**Порядок электронного документооборота**

при осуществлении информационно-технологического обслуживания

в рамках Условий осуществления расчетов с использованием СБП

(Условия СБП)

г. Казань

Редакция № 1 от «01» марта 2022 года

**В рамках настоящего Порядка электронного документооборота (далее – Порядок, ЭДО), применяются термины и определения, указанные в Условиях осуществления расчетов с использованием СБП, если иное не указано в настоящем Порядке.**

Общество с ограниченной ответственностью «Банк 131» (далее – «Банк»), с одной стороны, и юридическое лицо или индивидуальный предприниматель, заключившее(-ий) с Банком Соглашение об использовании СБП (в соответствии с Условиями СБП) (далее – «Клиент»), с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. Предмет Соглашения
   1. Настоящее Соглашение устанавливает порядок организации и проведения электронного документооборота с использованием Электронной подписи между Сторонами в рамках Соглашения об использовании СБП.
   2. Перечень и формы Электронных документов, которые Стороны могут подписывать и передавать друг другу в рамках настоящего Соглашения, определяются Банком и размещены по адресу: https://developer.131.ru/ [.](https://developer.131.ru/)
   3. Клиент реализует свое право на обмен Электронными документами, подписанными Электронной подписью, только через своих надлежаще уполномоченных Представителей. Такими Представителями могут быть как дееспособные физические лица, наделенные учредительными документами Клиента правом единолично действовать от имени последнего без доверенности, так и дееспособные физические лица, действующие от имени Клиента на основании доверенности. Уполномоченные Представители Клиента определяются Клиентом в Заявлении[[1]](#footnote-1).
2. Порядок заключения Соглашения
   1. Настоящее Соглашение состоит из настоящего Порядка и Заявления о признании и сверке ключа электронной подписи (далее – «Заявление», приложение № 1). Актуальная редакция Соглашения размещена по адресу: https://developer.131.ru/.
   2. Соглашение не является публичной офертой. Банк вправе отказаться от заключения Соглашения с Клиентом в случае, если Клиент не имеет заключенного с Банком соглашения об использовании СБП.
   3. Соглашение заключается путем принятия Сторонами условий Порядка и подписания Заявления в двух экземплярах. Соглашение считается заключенным с даты подписания Заявления.
3. Порядок информационно-технического взаимодействия
   1. Стороны осуществляют информационно-технологическое взаимодействие в соответствии с Протоколом информационного обмена (далее – «API») и Инструкцией по обеспечению информационной безопасности (приложение № 2), актуальные редакции и описания которых размещены по адресу: https://developer.131.ru/
   2. Банк вправе в одностороннем порядке вносить изменения в API и ЭДО, в порядке, указанном в Условиях СБП.
   3. Стороны самостоятельно и за свой счет поддерживают собственную аппаратно-техническую инфраструктуру, необходимую для исполнения Соглашения, предпринимают возможные меры для защиты передаваемой в рамках Соглашения информации от несанкционированного доступа, копирования и распространения, в том числе, предусмотренные применимым законодательством.
   4. Клиент соглашается, что Банк не может гарантировать Клиенту отсутствие перерывов, связанных с техническими неисправностями, проведением профилактических работ, а также полную и безошибочную работоспособность API и каналов связи. Клиент обязуется своевременно информировать Банк обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих надлежащему исполнению настоящего Соглашения, в соответствии с Условиями СБП.
4. Электронная подпись
   1. Соглашение предусматривает использование усиленной неквалифицированной электронной подписи (далее – «Электронная подпись»), которая позволяет обеспечить подтверждение авторства, подлинности и целостности подписанных Электронных документов.
5. Средства электронной подписи
   1. Для создания и проверки Электронной подписи, создания ключа Электронной подписи и ключа проверки Электронной подписи должны использоваться средства электронной подписи, которые:

5.1.1. позволяют установить факт изменения подписанного Электронного документа после момента его подписания;

5.1.2. обеспечивают практическую невозможность вычисления ключа Электронной подписи из электронной подписи или из ключа проверки Электронной подписи.

