**Соглашение № \_\_\_\_\_**

**об электронном взаимодействии**

**г. Мурманск «\_\_\_»\_\_\_\_\_\_\_\_\_2015 г.**

Управление финансов администрации города Мурманск, именуемое в дальнейшем «Оператор», в лице начальника управления Умушкиной Ольги Викторовны, действующего на основании Положения, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Участник», в лице, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые «Стороны», заключили настоящее соглашение (далее – Соглашение) о нижеследующем.

**1. ПРЕДМЕТ СОГЛАШЕНИЯ**

1.1. Соглашение регулирует отношения между Оператором и Участником по обмену электронными документами при использовании автоматизированной информационной системы по составлению и исполнению бюджета муниципального образования город Мурманск «Бюджет-Смарт» и «Бюджет-Web»(далее – АИС «Бюджет-Смарт» («Бюджет-Web»)) в соответствии с «Правилами электронного документооборота» (далее – Правила), являющимися приложением к настоящему Соглашению (Приложение № 1).

1.2 Соглашение определяет права и обязанности Сторон, возникающие при осуществлении электронного документооборота (далее – ЭДО) в АИС «Бюджет-Смарт» («Бюджет-Web») с учетом обеспечения информационной безопасности.

1.3 Соглашение определяет условия и порядок обмена электронными документами (далее – ЭД) при осуществлении ЭДО между Сторонами в АИС «Бюджет-Смарт» («Бюджет-Web»).

**2. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

2.1. При осуществлении обмена ЭД с использованием АИС «Бюджет-Смарт» («Бюджет-Web») Стороны обязуются:

2.1.1. Руководствоваться законодательством Российской Федерации, нормативными актами управления финансов администрации города Мурманск, эксплуатационной документацией на программное обеспечение (далее – ПО) (включая средства криптографической защиты информации (далее – СКЗИ)) и настоящим Соглашением.

2.1.2. При компрометации закрытых ключей электронных подписей (далее – закрытый ключ подписи) руководствоваться п.4.3 Правил (Приложение № 1).

2.2. Стороны признают, что:

2.2.1. ЭД, сформированные каждой из участвующих в ЭДО Сторон, имеют равную юридическую силу с соответствующими документами на бумажных носителях информации, если они подписаны корректными электронными подписями (далее – ЭП) лиц, имеющих право подписи соответствующих документов (далее – уполномоченные лица), и для этих ЭП соблюдены следующие условия:

* сертификаты ключей подписей (далее – сертификаты), относящиеся к этим ЭП, изданы удостоверяющим центром и не утратили силу (действуют) на момент проверки или на момент подписания ЭД;
* подтверждена подлинность этих ЭП в ЭД;
* ЭП используется в соответствии со сведениями, указанными в сертификате.

2.2.2. Применяемые в АИС «Бюджет-Смарт» («Бюджет-Web») сертифицированные СКЗИ и ЭП обеспечивают конфиденциальность, целостность и подлинность ЭД при осуществлении Сторонами обмена ЭД с использованием общедоступных каналов связи и нескомпрометированных закрытых ключей подписи уполномоченных лиц.

2.2.3. ЭП в ЭД, при выполнении условий Соглашения, признаются равнозначными собственноручным подписям уполномоченных лиц. ЭД, подписанные ЭП, имеют равную юридическую силу с документами на бумажных носителях информации, подписанных собственноручными подписями уполномоченных лиц и оформленных в установленном порядке.

2.2.4. ЭД, подписанные ЭП не являющимися корректными, приему и исполнению не подлежат.

2.3. Оператор обязуется:

2.3.1. Предоставить информацию о технических требованиях, предъявляемых к автоматизированному рабочему месту (далее - АРМ), оборудованному необходимым ПО и СКЗИ, Участника, требующимся для подключения к АИС «Бюджет-Смарт» («Бюджет-Web»).

2.3.3. Принимать и исполнять оформленные должным образом ЭД Участника АИС «Бюджет-Смарт» («Бюджет-Web») в соответствии с настоящим Соглашением.

2.3.4.Предоставлять Участнику актуальные справочники, используемые в АИС «Бюджет-Смарт» («Бюджет-Web») и необходимые для подготовки ЭД.

2.3.5. При изменении порядка и/или правил обработки ЭД, при необходимости, своевременно предоставлять Участнику информацию о технических требованиях к модернизированным СКЗИ для АРМ Участника.

2.4. Оператор имеет право:

2.4.1. Отказывать Участнику в приеме, исполнении ЭД с указанием мотивированной причины отказа.

2.4.2. Приостанавливать обмен ЭД при:

* несоблюдении Участником требований по передаче ЭД и обеспечению информационной безопасности, предусмотренных законодательством Российской Федерации и условиями настоящего Соглашения;
* разрешении спорных ситуаций, а также для выполнения неотложных, аварийных и ремонтно-восстановительных работ на АРМ Оператора.

В случае невозможности передачи ЭД в АИС «Бюджет-Смарт» («Бюджет-Web») Участник оформляет и передает Оператору документы на бумажных носителях или в виде ЭД на магнитном носителе только по согласованию с Оператором.

2.5. Участник обязуется:

2.5.1. Назначать лиц, отвечающих за организацию и обеспечение бесперебойной эксплуатации программно-технических средств АРМ Участника, согласно составу пользователей, определенному в Правилах (Приложение №1). Назначение оформляется приказом руководителя Участника.

2.5.2. Передавать Оператору должным образом оформленные ЭД и получать от Оператора электронные сообщения, подтверждающие получение и обработку ЭД.

