцией по перевыпуску сертификатов», размещенной на Сайте Банка. Направляемый в электронном виде Удостоверяющему центру запрос на получение Сертификата автоматически подписывается ЭП, сформированной действующим Ключом ЭП Владельца сертификата. При этом запрос равнозначен заявлению на выдачу Сертификата, заверенному собственноручной подписью Уполномоченного лица Клиента и печатью Клиента.

5.2.9. После направления Удостоверяющему центру Уполномоченным лицом Клиента запроса на получение Сертификата и получения Банком информации о его направлении, Банком как Агентом в течение одного рабочего дня подтверждается указанный запрос.

5.2.10. Удостоверяющим центром после подтверждения запроса Банком в срок не позднее трех рабочих дней выпускается Сертификат, соответствующий Открытому ключу, и Уполномоченному лицу Клиента на адрес электронной почты, указанный при создании запроса на получение Сертификата, направляется ссылка на получение Сертификата.

5.2.11. В случае полной регистрации Уполномоченного лица Клиента:

5.2.11.1. Уполномоченным лицом Клиента после получения ссылки для установки Сертификата в соответствии с «Инструкцией по подключению к системе», размещенной на Сайте Банка, устанавливается полученный по ссылке Сертификат на Ключевой носитель и производится распечатка в двух экземплярах каждого акта приема-передачи Сертификата по форме Приложения №5 к Правилам, после чего указанные акты подписываются Владельцем сертификата и заверяются печатью организации;

5.2.11.2. Клиентом предоставляется в Банк по одному экземпляру каждого заявления на выдачу Сертификата по форме Приложения №4 к Правилам, по два экземпляра каждого акта приема-передачи Сертификата по форме Приложения №5 к Правилам на каждого Уполномоченного лица Клиента.

5.2.12. В случае перевыпуска Сертификата Уполномоченного лица Клиента:

5.2.12.1. после получения от Удостоверяющего центра ссылки для установки Сертификата Уполномоченным лицом Клиента устанавливается полученный по ссылке Сертификат на Ключевой носитель в соответствии с «Инструкцией по перевыпуску сертификатов», размещенной на Сайте Банка;

5.2.12.2. в процессе установки Сертификата Уполномоченным лицом Клиента производится подписание каждого акта приема-передачи Сертификата Ключом ЭП, принадлежащим Владельцу сертификата.

5.2.12.3. обязательно предоставление в Банк заявлений на выдачу Сертификата и актов приема-передачи Сертификата на бумажном носителе с подписью Уполномоченного лица Клиента и печатью (при наличии).

5.2.13. Возможность работы Уполномоченного лица Клиента в Системе предоставляется не позднее двух рабочих дней после получения Банком оформленных должным образом заявлений на получение Сертификатов, актов приема-передачи Сертификатов (в том числе, направленных в электронном виде Удостоверяющему центру и заверенных ЭП этого Уполномоченного лица Клиента) при положительной сверке информации, содержащейся в них, с информацией, зарегистрированной в Удостоверяющем центре.

5.2.14. Подписанные Сторонами акты приема-передачи Сертификата (по форме Приложения №5 к Правилам) каждого Уполномоченного лица Клиента являются неотъемлемыми частями Соглашения.

5.2.15. «Инструкция по подключению к системе «Интернет Банк-Клиент» и «Инструкция по перевыпуску сертификатов», размещенные на Сайте Банка, являются неотъемлемой частью настоящих Правил.

5.2.16. Для получения доступа с помощью Логина и Постоянного пароля:

5.2.16.1. Клиент (Уполномоченное лицо Клиента) обращается в Банк с заявлением на предоставление Логина для работы в Системе (Приложение №11 к настоящим Правилам).

5.2.16.2. Информация о присвоенном Логине передается Клиенту (Уполномоченному лицу Клиента) работником Офиса Банка.

5.2.16.3. Не позднее рабочего дня, следующего за днем присвоения Логина, на Зарегистрированный номер телефона Клиента посредством SMS-сообщения высылается технический (временный) пароль, необходимый для первого входа в систему.

5.2.16.4. При первом входе в систему Клиент (Уполномоченное лицо Клиента) самостоятельно устанавливает Постоянный пароль.

5.2.16.5. Последующий вход в систему осуществляется исключительно с использованием Логина и Постоянного пароля.

5.2.16.6. В случае если для подписания ЭД необходимо две подписи, возможен вариант использования одним из Уполномоченных лиц Логина и пароля, а вторым – через стандартный (web) интерфейс Системы с помощью защищенного носителя.

5.2.17 Для получения доступа с помощью КЭП ФНС (при наличии технической возможности со стороны Банка и Клиента):

5.2.17.1. Клиент (Уполномоченное лицо Клиента) обращается в Банк с заявлением на регистрацию КЭП ФНС для работы в Системе (Приложение № 2 б к настоящим Правилам).

5.2.17.2. Клиент (Уполномоченное лицо Клиента) передает в Банк открытую часть ключа сертификата КЭП ФНС, которая подлежит регистрации в Системе.

5.2.17.3. После успешной регистрации сертификата ключа проверки КЭП ФНС в Системе, производится распечатка акта приема-передачи Сертификата КЭП ФНС по форме Приложения № 12 к Правилам в двух экземплярах, после чего указанные акты подписываются Владельцем сертификата и заверяются печатью организации (при наличии).

5.2.17.4. Обязательно предоставление в Банк актов приема-передачи сертификата ключа проверки КЭП ФНС на бумажном носителе с подписью Уполномоченного лица Клиента и печатью (при наличии).

5.2.17.5. Возможность работы Уполномоченного лица Клиента в Системе предоставляется не позднее двух рабочих дней после получения Банком оформленных должным образом актов приема-передачи сертификата ключа проверки КЭП ФНС.

5.2.17.6. Подписанные Сторонами акты приема-передачи сертификата ключа проверки КЭП ФНС Уполномоченного лица Клиента являются неотъемлемыми частями Соглашения.

5.3. **Условия отказа в заключении Соглашения.**

5.3.1. Отказ Клиенту в заключении Соглашения возможен по причине:

5.3.1.1. отказа в передаче Банку, Удостоверяющему центру и Оператору Системы персональных данных Уполномоченного лица Клиента;

5.3.1.2. имевшимся ранее фактам отключения Клиента от Системы по инициативе Банка по основаниям негативного характера: нарушение условий оплаты Услуг Банка за использование Системы, нарушению Правил и прочим;

5.3.1.3. наличия повышенных рисков Банка, связанных с использованием Системы Клиентом.

5.4. **Правила обмена электронными документами.**

5.4.1. Клиент допускается к использованию Системы круглосуточно. Возможно временное прекращение работы Системы для проведения регламентных, профилактических, иных работ суммарно не более чем на 3 (три) часа в сутки в рабочие дни и не более чем на 12 (двенадцать) часов — в выходные и праздничные дни. В отдельных случаях в выходные
и праздничные дни работа Системы может быть приостановлена на срок более 12 (двенадцати) часов с предварительным уведомлением Клиента не позднее 1 (одного) рабочего дня путем размещения информации на Сайте Банка либо иным способом извещения в соответствии с п.7.6 Правил, обеспечивающим возможность получения Клиентом указанной информации.

5.4.2. Проведение всех операций и получение всей информации в Системе осуществляется Клиентом в режиме online посредством сети Интернет во время сеансов связи с Системой.

5.4.3. Инициатором сеансов связи с Банком всегда является Клиент. Любая просрочка в выполнении Банком своих обязательств, которая произошла из-за отсутствия

инициативы Клиента в установлении сеанса связи с Банком, не влечет за собой ответственности Банка.

5.4.4. Все действия в Системе Клиент осуществляет в соответствии с документацией, инструкциями пользователя, размещенными на сайте www.faktura.ru.

5.4.5. Система может использоваться для обмена ЭД, в том числе Платежными ЭД, Неплатежными ЭД.

5.4.6. Оформление и содержание ЭД в Системе должно соответствовать документации, размещенной на сайте www.faktura.ru.

5.4.7. ЭД в Системе хранятся в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения ЭД составляет не менее 5 (пяти) лет.

5.4.8. Обмен ЭД в рамках Системы осуществляется в порядке и на условиях, определённых Правилами ЭДО КИС «BeSafe», Правилами работы Удостоверяющего центра «AUTHORITY» и Правилами сервиса «Faktura.ru». Правила определения лица, подписывающего электронный документ, по его ЭП/Простой ЭП определены Правилами ЭДО КИС «BeSafe».

5.4.9. ЭД признается полученным Стороной, которая получает ЭД с использованием Системы:

5.4.9.1. при отправке от Клиента Банку: с момента получения ЭД Банком;

5.4.9.2. при отправке от Банка Клиенту: с момента получения ЭД Клиентом.

5.4.10. Технология КИС «BeSafe» не позволяет направлять Клиенту ЭД с некорректной ЭП Банка.