* 1. Клиент обязан самостоятельно и за свой счет выбрать средства Электронной подписи и создать ключ Электронной подписи и ключ проверки Электронной подписи, в соответствии с Условиями СБП и требованиями законодательства РФ.

1. Порядок электронного документооборота
   1. Перед началом осуществления электронного документооборота Банк и Клиент обмениваются ключами проверки Электронной подписи. Ключ проверки Электронной подписи Банка может быть опубликован в открытом доступе по адресу: https://developer.131.ru/.
   2. Электронный документооборот включает следующие этапы: создание, передачу, проверку подлинности, учет и хранение Электронных документов.
   3. Создание Электронного документа включает в себя непосредственное формирование Электронного документа и его подписание Электронной подписью с использованием ключа Электронной подписи.
   4. Передача подписанного Электронного документа осуществляется исключительно с использованием API.
   5. Проверка подлинности Электронного документа включает в себя проверку соответствия Электронного документа требованиям к его формату и порядку заполнения, а также проверку подлинности Электронной подписи с использованием ключа проверки Электронной подписи.

Для проверки Электронной подписи Стороны используют средство Электронной подписи, которое:

* + 1. формирует хэш из исходного Электронного документа по алгоритму, определенному в Заявлении;
    2. преобразует полученную Электронной подпись с использованием ключа проверки Электронной подписи;
    3. сравнивает значение, полученное на шаге 1 со значением, полученным на шаге 2.

Если значения совпали, то подлинность Электронной подпись считается подтвержденной. Если не совпали, то считается, что подлинность Электронной подписи не подтверждена, и проверяющая Сторона должна немедленно сообщить об этом другой Стороне.

* 1. Учет Электронных документов осуществляется путем ведения электронных журналов учета поступающих и исходящих Электронных документов, подписанных Электронной подписью. Ведение электронных журналов учета осуществляется программно-аппаратными и техническими средствами Банка. Моментом получения Электронного документа является момент его отражение в журнале учета.
  2. Хранение Электронных документов, поступивших в Банк или исходящих от Банка, осуществляется в архиве Банка в течение сроков, установленных для документов соответствующего вида, но не менее пяти лет с момента получения Электронного документа. В случае возникновения споров относительно содержания Электронных документов приоритет имеют Электронные документы, хранящиеся в архиве Банка.

1. Признание Электронных документов
   1. Стороны признают, что Электронные документы, подписанные Электронной подписью, являются равнозначными по своей юридической силе документам на бумажном носителе, подписанным собственноручно и заверенным печатью (при наличии).
   2. Предусмотренные для Электронного документа правовые последствия наступают только в случае, если получен положительный результат проверки Электронной подписи этого Электронного документа, при условии соблюдения требований к формату и порядку заполнения Электронного документа, установленных настоящим Соглашением, Условиями СБП, Банковскими правилами, Правилами и Стандартами ОПКЦ СБП и законодательством Российской Федерации.
2. Ответственность Сторон
   1. Стороны принимают на себя все риски, связанные с работоспособностью своего оборудования и каналов связи, сохранностью и конфиденциальностью ключей Электронной подписи.
   2. В случае невыполнения или ненадлежащего выполнения своих обязательств одной из Сторон, другая Сторона имеет право потребовать от такой Стороны исполнения принятых на себя обязательств, а также возмещения причиненного ей ущерба.
   3. Клиент несет ответственность за конфиденциальность ключа Электронной подписи, а также за действия своих работников при использовании Электронной подписи. Банк не несет ответственности за убытки, понесенные Клиентом в связи с несанкционированным использованием Электронной подписи неуполномоченными лицами.
3. Конфиденциальность
   1. Стороны обязуются обеспечивать конфиденциальность ключей Электронной подписи, в частности, не допускать использование принадлежащих им ключей Электронной подписи без согласия Сторон. Не использовать ключ Электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа Электронной подписи нарушена.
   2. Сторона, допустившая компрометацию ключа Электронной подписи, несет ответственность за Электронные документы, подписанные с использованием скомпрометированного ключа Электронной подписи. Ключ Электронной подписи Стороны считается действующим до даты получения другой Стороной уведомления об аннулировании (отзыве) соответствующего ключа Электронной подписи.
   3. Стороны обязуются в течение не более чем одного календарного дня информировать друг друга обо всех случаях нарушения конфиденциальности ключей Электронной подписи (в т.ч. утраты, хищения, несанкционированного доступа к ключу Электронной подписи). При этом исполнение Соглашения приостанавливается до проведения смены ключей Электронной подписи. Смена ключей Электронной подписи осуществляется посредством подписания Сторонами нового Заявления.
4. Форс-мажор