2.5.3. Не вносить исправления, изменения или дополнения, а также не передавать третьим лицам закрытые ключи подписи, ПО (в том числе СКЗИ и ключевую документацию к ним) и соответствующую техническую документацию.

2.5.4. Формировать новые закрытые и открытые ключи подписи в случае компрометации действующих закрытых ключей подписи или за 10 рабочих дней до истечения срока действия сертификатов.

2.5.5. Исполнять требования по обеспечению информационной безопасности АРМ Участника, изложенные в разделе 4 Правил (Приложение № 1).

2.5.6. Соблюдать требования предоставленной Оператором документации.

2.6. Участник имеет право:

2.6.1. Требовать от Оператора исполнения принятых от Участника ЭД.

2.6.2. Требовать от Оператора приостановления исполнения (обработки) всех ЭД в случаях компрометации закрытых ключей подписи Участника.

**3. ОТВЕТСТВЕННОСТЬ СТОРОН**

3.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.

3.2. Каждая из Сторон несет ответственность за содержание всех ЭД, предусмотренных настоящим Договором, подписанных ЭП уполномоченных лиц Сторон.

3.3. Стороны не несут ответственности за возможные временные задержки исполнения и/или искажения ЭД, возникающие по вине лиц, предоставляющих услуги связи для использования в АИС «Бюджет-Смарт» («Бюджет-Web»).

3.4. Оператор не несет ответственности за убытки Участника, возникшие вследствие несвоевременного контроля Участником электронных сообщений, подтверждающих получение и обработку ЭД, неисполнения Участником ЭД, а также за несоблюдение Участником мер по обеспечению защиты от несанкционированного доступа к информации, в том числе и закрытым ключам подписи, на АРМ Участника.

3.5. Сторона не несет ответственность за убытки другой Стороны, возникшие вследствие несвоевременного сообщения о компрометации закрытых ключей подписи представителями другой Стороны, участвующими в АИС «Бюджет-Смарт» («Бюджет-Web»).

3.6. Участник несет ответственность за соблюдение требований предоставленной Оператором документации.

3.7. В случае неработоспособности АРМ Участника, произошедшей по вине Участника, а также в случае необходимости переноса ПО АРМ Участника на другое аппаратное обеспечение, Участник обязуется в срок не более 3-х рабочих дней обеспечить работоспособность АРМ Участника.

**4. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ**

4.1. При возникновении конфликтных ситуаций, возникающих в ходе обмена ЭД между Сторонами, Стороны должны стремиться разрешить их путем переговоров.

4.2. В случае, если конфликтная ситуация не урегулирована в результате переговоров Сторон, создается Комиссия из представителей Сторон в соответствии с Правилами (Приложение № 1).

4.3. Споры и разногласия, по которым Стороны не могут достигнуть соглашения, подлежат разрешению в суде в соответствии с законодательством Российской Федерации.

**5. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ, ПОРЯДОК ЕГО ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ**

5.1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ года.

5.2. Срок начала исполнения обязательств по Соглашению определяется Оператором, при условии обязательного уведомления Участника (в срок не менее чем за 5 рабочих дней до даты начала исполнения обязательств по настоящему Соглашению).

5.3. В случае принятия нормативного акта уполномоченным государственным органом по вопросам, регулируемым настоящим Соглашением, соответствующие положения Соглашения подлежат изменению по инициативе одной из Сторон.

5.4. Настоящее Соглашение может быть расторгнуто по письменному соглашению Сторон.

**6. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ**

6.1. Обмен электронными документами при осуществлении ЭДО Стороны осуществляют на безвозмездной основе.

6.2. По взаимному согласию Сторон в текст Соглашения могут вноситься изменения и дополнения.

6.3. Все изменения и дополнения к настоящему Соглашения имеют юридическую силу и являются действительными, если они составлены в письменном виде и подписаны Сторонами.

6.4. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

**8. АДРЕСА И РЕКВИЗИТЫ СТОРОН**

|  |  |
| --- | --- |
| **Оператор:** | **Участник:** |
| Управление финансов администрации  183006, г. Мурманск,  пр. Ленина, д. 75 |  |

**9. ПОДПИСИ СТОРОН**

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |  |
| --- | --- |
|  | Приложение № 1  к Соглашению об электронном взаимодействии  № \_\_\_\_\_от\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**ПРАВИЛА**

электронного документооборота

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

**1.1. Термины и определения**

В целях настоящего документа используются следующие термины и определения:

**Автоматизированное рабочее место** (далее – АРМ)– установленные у Оператора и Участника (далее – Стороны) программное обеспечение (далее – ПО) и технические средства, включая средства криптографической защиты информации (далее – СКЗИ), предназначенные для работы в системах электронного документооборота управления финансов администрации города Мурманск «Бюджет-Смарт» и «Бюджет-Web» (далее – АИС «Бюджет-Смарт» («Бюджет-Web»)).

**Администратор АРМ Участника** – сотрудник Участника, отвечающий за обеспечение бесперебойной эксплуатации ПО и технических средств АРМ Участника, контроль мероприятий по защите информации, хранение и учет электронных документов (далее – ЭД), взаимодействие с Оператором по техническим вопросам и вопросам обеспечения безопасности информации. На администратора АРМ Участника могут возлагаться задачи по отправке/приему электронных документов и сообщений.

**Администратор информационной безопасности Оператора** (далее – администратор информационной безопасности) – лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена ЭД с Участником.

