

# РЕГЛАМЕНТ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ С ИСПОЛЬЗОВАНИЕМ СЕРВИСА FAKTURA.RU ЮРИДИЧЕСКИХ ЛИЦ, ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ, ФИЗИЧЕСКИХ ЛИЦ, ЗАНИМАЮЩИХСЯ В УСТАНОВЛЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ПОРЯДКЕ ЧАСТНОЙ ПРАКТИКОЙ В АО «БАНК 131»

## 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Регламенте дистанционного банковского обслуживания с использованием Сервиса Faktura.ru юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» (далее – Регламент) применяются термины и определения, указанные в Правилах комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» (и приложениях к ним), далее – Правила, если иное не указано в настоящем Регламенте.

**Альтернативный фактор подтверждения** – процедура дополнительного согласования Клиентом платёжных (расчётных) Электронных документов, отмеченных системой фрод-мониторинга Банка (FRAMOS) как подозрительные. Подтверждение выполняется способом, отличным от первичного (например, если документ подписан через SMS-код, альтернативным фактором выступает Сертификат).

**Аутентификационные данные** – Логин, Пароль, а также иные данные Клиента, используемые для доступа в Систему ДБО Faktura.ru.

**Владелец Сертификата** (Владелец Сертификата ключа проверки электронной подписи) – Представитель.

**Заявление** – Заявление о заключении договора комплексного банковского обслуживания АО «Банк 131»/Заявление об использовании в качестве Системы информационного обмена с АО «Банк 131» Системы ДБО Faktura.ru.

**Имитовставка** – последовательность данных фиксированной длины, вычисленная на основе сообщения и секретного (симметричного) ключа с целью обеспечения возможности обнаружения подмены и/или имитации сообщения. Позволяет обеспечить целостность электронного сообщения.

**Компрометация Электронной подписи** – наличие оснований полагать, что доверие к тому, что используемые ключи/средства Электронной подписи, Аутентификационные данные, Абонентский номер и/или сами Электронные подписи или их носители утрачены/доступны неуполномоченным лицам/могут быть использованы без согласия уполномоченных лиц.

**Корпоративная информационная система «BeSafe» (КИС «BeSafe»)** – система, организованная Закрытым акционерным обществом «Центр Цифровых Сертификатов» (ИНН 5407187087) и представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в Системе ДБО Faktura.ru в соответствии с «Правилами электронного документооборота корпоративной информационной системы «BeSafe».

**Клиент** – юридическое лицо (за исключением кредитных организаций), индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, обладающее полной право- и дееспособностью, обратившееся в Банк в собственных интересах, которому Банк оказывает услугу на разовой основе либо которое принимается на обслуживание, предполагающее длящийся характер отношений, при осуществлении банковских операций и других сделок, указанных в статье 5 Федерального закона "О банках и банковской деятельности", в рамках заключенного с Банком Договора Продукта, предусматривающего обмен Электронными документами, и присоединившееся к Правилам.

**Мобильная подпись** – технология, позволяющая обеспечивать целостность простых ЭД с помощью реализации механизма установки Имитовставки на простой ЭД на мобильном устройстве клиента.

**Мобильное приложение** – программное обеспечение для мобильного устройства (смартфона, планшета), разработанное Банком или по поручению Банка третьими лицами, предоставляющее Клиенту и/или Уполномоченному Представителю Клиента возможность удалённого доступа к функционалу Системы ДБО [Faktura.ru](http://Faktura.ru)

**Ответственный сотрудник** – сотрудник Банка, уполномоченный производить взаимодействие (включая обслуживание) с Клиентом на любом из этапов оказания услуг последнему, в том числе, уполномоченный на проведение идентификации Клиента и его уполномоченного Представителя, а также на прием от Клиента документов, в том числе Заявлений от уполномоченных Представителей Клиента, в целях регистрации, предоставления доступа и использования Системы ДБО Faktura.ru Клиентом и его уполномоченными Представителями.

**Положение Банка России от 31.01.2025 № 851-П** – Положение от 31.01.2025 № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

**Система дистанционного банковского обслуживания «ФАКТУРА.RU»** (Система ДБО Faktura.ru) – Система информационного обмена, обеспечивающая информационное и технологическое взаимодействие между Банком и Клиентом в рамках банковского обслуживания.

**Сертификат ключа проверки электронной подписи (Сертификат)** – Электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром.

**Система лимитов** – многоступенчатый механизм контроля максимальных разрешённых сумм исходящих операций в российских рублях (для валют – пересчёт по курсу ЦБ РФ), действующий в календарные сутки по часовому поясу МСК.

**Удостоверяющий Центр** – удостоверяющий центр «Authority», созданный Закрытым акционерным обществом «Центр Цифровых Сертификатов», который осуществляет изготовление Сертификатов ключей проверки электронных подписей для Клиентов с целью осуществления электронного документооборота в рамках КИС «BeSafe». Удостоверяющий центр осуществляет изготовление цифровых сертификатов в соответствии с «Правилами работы Удостоверяющего Центра (AUTHORITY)».

**УНЭП** – усиленная неквалифицированная электронная подпись, размещенная на ФКН Рутокен

**ФКН** – средство криптографической защиты информации, предназначенное для хранения Ключа ЭП. Выдается Клиенту на основании Акта приема-передачи ФКН Системы ДБО Faktura.ru (форма документа определена Приложением № 2 к настоящему Регламенту).

**Фрод-мониторинг (FRAMOS)** – автоматизированная система Банка, анализирующая операции на признаки осуществления перевода денежных средств без добровольного согласия Клиента или с согласия, полученного под влиянием обмана.

**ФинЦЕРТ** – Центр взаимодействия и реагирования Департамента информационной безопасности, являющийся структурным подразделением Банка России.

**Черные списки ФинЦЕРТ** – базы данных Банка России (по номерам счетов и ИНН) и бюллетени МВД РФ, содержащие сведения о случаях перевода денежных средств без добровольного согласия, используемые для автоматической блокировки доступа в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ.

**Федеральный закон от 27.06.2011 № 161-ФЗ** – Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

**Федеральный закон от 27.07.2006 № 152-ФЗ** – Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

ЭД – электронный документ.

ЭП – электронная подпись.

ЭСП – электронное средство платежа.

## 2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Регламент регулирует отношения, возникшие в процессе оказания Банком услуг в рамках Соглашения об осуществлении информационного взаимодействия с использованием Системы информационного обмена - Системы дистанционного банковского обслуживания Faktura.ru (Системы ДБО Faktura.ru) при подключении и использовании Клиентом и Уполномоченными Представителями Клиента Системы ДБО Faktura.ru и является соглашением между Банком и Клиентом, определяющим порядок и условия взаимодействия при выпуске и использовании ЭП в рамках указанной корпоративной информационной системы электронного документооборота.