10.1.Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по Соглашению в случае наступления форс-мажорных обстоятельств, таких как: стихийные и техногенные катастрофы, военные действия, гражданские беспорядки, эпидемии, пандемии, крах мировой экономической и финансовой системы, принятие нормативных актов ограничительного характера. К числу форс-мажорных обстоятельств также относятся: сбой или отказ программно-аппаратных средств и оборудования, отказ или отключение систем связи, электроснабжения, вмешательство третьих лиц (DDoS-атака) и т.п.

10.2.При наступлении форс-мажорных обстоятельств, Сторона, подвергнувшаяся их влиянию, должна в течение 3 (трех) календарных дней уведомить об этом другую Сторону. Сторона, пропустившая срок уведомления, лишается права ссылаться на указанные обстоятельства, как на основание, освобождающее от ответственности.

1. Порядок разрешения споров

11.1.Настоящее Соглашение подлежит регулированию и толкованию в соответствии с законодательством Российской Федерации (применимое законодательство).

11.2.В случае возникновения разногласий по вопросам исполнения условий Соглашения, Стороны принимают все меры по их разрешению путем переговоров.

11.3.Любые споры между Сторонами, предметом которых является оспаривание содержания Электронного документа, передаются для разрешения специально создаваемой экспертной комиссии. Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон. Комиссия должна установить авторство, подлинность и целостность Электронной подписи оспариваемого Электронного документа. Результаты работы экспертной комиссии оформляются актом, который должен быть подписан Сторонами. С момента подписания акта Стороны признают бесспорность сведений, указанных в данном акте. Порядок разбора конфликтных ситуаций указан в приложении № 3.

11.4.В случае невозможности урегулировать разногласия путём переговоров, споры разрешаются в Арбитражном суде Республики Татарстан с применением норм материального и процессуального права Российской Федерации.

11.5.Письменный досудебный претензионный порядок урегулирования споров является обязательным. Срок ответа на претензию – 30 (Тридцать) календарных дней с момента ее получения.

1. Уведомления

12.1.Если иной порядок не предусмотрен настоящим Соглашением, и Соглашением об использовании СБП, то любые письма, уведомления и документы, передаваемые Сторонами друг другу в рамках Соглашения по электронной почте, адреса которой указаны в Заявлении буду считаться надлежащим образом отправленными и полученными, если они направлены с/на адреса электронной почты, указанные Сторонами в Заявлении. Указанный порядок не применяется в случаях, предусмотренных Условиями СБП и/или Правилами, а также в установленном законодательством РФ случаях.

12.2.Изменение адреса электронной почты Сторон (п. 12.1), осуществляется посредством отправки электронного сообщения с ранее указанных адресов электронной почты, содержащего четкое указание на новый адрес электронной почты для осуществления связи.

1. Изменение Соглашения

13.1.Банк вправе в одностороннем внесудебном порядке вносить в Соглашение любые изменения и/ или дополнения, посредством размещения по адресу https://developer.131.ru/новой редакции Соглашения.