5.4.11. Платежный ЭД в Системе может принимать следующие статусы:

5.4.11.1. «Подготовлен» — ЭС создано Уполномоченным лицом Клиента, обладающим соответствующими правами, но не отправлено в Банк; Уполномоченное лицо Клиента имеет право исправлять, удалять, отправлять в Банк ЭС, имеющее данный статус, при наличии соответствующих на это прав; ЭД, имеющие иные статусы, исправлению не подлежат;

5.4.11.2. «Подписан» — ЭД создан и подписан Уполномоченным лицом Клиента, наделенного правом подписи, и должен быть подписан следующим Уполномоченным лицом Клиента с правом подписи, если в соответствии с карточкой с образцами подписей и оттиска печати к Договору Счета/Депозита, требуется несколько подписей расчетных документов; Уполномоченное лицо Клиента, подписавшее документ, имеет право удалить ЭД, имеющий данный статус;

5.4.11.3. «Отправлен в банк» — ЭД подписан необходимым количеством ЭП и отправлен в Банк, но еще не получен Банком;

5.4.11.4. «Доставлен в банк» — ЭД физически доставлен в Банк;

5.4.11.5. «Принят банком» — ЭД получен Банком;

5.4.11.6. «Исполнен» — ЭД исполнен Банком; дата и время наступления безотзывности платежного ЭД указывается в примечании статуса «Исполнен»;

5.4.11.7. «Возвращен» — ЭД получен Банком, но не принят в обработку; Уполномоченное лицо Клиента, наделенное соответствующими правами, имеет возможность просмотреть в Системе причину возврата ЭД, указанную Банком;

5.4.11.8. «На подтверждении» — ЭД создан, но не отправлен в Банк, находится в ожидании подтверждения со стороны клиента;

5.4.11.9. «Пароль отправлен» — клиенту создан и отправлен одноразовый пароль для подтверждения ЭД;

5.4.11.10. «Ожидание» — ЭД подписан необходимым количеством ЭП и будет отправлен в Банк при наступлении заданных даты и времени.

5.4.12. Неплатежный ЭД в Системе может принимать следующие статусы:

5.4.12.1. «Подготовлен» — ЭС создано Уполномоченным лицом Клиента, обладающим соответствующими правами, но не отправлено в Банк; Уполномоченное лицо

Клиента имеет право исправлять, удалять, отправлять в Банк ЭС, имеющее данный статус, при наличии соответствующих на это прав; ЭД, имеющие иные статусы, исправлению не подлежат;

5.4.12.2. «Отправлен в банк» — ЭД подписан необходимым количеством ЭП и отправлен в Банк, но еще не получен Банком;

5.4.12.3. «Принят банком» — ЭД получен Банком;

5.4.12.4. «Возвращен» — ЭД получен Банком, но не принят в обработку частично (часть файлов из состава неплатежного ЭД - файлового архива) или полностью; Уполномоченное лицо Клиента, наделенное соответствующими правами, просматривает в Системе причины возврата ЭД и (или) списки возвращенных ЭД, указанные Банком.

5.4.13. Клиент самостоятельно получает информацию о статусе ЭД с использованием Системы.

5.4.14. При получении от Клиента ЭД Банк осуществляет проверку соответствия ЭП Клиента содержимому ЭД и в случае ее успешного завершения принимает ЭД к обработке.

5.4.15. ЭД обрабатывается Банком в операционное время, а в случаях предоставления дополнительной услуги о продлении операционного дня (проведение платежей по окончании операционного времени) — в предусмотренное Договором Счета время.

5.4.16. При обработке Банком ЭД осуществляется контроль правильности заполнения реквизитов в соответствии с законодательством Российской Федерации и нормативно--правовыми актами Банка России.

5.4.17. В случае выявления несоответствий в ходе проверки и (или) наличия иных оснований, препятствующих совершению операции по Счету, исполнение Платежного ЭД не проводится. При этом не позднее следующего рабочего дня Платежному ЭД устанавливается статус «Возвращен» с указанием причины отказа в исполнении Платежного ЭД.

5.4.18. В случае выявления несоответствий в ходе проверки и (или) наличия иных оснований, препятствующих его исполнению, исполнение Неплатежного ЭД не проводится. При этом не позднее следующего рабочего дня Неплатежному ЭД устанавливается статус «Возвращен».

5.4.19. Отзыв Платежного ЭД осуществляется в соответствии с порядком отзыва распоряжений на списание денежных средств со Счета предусмотренным Договором Счета/Депозита.

5.4.20. Отзыв Неплатежного ЭД осуществляется в соответствии с документацией Системы.

5.4.21. Датой и временем исполнения Платежного ЭД в Системе считается дата и время наступления безотзывности Платежного ЭД.

5.4.22. Не позднее рабочего дня, следующего за днем совершения операций по Счету, Банк посредством Системы выдает Клиенту выписку по Счету в ответ на запрос об ее предоставлении, направленный Уполномоченным лицом Клиента посредством Системы.

5.4.23. Банк направляет Клиенту уведомление о совершении каждой операции по Счету с использованием Системы путем уведомления об изменении состояния Платежного ЭД, доступного для просмотра в Системе, или путем выдачи выписки по Счету на бумажном носителе при обращении Клиента или его уполномоченного представителя в Офис банка не позднее рабочего дня, следующего за днем совершения операции по Счету. В случае если в течение рабочего дня, следующего за днем совершения операции, Клиент не осуществляет сеанса связи с Системой для просмотра состояния соответствующего Платежного ЭД или, если Клиент или его уполномоченный представитель не обратились в офис Банка за выпиской по Счету на бумажном носителе, уведомление, направленное Банком, считается полученным Клиентом в рабочий день, следующий за днем совершения операции.

5.4.24. В дополнение к информированию Клиента о совершении каждой операции с использованием Системы способом, предусмотренным п.5.4.23 Правил, Клиент вправе подать «Заявление о направлении дополнительной информации для обеспечения информационной безопасности работы в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №1 к Правилам, выбрав

предусмотренный(-ые) Банком способ(-ы) дополнительного уведомления о совершении каждой операции с использованием Системы, или воспользоваться дополнительной услугой SMS-информирования, Push-уведомлений.

5.5. **Порядок приостановки обслуживания Клиента в системе.**

5.5.1. Банк приостанавливает обслуживание Клиента в Системе в случаях:

5.5.1.1. получения от Клиента уведомления о компрометации Закрытого ключа в порядке, предусмотренном разделом 6 Правил;

5.5.1.2. прекращения для Уполномоченного лица Клиента действия прав подписи или Ограниченного доступа в Систему — в части доступа в Систему данного Уполномоченного лица Клиента;

5.5.1.3. возникновения технических неисправностей при работе с Системой — до их устранения;

5.5.1.4. не осуществления ежегодного планового перевыпуска Сертификата/КЭП ФНС Уполномоченного лица Клиента — в части доступа в Систему данного Уполномоченного лица Клиента;

5.5.1.5. предусмотренных Договором Счета/Депозита.

5.5.2. Банк имеет право приостановить обслуживание Клиента в Системе в случаях:

5.5.2.1. возникновения спорной ситуации, связанной с исполнением Соглашения — до разрешения спора;

5.5.2.2. нарушения действующих законодательных или иных правовых актов Российской Федерации и нормативных актов Банка России;

5.5.2.3. неисполнения Клиентом условий настоящих Правил, Правил КИС «BeSafe» или Правил сервиса «Faktura.ru»;

5.5.2.4. невозможности взимания платы в соответствии с Тарифами за обслуживание в Системе и совершение операций по Счету с использованием Системы ввиду недостаточности денежных средств на Счете Клиента по истечении двух месяцев с даты последней оплаты и направления требования Клиенту о погашении задолженности. Требование направляется устно либо в электронном виде (посредством Системы или электронной почты Клиента);

5.5.2.5. непредставления Клиентом документов по запросу Банка в случаях, предусмотренных Договором Счета/Депозита;

5.5.2.6. признания операции Клиента сомнительной/подозрительной, согласно п.8.4.9 настоящих Правил;

5.5.2.7. при выявлении операции, совершенной с использованием ЭСП, содержащегося в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента Банка России (далее – база), а также сведений федерального органа исполнительной власти в сфере внутренних дел о совершённых противоправных действиях Банк приостанавливает использование Клиентом ЭСП путем блокировки Сертификата ключа ЭП уполномоченного (-ых) сотрудника (-ов) организации. Приостановление использования Клиентом ЭСП производится на период нахождения указанных сведений в базе.

5.5.2.8. иных случаях, предусмотренных Договором Счета/Депозита.

5.5.3. Приостановка обслуживания Клиента в Системе не прекращает обязательств Сторон, возникших до момента приостановки обслуживания Клиента в Системе.

5.5.4. В случае приостановки обслуживания Клиента в Системе, а также в иных случаях невозможности предоставления услуг по Соглашению, обслуживание Клиента производится в порядке, установленном Договором Счета/Депозита.