2.2. Настоящий Регламент является неотъемлемой и составной частью Правил и Общих условий осуществления информационного взаимодействия с использованием Систем информационного обмена.

2.3. Для подключения Клиента к Системе ДБО Faktura.ru и ее использования последний должен присоединиться к Правилам (включая настоящий Регламент) и Общим условиям осуществления информационного взаимодействия с использованием Систем информационного обмена путем подписания Заявления.

2.4. Обмен ЭД между Банком и Клиентом с использованием Системы ДБО Faktura.ru осуществляется в рамках Правил (включая приложения к ним), приобретенных Клиентом продуктов и услуг Банка и их условий, а также иных заключенных между Банком и Клиентом сделок (если использование Системы ДБО Faktura.ru предусмотрено ими), а также при условии, что обслуживание Клиента может быть осуществлено с использованием Системы ДБО Faktura.ru.

2.5. Клиент признает, что используемая Система ДБО Faktura.ru является достаточной для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а используемые средства защиты информации, обеспечивающие разграничение доступа, шифрование, контроль целостности и формирование ЭП, являются достаточными для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых ЭД, обеспечения целостности информации, условий неотказуемости, неизменности, достоверности, отсутствия искажений, а также разрешения спорных ситуаций при условии соблюдения Сторонами мер безопасности, в том числе обеспечения Клиентом надлежащей защиты Клиентской части Системы ДБО Faktura.ru от несанкционированного доступа. При использовании Системы ДБО Faktura.ru Клиент/Представитель обязан соблюдать требования Инструкции по обеспечению информационной безопасности при работе в Системе ДБО Сервиса Faktura.ru, являющейся Приложением № 5 к настоящему Регламенту.

2.6. Подписание бланка Сертификата ключа проверки электронной подписи Клиентом означает взаимное признание Сторонами ЭП Клиента с момента регистрации ключа проверки ЭП Владельца Сертификата в Сервисе Faktura.ru, формирование сертификата и подтверждает получение Сертификата ключа проверки электронной подписи на бумажном носителе и/или в электронном виде посредством Сервиса Faktura.ru.

2.7. Клиент соглашается с тем, что ЭД Сторон, обмен которыми осуществляется в рамках Системы ДБО Faktura.ru, признаются ЭД, подписанными УНЭП /Мобильной подписью, и являются равнозначными документам на бумажных носителях, подписанными собственноручной подписью Клиента/Представителя и скрепленными печатью Клиента (при наличии), в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

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

2.9. Стороны признают в качестве единой шкалы времени при работе в Системе ДБО Faktura.ru местное время по месту расположения подразделения Банка, обслуживающего Клиента. Контрольным является время системных часов аппаратных средств Банка.

2.10. Клиент обязуется обеспечить допуск к работе и работу в Системе ДБО Faktura.ru только уполномоченных Представителей, с учетом ролей таких лиц при использовании Системы ДБО Faktura.ru.

2.11. Клиент осознает повышенный риск несанкционированного использования Системы ДБО Faktura.ru, включая компрометацию Ключей ЭП и несанкционированное удаленное управление Системой ДБО Сервиса Faktura.ru, при ненадлежащем соблюдении Клиентом мер безопасности.

2.12. Используя Систему ДБО Faktura.ru, Клиент приобретает возможность:

1. Формировать, подписывать ЭП и направлять в Банк расчетные (платежные) документы, в соответствии с законодательством Российской Федерации, в целях совершения операций по открытым в Банке Счетам Клиента;
  2. Формировать, подписывать ЭП и направлять в Банк распоряжения на отзыв платежных (расчетных) документов, ранее переданных в Банк;
  3. Получать от Банка выписки по Счету(-ам) в виде ЭД, содержащие информацию об операциях, совершенных по открытому(-ым) в Банке Счету(-ам) Клиента;
  4. Формировать, направлять и получать в/от Банка информацию свободного формата в виде ЭД (в том числе служебно-информационных сообщений), согласно функционально-техническим возможностям Системы ДБО Faktura.ru;
  5. Формировать, подписывать ЭП, направлять и получать в/от Банка ЭД, в соответствии с Правилами, приобретенными Клиентом продуктами и услугами Банка, а также в соответствии с условиями отдельных заключенных Сторонами сделок (если использование Системы ДБО Faktura.ru предусмотрено последними);
  6. Формировать, подписывать ЭП и направлять в Банк заявления (если это предусмотрено Правилами и при наличии технической возможности);
  7. Подтверждать платёжные документы, находящиеся в статусе «Требует подтверждения», с использованием Альтернативного фактора подтверждения;
  8. Настраивать и контролировать суточные лимиты операций через интерфейс Системы, при наличии технической возможности и соответствующих настроек Банка.
- 2.13. При получении ЭД Банк производит процедуры приема к исполнению, отзыва, возврата (аннулирования) платежного (расчетного) документа, в соответствии с Банковскими правилами, в том числе проверку:
1. Права распоряжения денежными средствами (проверка ЭП, запрос по отдельным платежам Клиента дополнительного подтверждения);
  2. Контроль целостности (неизменности) реквизитов платежного (расчетного) документа;
  3. Структурный контроль (проверка установленных реквизитов и максимального количества символов в реквизитах платежного (расчетного) документа);
  4. Контроль значений реквизитов;
  5. Контроль достаточности денежных средств. При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный ЭД Системой ДБО Faktura.ru не принимается и данный результат (ЭД) автоматически направляется Клиенту, а поручение, содержащееся в нем, Банком не исполняется.
- 2.14. Для проведения расчетных операций с использованием Системы ДБО Faktura.ru в обязанности Клиента входит соблюдение требований к программно-техническим средствам, определенным Приложением № 6 к настоящему Регламенту.
- 2.15. При получении ЭД Банк производит проверку УНЭП или Мобильной подписи. Проверка выполняется аппаратно-программным комплексом Банка в момент подписания Клиентом/Представителем документов в Системе ДБО Faktura.ru. При положительном результате проверки ЭД переходит из статуса «Новый» в статус «На исполнении». При отрицательном результате проверки ЭД переходит в статус «Отвергнут». Обеспечение проверки защищенного доступа к Системе ДБО Faktura.ru достигается применением защищенного протокола SSL/TLS в процессе установления соединения между web-сервером банка и Клиентом. Для подтверждения подлинности web-сервера выполняется сравнение доменного имени загружаемого web-сервера с указанным в сертификате. Протокол SSL/TLS используется в форме протокола https (прикладной протокол http поверх криптографического протокола SSL/TLS).
- 2.16. Формат ЭД определяется функционально-техническими возможностями Системы ДБО Faktura.ru, экранной формы клиентской части Системы ДБО Faktura.ru. Каждый ЭД, направляемый Клиентом в Банк с использованием Системы ДБО Faktura.ru, должен содержать ЭП Клиента/Представителя. ЭП Клиента/Представителя, содержащаяся в ЭД Клиента, подтверждает авторство Клиента/Представителя и является средством проверки неизменности содержания ЭД, так как любое изменение ЭД, после его подписания ЭП, нарушает целостность ЭП.
- 2.17. ЭД должен быть подписан ЭП только Клиента/Представителя, имеющего право распоряжения денежными средствами на Счете (для платежных (расчетных) ЭД), данные о которых указаны в Заявлении /Заявлении на приобретение/изменение продукта. Если ЭД должен быть подписан несколькими подписями Представителей, в соответствии с Заявлением /Заявлением на приобретение/изменение продукта, /Карточкой с образцами подписей и оттиском печати, и