**Владелец сертификата ключа подписи** – физическое лицо, на имя которого Уполномоченным удостоверяющим центром (далее – УУЦ) выдан сертификат ключа подписи (далее – Сертификат), и которое владеет соответствующим закрытым ключом подписи, позволяющим с помощью средств электронной подписи (далее – ЭП) создавать свою ЭП в ЭД (подписывать ЭД).

**Закрытый ключ электронной подписи** – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи.

**Заявка на получение сертификата ключа подписи** – документ на бумажном носителе, содержащий распечатку значения открытого ключа подписи Пользователя в шестнадцатеричной системе исчисления, наименование Участника и иные идентифицирующие Пользователя реквизиты, подписанный собственноручными подписями Пользователя и руководителя Участника и заверенный оттиском печати Участника.

**Компрометация криптоключей** – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

**Корректная ЭП –** ЭП лица, имеющего право подписи соответствующего документа, и для этой ЭП соблюдены следующие условия:

* сертификат, относящийся к этой ЭП, издан УУЦ и не утратил силу (действует) на момент проверки или на момент подписания ЭД;
* подтверждена подлинность этой ЭП в ЭД;
* ЭП используется в соответствии со сведениями, указанными в Сертификате.

**Носитель ключевой информации** – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

**Открытый ключ электронной подписи** – уникальная последовательность символов, соответствующая закрытому ключу ЭП, доступная Сторонам и предназначенная для подтверждения ЭП в ЭД. Принадлежность открытого ключа владельцу Сертификата в АИС «Бюджет-Смарт» («Бюджет-Web») подтверждается Сертификатом, изданным УУЦ.

**Отправитель** – юридическое лицо в АИС «Бюджет-Смарт» («Бюджет-Web»), которое само непосредственно направляет или от имени которого направляется ЭД.

**Подтверждение подлинности ЭП в ЭД –** положительный результат проверки принадлежности ЭП в ЭД владельцу Сертификата и отсутствия искажений в подписанном данной ЭП ЭД.

**Получатель** – юридическое лицо в АИС «Бюджет-Смарт» («Бюджет-Web»), которому ЭД отправлен самим отправителем или от имени отправителя.

**Пользователи** – лица Сторон, осуществляющие формирование, подписание, отправку/получение, проверку, хранение и учет ЭД или/и обеспечивающие эксплуатацию ПО и технических средств АРМ.

**Пользователь сертификата ключа подписи** – физическое лицо, использующее полученные у Оператора сведения о Сертификате для проверки принадлежности ЭП владельцу Сертификата.

**Программное обеспечение** (ПО) – совокупность программ и программных документов, необходимых для их эксплуатации.

**Сертификат ключа подписи** (Сертификат) **–** документ на бумажном носителе или ЭД с ЭП уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ ЭП и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности ЭП и идентификации владельца сертификата ключа подписи.

**Система электронного документооборота управления финансов администрации города Мурманск «Бюджет-Смарт» и «Бюджет-Web»** (АИС «Бюджет-Смарт» («Бюджет-Web»)) – совокупность ПО и технического оборудования, обеспечивающая процесс обмена электронными документами между Сторонами.

**Электронная подпись (ЭП) –** реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации.

**Уполномоченное лицо** – лицо, имеющее право подписи ЭД.

**Уполномоченный удостоверяющий центр** (УУЦ) – основной компонент инфраструктуры открытых ключей, осуществляющий выполнение целевых функций удостоверяющего центра.

**1.2. Предмет регулирования настоящих Правил электронного документооборота в системе электронного документооборота управления финансов администрации города Мурманск «Бюджет-Смарт» и «Бюджет-Web»**

1.2.1. Настоящие Правилаэлектронного документооборота в системе электронного документооборота управления финансов администрации города Мурманск «Бюджет-Смарт» и «Бюджет-Web» (далее – Правила) устанавливают общие принципы осуществления электронного документооборота (далее – ЭДО) между Сторонами.

1.2.2. Настоящие Правила не регулируют вопросы обмена электронными сообщениями не являющимися ЭД в соответствии с Соглашением об обмене ЭД, заключаемыми между Сторонами (далее – Соглашение).

**1.3. Документы, регулирующие ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»)**

1.3.1. ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web») регулируется следующими документами:

– Соглашением;

– технической документацией на АРМ Участника, включая документацию на СКЗИ;

– законодательными и другими нормативными правовыми актами Российской Федерации.

**1.4. Порядок и условия допуска Участника к осуществлению документооборота в АИС «Бюджет-Смарт» («Бюджет-Web»)**

1.4.1. Для допуска к осуществлению документооборота в АИС «Бюджет-Смарт» («Бюджет-Web») Участник должен выполнить следующие мероприятия:

- заключить Соглашение с Оператором об обмене ЭД;

- создать условия для размещения рабочего места с использованием средств криптографической защиты информации (далее – СКЗИ), в соответствии с разделом IV Инструкции «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденную приказом Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте РФ от 13.06.2001 № 152 (далее – Инструкция № 152);

- назначить приказом ответственных лиц за осуществление обмена электронными документами, в том числе должностных лиц, наделенных правом электронной подписи;

- установить необходимые для осуществления ЭДО СКЗИ;

- установить ПО АРМ Участника;

- подать заявление на изготовление сертификата ключа ЭП;

- после получения уведомления об изготовлении сертификата произвести установку сертификата на своем рабочем месте и подтвердить ее;

- предоставить Оператору Акт о готовности к обмену электронными документами (Приложение № 2 к настоящему Соглашению).

1.4.2. Участник обеспечивает защиту АРМ АИС «Бюджет-Смарт» («Бюджет-Web») от несанкционированного доступа в соответствии с требованиями нормативных документов и законодательства Российской Федерации.