13.2.Новой редакции Соглашения вступает в силу и подлежат применению к правоотношениям Сторон по истечении 10 (десяти) календарных дней с момента ее размещения по адресу: https://developer.131.ru/[.](https://developer.131.ru/)

13.3.Клиент обязан самостоятельно и своевременно знакомиться с новой редакций Соглашения. В случае неполучения Банком до вступления в силу новой редакции Соглашения письменного уведомления Клиента о расторжении Соглашения, новая редакция Соглашения считается безоговорочно принятой Клиентом, при этом заключение дополнительного соглашения к Соглашению не требуется.

1. Срок действия и порядок расторжения

14.1.Срок действия Соглашения ограничен сроком действия заключенного между Сторонами Соглашения об использовании СБП.

14.2.Банк вправе в одностороннем порядке отказаться от исполнения Соглашения, уведомив об этом Клиента не менее чем за 30 (тридцать) календарных дней любым доступным Банку способом.

14.3.Обязательства Сторон, возникшие до расторжения Соглашения, сохраняются до их полного исполнения.

1. Прочие условия

15.1.Настоящее Соглашение составлено на русском и английском языках. В случае возникновения противоречий приоритетным считается текст на русском языке.

15.2.Все приложения являются неотъемлемыми частями Соглашения, а именно:

15.2.1.Приложение № 1 - «Заявление»;

15.2.2.Приложение № 2 – «Инструкция по обеспечению информационной безопасности»;

15.2.3.Приложение № 3 – «Порядок разбора конфликтных ситуаций».

15.3.Стороны не вправе передать свои права и обязанности по Соглашению третьим лицам без предварительного письменного согласия другой Стороны.

15.4.Если какое-либо положение настоящего Соглашения будет признано недействительным или не имеющим законной силы в соответствии с применимым законодательством Российской Федерации, то такое положение должно быть приведено Сторонами в соответствие с применимым законодательством, при этом действительность и применимость любого другого положения Соглашения не будет затронута.

1. Реквизиты Банка

Общество с ограниченной ответственностью «БАНК 131»

Лицензия Банка России №3538 от 12.04.2019

ОГРН 1191690025746

ИНН/КПП 1655415696 / 165501001

Адрес: 420012, Российская Федерация, Республика Татарстан,

город Казань, улица Некрасова, дом 38

Кор/сч. 30101810822029205131 в Отделение-НБ Республика Татарстан

БИК: 049205131

**Приложение № 1 к Порядку электронного документооборота**

**ЗАЯВЛЕНИЕ О ПРИЗНАНИИ И СВЕРКЕ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ**

|  |  |
| --- | --- |
| **Банк** | **Клиент** |
| Общество с ограниченной ответственностью «Банк 131» | [Полное наименование Клиента] |
| [Полное ФИО владельца Электронной подписи] | [Полное ФИО владельца Электронной подписи]  *[Такими представителями могут быть как дееспособные физические лица, наделенные учредительными документами Клиента правом единолично действовать от имени Клиента без доверенности, так и дееспособные физические лица, действующие от*  *имени Клиента на основании доверенности]*  [Подпись владельца Электронной подписи] |
| Действующий на основании [документ] | Действующий на основании [документ]  *[Устав, Доверенность]* |
| Алгоритм Подписи RSA (2048 bit) | Алгоритм Подписи RSA (2048 bit) |
| Ключ проверки Электронной подписи Банка опубликован в открытом доступе по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **[**Открытая часть ключа проверки Электронной подписи**]** |
| **[**Адрес электронной почты**]** | **[**Адрес электронной почты**]** |