Соглашением о сочетании подписей к Карточке с образцами подписей и оттиском печати, ЭД должен быть подписан каждым из уполномоченных Представителей, согласно вышеуказанным документам, по одной ЭП из первой и второй группы подписей.

2.18. Система ДБО Faktura.ru автоматически отображает сведения о текущем этапе обработки Клиентом и/или Банком ЭД, посредством присвоения ЭД определенного статуса и его изменения.

2.19. Система присваивает ЭД следующие статусы:

1. «В картотеке» – присваивается ЭД, если при обработке платежа на счете Клиента оказалось недостаточно средств для совершения операции.
2. «Новый» – присваивается при создании и сохранении нового ЭД Клиентом.
3. «На исполнении» – присваивается ЭД при прохождении процедуры приема к исполнению, в том числе при запросе Банком от Клиента подтверждения совершаемой операции в случае использования УНЭП или Мобильной подписи.
4. «На обработке» – присваивается ЭД после его принятия к исполнению Банком.
5. «Исполнен» – присваивается ЭД после его исполнения Банком (в том числе после списания денежных средств со Счета Клиента на основании данного документа).
6. «Отвергнут» – присваивается ЭД, если он не может быть принят к исполнению в Банке. Для уточнения причины необходимо обратиться в Банк любым доступным Клиенту способом.
7. «Требуется подтверждения» – присваивается платёжному документу, отмеченному системой фрод-мониторинга (FRAMOS) как подозрительный и требующему дополнительного подтверждения с использованием Альтернативного фактора.

2.20. Созданный и подписанный ЭП ЭД Клиент отправляет в Банк с использованием Системы ДБО Faktura.ru.

2.21. Банк осуществляет проверку полученного от Клиента ЭД и принимает его к исполнению при условии положительного результата проверки, в том числе положительного результата всех процедур контроля, предусмотренных пунктами 2.14, 2.16 настоящего Регламента.

2.22. Результат проверки ЭД считается положительным, если он:

1. Оформлен в соответствии с действующим законодательством Российской Федерации;
2. Оформлен в соответствии с нормативными документами Банка России и требованиями Банка;
3. Оформлен в соответствии с требованиями, установленными заключенными Сторонами сделками, в соответствии с Правилами, включая положения настоящего Регламента;
4. Подписан надлежащей (надлежащими) ЭП Клиента/Представителя(-ей), имеющего(-их) право на распоряжение денежными средствами на Счете (для платежных (расчетных) ЭД), ЭП прошли проверку в Банке.

2.23. Клиент может отозвать переданный в Банк ЭД, в соответствии с требованиями законодательства Российской Федерации, заключенных Сторонами сделок, правилами совершения операций, с использованием Системы ДБО Faktura.ru. Отзываны могут быть только неисполненные ЭД, которые не дошли до статуса «Исполнен». Если запрос на отзыв исполнен, ЭД присваивается статус «Исполнен». В случае невозможности исполнения запроса на отзыв, ЭД вернется статус, в котором он находился до обработки Банком запроса на отзыв.

2.24. Клиент самостоятельно контролирует (отслеживает) этапы и результаты обработки отправленных в Банк ЭД в соответствующих разделах Системы ДБО Faktura.ru.

2.25. Банк и Клиент обмениваются по Системе ДБО Faktura.ru следующими ЭД:

1. платежные поручения;
2. запросы на отзыв документа;
3. выписки, содержащие информацию о движении средств по счетам;
4. документы для совершения валютных операций (заявления на перевод иностранной валюты, распоряжения на покупку/продажу валюты и т.п.);
5. документы валютного контроля;
6. иные платежные (расчетные) документы, применимые в рамках предусмотренных законодательством Российской Федерации и заключенных между Сторонами сделок форм безналичных расчетов (в соответствии с функциональными и техническими возможностями Системы Сервиса Faktura.ru);
7. произвольные документы (иные документы или письма, составленные в произвольной форме).

2.26. Все платёжные операции в Системе ДБО Faktura.ru подлежат проверке на соответствие установленным лимитам, которые действуют на нескольких уровнях приоритета (от высшего к низшему):

- уровень сотрудника;
- уровень организации;
- уровень Системы.

Лимиты распространяются на операции, инициированные с использованием Сертификата (в файле или на смарт-ключе) и при входе по Логину/Статическому паролю.

Лимиты не применяются при использовании устройства SafeTouch.

Операции классифицируются по уровню риска:

- **Запрещённые** – с запрещённых IP-адресов и на запрещённые счета;
- **Безрисковые** – на свои счета, в бюджет, в пользу банков (не проходят дополнительный контроль);
- **Оплата услуг** – совершенные через систему «Город» (могут быть отмечены как рискованные при превышении лимита);
- **Рисковые** – другие рублёвые и валютные платежи в пользу физических и юридических лиц.

Для рискованных операций автоматически определяется группа риска (Низкий, Средний, Высокий, Очень высокий) на основе:

- канала доступа (web-приложение, мобильный браузер, мобильное приложение);
- способа подписания (УНЭП/Мобильная подпись);
- типа получателя (физическое/юридическое лицо).

При превышении суточного лимита платёжный документ не отправляется на исполнение, а Клиент получает соответствующее уведомление.

2.27. Платёжные документы, отмеченные системой фрод-мониторинга (FRAMOS) как подозрительные, переводятся в статус «Требуется подтверждение». Для подтверждения такого документа Клиент обязан использовать способ подписания, отличный от первичного (Альтернативный фактор подтверждения). Попытка подтверждения тем же способом блокируется Системой.

2.28. Представителю может быть предоставлен доступ с правом просмотра и получения Электронных документов без права распоряжения. Клиент самостоятельно осуществляет контроль за соблюдением уполномоченными Представителями Клиента ограничений полномочий последних, неся при этом ответственность перед Банком и иными третьими лицами, а также риск возникновения неблагоприятных последствий, в том числе имущественного характера, при ненадлежащем исполнении указанной обязанности и(или) ее неисполнении.