**1.5. Пользователи Участника**

1.5.1. Пользователями Участника являются работники Участника, осуществляющие формирование, отправку/получение, проверку, хранение и учет электронных документов и/или обеспечивающие эксплуатацию программно-технических средств АРМ Участника.

1.5.2. Состав пользователей Участника утверждается приказом Участника. В соответствии с выполняемыми должностными обязанностями выделяются следующие обязательные категории работников, которые имеют допуск к работе в АИС «Бюджет-Смарт» («Бюджет-Web») (один пользователь Участника может совмещать несколько категорий):

– администратор АРМ обмена электронными документами (далее – администратор Участника) – работник Участника, отвечающий за организацию и обеспечение бесперебойной эксплуатации программно-технических средств АРМ Участника, за обеспечение и контроль мероприятий по защите информации, за хранение и учет ЭД, за взаимодействие с Оператором по техническим вопросам и вопросам обеспечения безопасности информации;

– оператор АРМ обмена электронными документами (далее – оператор Участника) – работник Участника, отвечающий за формирование, отправку/получение, проверку электронных документов;

– уполномоченные лица – должностные лица и работники Участника, наделенные правом ЭП в ЭД.

1.5.3. Пользователи Участника допускаются к работе в АИС «Бюджет-Смарт» («Бюджет-Web») на основании приказов. Копии приказов о назначении пользователей Участника направляются Оператору.

1.5.4. Пользователи Участника несут персональную ответственность за безопасность ключевой информации и обязаны обеспечивать ее сохранность, неразглашение и нераспространение.

1.5.5. Пользователи Участника должны быть ознакомлены под роспись с документами, регулирующими ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»), определенными настоящими Правилами.

**1.6. Порядок вступления в действие настоящих Правил, а также внесения в них изменений**

1.6.1. Настоящие Правила вступают в силу в отношении Участника после заключения Соглашения между Сторонами.

1.6.2. Изменения и дополнения в настоящие Правила вносятся в порядке, установленном Соглашением.

**1.7. Прекращение действия настоящих Правил**

1.7.1. Обязательства Сторон по исполнению настоящих Правил прекращаются при расторжении Соглашения.

1.7.2. Прекращение действия настоящих Правил не влияет на юридическую силу и действительность ЭД, которыми Стороны обменивались до прекращения действия настоящих Правил.

**2. ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ**

**2.1. Требования, предъявляемые к ЭД**

2.1.1. ЭД, сформированные в АИС «Бюджет-Смарт» («Бюджет-Web») и подписанные надлежащим количеством корректных ЭП, имеют юридическую силу наравне с бумажными документами, подписанными собственноручными подписями.

2.1.2 ЭД считаются надлежащим образом оформленными при условии их соответствия законодательству Российской Федерации, а также документам, регулирующими ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»).

2.1.3. ЭД, не отвечающие требованиям, предъявляемым к ЭД настоящими Правилами, рассматриваются Сторонами, как ЭД, не имеющие юридической силы.

**2.2. Использование ЭП в ЭД**

2.2.1. ЭД может быть подписан только ЭП уполномоченных лиц Сторон, для которых УУЦ изданы действующие Сертификаты.

2.2.2. Прекращение действия Сертификатов уполномоченных лиц Сторон не влияет на юридическую силу и действительность ЭД, которыми Стороны обменивались до прекращения действия Сертификатов.

**2.3. Использование ЭД**

2.3.1. ЭД, подписанный надлежащим количеством корректных ЭП уполномоченных лиц Сторон, имеет равную юридическую силу с документом, представленным на бумажном носителе, подписанном собственноручными подписями уполномоченных лиц Сторон, и не может быть оспорен только на том основании, что он выполнен в электронном виде.

2.3.2. ЭД может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего ЭД осуществляется копирование ЭД вместе со всеми ЭП.

2.3.3. Все экземпляры ЭД являются подлинниками данного ЭД.

**2.4. Представление сведений, содержащихся в ЭД, на бумажном носителе**

2.4.1. Сведения, содержащиеся в ЭД, могут быть представлены (распечатаны) на бумажном носителе. В этом случае их соответствие ЭД должно быть заверено Оператором или Участником в установленном порядке.

2.4.2. Программы, осуществляющие представление сведений, содержащихся в ЭД на бумажных носителях, являются составной частью ПО, используемого в АИС «Бюджет-Смарт» («Бюджет-Web»).

**3. ОРГАНИЗАЦИЯ ЭДО**

**3.1. ЭДО**

3.1.1 ЭДО включает:

– формирование ЭД и подписание их ЭП с использованием закрытых ключей подписи соответствующих уполномоченных лиц Сторон;

– отправку и доставку ЭД;

– проверку подлинности ЭП в доставленном ЭД:

– подтверждение получения ЭД;

– отзыв ЭД;

– учет ЭД (регистрацию входящих и исходящих ЭД);

– хранение ЭД;

– создание дополнительных экземпляров ЭД;

– создание представлений (распечатывание) ЭД в бумажном виде.

**3.2. Формирование ЭД и их ЭП**

3.2.1 Формирование ЭД и подписание их ЭП осуществляется согласно документам, регулирующим ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»), определенным настоящими Правилами.

**3.3. Отправка и доставка ЭД**

3.3.1. В отношениях между отправителем и получателем ЭД считается исходящим от отправителя, если ЭД отправлен лицом, уполномоченным действовать от имени отправителя в отношении данного ЭД.