Подписывая настоящее Заявление, Клиент подтверждает, что он ознакомлена и согласна с Порядком электронного документооборота при осуществлении информационно-технологического обслуживания в рамках Условий осуществления расчетов с использованием СБП (<https://developer.131.ru>) и его условиям без каких-либо правок, оговорок или исключений.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Банк | |  | Клиент | |
| ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «БАНК 131»  Лицензия Банка России №3538 от 12.04.2019  ОГРН: 1191690025746 ИНН/КПП: 1655415696 / 165501001  Адрес: 420012, Российская Федерация, Республика Татарстан, город Казань, улица Некрасова, дом 38  Корсчет 30101810822029205131 в Отделение-НБ Республика Татарстан БИК: 049205131 | | [НАЗВАНИЕ КЛИЕНТА]  [АДРЕС КЛИЕНТА]  [РЕГИСТРАЦИОННЫЙ НОМЕР]  [ИНН]  [БАНКОВСКИЕ РЕКВИЗИТЫ] |  | |
| [ФИО]  [Должность]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [ФИО]  [Должность]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |

Приложение № 2 к Порядку электронного документооборота

**Инструкция по обеспечению информационной безопасности**

В целях обеспечения информационной безопасности при работе с Протоколом информационного обмена (далее – «API») в рамках Условий СБП, Клиент наделяется следующими обязанностями:

1. Ключ Электронной подписи (далее по тексту – «ключ Электронной подписи») хранить только в недоступном для посторонних лиц месте и доступен исключительно уполномоченным Представителям Климента.
2. Не допускается:
   * снимать несанкционированные копии;
   * передавать ключ Электронной подписи лицам, к ним не допущенным.
3. Не использовать в качестве пароля:
   * последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);
   * последовательности повторяющихся букв или цифр;
   * идущие подряд в раскладке клавиатуры или в алфавите символы;
   * имена и фамилии;
   * ИНН или другие реквизиты Клиента.
4. Пароль должен:
   * быть не менее 8 символов;
   * содержать цифры, строчные и заглавные буквы;
   * содержать хотя бы 1 символ, не являющийся буквой или цифрой.
5. На компьютере должна быть установлена парольная защита на вход в операционную систему устройства.
6. Пароль пользователя в операционной системе устройства должен меняться Клиентом не реже одного раза в квартал.
7. Пароль доступа к ключу Электронной подписи хранить отдельно от ключа Электронной подписи.
8. Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам.
9. Использовать ключ Электронной подписи, только в момент подписания Электронных документов.
10. Использовать ключ Электронной подписи, только для подписания Электронных документов в рамках использования «API» согласно Условиям СБП.
11. Применять на рабочем месте лицензионные средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.
12. Если в качестве компьютера для работы по «API» используется переносной компьютер (ноутбук), должно быть исключено его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)
13. Осуществлять постоянный контроль отправляемых сообщений при работе «API».
14. В случае выявления признаков компрометации ключа Электронной подписи или выявления вредоносного кода в компьютере, используемом для работы «API», необходимо немедленно уведомить Банк по телефонам: (843) 598-31-40, (843) 598-31-39 с 9 часов 00 минут до 18 часов 00 минут (в рабочие дни), либо лично явиться в Банк с целью блокирования скомпрометированных ключей Электронной подписи с последующей их заменой.
15. К событиям, связанным с компрометацией ключей Электронной подписи, в том числе, относятся:
    * утеря (утрата) носителя ключа Электронной подписи, в том числе, с последующим его обнаружением;
    * обнаружение факта или угрозы использования (копирования) ключа Электронной подписи и/или пароля доступа к ключам Электронной подписи неуполномоченными лицами (несанкционированная отправка Электронных документов);
    * обнаружение ошибок в работе «API», в том числе, возникающих в связи с попытками нарушения информационной безопасности;
    * увольнение ответственного сотрудника Клиента, имевшего доступ к ключу Электронной подписи.
16. При обнаружении несанкционированных операций или утрате «API» немедленно уведомить Банк.
17. Использовать комбинации клавиш «Ctrl + Alt + Del» для идентификации пользователя в операционной системе.
18. Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы c API, заблокировать 3389 (RDP Remote desktop).
19. Включить в операционной системе журнал безопасности.
20. Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д.
21. Обеспечить возможность своевременного обновления системного и прикладного программного обеспечения.
22. Выделить стационарный компьютер только для работы «API».
23. Доступ в помещение, где размещен компьютер с «API», предоставлять только уполномоченным лицам Клиента.
24. 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.
25. Исключить доступ к компьютерам, используемым для работы по «API», посторонним лицам и персоналу Клиента, не уполномоченному на работу по «API» и/или обслуживание компьютеров.
26. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.
27. Банк не осуществляет рассылку электронных писем с просьбой прислать ключи Электронной подписи и/ или пароль используемые в «API» и никогда не запрашивает у Клиента эту информацию. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбой сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.) ни при каких обстоятельствах не сообщайте данную информацию и сообщите об этом в Банк.
28. Клиент самостоятельно и единолично несет ответственность за обеспечение конфиденциальности паролей, ключей Электронной подписи, и иных данных, полученных от Банка или сгенерированных Клиентом самостоятельно для целей их использования при работе «API», а также за обеспечение конфиденциальности и неразглашение данных, документов и сведений, полученных и(или) отправленных с использованием «API».