### **3. ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ**

3.1. Порядок регистрации Клиента/Представителя в Системе ДБО Faktura.ru:

3.1.1. Под регистрацией понимается внесение в реестры Сервиса Faktura.ru регистрационной информации на основании Заявления и/или Заявления на приобретение/изменение продукта.

3.1.2. При приеме Заявления в офисе Банка Ответственный работник идентифицирует Клиента/Представителя с использованием документов, удостоверяющих личность, и документов, подтверждающих полномочия. Банк вправе отказать в приеме Заявления без объяснения причин такого отказа. Отказ в приеме Заявления влечет отказ в регистрации Уполномоченного Представителя Клиента в Системе ДБО.

3.1.3. При выборе Клиентом метода работы с использованием Мобильной подписи Ответственный работник направляет на указанный адрес электронной почты ссылку для прохождения саморегистрации.

3.1.4. При выборе Клиентом метода работы в Системе ДБО Faktura.ru. с использованием УНЭП, хранящейся на ФКН, Ответственный работник передает должным образом упакованный ФКН Уполномоченному Представителю Клиента.

Факт передачи ФКН, а также целостность упаковки подтверждается собственноручной подписью Уполномоченного Представителя Клиента в Акте приема-передачи ФКН Системы ДБО Faktura.ru.. Форма Акта определяется Банком в Приложении №2 к настоящему Регламенту. В случае нарушения целостности упаковки ФКН Уполномоченный Представитель Клиента должен указать об этом в Акте. При отсутствии соответствующей отметки в Акте, Стороны определили считать целостность упаковки ФКН не нарушенной, а сам ФКН надлежащим образом полученным уполномоченным Представителем Клиента.

3.1.5. Клиент/Представитель считаются подключенным к Системе ДБО Faktura.ru. с момента выполнения действий, содержащихся в п. 2.3. Регламента, а также с момента регистрации в Сервисе Faktura.ru.

3.2. Порядок смены и восстановления Логина и Статического пароля.

3.2.1. Клиент/Представитель может самостоятельно изменить Логин и Статический пароль в Системе.

Восстановление пароля в дистанционном режиме осуществляется без участия сотрудников Банка через ссылку «Забыли пароль?» на странице авторизации или в Мобильном приложении.

Для восстановления Клиент обязан:

1. Ввести Логин и ИНН организации (10 или 12 символов);
2. Ввести Одноразовый пароль из SMS-сообщения;
3. Указать дополнительную информацию: кодовое слово и/или третью группу цифр корпоративной карты (в зависимости от настроек Банка);
4. Дважды ввести новый пароль.

При трёхкратном неверном вводе кодового слова процедура приостанавливается, а Логин блокируется. Разблокировка возможна только при личном обращении в Банк с предоставлением документов, удостоверяющих личность и полномочия и заполнением соответствующего заявления.

3.3. Порядок смены Абонентского номера:

- Для изменения Абонентского номера Уполномоченный Представитель Клиента обращается в офис Банка с соответствующим заявлением;
- Дистанционная смена возможна при наличии полномочий подписывать документы, необходимые для изменения условий использования Системы ДБО Faktura.ru;
- Дистанционная смена невозможна в случае Компрометации Электронной подписи.

3.4. Смена Логина, Статического пароля, Абонентского номера, а также разблокировка доступа в Систему ДБО Faktura.ru через офис Банка производится при условии невозможности выполнить действия, предусмотренные п. 3.2., п. 3.3. настоящего Регламента, с учетом предъявления Клиентом/Представителем Заявления о смене Логина и Статического пароля/разблокировке доступа в Систему ДБО Faktura.ru/смене Абонентского номера, оформляемого по форме Банка (Приложение № 1 к настоящему Регламенту).

3.5. В случае возникновения необходимости осуществить смену номера мобильного телефона сотрудника Клиента, уполномоченного на взаимодействие с Банком в рамках защиты платежей от несанкционированных переводов, Клиентом/Представителем посредством Системы ДБО Faktura.ru оформляется Заявление о замене мобильного телефона для направления одноразовых паролей и информирования о совершении операций (форма представлена в Приложении № 3 к настоящему Регламенту). В случае невозможности совершить смену номера мобильного телефона в дистанционном режиме, смена номера мобильного телефона возможна в офисе Банка.

#### **4. ПОРЯДОК ВЫПУСКА СЕРТИФИКАТОВ ПРОВЕРКИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ**

4.1. Для получения Сертификата ключа проверки электронной подписи<sup>1</sup> каждый Клиент/Представитель Клиента должен лично:

1. создать Сертификат с помощью средств Faktura.ru;
2. подписать и направить в Банк сканированную копию Сертификата на адрес электронной почты Банка dbo@131.;

<sup>1</sup> Форма Сертификата должна соответствовать требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»

3. предоставить оригинал Сертификата на бумажном носителе в течение 5 (Пяти) рабочих дней.
- 4.2. При поступлении в Банк запроса на активацию Сертификата ключа проверки электронной подписи в электронном виде, Ответственный работник Банка сверяет данные, содержащиеся в указанном запросе в электронном виде с данными, указанными в запросе, представленном Клиентом на электронный почтовый ящик [dbo@131.ru](mailto:dbo@131.ru). и завершает формирование ЭП,
- 4.3. При положительном результате проверки Банк активирует Сертификат, предоставляя доступ Клиента/Представителю в Систему Сервиса Faktura.ru
- 4.4. По окончании активации Клиент/Представитель Клиента получает возможность использовать УНЭП.
- 4.5. Каждому Представителю необходимо отдельно создать Сертификат.
- 4.6. Сертификат подлежит отзыву в случае компрометации или получения нового Сертификата.
- 4.7. Срок действия Сертификата составляет один календарный год с даты начала его активации Банком. Сертификат действует в пределах срока должностных полномочий Владельца Сертификата.
- 4.8. Клиент обязан самостоятельно контролировать срок действия Сертификата и своевременно (не менее чем за 10 календарных дней до окончания срока действия) совершать процедуру смены Сертификата, с последующим предоставлением в Банк (в сроки, установленные п. 4.1. настоящего Регламента) Сертификата.