3.3.2. ЭД не считается исходящим от отправителя, если получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что ЭД не исходит от отправителя, или получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что получен искаженный ЭД.

**3.4. Проверка подлинности доставленного ЭД**

3.4.1. Проверка подлинности ЭД включает:

* проверку ЭД на соответствие документам, регулирующим ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»), определенным настоящими Правилами;
* проверку подлинности всех ЭП в ЭД;
* проверку статуса соответствующих Сертификатов на момент подписания или приема соответствующего ЭД.

3.4.2. В случае положительного результата проверки подлинности ЭД, данный ЭД принимается к исполнению. В противном случае данный ЭД к исполнению не принимается, о чем получатель должен послать уведомление отправителю с указанием причины непринятия документа к исполнению.

3.4.3. Не принятые к исполнению ЭД сохраняются на случай разрешения относительно них конфликтных ситуаций.

**3.5. Подтверждение получения ЭД**

3.5.1 Подтверждение получения ЭД (уведомление) производится в автоматическом режиме, согласно документам, регулирующим ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»), определенным настоящими Правилами.

**3.6. Отзыв ЭД**

3.6.1. Участник вправе отозвать отправленный ЭД согласно документам, регулирующим ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»), определенным настоящими Правилами.

3.6.2. ЭД может быть отозван отправителем до начала его обработки (исполнения) получателем.

**3.7. Учет ЭД**

3.7.1. Учет ЭД осуществляется путем ведения электронных журналов учета в АРМ Участника.

3.7.2. Срок хранения электронных журналов учета определяется сроком хранения учитываемых ЭД.

**3.8. Хранение ЭД**

3.8.1. ЭД должны храниться с сохранением всех реквизитов (полей), включая все ЭП. Допускается хранение ЭД в виде последовательности всех полей ЭД (включая все ЭП) в записи базы данных.

3.8.2. Срок хранения ЭД должен соответствовать сроку хранения соответствующих документов на бумажных носителях.

3.8.3. Хранение ЭД должно сопровождаться хранением соответствующих электронных журналов учета, Сертификатов, подтверждений о доставке ЭД, а также ПО, обеспечивающего возможность работы с электронными журналами и проверки ЭП хранимых ЭД.

**4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**4.1. Общие требования обеспечения защиты информации в АИС «Бюджет-Смарт» («Бюджет-Web»).**

4.1.1. В случае обмена конфиденциальной информацией Участник должен выполнять требования Инструкции № 152.

4.1.2. Учет СКЗИ, а также изготовление ключей ЭП осуществляет администратор АРМ Участника в Журнале поэкзэмплярного учета СКЗИ (приложение № 2 к Инструкции № 152).

**4.2. Управление ключевой информацией**

4.2.1. Управление ключевой информацией осуществляют администраторы информационной безопасности, уполномоченные лица УУЦ и администраторы АРМ Участника.

4.2.2. Ключевая информация содержит сведения конфиденциального характера, хранится на учтенных в установленном порядке носителях ключевой информации и не подлежит передаче третьим лицам.

4.2.3. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения. При обращении с ними должны выполняться требования Инструкции № 152 и иных документов, регламентирующих порядок обращения с информацией ограниченного распространения в органах исполнительной власти, и настоящих Правил.

4.2.4. Учет носителей ключевой информации осуществляют администраторы АРМ Участника по соответствующим учетным формам (п. 4.1.2)

4.2.5. Требования по организации хранения и использования носителей ключевой информации.

4.2.5.1. Порядок хранения и использования носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.

4.2.5.2. Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

4.2.5.3. Не разрешается:

* производить несанкционированное копирование носителей ключевой информации;
* знакомить или передавать носители ключевой информации лицам, к ним не допущенным;
* выводить закрытые ключи подписи на дисплей или принтер;
* вставлять носитель ключевой информации в считывающее устройство других компьютеров;
* оставлять носитель ключевой информации без присмотра на рабочем месте;
* записывать на носитель ключевой информации посторонние файлы.

4.2.6. Порядок работы с ключами ЭП.

4.2.6.1. Формирование открытого и закрытого ключей подписи и соответствующей заявки на получение Сертификата должно осуществляться уполномоченными лицами Участника.

4.2.6.2. Запрос на издание Сертификата Пользователя в электронном виде передается на утверждение в УУЦ.

4.2.6.3. Заявки, оформленные и подписанные в установленном порядке, сопровождающиеся документами, подтверждающими права уполномоченных лиц на подпись документов, направляются в УУЦ, который при наличии соответствующего запроса на издание Сертификата, обеспечивает издание УУЦ Сертификата.

4.2.6.4. Ответственность за соответствие сведений, указанных в Сертификате, сведениям, указанным в Заявке и в представленных для регистрации сопровождающих документах уполномоченных лиц Участника, несет УУЦ, утвердивший запрос на издание Сертификата.

4.2.6.5. Пользователи Участника получают изданные УУЦ Сертификаты в установленном порядке.

4.2.6.6. Владельцы Сертификатов несут персональную ответственность за безопасность (сохранение в тайне) своих закрытых ключей подписи и обязаны обеспечивать их сохранность, неразглашение и нераспространение.

4.2.6.7. Срок действия Сертификата указывается в Сертификате. Владелец Сертификата получает право использования соответствующего закрытого ключа подписи для подписи ЭД в течении срока действия Сертификата.

4.2.6.8. Сертификат пользователя Участника доступен всем участникам АИС «Бюджет-Смарт» («Бюджет-Web») после опубликования его в справочнике сертификатов ключей подписи УУЦ.

4.2.6.9. Срок действия открытого и закрытого ключей подписи и соответствующих Сертификатов – один год.