6. **Порядок взаимодействия сторон в случае компрометации** ЭСП **и (или) использования электронного средства платежа без добровольного согласия Клиента.**

<u>В случае обнаружения компрометации ЭСП Клиентом:</u>

6.1. В случае Компрометации ЭСП Клиент обязан направить в Банк соответствующее уведомление. Уведомление может быть направлено путем:

6.1.1. устного обращения Клиента в Операционный отдел Банка с последующей обязательной подачей в Офис Банка соответствующего письменного заявления в следующем порядке:

6.1.1.1. Незамедлительно после обнаружения факта Компрометации ЭСП Клиент обращается в Операционный отдел Банка с соответствующим сообщением. При приеме сообщения Клиента по телефону Банк:

6.1.1.1.1. может вести аудиозапись разговора с Клиентом;

6.1.1.1.2. производит блокировку ЭСП, препятствующую совершению операций по Счету с использованием Системы при условии, что Банк имеет возможность установить, что сообщение исходит от Клиента, в том числе по кодовому слову, указанному Клиентом в «Заявлении о направлении дополнительной информации для обеспечения информационной безопасности работы в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №1 к Правилам;

6.1.1.1.3. при ведении аудиозаписи разговора фиксирует дату и время получения сообщения Клиента о Компрометации ЭСП путем озвучивания Клиенту текущей даты и времени по часам Системы, синхронизированным с серверами точного времени.

6.1.1.2. После обращения в Службу поддержки клиентов с сообщением о Компрометации ЭСП Клиент не позднее следующего рабочего дня должен подать в Офис банка «Заявление о блокировке ЭСП» по форме Приложения №6 к Правилам либо в свободной форме с указанием необходимой информации, подписанное лицом, наделенным правом подписи, и заверенное печатью в соответствии с Карточкой с образцами подписей;

6.1.1.3. После получения от Клиента «Заявления о блокировке закрытого ключа» в соответствии с требованиями п.6.1.1.2 Правил Банк считается должным образом уведомленным Клиентом о Компрометации ЭСП.

6.1.1.4. В случае, если Банк не получает от Клиента «Заявление о блокировке ЭСП» в соответствии с требованиями п.6.1.1.2 Правил, Банк не считается должным образом уведомленным Клиентом о Компрометации ЭСП, а обязанность Клиента направить указанное уведомление считается неисполненной. При этом Банк вправе произвести разблокировку ЭСП;

6.1.2. подачи Клиентом в Офис банка соответствующего письменного заявления в следующем порядке:

6.1.2.1. Незамедлительно после обнаружения факта Компрометации ЭСП Клиент подает в Офис банка, «Заявление о блокировке ЭСП» по форме Приложения №6 к Правилам либо в свободной форме с указанием необходимой информации, подписанное лицом, наделенным правом подписи, и заверенное печатью в соответствии с Карточкой с образцами подписей. При приеме заявления Клиента Банк:

6.1.2.1.1. производит блокировку ЭСП, препятствующую совершению операций по Счету с использованием Системы;

6.1.2.1.2. фиксирует в заявлении в качестве даты и времени его приема текущую дату и время по часам Системы, синхронизированным с серверами точного времени.

6.1.2.2. После получения от Клиента «Заявления о блокировке ЭСП» в соответствии с требованиями п.6.1.2.1 Правил, Банк считается должным образом уведомленным Клиентом о Компрометации ЭСП.

6.2. В случае неожиданного выхода из строя ЭУ или обнаружения вирусного заражения ЭУ, ЭСП Клиента считается скомпрометированным и Клиент обязан руководствоваться в своих дальнейших действиях главой 6 настоящего Правил, включая незамедлительное уведомление Банка о Компрометации в соответствии с п. 6.1.1.

6.3. Дальнейшее использование Клиентом компрометированного Закрытого ключа и/или Логина и Постоянного пароля Уполномоченного лица Клиента не допускается.

6.4. Банк проверяет наличие ЭД, поступивших в Банк на обработку с использованием Системы и не исполненных на момент поступления от Клиента уведомления о Компрометации ЭСП в порядке, предусмотренном п.6.1 Правил. В случае наличия указанных ЭД Банк прекращает их обработку с установкой для каждого из них статуса «Возвращен».

6.5. В случае обнаружения факта использования ЭСП (операций, совершенных с использованием ЭСП) Клиента без добровольного согласия Клиента, в дополнение к действиям, предписанным п.6.1:

6.5.1. Клиент обязан направить соответствующее уведомление путем подачи в Офис банка «Заявления об операции, совершенной без добровольного согласия клиента» по форме Приложения №7 к Правилам незамедлительно после обнаружения факта использования ЭСП без добровольного согласия Клиента, но не позднее рабочего дня, следующего за днем получения от Банка уведомления о совершенной операции способом, предусмотренным п.5.4.23 Правил.

6.5.2. Для сохранения доказательств использования ЭСП без добровольного согласия Клиента Клиенту необходимо строго соблюдать последовательность нижеизложенных действий, которые рекомендуется производить коллегиально и протоколировать:

6.5.2.1. Незамедлительно прекратить любые действия с ЭУ, используемыми для работы с Системой.

6.5.2.2. ЭУ перевести в режим «Гибернация» и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi и др.). В случае затруднения перевода ЭУ в режим гибернации — обесточить ЭУ (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь аккумуляторную батарею из ноутбука и т.п.).

6.5.2.3. Не предпринимать каких-либо действий для самостоятельного или с привлечением сторонних специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ.

6.5.2.4. Не отправлять ЭУ в сервисные службы для восстановления работоспособности.

6.5.3. Банк настоятельно рекомендует Клиенту:

6.5.3.1. незамедлительно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств;

6.5.3.2. незамедлительно обратиться в суд с исковым заявлением в отношении получателя денежных средств о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 Гражданского Кодекса Российской Федерации), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения.

6.5.4. Клиент не позднее следующего рабочего дня должен направить в Офис банка «Справку по факту инцидента информационной безопасности в системе дистанционного банковского обслуживания «Банк-клиент»» по форме Приложения №8 Правил с приложением документов, указанных в Приложении №9 к Правилам.

6.5.5. Для возобновления работы в Системе Клиент должен произвести настройку не используемого ранее ЭУ согласно требованиям Правил.

6.6. Возобновление работы в Системе Уполномоченного лица Клиента, Закрытый ключ и/или Логин и Постоянный пароль которого был(и) скомпрометирован(ы), производится после повторной подачи заявления по форме Приложения №2 или №2а к Правилам и прохождения указанным Уполномоченным лицом Клиента процедуры полной регистрации, предусмотренной в разделе 5.2 Правил.

6.7. Продолжение работы в Системе Уполномоченного лица Клиента, Закрытый ключ и/или Логин и Постоянный пароль которого не был(и) скомпрометирован(ы), допускается при отсутствии у Сторон оснований, допускающих использование ЭСП без добровольного согласия Клиента.

6.8 **В случае выявления Банком Клиента, по которому 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 ЭСП, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, Банк приостанавливает использование Клиентом ЭСП на период нахождения указанных сведений в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.**

При этом обслуживание счетов Клиента не приостанавливается. Распоряжения Клиента на перевод денежных средств принимаются на бумажных носителях, подписанные уполномоченным лицом (лицами) и заверенные оттиском печати Клиента в соответствии с карточкой с образцами подписей и оттиска печати, оформленной в Банке. Наличные денежные средства выдаются по денежному чеку, оформленному Клиентом.

После приостановления использования Клиентом ЭСП, Клиент вправе подать заявление в Банк России, в том числе через обслуживающий Банк об исключении его данных из базы, т.е. о разблокировке. В случае наличия у Банка оснований полагать, что включение сведений, относящихся к Клиенту и (или) его ЭСП в базу является необоснованным, Банк вправе самостоятельно (без участия Клиента) направить в Банк России мотивированное заявление об исключении сведений.

Мотивированное решение об удовлетворении или об отказе в удовлетворении заявления Клиента принимается в срок, не превышающий 15 рабочих дней. Решение об отказе в удовлетворении таких заявлений Клиент вправе обжаловать в суд в соответствии с законодательством Российской Федерации.

В случае выявления Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента:

6.9. При выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, Банк приостанавливает прием к исполнению распоряжения Клиента на два дня.

После введения ограничения на перевод Банк незамедлительно сообщает Клиенту следующую информацию любым доступным способом (по телефону, электронной почте, посредством системы Банк-Клиент):

- о приостановке выполнения операции по переводу денежных средств;
- о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия Клиента;
- о возможности подтвердить распоряжение не позднее одного дня, следующего за днём приостановления приёма к исполнению указанного распоряжения.

При предоставлении Клиенту информации в соответствии с п.6.8. Правил Банк вправе в дополнение к подтверждению запросить у Клиента дополнительную информацию, что перевод денежных средств не является переводом денежных средств без добровольного согласия Клиента, и (или) направить Клиенту информацию о необходимости совершить повторную операцию.

При получении подтверждения факта создания распоряжения непосредственно Клиентом, распоряжение исполняется Банком.

При неполучении от Клиента подтверждения распоряжения, указанное распоряжение считается не принятым к исполнению. Распоряжение возвращается Клиенту со статусом «Возвращен» с указанием причины отказа.