## 5. ПОРЯДОК ИСПОЛЬЗОВАНИЯ МОБИЛЬНОЙ ПОДПИСИ

- 5.1. Мобильная подпись предоставляется в качестве альтернативы Одноразовым паролям (СМС/PUSH) для Клиентов, использующих авторизацию по Логину/Статическому паролю.
- 5.2. Мобильная подпись выпускается и управляется исключительно в Мобильном приложении Faktura.ru для ОС Android (версия 11.0 и выше).
- 5.3. Для выпуска и использования Мобильной подписи на устройстве Клиента должны быть активированы:
- биометрические данные (TouchID/FaceID) или
  - код разблокировки устройства.
- 5.4. Самостоятельное подключение доступно после авторизации в Мобильном приложении и подтверждения операции Одноразовым паролем для регистрации открытого ключа.
- 5.5. Режимы использования Мобильной подписи настраиваются Банком:
1. **Отключён** – подтверждение выполняется через SMS/PUSH;
  2. **Мягкий режим** – Клиенту предлагается подключить Мобильную подпись, но сохраняется возможность использования SMS/PUSH;
  3. **Строгий режим** – Клиенту отображается обязательное требование подключения. Без подключения подтверждение платёжных документов через SMS/PUSH становится недоступным.
- 5.6. Срок действия сессии подтверждения. После успешной авторизации через биометрию/код разблокировки Клиент может подтверждать документы без повторного ввода биометрических данных в течение 1 (Одного) часа. По истечении указанного срока потребуются повторное подтверждение. Время на подтверждение каждой операции ограничено 5 минутами.
- 5.7. **Групповое подписание.** Мобильная подпись поддерживает групповое подписание платёжных поручений в Мобильном приложении.
- 5.8. **Имитовставка.** Для обеспечения целостности и безопасности электронного сообщения при использовании Мобильной подписи применяется имитовставка в соответствии с требованиями Положения Банка России от 30.01.2025 № 851-П.

---

## 6. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

- 6.1. За 30 (Тридцать) дней до окончания срока действия Сертификата Система Faktura.ru сообщает о скором его окончании.
- 6.2. До истечения срока действия Клиент/Представитель имеет возможность провести плановую процедуру смены Ключей Электронной подписи.
- 6.3. Клиент/Представитель формирует новый Ключ Электронной подписи и Сертификат, подписывает его действующим ключом и направляет в Банк.
- 6.4. При поступлении обновленного Сертификата Ответственный работник обрабатывает запрос на активацию.
- 6.5. Банк осуществляет активацию Сертификата. В случае отказа Клиент/Представитель вправе лично обратиться в Банк.
- 6.6. После завершения процедуры смены Ключа Электронной подписи Клиент/Представитель может использовать исключительно новый Ключ.
- 

## **7. ПОРЯДОК БЛОКИРОВКИ И ВОССТАНОВЛЕНИЯ ДОСТУПА К СИСТЕМЕ ДБО FAKTURA.RU**

7.1. Основанием для блокировки доступа являются:

- 7.1.1. Получение Банком Заявления на приобретении/изменения продукта;
- 7.1.2. Компрометация ЭП;
- 7.1.3. Замена Карточки с образцами подписей;
- 7.1.4. Прекращение или изменение полномочий Клиента/Представителя;
- 7.1.5. Смена Абонентского номера;
- 7.1.6. Утрата Аутентификационных данных без признаков Компрометации;
- 7.1.7. Непредставление или представление недостоверных сведений;
- 7.1.8. Выявление Банком или автоматической системой мониторинга (FRAMOS) операций, соответствующих признакам осуществления перевода денежных средств без добровольного согласия Клиента, а также наличие сведений о Клиенте (его счетах или ИНН) в Черных списках Банка России или бюллетенях МВД РФ (в соответствии с требованиями Федерального закона от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон "О национальной платежной системе" и статьей 9 № 161-ФЗ);
- 7.1.9. Направление Клиентом Заявления о приостановлении/возобновлении обслуживания в Системе дистанционного банковского обслуживания Faktura.ru (по форме Приложения № 4 к настоящему Регламенту).

7.2. Основанием для восстановления доступа к Системе ДБО Faktura.ru уполномоченным лицам Клиента является передача посредством Системы ДБО Faktura.ru в Банк Заявления о приостановлении/возобновлении обслуживания в Системе ДБО Faktura.ru (по форме Приложения № 4 к настоящему Регламенту).

**7.3. Блокировка по Черным спискам ФинЦЕРТ.** При совпадении данных Клиента (номера счёта или ИНН) с актуальными списками ЦБ РФ/МВД, Система Faktura.ru выполняет автоматическую блокировку доступа.

Режимы блокировки:

1. Проверка списков ЦБ и МВД – блокировка при обнаружении в любом из списков;
2. Проверка списков ЦБ и МВД (информирование по ЦБ) – блокировка только при совпадении со списком МВД; при совпадении со списком ЦБ Банк получает e-mail уведомление;
3. Проверка только списков МВД.

Информирование: Клиент получает SMS-сообщение (обязательно). Банк получает автоматическое e-mail уведомление с указанием ФИО, ключа, источника списка и даты блокировки.

7.4. Блокировка доступа осуществляется незамедлительно после получения соответствующего запроса и аутентификации.

7.5. Восстановление доступа происходит после снятия ограничений, наложенных в соответствии с требованиями Федерального закона от 27.06.2011 № 161-ФЗ.

**Особые условия:**

1. Если Клиент удалён из Черных списков, Система автоматически разблокирует доступ и информирует Клиента (СМС) и Банк (e-mail);
2. Если доступ был разблокирован Банком вручную, но Клиент остаётся в Черных списках, повторная автоматическая блокировка не происходит до внесения изменений в досье/права Клиента;
3. Если Клиент повторно попадает в списки после ручной разблокировки, Система блокирует его автоматически;
4. При ручной разблокировке уведомления о разблокировке Клиенту и Банку не направляются.

**8. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ ИЛИ ПОДОЗРЕНИИ НА КОМПРОМЕТАЦИЮ ЭЛЕКТРОННОЙ ПОДПИСИ**

8.1. При выявлении Компрометации ЭП Стороны уведомляют друг друга способами, установленными при заключении договорных отношений.

8.2. Процедура Альтернативного фактора подтверждения. При срабатывании системы FRAMOS платёжный документ переходит в статус «Требует подтверждения». Клиент обязан подтвердить его, используя метод подписания, отличный от первичного.

Попытка подтверждения тем же методом, что и первичное подписание, блокируется Системой с выводом соответствующего сообщения. Документы, ожидающие альтернативного подтверждения, доступны в разделе «Платежи» или через поиск по статусу.

8.3. С момента получения Банком уведомления Клиента о компрометации доступ к Системе ДБО Faktura.ru блокируется до момента разблокировки.

8.4. Клиент не вправе использовать скомпрометированную Электронную подпись после уведомления.

**9. ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ**

9.1. Внеплановая смена выполняется в случае:

1. установленного факта Компрометации ЭП;
2. изменения регистрационных данных уполномоченного лица организации;
3. выхода из строя ФКН;
4. внесения сертификата в список отозванных.

9.2. После получения Уведомления о компрометации Банк отзывает Сертификат.

9.3. Для активации нового ключа Уполномоченный Представитель Клиента лично обращается в Банк с заявлением.

**10. ПОРЯДОК РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ**

10.1. Процедура проверки подлинности ЭП выполняется по инициативе Банка или Клиента.

10.2. Стороны признают информацию в системных журналах Банка достаточной для проверки подлинности.

10.3. При возникновении споров, связанных с операциями, подтверждёнными Мобильной подписью или Альтернативным фактором, Стороны признают достаточным доказательством логи Системы, фиксирующие:

- результат биометрической проверки/кода разблокировки на устройстве Клиента;
- статус сессии (до 1 часа);
- время нажатия кнопки подтверждения;
- данные Имитовставки, обеспечивающей целостность сообщения в соответствии с требованиями Положения Банка России от 30.01.2025 № 851-П.

10.4. Проверка выполняется Согласительной комиссией.

10.5. Решение комиссии принимается большинством голосов и оформляется актом.

10.6. Банк не несёт ответственности, если:

- ключ проверки ЭП принадлежал Представителю;
- Сертификат был действителен на момент получения документа;
- не установлен факт получения Банком Уведомления о компрометации до исполнения документа.

## 11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Регламент составлен на русском и английском языках. В случае расхождения в толковании текстов преимущественную силу имеет версия Правил, составленная на русском языке.

11.2. Правоотношения Сторон, урегулированные Регламентом, а также любые иные правоотношения Сторон, связанные с выполнением Регламента, подлежат регулированию и толкованию в соответствии с законодательством Российской Федерации.

11.3. В случае, если любая из Сторон откажется от исполнения решения Согласительной комиссии, все споры и разногласия подлежат разрешению в соответствии с настоящим пунктом. Все споры, возникающие между Клиентом и Банком в рамках выполнения Регламента или в связи с ним, подлежат разрешению в соответствии с законодательством Российской Федерации путем переговоров, а в случае невозможности такого решения - в Арбитражном суде Республики Татарстан. Клиент вправе обратиться в Банк с письменной претензией, подписанной Уполномоченным Представителем Клиента и скрепленной печатью последнего (при наличии) путем обращения в офис Банка, по его юридическому адресу. Письменный досудебный порядок урегулирования споров с Банком, в рамках настоящего Регламента, является обязательным. Срок ответа на досудебную претензию – 15 (пятнадцать) рабочих дней с даты ее получения Банком.

11.4В случае изменения положений законодательства Российской Федерации, при которых положения Регламента входят в противоречие с положениями законодательства Российской Федерации, к таким правоотношениям Сторон подлежат применению положения законодательства Российской Федерации.

11.5В случае признания какого-либо условия Регламента недействительным, это не влечет недействительности Регламента в целом и/или любых иных положений Регламента. Взамен недействительного положения к правоотношениям Сторон подлежат применению нормы законодательства Российской Федерации.

11.6. Банк вправе в одностороннем, внесудебном порядке вносить изменения в Регламент и/или приложения к нему. Изменения в Регламент вступают в силу и подлежат применению к правоотношениям Сторон по истечении 10 (Десяти) календарных дней с момента размещения таких изменений или новой редакции Регламента на ресурсе: <https://131.ru/contracts> или доведения до сведения Клиента таких изменений любым иным доступным Банку способом. До начала каждого взаимодействия с Банком с использованием Системы ДБО Faktura.ru., в том числе направления в адрес Банка любого Электронного документа, а также не реже одного раза в 10 (Десять) календарных дней, Клиент и его Уполномоченные Представители обязаны знакомиться с Регламентом, а также изменениями в нем. Не ознакомление или несвоевременное ознакомление Клиента и/или его Уполномоченных Представителей с изменениями, внесенными в Регламент, не является основанием для их неприменения к правоотношениям Сторон. В случае несогласия Клиента с изменениями в Регламент, последний вправе расторгнуть Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена в рамках использования Системы ДБО Faktura.ru, в порядке и на условиях, указанных в Правилах, если иное не указано в отдельном соглашении Сторон, письменно уведомив об этом Банк не позднее даты вступления таких изменений в силу, согласно Регламенту. В случае неполучения Банком, до вступления в силу изменений в Регламент письменного уведомления Клиента, изменения считаются безоговорочно принятыми Клиентом, заключение дополнительных соглашений Сторонами не требуется.

Приложение № 1  
к Регламенту дистанционного банковского  
обслуживания с использованием Системы Faktura.ru  
юридических лиц, индивидуальных предпринимателей,  
физических лиц, занимающихся в установленном  
законодательством Российской Федерации порядке  
частной практикой в АО «Банк 131»

**Заявление**

**о смене логина и статического пароля**

**/разблокировку доступа в системе ДБО ФАКТУРА.RU /смене Абонентского номера**

г. Казань

«\_\_» \_\_\_\_20\_\_ г.

ФИО	
Серия и номер документа, удостоверяющего личность	
Орган и дата выдачи документа, удостоверяющего личность	
Действующий на основании	
От имени Клиента	
ОГРН	
Адрес электронной почты <sup>2</sup>	
Абонентский номер <sup>3</sup>	

В соответствии с Регламентом дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО ФАКТУРА.RU. прошу:

– разблокировать доступ в Систему ДБО ФАКТУРА.RU, с использованием ранее предоставленных данных для доступа (с условиями и причинами блокировки согласен, претензий к АО «Банк 131» не имею);

- установить новый Абонентский номер для доступа в Систему ДБО ФАКТУРА.RU, прохождения процедуры аутентификации и подписания Электронных документов при ее использовании, для указанных Уполномоченных лиц: + (\_\_\_\_) \_\_\_\_\_;

Уведомления о совершенных операциях прошу направлять:

по адресу электронной почты

на Абонентский номер:

Настоящим подтверждаю, что указанный в настоящем заявлении Абонентский номер принадлежит исключительно и только мне, иные лица не имеют доступа к нему.

\_\_\_\_\_/\_\_\_\_\_/«\_\_» \_\_\_\_20\_\_ г /

(Подпись)

(ФИО)

(Дата)

<sup>2</sup> Укажите адрес электронной почты уполномоченного лица. Обязательное поле

<sup>3</sup> Укажите абонентский номер уполномоченного лица. Обязательное поле.

М.П.

**Заполняется Банком**

---

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены

Заявление зарегистрировано в Банке « \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_ « \_\_\_\_ »  
\_\_\_\_\_ 20 \_\_\_\_ г

(должность)                      (подпись)                      (расшифровка подписи)                      (дата)

Работник Банка, проверивший ЭП:

Приложение № 2  
к Регламенту дистанционного банковского  
обслуживания с использованием Системы Faktura.ru  
юридических лиц, индивидуальных предпринимателей,  
физических лиц, занимающихся в установленном  
законодательством Российской Федерации порядке  
частной практикой в АО «Банк 131»

АКТ № \_\_\_\_

приема-передачи ФКН Системы ДБО FAKTURA.RU.

г. Казань

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

АО «Банк 131», именуемое в дальнейшем Банк, в лице \_\_\_\_\_, действующего(-ей) на основании \_\_\_\_\_ с одной стороны, и \_\_\_\_\_, именуемый в дальнейшем «Клиент», в лице \_\_\_\_\_

\_\_\_\_\_, действующего(-ей) на основании \_\_\_\_\_, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», в рамках Регламента дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО FAKTURA.RU. (далее – «Регламент») (заявление о присоединении № \_\_\_\_ от \_\_\_\_ \_\_\_\_\_ 20\_\_ г.), составили настоящий Акт о нижеследующем:

Банком передан, а Клиентом принят ФКН, целостность которого не нарушена, с целью использования Системы ДБО FAKTURA.RU. в соответствии с Правилами комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131», Общими условиями осуществления информационного взаимодействия с использованием Системы информационного обмена и Регламентом:

п/п	ФИО (Представителя)	ФКН
1.		электронный ключ Рутокен «Рутокен ЭЦП 2.0» № _____

**Передал**  
АО «Банк 131»  
420012, Республика Татарстан,  
г. Казань, ул. Некрасова, д. 38  
ИНН/ОГРН 1655505780/1241600056390

**Принял**  
**Наименование**  
**Адрес**  
**ИНН/ОГРН**

**От Банка:**

**от Клиента:**

\_\_\_\_\_ (должность)

\_\_\_\_\_ (должность) М.П.

\_\_\_\_\_ (подпись) \_\_\_\_\_ (расшифровка подписи)

\_\_\_\_\_ (подпись) \_\_\_\_\_ (расшифровка подписи)





Приложение № 5  
к Регламенту дистанционного банковского  
обслуживания с использованием Системы Faktura.ru  
юридических лиц, индивидуальных предпринимателей,  
физических лиц, занимающихся в установленном  
законодательством Российской Федерации порядке  
частной практикой в АО «Банк 131»

**Инструкция по обеспечению информационной безопасности при работе в Системе ДБО FAKTURA.RU.**

В целях обеспечения информационной безопасности при работе в Системе ДБО FAKTURA.RU АО «Банк 131», **Клиент обязан:**

1. При осуществлении доступа к Системе ДБО FAKTURA.RU, удостовериться в правильности указанного адреса в адресной строке браузера (<https://bank.131.ru/>) и наличии значка защищенного соединения (замок), исключая выход на сайты, внешне маскирующиеся под Систему ДБО FAKTURA.RU.
2. При использовании Мобильной подписи и/или иного вида Электронной подписи внимательно проверять информацию об Операции, полученную в СМС-сообщении или в PUSH-сообщении.
3. Своевременно устанавливать доступные обновления операционной системы и приложений.
4. Не подвергать используемое устройство операциям повышения привилегий / взлома операционной системы устройства (jail-break, rooting).
5. Использовать антивирус для устройств, своевременно устанавливать на него обновления вирусных баз.
6. Никогда не передавать свое устройство и/или sim-карту третьим лицам.
7. Ключи Усиленной неквалифицированной Электронной подписи хранить только на ФКН в недоступном для посторонних и неуполномоченных лиц месте (запирающиеся персональный сейф, металлический шкаф).
8. Не снимать копии с ФКН, не передавать ФКН лицам, к ним не допущенным, не записывать на ФКН постороннюю информацию.
9. Не использовать в качестве Статического пароля:
  - последовательность символов, состоящих из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);
  - последовательность повторяющихся букв или цифр;
  - идущие подряд в раскладке клавиатуры или в алфавите символы;
  - имена и фамилии;
- ИНН или другие реквизиты Клиента/Уполномоченного Представителя Клиента.

**При использовании Мобильной подписи (ОС Android 11.0+):**

- Для выпуска и использования Мобильной подписи на устройстве должны быть активированы биометрические данные (TouchID/FaceID) или код разблокировки устройства.
- После успешной авторизации через биометрию/код разблокировки Клиент может подтверждать документы без повторного ввода биометрических данных в течение 1 (Одного) часа. По истечении указанного срока потребуется повторное подтверждение.
- Время на подтверждение каждой операции ограничено 5 (Пяти) минутами.
- Для обеспечения целостности и безопасности электронного сообщения при использовании Мобильной подписи применяется Имитовставка в соответствии с требованиями Положения Банка России от 30.01.2025 № 851-П.

- Мобильная подпись поддерживает групповое подписание платёжных поручений в Мобильном приложении.

При выявлении признаков Компрометации ЭП или вредоносного программного обеспечения немедленно уведомить Банк по телефону 8 (800) 100-13-10 (обращения принимаются в круглосуточном режиме) и направить Уведомление по форме Приложения №4. Не восстанавливать работоспособность поврежденного персонального компьютера до проведения экспертизы.

#### **Требования к Статическому паролю:**

- Длина пароля должна быть не менее 8 символов.
- В числе символов пароля должны присутствовать строчные и прописные буквы, цифры и специальные символы (!, ", #, \$, %, &, ', (, ), \*, +, -, ., /, @, :, ;, <, =, >, ?, [, \, ], ^, \_, `, {, }, ~);
- Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, а также выбирать пароли, которые уже использовались ранее;
- Личный пароль Клиент не имеет права сообщать никому;
- При смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 4 символа;
- Срок действия пароля пользователя не более 1года (365 дней).
- Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).
- После 5-и неудачных попыток ввода пароля, учетная запись Клиента блокируется до выяснения причин ввода неправильного пароля.
- Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в доступных третьим лицам местах, передавать неуполномоченным лицам.

#### **Необходимо:**

- Установить на персональном компьютере (ноутбуке) парольную защиту на вход в Операционную систему.
- Хранить пароль доступа к ключу УНЭП отдельно от ФКН.
- Подключать ФКН, содержащий ключ ЭП, только в момент использования Системы ДБО ФАКТУРА.RU и подписания Электронных документов. Не оставлять ФКН, содержащий ключ ЭП, постоянно подключенным к компьютеру.
- Не использовать ФКН, содержащий ключ ЭП, для каких-либо других целей, в частности, не хранить на нём информацию произвольного содержания, не относящегося к работе с Системой ДБО ФАКТУРА.RU.
- Не копировать содержимое ФКН, содержащего ключ ЭП, и не передавать его никому даже на короткое время.
- Закончив работу в Системе ДБО ФАКТУРА.RU или прервав её (даже на несколько минут), извлечь ФКН, содержащий ключ УНЭП, и убрать его в недоступное другим лицам место.
- Применять на рабочем месте лицензионные средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.
- Если в качестве компьютера для работы в Системе ДБО ФАКТУРА.RU используется переносной компьютер (ноутбук), исключить его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)
- Осуществлять постоянный контроль отправляемых платёжных (расчетных) документов при работе с Системой ДБО ФАКТУРА.RU, а также за состоянием расчетных (банковских) счетов, операциям по ним и остаткам.
- В случае выявления признаков Компрометации ЭП или выявления вредоносного кода в компьютере, используемом для работы в Системе ДБО ФАКТУРА.RU, необходимо немедленно уведомить Банк по телефонам: 8 (800) 100 13 10 , либо лично явиться в Банк с целью блокирования скомпрометированных ключей ЭП с последующей их заменой.

#### **К событиям, связанным с Компрометацией Электронной подписи, в том числе, относятся:**

- утрата ФКН, с последующим обнаружением или без такового;
- нарушение правил хранения, использования и уничтожения (в том числе после окончания срока действия) ключа УНЭП;

- утеря, передача и/или предоставлением доступа неуполномоченным третьим лицам к аппаратным средствам (в том числе мобильным телефонам или иным) и/или SIM-карте с Абонентским номером, в том числе который используется для направления Временного и/или Одноразового пароля;
- наличие подозрений, что Средства подтверждения Электронного документа стали известны неуполномоченным третьим лицам;
- возникновение подозрений на утечку информации или ее искажение;
- несанкционированное копирование или подозрение на копирование Временного, Статического пароля, функционального ключевого носителя, аппаратного средства и/или SIM-карты с Абонентским номером;
- несанкционированный доступ к адресу электронной почты, указанному в Заявлении;
- прекращение полномочий или увольнение Уполномоченных лиц, имеющих доступ к Средству подтверждения;
- случаи, когда нельзя достоверно установить, что произошло с ФКН (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц, другие виды разглашения ключевой информации).

При обнаружении несанкционированных доступов в Систему ДБО ФАКТУРА.RU, платежных и иных операций в Системе ДБО ФАКТУРА.RU, Компрометации или подозрении на Компрометацию Электронной подписи немедленно уведомить Банк и направить «Уведомление о компрометации» в порядке, установленном Регламентом дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой в АО «Банк 131» с использованием Системы ДБО ФАКТУРА.RU, а также обратиться с соответствующим заявлением в правоохранительные органы.

Запрещено восстанавливать работоспособность поврежденного компьютера до проведения технической экспертизы. Работу с Системой ДБО ФАКТУРА.RU разрешено проводить только после новой установки операционной системы с форматированием жестких дисков и после смены всех ключей ЭП клиента.

#### **Требования:**

- Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по Системе ДБО ФАКТУРА.RU, заблокировать 3389 (RDP Remote desktop).
- Включить в операционной системе журнал безопасности Windows.
- Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО).
- Обеспечить возможность своевременного обновления системного и прикладного программного обеспечения.
- Доступ в помещение, где размещен компьютер с Системой ДБО ФАКТУРА.RU, предоставлять только Уполномоченным лицам.
- Компьютер, с которого осуществляется подготовка и отправка Электронных документов в Банк, рекомендуется выделить в отдельный сегмент сети с обязательным исключением его из общей локальной сети Клиента.
- Исключить доступ к компьютерам, используемым для работы в Системе ДБО ФАКТУРА.RU, посторонних лиц и персонала, неуполномоченных на работу в Системе ДБО ФАКТУРА.RU и/или обслуживание компьютеров.
- При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.
- Запрещено передавать логины и пароли третьим лицам в том числе иным Уполномоченным Представителям Клиента.

АО «Банк 131» не осуществляет рассылку электронных писем с просьбой прислать ключи Электронных подписей и/или пароль к Системе ДБО ФАКТУРА.RU и никогда не запрашивает у Клиента эту информацию.

Банк не осуществляет звонков, рассылку сообщений по электронной почте, SMS-сообщений, или иными способами, с просьбой сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.). При получении такого запроса ни при каких обстоятельствах Клиент не должен сообщать данную информацию и должен немедленно сообщить об этом в Банк.

Приложение № 6  
к Регламенту дистанционного банковского  
обслуживания с использованием Системы Faktura.ru  
юридических лиц, индивидуальных предпринимателей,  
физических лиц, занимающихся в установленном  
законодательством Российской Федерации порядке  
частной практикой в АО «Банк 131»

**Требования к программно-техническим средствам для проведения расчетных операций в электронной форме с использованием Системы ДБО ФАКТУРА.RU**

1. Требования к программно-техническим средствам (приобретаются Клиентом за собственный счет у третьих лиц):

**1.1. При использовании УНЭП:**

- Персональный компьютер с портом USB и предустановленной операционной системой (ОС) Windows 7 и выше, MacOS<sup>4</sup>
- Интернет-браузер актуальной версии: Chrome 47 и выше / Firefox 44.0 и выше / Internet Explorer 10 и выше / Opera 36 и выше / Safari 9 и выше;
- доступ в сеть Интернет;
- принтер.

2. Для использования Системы ДБО ФАКТУРА.RU с применением УНЭП необходим выделенный компьютер с предустановленной операционной системой семейства Microsoft Windows. Если, по желанию Клиента, установка Системы ДБО ФАКТУРА.RU производится на компьютер с предустановленными ОС сторонних производителей, Банк не несет ответственности за работоспособность Системы ДБО ФАКТУРА.RU.

**При эксплуатации Системы ДБО ФАКТУРА.RU запрещается:**

- Установка программного обеспечения сторонних фирм, а также сознательное внесение изменений в файлы программного и информационного обеспечения Системы ДБО ФАКТУРА.RU;
- Доступ к Системе ДБО ФАКТУРА.RU неуполномоченных лиц;

**При эксплуатации Системы ДБО ФАКТУРА.RU Клиент обязан:**

- Использовать систему ДБО ФАКТУРА.RU только на исправном и проверенном на отсутствие компьютерных вирусов персональном компьютере (ноутбуке);
- Исключить возможность заражения компьютера с установленной Системой ДБО ФАКТУРА.RU программными вирусами или другими вредоносными программами;
- Использовать только легальное и лицензионное программное обеспечение;
- Обеспечить техническую исправность оборудования, входящего в состав рабочего места Системы ДБО ФАКТУРА.RU;
- Применять средства антивирусной защиты и обеспечить регулярное обновление антивирусных баз.

Необходимость резервного копирования рабочего места пользователя Системы ДБО ФАКТУРА.RU определяет Клиент и при необходимости осуществляет его собственными силами.

---

<sup>4</sup> Инструкция по работе с MacOS размещена на официальном сайте Банка.