4.2.6.10. За 10 рабочих дней до окончания срока действия Сертификата его владелец обязан выполнить формирование новых открытого и закрытого ключей подписи, соответствующего запроса на издание Сертификата и оформить заявку на получение нового Сертификата.

4.2.6.11. После окончания срока действия Сертификата его владелец теряет право использования закрытого ключа подписи, соответствующего отзываемому Сертификату и уничтожает указанный закрытый ключ подписи.

4.2.6.12. УУЦ обеспечивает хранение Сертификатов в течение срока хранения ЭД.

4.2.7. Все работы, связанные с управлением списком отозванных сертификатов и поддержанием его в актуальном состоянии, обеспечиваются УУЦ.

**4.3. Порядок действий при компрометации закрытых ключей подписи**

4.3.1. К событиям, связанным с компрометацией закрытых ключей подписи, относятся хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых закрытые ключи подписи могли стать доступными неуполномоченным лицам и (или) процессам.

4.3.2. При компрометации закрытого ключа подписи владелец соответствующего ему Сертификата немедленно прекращает его использование и незамедлительно сообщает об этом в соответствующий УУЦ и администратору безопасности информации Оператора.

4.3.3. После получения от владельца Сертификата Участника сообщения о компрометации закрытого ключа подписи уполномоченное лицо УУЦ или администратор безопасности информации проверяет достоверность полученного сообщения. В случае подтверждения полученной информации, инициируется процедура отзыва или приостановления действия соответствующего Сертификата.

4.3.4. Дата и время, с которой Сертификат считается недействительным в АИС «Бюджет-Смарт» («Бюджет-Web»), устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанного в списке отозванных сертификатов.

4.3.5. Уведомление о компрометации закрытых ключей подписи должно быть подтверждено официальным уведомлением Участника о компрометации в письменном виде. Уведомление должно содержать идентификационные параметры Сертификата. В случае непредставления уведомления, УУЦ вправе отказать в выдаче нового Сертификата.

4.3.6. Использовать скомпрометированные закрытые ключи подписи для подписи ЭД запрещается. При получении ЭД, подписанного скомпрометированным закрытым ключом подписи, данный ЭД считается недействительным, о чем получатель обязан отправить уведомление отправителю с указанием причины отказа исполнения документа.

4.3.7. В случае компрометации закрытого ключа и отзыва соответствующего Сертификата с публикацией в списке отозванных сертификатов, Участник установленным порядком изготавливает новые открытый и закрытый ключи подписи.

4.3.8 Сертификат, соответствующий скомпрометированному закрытому ключу, хранится в установленном порядке в УУЦ для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

**4.4. Отзыв сертификата ключа подписи**

4.4.1. УУЦ отзывает Сертификат Участника в следующих случаях:

* в случае компрометации;
* в случае прекращения действия Соглашения в отношении данного Участника;
* по заявлению в письменном виде владельца Сертификата, заверенному Участником.

4.4.2. В случае отзыва или приостановления действия Сертификата пользователя Участника УУЦ обеспечивает публикацию списка отозванных сертификатов с указанием серийного номера Сертификата, даты, времени и причины аннулирования. Дата и время, с которых Сертификат считается недействительным в АИС «Бюджет-Смарт» («Бюджет-Web»), устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанных в списке отозванных сертификатов.

**5. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ**

**В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭДО**

**5.1. Возникновение конфликтных ситуаций в связи с осуществлением ЭДО в АИС «Бюджет-Смарт» («Бюджет-Web»)**

5.1.1. В связи с осуществлением ЭДО возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения ЭД, а также использования в данных документах ЭП. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

* оспаривание факта отправления и/или получения ЭД;
* оспаривание времени отправления и/или получения ЭД;
* оспаривание содержания отправленного/полученного ЭД;
* оспаривание подлинности экземпляров ЭД;
* оспаривание целостности ЭД;
* оспаривание идентичности лица, заверившего ЭД ЭП;
* оспаривание полномочий лица, заверившего ЭД ЭП;

5.1.2. Конфликтные ситуации разрешаются (урегулируются) Сторонами в рабочем порядке и/или по итогам работы комиссии по разрешению конфликтной ситуации (далее – Комиссия).

5.1.3. В случае невозможности разрешения конфликтной ситуации в рабочем порядке и/или по итогам работы Комиссии, Стороны разрешают конфликтную ситуацию в претензионном порядке, либо в суде в порядке, установленном законодательством Российской Федерации.

**5.2. Уведомление о конфликтной ситуации**

5.2.1. В случае возникновения обстоятельств, свидетельствующих, по мнению одной из Сторон, о возникновении и/или наличии конфликтной ситуации, данная Сторона (далее – Сторона-инициатор) незамедлительно извещает другую заинтересованную Сторону о возможном возникновении и/или наличии конфликтной ситуации, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также ее предполагаемых причинах.

5.2.2. Стороны, которым было направлено извещение о конфликтной ситуации и участвующие в ее разрешении (далее – Стороны-ответчики), обязаны не позднее чем в течение следующего рабочего дня проверить наличие указанных в извещении обстоятельств, и по необходимости принять меры по разрешению конфликтной ситуации со своей стороны.

5.2.3. В тот же срок Стороны-ответчики извещают доступными способами Сторону-инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации.

**5.3. Разрешение конфликтной ситуации в рабочем порядке**

5.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Сторона-инициатор удовлетворена информацией, полученной в извещениях Сторон-ответчиков, и не имеет к ним претензий в связи с конфликтной ситуацией.