6.10. При выявлении операции, по которой получатель денежных средств находится в базе сведений Банка России и(или) федерального органа исполнительной власти в сфере внутренних дел о совершённых противоправных действиях Банк приостанавливает выполнение такой операции. После введения данного ограничения Банк незамедлительно сообщает Клиенту следующую информацию любым доступным письменным способом (по зарегистрированной электронной почте, посредством системы Банк-Клиент, заявления на бумажном носителе):

- о приостановке выполнения операции по переводу денежных средств;
- о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия Клиента;

• о возможности подтвердить распоряжение любым доступным письменным способом (по зарегистрированной электронной почте, посредством системы Банк-Клиент, заявления на бумажном носителе) не позднее одного дня, следующего за днём приостановления приёма к исполнению указанного распоряжения.

После получения вышеуказанного подтверждения Клиента, Банк приостанавливает прием к исполнению подтвержденного распоряжения на два дня со дня получения от Клиента подтверждения распоряжения (период охлаждения). Банк незамедлительно уведомляет Клиента о приостановлении приема к исполнению подтвержденного распоряжения с указанием причины такого приостановления и срока такого приостановления любым доступным способом (по телефону, электронной почте, посредством системы Банк-Клиент).

При неполучении от Клиента письменного подтверждения распоряжения, указанное распоряжение считается не принятым к исполнению. Распоряжение возвращается Клиенту со статусом «Возвращен» с указанием причины отказа.

7. Прочие условия.

7.1. Стороны осознают риски, возникающие при использовании Системы:

7.1.1. риск изготовления Закрытого ключа и Сертификата или выдачи Логина и временного пароля для доступа в систему на неуполномоченное лицо;

7.1.2. риск Компрометации Закрытого ключа;

7.1.3. риск Компрометации Логина и Постоянного пароля;

7.1.4. риск атаки на ЭУ, в том числе с использованием вредоносного кода с целью совершения операции без согласия Клиента;

7.1.5. риск утраты доказательств совершения мошенничества в случае обнаружения факта использования ЭСП без согласия Клиента.

7.2. Стороны минимизируют риски, связанные с использованием Системы, исполнением обязательных требований и следованием рекомендациям положений настоящего Правил, Правил КИС «BeSafe», Правил сервиса «Faktura.ru», а также Договора Счета/Депозита.

7.3. Клиент дает согласие на предоставление доступа Оператору Системы к банковской тайне Клиента, принимая во внимание, что настоящие Правила предусматривает конфиденциальность и неразглашение информации, которой обмениваются Стороны и Оператор Системы в рамках Системы.

7.4. Сторона, передающая персональные данные Уполномоченных лиц Стороны другой Стороне, Оператору Системы и Удостоверяющему центру во исполнение Соглашения, гарантирует получение согласия Уполномоченных лиц Стороны на обработку и передачу их персональных данных другой Стороне, Оператору Системы и Удостоверяющему центру. Сторона, получающая по Соглашению персональные данные Уполномоченных лиц другой Стороны, должна использовать их только в целях исполнения Соглашения, а также хранить конфиденциальность данной информации.

7.5. Стороны признают, что взаимодействие в рамках Системы не нарушает прав собственности Сторон в отношении информации, передаваемой с использованием Системы, а также не нарушает обязательств Сторон по неразглашению информации.

7.6. Сторона считается извещенной надлежащим образом любым из следующих способов:

7.6.1. со дня размещения информации на Сайте Банка;

7.6.2. со дня направления извещения с использованием Системы;

7.6.3. со дня получения извещения одной Стороной от другой Стороны;

7.6.4. по истечении 6 рабочих дней со дня направления извещения заказным письмом по почте;

7.6.5. со дня размещения для Клиента информации на стендах в помещениях Банка.

7.7. Во всем остальном, что прямо не предусмотрено Соглашением, Стороны руководствуются, действующим законодательством РФ и правовыми актами Банка России.

8. Права и обязанности Сторон.

8.1. **Взаимные права и обязанности Сторон.**

8.1.1. Стороны принимают на себя обязательства рассматривать всю информацию, полученную в ходе работы с Системой, как конфиденциальную, не подлежащую разглашению, и каждая Сторона отвечает за соблюдение данного требования с учетом п.п. 7.3, 7.4, 8.1.2 Правил. Обязательства соблюдения конфиденциальности указанной информации остаются в силе неограниченное время.

8.1.2. Банк освобождается от обязательств по сохранению конфиденциальности информации, передаваемой в сообщениях электронной почты и SMS-уведомлениях, Push-уведомлениях, направляемых Клиенту в порядке, предусмотренном Правилами.

8.1.3. При обмене ЭД с использованием Системы Стороны обязуются руководствоваться правилами и требованиями, установленными Банком России, действующим законодательством Российской Федерации, Правилами, Договором Счета/Депозита, Правилами КИС «BeSafe» и Правилами сервиса «Faktura.ru».

8.1.4. Стороны обязаны за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для проведения электронных расчетов в Системе и получения уведомлений, оплачивать услуги предоставления доступа в Интернет, электронной почты и мобильной связи.

8.2. **Клиент имеет право:**

8.2.1. Использовать Систему для осуществления обмена ЭД с Банком.

8.2.2. Получать по телефону техническую поддержку и консультации по вопросам использования Системы, обращаясь в Службу технической поддержки клиентов.

8.2.3. В целях разрешения проблемных ситуаций, связанных с использованием Системы, санкционировать удаленное подключение на просмотр сотрудником Службы технической поддержки клиентов к ЭУ Уполномоченного лица Клиента с использованием для этого технических средств (программного обеспечения), определенных Банком.

8.2.4. Изменить состав Уполномоченных лиц Клиента в порядке, предусмотренном разделом 5.2 Правил, подав в Офис банка «Заявление на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №2 к Правилам или «Заявление на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Банк-клиент» по форме Приложения №2а к Правилам.

8.3. **Клиент обязуется:**

8.3.1. Немедленно информировать Банк о прекращении полномочий Уполномоченного лица Клиента для своевременного блокирования Банком доступа в Систему и прекращения обработки ЭД (при их наличии), подписанных ЭП с использованием Закрытых ключей лиц, утративших на то полномочия. В случае отзыва доверенности на Уполномоченное лицо, временной невозможности исполнять полномочия, указанные в доверенности (по причине командировки, отпуска, болезни и т.д.) Клиент обязан информировать Банк незамедлительно с момента наступления указанного события путем направления Неплатежного ЭД либо подачей в Офис Банка соответствующего письменного извещения. Банк приостанавливает доступ Уполномоченного лица Клиента в Систему со дня получения указанного извещения. Все риски, связанные с невыполнением указанного требования и совершения действий в Системе неуполномоченными лицами несет Клиент.

8.3.2. При создании Платежного ЭД проверять корректность указания реквизитов распоряжения на списание денежных средств. Положительный результат проверки корректности реквизитов подтверждать созданием ЭП на ЭС.

8.3.3. Контролировать соответствие суммы платежа и остатка средств на Счете в течении операционного времени обслуживания и осуществлять платежи только в пределах этого остатка за исключением случаев предоставления Банком овердрафта по Счету Клиента, условия которого согласовываются Сторонами отдельно.

8.3.4. Предоставлять в Банк достоверные и актуальные сведения, необходимые для работы в Системе.

8.3.5. Самостоятельно обеспечить доступность и работоспособность канала доступа к сети Интернет, каналов получения уведомлений и разовых паролей, направляемых Клиенту при использовании Системы.

8.3.6. Осуществлять проверку исполнения Уполномоченными лицами Клиента требований Правилам и надежности хранения ими Ключевых носителей.

8.3.7. Не передавать третьим лицам права или обязанности, предусмотренные Соглашением, за исключением случаев, предусмотренных Правилами.

8.3.8. Повторно проходить процедуру полной регистрации в Системе Уполномоченного лица Клиента в случае изменения его персональных данных.

8.3.9. Ежегодно на основании уведомления Системы о приближении срока окончания действия Сертификата/КЭП ФНС самостоятельно инициировать процедуру плановой замены Закрытого ключа и перевыпуска Сертификата каждым Уполномоченным лицом Клиента.

8.3.10. Регулярно знакомиться с информацией и уведомлениями Банка, размещаемыми на Сайте Банка.

8.3.11. Регулярно проверять наличие и знакомиться с:

8.3.11.1. новой редакцией Правил, размещаемой на Сайте Банка;

8.3.11.2. новой редакцией Правил КИС «BeSafe», размещаемой на сайте https://besafe.ru/;

8.3.11.3. новой редакцией Правил сервиса «Faktura.ru», размещаемой на сайте https://faktura.ru/.

8.3.12. После расторжения Соглашения не передавать третьим лицам Закрытые ключи, Ключевые носители, конфиденциальные данные, относящиеся к Соглашению, и уничтожить все имеющиеся копии программного обеспечения, необходимые для работы в Системе.

8.3.13. Если при получении уведомления или запроса Банка, указанного в п.8.4.10 настоящих Правил, Клиентом будет установлено, что Платежный ЭД сформирован от его имени без согласия Клиента, последний обязан незамедлительно уведомить Банк о Компрометации Закрытого ключа в порядке, установленном разделом 6 настоящих Правил.