Приложение № 3 к Порядку электронного документооборота

**Порядок разбора конфликтных ситуаций**

Любые споры между Сторонами, предметом которых является установление подлинности Электронной подписи в Электронном документе, т.е. целостности текста и аутентичности отправителя Электронного документа, передаются для разрешения специально создаваемой экспертной комиссии.

Экспертная комиссия созывается на основании письменного заявления (претензии) любой из Сторон. В указанном заявлении Сторона указывает реквизиты оспариваемого подписанного Электронного документа и лиц, уполномоченных представлять интересы этой Стороны в составе экспертной комиссии.

Не позднее 3 (трех) рабочих дней с момента получения другой Стороной заявления (претензии), Стороны определяют дату, место и время начала работы экспертной комиссии, определяют, какая Сторона предоставляет помещение и производит конфигурирование средств Электронной подписи.

Полномочия членов экспертной комиссии подтверждаются доверенностями, выданными в установленном законодательством Российской Федерации порядке.

Состав экспертной комиссии формируется в равных пропорциях из представителей Сторон.

Экспертиза оспариваемого Электронного документа осуществляется в присутствии всех членов экспертной комиссии.

Экспертиза осуществляется в четыре этапа:

1. Стороны совместно устанавливают, конфигурируют и тестируют средство Электронной подписи.
2. Стороны предоставляют свои ключи Электронной подписи и ключи проверки Электронной подписи, используемые для создания Электронной подписи оспариваемого Электронного документа.
3. Экспертная комиссия сравнивает предоставленные ключи проверки Электронной подписи с ключами, указанными в Заявлении. Ключи проверки Электронной подписи и коды, которые совпали, признаются подлинными.
4. Если третий этап успешно пройден, то экспертная комиссия производит проверку подлинности Электронной подписи в оспариваемом Электронном документе.

Результаты экспертизы оформляются в виде письменного заключения - акта экспертной комиссии, подписываемого всеми членами экспертной комиссии. Акт составляется немедленно после завершения последнего этапа экспертизы. В акте фиксируются результаты всех этапов проведенной экспертизы, а также все существенные реквизиты оспариваемого электронного документа. Акт составляется в двух экземплярах – по одному для каждой из Сторон. Акт экспертной комиссии является окончательным и пересмотру не подлежит.

Подтверждение подлинности Электронной подписи в акте, будет означать, что оспариваемый Электронный документ имеет юридическую силу и влечет возникновение соответствующих прав и обязательств у Сторон.

В случае отсутствия согласия по спорным вопросам и добровольного исполнения решения экспертной комиссии, все материалы по этим вопросам могут быть переданы на рассмотрение в Арбитражный суд Республики Татарстан, в порядке и на условиях, указанных в Соглашении об использовании СБП.

1. Заявление об использовании СБП/Заявление на изменение пользователей СБП. [↑](#footnote-ref-1)