5.3.2. В случае если Сторона-инициатор не удовлетворена информацией, полученной от Сторон-ответчиков, для рассмотрения конфликтной ситуации формируется Комиссия.

**5.4. Формирование Комиссии по разрешению конфликтной ситуации**

5.4.1. В случае, если конфликтная ситуация не была разрешена в рабочем порядке, Сторона-инициатор, должна не позднее чем в течение двух рабочих дней после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации (далее – Уведомление) с предложением о формировании Комиссии по разрешению конфликтной ситуации Стороне-ответчику.

5.4.2. Уведомление должно содержать информацию о предмете и существе конфликтной ситуации, обстоятельствах, по мнению Стороны-инициатора, свидетельствующих о наличии конфликтной ситуации, возможных причинах и последствиях ее возникновения.

5.4.3. Уведомление должно содержать информацию с указанием фамилий, имен, отчеств, должностей и контактной информации должностных лиц Стороны-инициатора, уполномоченных в разрешении конфликтной ситуации.

5.4.5. Уведомление составляется на бумажном носителе, подписываются должностными лицами Стороны-инициатора, уполномоченными в разрешении конфликтной ситуации и передаются Стороне-ответчику в установленном порядке, обеспечивающим подтверждение вручения корреспонденции.

5.4.6. Уведомление может быть составлено и направлено в форме ЭД. При этом факт их доставки должен быть подтвержден.

**5.5. Формирование комиссии по разрешению конфликтной ситуации, ее состав**

5.5.1. Стороны, в течение трех рабочих дней с даты получения Уведомления Стороной-ответчиком, формируют Комиссию, состоящую из равного числа представителей Сторон. Формирование Комиссии подтверждается актом, подписанным Сторонами.

5.5.2. Устанавливается десятидневный срок работы Комиссии. В исключительных случаях срок работы Комиссии по согласованию Сторон может быть дополнительно продлен не более чем на десять дней.

5.5.3. В состав Комиссии назначаются представители служб информационно-технического обеспечения и служб обеспечения информационной безопасности, а также представители подразделений-исполнителей ЭД.

5.5.4. По инициативе любой из Сторон к работе Комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, в том числе представители поставщиков средств защиты информации. При этом Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

5.5.5. Лица, входящие в состав Комиссии должны обладать необходимыми знаниями и опытом работы в области подготовки и исполнения электронных документов, построения и функционирования АИС «Бюджет-Смарт» («Бюджет-Web»), организации и обеспечения информационной безопасности при обмене ЭД, должны иметь соответствующий допуск к необходимым для проведения работы Комиссии документальным материалам и программно-техническим средствам.

5.5.6. При участии в Комиссии представителей сторонних органов и организаций их право представлять соответствующие органы и организации должно подтверждаться официальным документом (доверенностью, предписанием, копией приказа или распоряжения).

**5.6. Задачи, права и полномочия комиссии по разрешению конфликтной ситуации**

5.6.1. Задача Комиссии – установить на организационно-техническом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о наличии конфликтной ситуации, ее причинах и последствиях.

5.6.2. Комиссия имеет право получать доступ к необходимым для проведения ее работы документальным материалам Сторон, на бумажных и электронных носителях.

5.6.3. Комиссия имеет право ознакомления с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета электронных документов.

5.6.4. Комиссия имеет право ознакомления с условиями и порядком эксплуатации Сторонами программно-технических средств обмена электронными документами.

5.6.5. Комиссия имеет право ознакомления с условиями и порядком изготовления, использования и хранения Сторонами ключевой информации, а также иной конфиденциальной информации и ее носителей, необходимых для работы средств обмена ЭД.

5.6.6. Комиссия имеет право получать объяснения от должностных лиц Сторон, обеспечивающих обмен ЭД.

5.6.7. Комиссия вправе получать от Сторон любую иную информацию, относящуюся, по ее мнению, к рассматриваемой конфликтной ситуации.

5.6.8. Для проведения необходимых проверок и документирования данных, Комиссией могут применяться специальные программно-технические средства.

5.6.9. Комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов, кроме организационно-технической.

**5.7. Протокол работы комиссии по разрешению конфликтной ситуации**

5.7.1. Все действия, предпринимаемые Комиссией для выяснения фактических обстоятельств, а также выводы, сделанные комиссией, заносятся в Протокол работы Комиссии.

5.7.2. Протокол работы Комиссии должен содержать следующие данные:

* состав Комиссии с указанием сведений о фамилиях, именах, отчествах, местах работы, занимаемых должностях;
* краткое изложение обстоятельств, свидетельствующих, по мнению Стороны-инициатора, о возникновении и/или наличии конфликтной ситуации;
* установленные Комиссией фактические обстоятельства;
* мероприятия, проведенные Комиссией для установления наличия, причин возникновения и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;
* выводы, к которым пришла Комиссия в результате проведенных мероприятий;
* подписи всех членов комиссии.

5.7.3. В случае, если мнение члена или членов Комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов Комиссии, в Протокол заносится соответствующая запись, которая подписывается членом или членами Комиссии, чье особое мнение отражает соответствующая запись.

5.7.4. Протокол составляется в форме документа на бумажном носителе, по экземпляру каждой Стороне. По обращению любого из членов Комиссии Стороной, к которой было направлено обращение, ему должна быть выдана заверенная копия Протокола.