8.3.14. Просматривать в Системе причины возврата платежных\неплатежных ЭД и (или) списки возвращенных неплатежных ЭД, указанные Банком.

8.4. **Банк имеет право:**

8.4.1. Приостанавливать обработку ЭД, поступающих через Систему, для проведения регламентных, профилактических, иных работ суммарно не более чем на 3 (три) часа в сутки в рабочие дни и не более чем на 12 (двенадцать) часов — в выходные и праздничные дни.

8.4.2. В отдельных случаях в выходные и праздничные дни приостанавливать работу Системы на срок более 12 (двенадцати) часов с предварительным уведомлением Клиента не позднее 1 (одного) рабочего дня путем размещения информации на Сайте Банка.

8.4.3. В одностороннем порядке вносить изменения в Правила.

8.4.4. Самостоятельно определять порядок и условия обмена ЭД с Клиентом с использованием Системы, не противоречащие Правилам КИС «BeSafe» и Правилам сервиса «Faktura.ru».

8.4.5. Самостоятельно принимать решение о приостановке доступа Клиента в Систему в случаях выявления признаков нарушения безопасности, наличия информации о компрометации Закрытого ключа и подозрения на использование ЭСП без согласия Клиента.

8.4.6. В целях разрешения проблемных ситуаций, связанных с использованием Системы, осуществлять санкционированное Клиентом удаленное подключение на просмотр сотрудником Службы технической поддержки клиентов Банка к ЭУ Уполномоченного лица Клиента с использованием для этого технических средств (программного обеспечения).

8.4.7. Определять технические средства (программное обеспечение) пригодные и безопасные для использования в соответствии с п.8.4.6 Правил.

8.4.8. По своему усмотрению в рамках мер по управлению информационными и финансовыми рисками в случаях, когда непринятие мер может повлечь возникновение угрозы безопасности работы Системы, устанавливать для Платежных ЭД разовые и накопительные лимиты на сумму.

8.4.9. Отказать в проведении операции по Счету и/или приостановить исполнение распоряжения Клиента, а также приостановить проведение всех расчетов с использованием Системы:

а) в случаях выявления Банком сомнительной/подозрительной операции Клиента, при условии незамедлительного уведомления об этом Клиента посредством направления ему соответствующего ЭД;

б) в иных случаях, установленных Правилами, Договором Счета/Депозита и действующим законодательством Российской Федерации, уведомив об этом Клиента (посредством направления ему ЭД) не позднее следующего рабочего дня с момента наступления соответствующего события.

8.4.10. В случае возникновения подозрений об использовании ЭСП без согласия Клиента и в целях повышения безопасности работы в Системе, Банк вправе по своему усмотрению дополнительно запрашивать у Клиента подтверждение направления Клиентом поступившего в Банк Платежного ЭД.

8.4.11. Возвращать Клиенту Платежные/Неплатежные ЭД, при обработке которых:

- выявлены несоответствия в ходе проверки,
- либо выявлена отправка Неплатежного ЭД в виде Потенциально опасного файла или отправка в составе архива, содержащего вложенные архивы и (или) Потенциально опасные файлы,
- либо выявлены иные основания, препятствующие его исполнению.

8.5. **Банк обязуется:**

8.5.1. Осуществить регистрацию Уполномоченного лица Клиента в Системе в случае корректного заполнения заявлений и исполнения всех условий и требований, предусмотренных Правилами.

8.5.2. Обеспечивать бесперебойную обработку ЭД, полученных в Системе.

8.5.3. Фиксировать направленные Клиенту уведомления о совершении каждой операции с использованием ЭСП в порядке, предусмотренном п.5.4.23 Правил, а также хранить соответствующую информацию не менее 3 (трех) лет.

8.5.4. Обеспечить возможность направления Клиентом Банку уведомления о Компрометации Закрытого ключа в порядке, предусмотренном п.6.1 Правил.

8.5.5. Фиксировать полученные от Клиента уведомления о Компрометации ЭСП в порядке, предусмотренном п.6.1 Правил, а также хранить соответствующую информацию не менее 3 (трех) лет.

8.5.6. Приостановить использование Клиентом ЭСП в порядке, предусмотренном разделом 6 Правил, в случае получения от Клиента уведомления о компрометации ЭСП в порядке, предусмотренном п.6.1 Правил.

8.5.7. Заявления, полученные от Клиента в порядке, предусмотренном в п.6.5.1 Правил хранить не менее трех лет.

8.5.8. Рассмотреть Заявление о совершении операций без согласия Клиента (Приложение № 7 к Правилам) в течение 30 дней со дня получения

8.5.9. В течение 20 (Двадцати) рабочих дней предоставлять по запросу Клиента копии фрагментов журнала работы Клиента в Системе, относящихся к событиям, случившимся не ранее, чем за 3 (Три) года до момента предоставления указанного запроса, с указанием:

8.5.9.1. периода времени и Сертификата, с помощью которого осуществлялся доступ к Счетам Клиента в Системе и создавались ЭД;

8.5.9.2. отправленных Клиенту в рамках Системы SMS-сообщений.

8.5.10. Осуществлять по телефону техническую поддержку и консультирование Клиента по вопросам использования Системы по Телефонам Службы технической поддержки клиентов в Рабочее время Службы технической поддержки клиентов.

8.5.11. Незамедлительно посредством Системы уведомить Клиента о введении лимитов в соответствии с п.8.4.8 с подробным описанием условий и срока их действия, а также причин установления лимитов.

8.5.12. При расторжении с Клиентом Соглашения блокировать возможность использования в Системе Закрытых ключей и Сертификатов Уполномоченных лиц Клиента.

9. **Порядок расчетов.**

9.1. За обслуживание в Системе и совершение операций по Счету с использованием Системы Клиент уплачивает Банку комиссии в соответствии с Тарифами, действующими в Банке на дату совершения операции, а также условиями Договора Счета/Депозита.

9.2. Настоящим Клиент поручает Банку списывать со Счета Клиента плату за услуги, предоставляемые Банком по Соглашению с применением банковских ордеров или иных расчетных документов, предусмотренных нормативными документами Банка России.

9.3. Клиент должен ежемесячно обеспечивать наличие на Счете денежных средств, достаточных для оплаты Банку комиссии за услуги, предоставляемые Банком по Соглашению в соответствии с Тарифами.

10. **Ответственность.**

10.1. Каждая из Сторон несет ответственность за необеспечение сохранности, разглашение и распространение Закрытых ключей, кодовых слов, паролей и другой конфиденциальной информации, а также за их несанкционированное использование, и принимает на себя все риски, связанные с данными нарушениями.

10.2. Стороны несут ответственность за недостоверность информации, предоставляемой друг другу.

10.3. Банк не несет ответственности за задержку в формировании выписки по Счету Клиента, если она связана с задержкой получения Банком информации об исполнении перевода денежных средств оператором платежной системы или банком-корреспондентом по причинам, от Банка не зависящим.

10.4. Банк несет ответственность за несоблюдение сроков проведения расчетных операций по Счету Клиента на основании надлежащим образом оформленных и своевременно доставленных платежных ЭД в соответствии с Договором Счета/Депозита.

10.5. Банк не несет ответственности за неисполнение или ненадлежащее исполнение распоряжений Клиента, произошедшее из-за нарушения Клиентом порядка пользования Системой, условий Соглашения и иных обязательств, принятых им на себя в связи с подключением и использованием Системы, а также пользование Системой неуполномоченными лицами.

10.6. Каждая из Сторон несет ответственность по всем документам, подписанным электронной цифровой подписью уполномоченных ею лиц, как в период действия Соглашения, так и после прекращения его действия в соответствии с действующим законодательством Российской Федерации.

10.7. Ни одна из Сторон не несет ответственности за ущерб, возникший вследствие некачественного функционирования каналов связи, вне зависимости от причин.

11. **Порядок разрешения конфликтных ситуаций и споров.**

11.1. Заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом его ЭСП, рассматриваются Банком с направлением Клиенту письменного ответа в срок не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования ЭСП для осуществления трансграничного перевода денежных средств.

11.2. Все разногласия, споры и конфликтные ситуации, возникающие между Сторонами при исполнении Соглашения, разрешаются с учетом взаимных интересов путем переговоров и в

соответствии с положениями Правил, Правилами КИС «BeSafe» и Правилами сервиса «Faktura.ru».

11.3. Все споры, конфликтные ситуации и разногласия, связанные с совершением каких-либо действий, операций в рамках Правил или с использованием Системы, разрешаются Сторонами на основании данных Журнала системы в порядке, предусмотренном Правилами.

11.4. Заверенная выписка из Журнала системы, содержащая регистрацию событий в Системе, имеющих отношение к предмету спора предоставляется Оператором Системы по письменному запросу Банка.

11.5. В случае не достижения соглашения Сторон споры по Соглашению передаются на рассмотрение судебные органы в соответствии с действующим законодательством Российской Федерации.

12. Срок действия Соглашения и порядок его расторжения.

12.1. Соглашение вступает в силу с момента его подписания и действует в течение календарного года. Если ни одна из Сторон не заявит о своем желании расторгнуть Соглашение не позднее, чем за один месяц до окончания срока его действия, Соглашение автоматически продлевается на каждый последующий календарный год.

12.2. Клиент вправе в любое время расторгнуть Соглашение в одностороннем порядке, подав в Банк соответствующее письменное заявление. При этом Соглашение считается расторгнутым:

12.2.1. со следующего рабочего дня после получения Банком соответствующего заявления Клиента, в случаях, если в заявлении не указана дата его расторжения;

12.2.2. с даты, указанной в соответствующем заявлении Клиента, если она наступает позднее даты его получения Банком.

12.3. В случае, если у Клиента к Системе подключено несколько Счетов, закрытие Клиентом одного из указанных Счетов, влечет прекращение Банком дистанционного банковского обслуживания Клиента по данному Счету. Закрытие Клиентом последнего либо единственного Счета, подключенного к Системе, влечет автоматическое расторжение Соглашения.

12.4. Банк вправе в одностороннем порядке расторгнуть Соглашение в случае отсутствия у Банка технической возможности осуществления дистанционного банковского обслуживания Клиента,

а также в случае нарушения Клиентом существенных условий Соглашение, направив Клиенту соответствующее уведомление с указанием причин за 10 (десять) календарных дней до даты расторжения Соглашения. В целях Соглашения существенными признаются следующие условия:

- соблюдение Клиентом положений Правил КИС «BeSafe» и Правил сервиса «Faktura.ru»;
- соблюдение Клиентом п.5.1.12 Правил.

В иных случаях допускается расторжение Соглашения в порядке, предусмотренном действующим законодательством Российской Федерации.

12.5. Расторжение Соглашения не прекращает обязательств Сторон, возникших до момента расторжения Соглашения.

12.6. При расторжении Соглашения, уплаченные Клиентом комиссии возврату не подлежат.

Приложение № 1
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Заявление о направлении дополнительной информации для обеспечения информационной безопасности работы в системе дистанционного банковского обслуживания «Интернет Банк-Клиент»

_____
(Наименование Клиента)
_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,

просит ИКБР «ЯРИНТЕРБАНК» (ООО):

1. Направлять дополнительные уведомления о совершенных в Системе операциях на адрес электронной почты: _____

2. Установить другие защитные меры*:

☐ Установить лимит на сумму документа _____ _____
(цифрами) (прописью)

☐ Установить дневной лимит на сумму документов _____ _____
(цифрами) (прописью)

_____ _____ (_____)
(Должность руководителя) (Подпись) (Ф.И.О.)
М.П.

Дата составления «__» _____20__г.

Заполняется сотрудником БАНКА:
Данная заявка получена и проверена:
_____ _____ (_____)
(Должность) (Подпись) (Ф.И.О.)

Дата получения «__» _____20__г.

_____

*Устанавливаются после консультации со Службой технической поддержки клиентов, при наличии технической возможности.

Приложение 1а

Анкета о выявлении признаков осуществления перевода денежных средств без согласия Клиента

_____

Наименование организации/ФИО индивидуального предпринимателя/ ФИО лица, занимающегося в соответствии с законодательством Российской Федерации частной практикой

ИНН _____

№	Вопрос	Ответ	Уточнения
1	Считаете ли Вы необходимым ограничить IP-адрес(а) оборудования, с которого(ых) Банк уполномочен принимать платежные документы Вашей организации для дальнейшей обработки	Нет ☐ Да ☐ (если Да, то укажите эти адреса в следующей графе)	IP-адрес(а) _____ _____ _____
2	Считаете ли вы необходимым дополнительно согласовывать с Банком обработку платежных документов Вашей организации на сумму свыше указанной (согласование проводится посредством обмена электронными сообщениями по системе «Банк-Клиент» либо через мессенджер Яндекс.Мессенджер)	Нет ☐ Да ☐ (если Да, то укажите эту сумму в следующей графе)	Сумма свыше _____
3	Выберите способ согласования обработки платежных документов Вашей организации с Банком свыше суммы, указанной в предыдущем пункте	Обмен электронными сообщениями по системе «Банк-Клиент» ☐ Обмен сообщениями через мессенджер Яндекс.Мессенджер ☐	Номер (а) телефонов _____ _____ _____

_____ _____ (_____)

(Должность руководителя) (Подпись) (Ф.И.О.)

М.П.

Дата составления «__» _____20__г.

Заполняется сотрудником БАНКА:

Данная заявка получена и проверена:

_____ _____ (_____)

(Должность) (Подпись) (Ф.И.О.)

Дата получения «__» _____20__г.

Приложение № 2
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Заявление на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Интернет Банк-Клиент»

_____
(Наименование Клиента)
_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,
просит ИКБР «ЯРИНТЕРБАНК» (ООО) сертифицировать ключ проверки электронной подписи и ключ шифрования в системе «Интернет Банк-Клиент» для уполномоченного лица с указанными правами.

Ф.И.О. уполномоченного лица Клиента*_____
Основной тел. номер мобильной связи*[1]
□ SMS-пароль на вход (на основной тел. номер)
□ Уведомления о входе в систему на электронный адрес:
□ Доверенные IP-адреса[2] _____
□ Использовать действующий сертификат с правом доступа к счету № [3]_____,
принадлежащим Клиенту: _____
□ защищенный носитель серийный номер _____ получен

Номера счетов*	Распоряжение по счету, в том числе с правом создания и подписи Платежных и Неплатежных ЭД	Аннулирование прав
	□	□
	□	□
	□	□
	□	□
	□	□

Уполномоченное лицо Клиента*_____(_____)
(Подпись) (Ф.И.О.)

_____ _____(_____)
(Должность руководителя) (Подпись) (Ф.И.О.)
М.П. Дата составления «__» _____20__г.

Заполняется сотрудником БАНКА:
Данная заявка получена и проверена:
_____ _____ (_____)
(Должность) (Подпись) (Ф.И.О.)
Дата получения «__» _____20__г.

* Обязательно к заполнению.
[1] Используется для направления и запроса информации по вопросам использования Системы и обработки ЭД.
[2] Доступ в Систему с прочих IP-адресов будет заблокирован.
[3] Указать любой счет с правом доступа из Системы.

Приложение № 2а

к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Заявление на предоставление/изменение прав ограниченного доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Интернет Банк-Клиент»

_____

(Наименование Клиента)

_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,

просит ИКБР «ЯРИНТЕРБАНК» (ООО) сертифицировать ключ проверки электронной подписи и ключ шифрования в системе «Интернет Банк-Клиент» для уполномоченного лица с указанными правами.

Ф.И.О. уполномоченного лица Клиента*_____

Основной тел. номер для получения SMS** №_____

□ SMS-пароль на вход (на основной тел. номер)

□ Уведомления о входе в систему на электронный адрес:

□ Доверенные IP-адреса[1]_____

Использовать действующий сертификат с правом доступа к счету[2] №_____,

принадлежащим Клиенту: _____

□ защищенный носитель серийный номер _____ получен.

Номера счетов*	Ограниченный доступ в Систему[3]	Право создания сообщений	Аннулирование прав
	□	□	□
	□	□	□
	□	□	□
	□	□	□
	□	□	□

Уполномоченное лицо Клиента*_____(_____)

(Подпись) (Ф.И.О.)

_____ _____(_____)

(Должность руководителя) (Подпись) (Ф.И.О.)

М.П. Дата составления «__» _____20__г.

Заполняется сотрудником БАНКА:

Данная заявка получена и проверена:

_____ _____ (_____)

(Должность) (Подпись) (Ф.И.О.)

Дата получения «__» _____20__г.

_____

* Обязательно к заполнению.

** Обязательно к заполнению при неиспользовании Защищенного носителя [1] Доступ в Систему с прочих IP-адресов будет заблокирован.

[2] Указать любой счет с правом доступа из Системы.

[3] Заявление на предоставление прав Ограниченного доступа в Систему (просмотр получаемой из Банка информации, запрос выписки, создание электронного сообщения, прием электронного документа) заполняется при наличии только таких прав (без прав распоряжения денежными средствами).

Приложение № 2 б
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Заявление на распоряжение по счету/изменение прав доступа уполномоченного лица клиента в системе дистанционного банковского обслуживания «Интернет Банк-Клиент»

_____
(Наименование Клиента)
_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,
просит ИКБР «ЯРИНТЕРБАНК» (ООО) зарегистрировать квалифицированный сертификат ключа проверки КЭП ФНС в системе «Интернет Банк-Клиент» для уполномоченного лица с указанными правами.

Ф.И.О. уполномоченного лица Клиента*_____
Основной тел. номер мобильной связи*[1]
□ SMS-пароль на вход (на основной тел. номер)
□ Уведомления о входе в систему на электронный адрес:
□ Доверенные IP-адреса[2]_____
□ Использовать действующий сертификат КЭП ФНС с правом доступа к счету[3]

№ _____, принадлежащим Клиенту:
_____

Номера счетов*	Распоряжение по счету, в том числе с правом создания и подписи Платежных и Неплатежных ЭД	Аннулирование прав
	□	□
	□	□
	□	□
	□	□
	□	□

Уполномоченное лицо Клиента*_____(_____)
(Подпись) (Ф.И.О.)

_____ _____(_____)
(Должность руководителя) (Подпись) (Ф.И.О.)
М.П. Дата составления «__» _____20__г.

Заполняется сотрудником БАНКА:
Данная заявка получена и проверена:
_____ _____ (_____)
(Должность) (Подпись) (Ф.И.О.)
Дата получения «__» _____20__г.

_____

* Обязательно к заполнению.
[1] Используется для направления и запроса информации по вопросам использования Системы и обработки ЭД.
[2] Доступ в Систему с прочих IP-адресов будет заблокирован
[3] Указать любой счет с правом доступа из Системы.

Приложение № 3
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Требования и рекомендации по настройке электронного устройства Клиента для работы в Системе

1. Требования к операционной системе:

- Windows 7/8/10/11 x86, x64.
- Mac OS 10.14, 10.15 или 11

2. Требования к браузеру:

- Google Chrome (текущая версия установленным расширением Faktura.ru)
- Yandex (текущая версия установленным расширением Faktura.ru)
- Edge (текущая версия установленным расширением Faktura.ru)
- Safari (текущая версия).

3. Свойства браузера:

Закладка Дополнительно TLS 1.0 — включено, Использовать HTTP 1.1 через прокси-соединения — включено, Не сохранять зашифрованные страницы на диск — включено.
Закладка Безопасность: Выполнять сценарии элементов ActiveX, помеченных как безопасные — Включить, Скачивание подписанных элементов ActiveX — Предлагать, Запуск элементов ActiveX и модулей подключения — Включить, Разрешить метаобновление — Включить.

4. Требования к настройке брандмауэра (прокси-сервера):

Устанавливать исходящие соединения по 443 порту (TLS), а также загружать файлы размером более 1МБ.

5. Рекомендации к настройке брандмауэра (прокси-сервера):

Разрешить исходящие соединения на:
faktura.ru, TCP порты: 80, 443
www.faktura.ru, TCP порты: 80, 443
www.authority.ru, TCP порты: 80, 443
secure.authority.ru, TCP порты: 443
Запретить иные исходящие и входящие подключения.

6. Порядок настройки программного обеспечения.

Порядок настройки программного обеспечения производится в соответствии с «Инструкцией по подключению к системе», размещенной на Сайте Банка. Использование иного программного обеспечения или специфическая настройка ЭУ могут негативно сказываться на работоспособности Системы.

Приложение № 4
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

АГЕНТУ Удостоверяющего центра «AUTHORITY»
ИКБР «ЯРИНТЕРБАНК» (ООО)
/ в Удостоверяющий центр «AUTHORITY»

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:* _____ Уникальный номер запроса (только для удаленной выдачи):_____.

С Правилами *Электронного документооборота* корпоративной информационной *Системы «BeSafe» (далее - «Система «BeSafe»)***,** которые расположены в сети Интернет по адресу www.besafe.ru, ознакомлены, согласны и обязуемся выполнять.

Признаем, что получение документа, подписанного *Электронной подписью Участника Системы "BeSafe"* (далее - *«Участник»)***,** юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц *Участника* и оттиском печати *Участника***.** Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Ключ электронной подписи*, *Электронная подпись* и *Сертификат ключа проверки электронной подписи Участника* созданы в соответствии с Правилами *Системы «BeSafe»***.**

Реквизиты *Клиента*:

ФИО уполномоченного лица организации	
Наименование организации	
Контактный телефон	
E-mail	

Настоящим соглашаюсь с обработкой своих персональных данных ЗАО «Центр Цифровых сертификатов» и признаю, что персональные данные, заносимые в Сертификаты, относятся к общедоступным персональным данным.

_____(подпись уполномоченного лица организации)
_____(Ф.И.О. уполномоченного лица организации)

М.П. (если применимо)

принято *Агентом Удостоверяющего центра / Удостоверяющим центром:*

(полное наименование *Агента)*
_____ (дата)
_____ (подпись уполномоченного лица *Агента)*
_____ (ФИО уполномоченного лица *Агента)*

М.П.

Приложение № 5
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

АКТ ПРИЕМА - ПЕРЕДАЧИ *СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ*

"____" _____201__г.

Юридическое лицо _____, именуемое в дальнейшем *"Клиент"*, представленное своим уполномоченным лицом _____, с одной стороны, и ИКБР «ЯРИНТЕРБАНК» (ООО) , именуем(-ый)(-ая) в дальнейшем *"Агент"*, в лице _____, действующ(-его)(-ей) на основании _____, с другой стороны, в соответствии с Правилами работы *Удостоверяющего Центра* «AUTHORITY», составили настоящий Акт приема - передачи о следующем:

1. *Агент* произвел проверку данных *Клиента*, *Удостоверяющий центр* осуществил изготовление *Сертификата ключа проверки электронной подписи* (далее - *«Сертификат»*) и передал _____ *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* перед *Клиентом* выполнены в точном соответствии с Правилами работы *Удостоверяющего Центра* «AUTHORITY», претензий у *Клиента* не имеется.

От *Агента* (Банка, Компании)
_____ /
(подпись) (ФИО)

(дата подписи)

М.П.

От *Клиента*
_____ /
(подпись) (ФИО)

(дата подписи)

М.П. (если применимо)

Приложение № 6
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Заявление о блокировке ЭСП
в системе дистанционного банковского обслуживания «Интернет Банк-Клиент»

_____
(Наименование Клиента)
_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,

настоящим уведомляет о компрометации закрытого ключа, используемого в системе дистанционного банковского обслуживания «Интернет Банк-Клиент», в связи с обнаружением:

□ утраты закрытых ключей
□ утраты Логина и/или Постоянного пароля
□ доступа к защищенному носителю или в систему неуполномоченных лиц
□ наличия операции, совершенной без согласия Клиента

Прошу Вас считать скомпрометированными и заблокировать Закрытые ключи и/или Логин и Постоянный пароль, используемые в системе дистанционного банковского обслуживания «Интернет Банк-Клиент» Уполномоченным(-ми) лицом(-ами):

_____

_____

_____

_____ _____

(_____)

(Должность руководителя) (Подпись) (Ф.И.О.)

М.П. Дата составления «__» _____20__г.

Заявление от Клиента получил

_____ _____ _____ _____ _____

(Должность) (Подпись) (Ф.И.О.) (Дата) (Время)

Приложение № 7
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Заявление об операции, совершенной без согласия клиента
в системе дистанционного банковского обслуживания «Интернет Банк-Клиент»

_____
(Наименование Клиента)
_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,
настоящим уведомляет об обнаружении в выписке по счету
_____ операции, совершенной без согласия Клиента.

Реквизиты операции по переводу денежных средств:

Дата документа: _____

Номер документа: _____

Наименование плательщика: _____

ИНН плательщика: _____

Номер счета плательщика: _____

БИК банка плательщика: _____

Наименование банка плательщика: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

БИК банка получателя: _____

Наименование банка получателя: _____

Сумма документа: _____

Назначение: _____

_____

_____

_____ _____

(_____)

(Должность руководителя) (Подпись) (Ф.И.О.)

М.П. Дата составления «__» _____20__г.

Заявление от Клиента получил

_____ _____ _____ _____ _____

(Должность) (Подпись) (Ф.И.О.) (Дата) (Время)

Приложение № 8
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Справка по факту инцидента информационной безопасности в системе дистанционного банковского обслуживания «Интернет Банк-Клиент»

_____
(Наименование Клиента)
_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,

настоящим доводит дополнительную информацию по факту обнаружения операции, совершенной без согласия клиента «__» _____20__г.

Количество электронных устройств (ЭУ), настроенных для доступа в Систему:_____.

- Для доступа в Систему используются:
  - □ корпоративные ЭУ
  - □ личные ЭУ
  - □ ЭУ, находящиеся в общественном пользовании
- Для подписи документов используется:
  - □ Логин и Постоянный пароль
  - □ Закрытый ключ
- Периодичность смены пароля системы ДБО:_____
- □ соблюден порядок подготовки ЭУ к установке Системы в соответствии с Правилами
- ЭУ расположен и используется в помещении с доступом: □ свободным / □ ограниченным
- □ ЭУ размещен способом, не позволяющим производить визуальное наблюдение за экраном ЭУ и его клавиатурой
- используется программное обеспечение для работы в Системе: _____
  _____
- □ используется только лицензионное программное обеспечение
- □ операционная система и приложения обновляются _____
  (Периодичность)
- □ используется антивирусное программное обеспечение: _____
- □ антивирусное программное обеспечение обновляется _____
  (Периодичность)
- □ производится обмен сообщениями электронной почты на ЭУ
- □ используются средства сетевой защиты: _____
- □ на ЭУ запрещены входящие соединения из сети Интернет
- □ с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений операционной системы, программного обеспечения, в том числе антивирусного, число разрешенных сайтов составляет _____
- □ обеспечивается возможность доступа к ЭУ только уполномоченных лиц
- Ключевые носители хранятся _____
  (Место хранения)
- Уполномоченные лица в операционной системе наделены правами
  - □ пользователей
  - □ администраторов

- пароль на защищенный носитель состоит из ___ символов и содержит:
  - □ буквы в нижнем регистре
  - □ буквы в верхнем регистре
  - □ цифры
  - □ спецсимволы (например, !»№;%:?*()_+/ и т.п.)
- □ обеспечивается возможность доступа к защищенным носителям только уполномоченных лиц
- □ ведется аудит событий, регистрирующий возникающие ошибки работы операционной системы и приложений, вход пользователей и запуск программ
- □ отчуждаемые носители информации (флеш-накопители, дискеты, диски и т.п.) используются в среднем _____ для целей _____
  (Периодичность)
- Интернет на ЭУ используется для целей _____

  _____
- Иная информация, имеющая отношение к инциденту:

  _____

  _____

  _____

  _____
- По факту хищения денежных средств:
  - □ Клиент не намерен обращаться в правоохранительные органы.
  - □ Клиент намерен обратиться в правоохранительные органы.
  - □ Клиент обратился в правоохранительные органы. Заявление принято в _____

    _____
    (Район, округ, город, субъект федерации и иные идентифицирующие ОВД данные)
    _____ и зарегистрировано за № _____ в КУСП.
- О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелицензированного и контрафактного программного обеспечения в соответствии со статьей 146 УК Российской Федерации предупрежден.

_____ _____

(_____)

(Должность руководителя) (Подпись) (Ф.И.О.)

М.П. Дата составления «__» _____20__г.

Приложение № 9
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Перечень документов, которые Клиент предоставляет в Банк в случае выявления операции, совершенной без согласия Клиента

1. Копия лицензии на операционную систему ЭУ.
2. Копия счета или чека на приобретение операционной системы ЭУ.
3. Описание используемого программного обеспечения (перечень использованного лицензионного и нелицензионного программного обеспечения на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).
4. Копия договора на оказание услуг доступа в Интернет.
5. Описание организации доступа в сеть Интернет на рабочем месте.
6. Копия счета или чека на оказание доступа в сеть Интернет на повременной основе (при наличии).
7. Копия заявления в правоохранительные органы (при наличии).
8. Копия лицензии на антивирусное программное обеспечение.
9. Копия счета или чека на антивирусное программное обеспечение.
10. Описание антивирусной защиты рабочего места (наличие установленного на жестком диске ЭУ антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на ЭУ вредоносных программ).
11. Копия лицензии на СКЗИ КЭП ФНС.

Приложение № 10
к Правилам системы дистанционного банковского обслуживания
«Интернет Банк-Клиент»

СОГЛАШЕНИЕ
о **присоединении к системе дистанционного банковского обслуживания**
«Интернет Банк-Клиент»

г. Ярославль « ___ » _____ 20_

ИНВЕСТИЦИОННЫЙ КОММЕРЧЕСКИЙ БАНК РАЗВИТИЯ «ЯРИНТЕРБАНК» (ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ), базовая лицензия на осуществление банковских операций № 2564 именуемое в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____ именуемый в дальнейшем «Клиент», в лице _____ действующего на основании _____, с другой стороны, в дальнейшем совместно именуемые «Стороны», заключили настоящее Соглашение (далее — «Соглашение») о нижеследующем:

1. Стороны договариваются о дистанционном банковском обслуживании Клиента путем обмена документами в электронной форме, подписанными Электронной подписью, в соответствии с «Правилами системы дистанционного банковского обслуживания «Интернет Банк-Клиент», далее — «Правила».
2. Правилами определены условия оказания услуг по дистанционному банковскому обслуживанию «Интернет Банк-Клиент», требования к техническому и информационному обеспечению процессов формирования, обработки и хранения ЭД.
3. Подписанием Соглашения Клиент подтверждает, что полностью и безусловно присоединяется к Правилам, до подписания Соглашения ознакомлен с содержанием Правил, а также с Тарифами на расчетно-кассовое обслуживание корпоративных Клиентов ИКБР «ЯРИНТЕРБАНК» (ООО) в валюте РФ и Тарифами на расчетно-кассовое обслуживание корпоративных Клиентов ИКБР «ЯРИНТЕРБАНК» (ООО) в иностранной валюте, Правилами электронного документооборота корпоративной информационной системы «BeSafe», Правилами работы сервиса «Faktura.ru», Инструкцией по подключению к Системе и Инструкцией по перевыпуску сертификатов.*
4. Стороны определяют, что дистанционное банковское обслуживание Клиента осуществляется по всем счетам, открытым Клиентом в Банке.
5. По взаимному согласию Стороны определили, что право Электронной подписи ЭД имеют Уполномоченные лица, указанные в карточке с образцами подписей и оттиска печати, доверенности.
6. Соглашение составлено в двух идентичных экземплярах равной юридической силы — по одному для каждой Стороны.

БАНК: ИКБР «ЯРИНТЕРБАНК» (ООО) Место нахождения: 150000, г. Ярославль, ул. Собинова, д. 30 БИК 047888728, ИНН 7601000618, корреспондентский счет 30101810300000000728 в Отделении Ярославль г. Ярославль, БИК 047888728, ИНН 7601000618, КПП 760401001, ОГРН 1027600000075 _____	**КЛИЕНТ:** _____ (Сокращенное наименование, место нахождения, _____ ОГРН/ОГРНИП, ИНН, контактные телефоны) _____
_____ (Должность руководителя)	_____ (Должность руководителя подразделения)
_____ /_____/ (Подпись) (Ф.И.О.)	_____ /_____/ (Подпись) (Ф.И.О.)
М. П.	М. П.

* Правила, Тарифы на расчетно-кассовое обслуживание корпоративных Клиентов ИКБР «ЯРИНТЕРБАНК» (ООО) в валюте РФ и Тарифы на расчетно-кассовое обслуживание корпоративных Клиентов ИКБР «ЯРИНТЕРБАНК» (ООО) в иностранной валюте, Инструкция по подключению к Системе и Инструкция по перевыпуску сертификатов размещены на сайте https://www.yarinterbank.ru/. Правила электронного документооборота корпоративной информационной системы «BeSafe» размещены на сайте www.besafe.ru. Правила работы сервиса «Faktura.ru» размещены на сайте www.faktura.ru.

Приложение № 11
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

Заявление на предоставление Логина

_____
(Наименование Клиента)
_____,

именуем ____ в дальнейшем Клиент, в лице _____

_____,
просит ИКБР «ЯРИНТЕРБАНК» (ООО) предоставить Логин для входа в Мобильное приложение/в web
(ненужное зачеркнуть)

версию для просмотра уполномоченного лица: _____
и зарегистрировать телефонный номер указанного лица + 7 (____) _____-____-____ в качестве Зарегистрированного номера телефона для работы через Мобильное приложение/ web версию для просмотра.

Уполномоченное лицо Клиента _____ (_____)
(Подпись) (Ф.И.О.)

_____ _____(_____)
(Должность руководителя) (Подпись) (Ф.И.О.)

М.П. Дата составления «__» _____20__г.

Заполняется сотрудником БАНКА:
Данная заявка получена и проверена:

_____ _____ (_____)
(Должность) (Подпись) (Ф.И.О.)

Дата получения: «__» _____20__г.

Согласно заявления Клиента присвоен Логин:

_____ _____ (_____)
(Должность) (Подпись) (Ф.И.О.)

Дата присвоения логина: «__» _____20__г.

Приложение № 12
к Правилам системы дистанционного банковского обслуживания «Интернет Банк-Клиент»

АКТ ПРИЕМА - ПЕРЕДАЧИ *Квалифицированного сертификата ключа проверки КЭП ФНС*

"____" _____20__г.

_____, именуемое в дальнейшем *"Клиент",* представленное
(наименование организации)

своим уполномоченным лицом _____, являющимся владельцем
(ФИО владельца Сертификата КЭП ФНС)

Квалифицированного сертификата ключа проверки КЭП ФНС (далее - *«Сертификат КЭП ФНС»)* с одной стороны, и ИКБР «ЯРИНТЕРБАНК» (ООО), именуемый в дальнейшем «*Агент",* в лице _____, действующ(-его)(-ей) на основании _____, с другой
(ФИО представителя Банка)

стороны, составили настоящий Акт приема - передачи о следующем:

1. *Клиент* предоставил *Агенту* открытую часть ключа для регистрации *Сертификата КЭП ФНС* в Удостоверяющем центре.
2. *Агент* произвел проверку данных *Клиента и полномочий уполномоченного лица Клиента, Удостоверяющий центр* осуществил регистрацию *Сертификата КЭП ФНС* для доступа в Систему Интернет Банк-Клиент ИКБР «ЯРИНТЕРБАНК» (ООО).

Идентификатор *Владельца сертификата*

Номер *Сертификата*

Годен с

Годен до

Ключ проверки электронной подписи

3. Обязательства *Агента* перед *Клиентом* выполнены, претензий у *Клиента* не имеется.

От *Агента*
_____ /
(подпись) (ФИО)

От *Клиента*
_____ /
(подпись) (ФИО)

М.П. (если применимо)