**5.8. Акт по итогам работы комиссии по разрешению конфликтной ситуации**

5.8.1. По итогам работы Комиссии составляется Акт, при этом Акт должен содержать следующую информацию:

* состав Комиссии;
* дату и место составления Акта;
* даты и время начала и окончания работы Комиссии;
* фактические обстоятельства, установленные Комиссией;
* краткий перечень мероприятий, проведенных Комиссией;
* выводы, к которым пришла Комиссия в результате проведенных мероприятий;
* подписи членов Комиссии;
* в случае наличия – особое мнение члена или членов Комиссии.

5.8.2. К Акту может прилагаться особое мнение члена или членов Комиссии, не согласных с выводами Комиссии, указанными в Акте. Особое мнение составляется в произвольной форме, подписывается членом или членами Комиссии, чье мнение оно отражает.

5.8.3. Акт составляется в форме документа на бумажном носителе, по одному экземпляру каждой Стороне. По обращению любого из членов Комиссии, Стороной, к которой было направлено обращение, ему должна быть выдана заверенная копия Акта.

**5.9. Разрешение конфликтной ситуации по итогам работы комиссии**

5.9.1. Акт Комиссии является основанием для принятия Сторонами решения по урегулированию конфликтной ситуации.

5.9.2. В срок не более трех рабочих дней со дня окончания работы Комиссии, Стороны на основании выводов Комиссии принимают меры по разрешению конфликтной ситуации и извещают другие Стороны о принятых мерах.

5.9.3. Конфликтная ситуация признается разрешенной по итогам работы Комиссии, если Стороны удовлетворены выводами, полученными Комиссией, мерами, принятыми другими участвующими в разрешении конфликтной ситуации Сторонами, и не имеют взаимных претензий.

**5.10. Претензионный порядок разрешения конфликтной ситуации**

5.10.1. В случае, если конфликтная ситуация не разрешена по итогам работы Комиссии, в случае прямого или косвенного отказа одной из Сторон от участия в работе, или если одной из Сторон создавались препятствия работе Комиссии, а также в иных случаях, если одна из Сторон считает, что ее права в связи с обменом ЭД были нарушены, она обязана направить Стороне, которая, по его мнению, нарушила ее права, Претензию.

5.10.2. Претензия должна содержать:

* изложение существа требований Стороны-инициатора;
* при возможности денежной оценки претензии – ее сумму и расчет;
* изложение фактических обстоятельств, на которых основываются требования Стороны-инициатора и доказательства, подтверждающие их, со ссылкой на соответствующие нормы законодательства и нормативных правовых актов;
* сведения о работе Комиссии и, в случае, если Комиссия работала в связи с рассматриваемой конфликтной ситуацией, копии материалов работы Комиссии, независимо от выводов Комиссии, согласия или несогласия с этими выводами Стороны-инициатора;
* иные документы, имеющие значение, по мнению Стороны-инициатора;
* перечень прилагаемых к Претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по Претензии.

5.10.3. Претензия составляется в форме документа на бумажном носителе, подписывается руководителем Стороны-инициатора либо его заместителем, заверяется печатью Стороны-инициатора. Претензия и прилагаемые к ней документы направляются в адрес Стороны-ответчика в установленном порядке, обеспечивающим подтверждение вручения корреспонденции.

5.10.4. Сторона, в адрес которой направлена Претензия, обязана в срок не позднее трех рабочих дней удовлетворить требования Претензии или представить мотивированный отказ в их удовлетворении. Непредставление ответа на Претензию в течение указанного срока является нарушением установленного настоящими Правилами претензионного порядка и может рассматриваться в качестве отказа в удовлетворении требований Претензии.

**5.11. Разрешение конфликтной ситуации судами**

5.11.1. В случае невозможности разрешения споров и разногласий по конфликтной ситуации в рабочем порядке, по итогам работы Комиссии или в претензионном порядке Стороны передают их на рассмотрение суда в порядке, установленном законодательством Российской Федерации.

|  |  |
| --- | --- |
|  | Приложение № 2  к Соглашению об электронном взаимодействии  № \_\_\_\_\_от\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

АКТ

о готовности к обмену электронными документами

г. Мурманск «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

Комиссия, назначенная приказом \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ года №\_\_\_\_\_, в составе:

Председатель комиссии:

Члены комиссии:

1. Провела проверку помещения, в котором размещено автоматизированное рабочее место обмена электронными документами, расположенного по адресу:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (обязательно указать кабинет)

а также проверила наличие охранно-пожарной сигнализации, средств опечатывания, наличия сейфов (металлических шкафов), соблюдения требований размещения автоматизированного рабочего места.

2. Провела проверку готовности программно-технических средств обмена электронными документами, в том числе средств защиты информации от несанкционированного доступа автоматизированных рабочих мест:

- средства криптографической защиты VipNet CSP;

- средства электронной подписи;

- средства антивирусной защиты.

3. Провела проверку наличия нормативной, технической, эксплуатационной и иной документации, регламентирующей обмен электронными документами.

4. Провела проверку подготовки лиц, ответственных за осуществление обмена электронными документами, а также лиц, уполномоченных правом электронной подписи, знания ими положений соответствующей нормативной, технической и эксплуатационной документации.

Заключение комиссии:

Помещение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (адрес), в котором размещено автоматизированное рабочее место со средствами криптографической защиты информации соответствует требованиям Инструкции «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ при Президенте Российской Федерации от 13.06.2001 № 152.

Лица, ответственные за осуществление обмена электронными документами, нормативно-техническую документацию по обмену электронными документами изучили.

Программно-технические средства и средства защиты информации от несанкционированного доступа установлены на автоматизированном рабочем месте в соответствии с нормативной технической документацией.

Председатель комиссии:

Члены комиссии: