ПРАВИТЕЛЬСТВО СВЕРДЛОВСКОЙ ОБЛАСТИ
МИНИСТЕРСТВО ФИНАНСОВ
СВЕРДЛОВСКОЙ ОБЛАСТИ

ПРИКАЗ

29.09.2017 № 417

г. Екатеринбург

О переходе на юридически значимый документооборот в программном комплексе «Бюджет – WEB»

В целях внедрения юридически значимого электронного документооборота при представлении бюджетной отчетности, сводной бухгалтерской отчетности государственных (муниципальных) бюджетных и автономных учреждений, отчетов по сети и контингентам получателей бюджетных средств, состоящих на бюджете субъекта Российской Федерации и бюджетах муниципальных образований в Министерство финансов Свердловской области в программном комплексе «Бюджет – WEB», в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», приказами Минфина России от 28.12.2010 № 191н «Об утверждении Инструкции о порядке составления и представления годовой, квартальной и месячной отчетности об исполнении бюджетов бюджетной системы Российской Федерации» и от 25.03.2011 № 33н «Об утверждении Инструкции о порядке составления, представления годовой, квартальной бухгалтерской отчетности государственных (муниципальных) бюджетных и автономных учреждений»:

ПРИКАЗЫВАЮ:

1. Установить, что с 1 января 2018 года бюджетная отчетность, сводная бухгалтерская отчетность государственных (муниципальных) бюджетных и автономных учреждений, отчетов по сети и контингентам получателей бюджетных средств, состоящих на бюджете субъекта Российской Федерации и бюджетах муниципальных образований, представляется главными администраторами средств областного бюджета, финансовыми органами городских округов, финансовыми органами муниципальных районов, Территориальным фондом обязательного медицинского страхования Свердловской области (далее – субъекты отчетности) в Министерство финансов Свердловской области в электронном виде, с использованием электронной

подписи, посредством формирования отчетных форм в базе данных программного комплекса «Бюджет – WEB», в соответствии с соглашением об обмене электронными документами.

2. Утвердить форму соглашения об обмене электронными документами в программном комплексе «Бюджет – WEB» (прилагается).

3. Утвердить Положение о порядке работы со средствами криптографической защиты информации в программном комплексе «Бюджет – WEB» (прилагается).

4. Отделу автоматизации бюджетного процесса в срок до 1 января 2018 года:

обеспечить настройку программного комплекса «Бюджет – WEB» для осуществления субъектами отчетности возможности подписания отчетных форм в электронном виде в базе данных программного комплекса «Бюджет – WEB» электронной подписью;

провести регистрацию квалифицированных сертификатов ключа проверки электронной подписи субъектов отчетности.

5. Контроль за исполнением настоящего приказа возложить на Заместителя министра финансов А.С. Старкова.

6. Настоящий приказ опубликовать на официальном интернет-портале правовой информации Свердловской области (www.pravo.gov66.ru).

Заместитель Губернатора
Свердловской области – Министр финансов  Г.М. Кулаченко

УТВЕРЖДЕНА
приказом Министерства финансов
Свердловской области
от 29.09.2017 № 417
«О переходе на юридически значимый
документооборот в программном
комплексе «Бюджет – WEB»

ФОРМА СОГЛАШЕНИЯ
об обмене электронными документами

г. Екатеринбург «____»_____20___

Раздел 1. Термины и определения, используемые в настоящем соглашении

Система – программный комплекс «Бюджет – WEB», правообладатель компания ООО «Кейсистем» (далее – разработчик), предназначенный для автоматизации процесса формирования, приема, передачи, обработки и хранения форм отчетности.

Юридически значимый электронный документооборот (ЮЗЭД) – документооборот на базе системы, в котором участники юридически значимого электронного документооборота совершают действия по принятию к исполнению документов в электронной форме, удостоверенных электронной подписью, и при этом несут ответственность за совершение, либо не совершение этих действий.

Организатор – Министерство финансов Свердловской области, участник и координатор юридически значимого электронного документооборота на базе системы, который осуществляет конфигурацию серверной части системы.

Телекоммуникационные каналы связи – это совокупность технических и программных средств, посредством которых осуществляется передача и прием информации между объектами. Используемые каналы связи определяются организатором.

Клиентская часть системы – аппаратно-программный комплекс, предназначенный для обработки и передачи данных по телекоммуникационным каналам связи с рабочих машин сотрудников на серверную часть системы.

Серверная часть системы – аппаратно-программный комплекс, предназначенный для хранения, обработки и передачи данных по телекоммуникационным каналам связи на клиентские части системы.

Регламент применения электронной подписи участниками юридически значимого электронного документооборота (регламент) – утвержденный организатором документ, фиксирующий техническую сторону организации юридически значимого электронного документооборота в программном комплексе «Бюджет – WEB».

Квалифицированная электронная подпись (ЭП) – электронная подпись, соответствующая следующим признакам:

получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи, получивших (получившего) подтверждения соответствия требованиям, установленным Федеральным законом от 6 апреля 2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ);

позволяет определить лицо, подписавшее электронный документ;

позволяет обнаружить факт внесения изменений в электронный документ после его подписания;

ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

Электронный документ – документ, в котором информация представлена в электронной форме в формате системы. Юридическая значимость электронного документа подтверждается ЭП.

Ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.

Средства криптографической защиты информации (СКЗИ) – аппаратные и (или) программные средства, обеспечивающие применение ЭП (создание, проверка ЭП, создание ключа ЭП и ключа проверки ЭП), и (или) шифрование при осуществлении электронного документооборота, а также обеспечивающие защиту информации по утвержденным стандартам и сертифицированные в соответствии с действующим законодательством.

Нарушение конфиденциальности ключа ЭП – утрата доверия к тому, что ключ используется только конкретным уполномоченным сотрудником и только по назначению.

Материальный носитель – материальный объект, используемый для записи и хранения информации, необходимой для подписания электронных документов ЭП.

Удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронной подписи, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ, и получившие аккредитацию.

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия УЦ требованиям Федерального закона № 63-ФЗ.

Квалифицированный сертификат ключа проверки электронной подписи (сертификат) – сертификат ключа проверки электронной подписи, выданный УЦ либо доверенным лицом УЦ в форме, требования к которой утверждены приказом ФСБ России от 27 декабря 2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Владелец Сертификата – лицо, которому в установленном Федеральным законом № 63-ФЗ порядке выдан сертификат ключа проверки ЭП.

Список отозванных сертификатов – электронный документ с электронной подписью УЦ, включающий в себя список серийных номеров сертификатов ключей проверки ЭП, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

Реестр сертификатов – справочник системы, который содержит перечень сертификатов Уполномоченных сотрудников участников.

Ключевой документ – ключевой носитель, содержащий ключ ЭП, а при необходимости – контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключа ЭП.

Правила подписания – настроечный параметр системы, позволяющий установить права на подписание электронных документов ЭП.

Правила проверки – настроечный параметр системы, позволяющий производить контроль на предмет наличия ЭП Уполномоченных сотрудников на определенных статусах электронных документов.

Статус электронного документа – атрибут электронного документа, идентифицирующий его состояние по определенному признаку.

Сторона – юридическое лицо, принимающее участие в юридически значимом электронном документообороте (в лице уполномоченных сотрудников) на базе системы, присоединившееся к соглашению об обмене электронными документами и осуществляющее формирование и передачу форм отчетности организатору.

Участник – сторона или организатор (вместе – участники).

Сотрудник – пользователь, имеющий имя и пароль для входа в систему и наделенный полномочиями для работы в системе.

Уполномоченный сотрудник – руководитель участника (либо лицо, его замещающее), главный бухгалтер участника (либо лицо, его замещающее), наделенные полномочиями по подписанию электронной подписью электронных документов в системе.

В случае передачи полномочий по ведению бюджетного учета иному государственному учреждению (органу государственной власти) отчетность подписывается руководителем субъекта отчетности, передавшего полномочия по ведению учета, и главным бухгалтером учреждения (органа власти), осуществляющего ведение бюджетного учета.

Уполномоченный сотрудник назначается приказом участника.

Раздел 2. Предмет соглашения

2.1. Настоящее соглашение определяет условия и порядок обмена электронными документами между участниками на базе системы.

2.2. Настоящее соглашение определяет права и обязанности участников, возникающие при осуществлении ЮЗЭД на базе системы с учетом обеспечения информационной безопасности.

2.3. Настоящее соглашение является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации. Сторона принимает условия настоящего соглашения путем присоединения к соглашению за счет подписания и предоставления организатору заявления о присоединении к настоящему соглашению по форме согласно приложению № 1 к настоящему соглашению.

2.4. Факт присоединения стороны к соглашению является полным принятием стороной условий соглашения и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении. Сторона, присоединившаяся к соглашению, принимает дальнейшие изменения (дополнения), вносимые в соглашение, в соответствии с условиями соглашения.

Раздел 3. Общие положения

3.1. Участники осуществляют передачу и прием юридически значимых электронных документов на базе системы по телекоммуникационным каналам связи.

3.2. С целью обеспечения авторства, целостности и конфиденциальности электронных документов при информационном взаимодействии участники используют сертифицированные, в соответствии с законодательством Российской Федерации, СКЗИ.

3.3. Используемые при информационном взаимодействии участников, электронные документы с ЭП, сформированные Участниками средствами СКЗИ, имеют равную юридическую силу с документами на бумажном носителе, подписанными соответствующими собственноручными подписями уполномоченных сотрудников участников. При этом для их ЭП соблюдены следующие условия:

сертификаты изданы УЦ и не утратили силу (действуют) на момент проверки или на момент подписания электронного документа;

ЭП используется в соответствии со сведениями, указанными в сертификате.

3.4. Участники признают, что используемые при ЮЗЭД в системе СКЗИ, реализующие функции создания ЭП, достаточны для подтверждения следующего:

электронный документ подписан уполномоченным сотрудником стороны его направившей (подтверждение авторства отправленного электронного документа);

электронный документ не претерпел изменений в процессе передачи (подтверждение целостности и подлинности электронного документа).

Раздел 4. Права и обязанности сторон

4.1. Организатор обязан:

4.1.1. Обеспечить функционирование серверной части системы и необходимого аппаратно-программного комплекса, а также обеспечить другой необходимой информацией для предоставления стороне возможности передачи юридически значимых электронных документов организатору.

4.1.2. При изменении регламента произвести (в соответствии с обновленным регламентом) настройки на серверной части системы и оповестить по телекоммуникационным каналам связи сторону об этих изменениях.

4.1.3. Немедленно уведомить сторону любым доступным способом в случаях выявления:

ошибок в работе системы при работе с ЭП (подписания ЭП, проверка ЭП и др.);

ошибок, возникающих в связи с попытками нарушения информационной безопасности;

компрометации ключа ЭП.

4.1.4. Вести актуальный реестр сертификатов уполномоченных сотрудников участников на основе принятых сертификатов и списка отозванных сертификатов от стороны.

4.1.5. Хранить материальные носители, содержащие ключи ЭП уполномоченных лиц организатора, в месте, исключающем доступ неуполномоченных лиц и (или) возможность повреждения материальных носителей.

4.1.6. При условии соответствия электронных документов, признакам и требованиям к юридически значимым электронным документам, указанным в регламенте (приложение № 3), принять от стороны электронный документ для дальнейшей проверки в соответствии с приказами организатора.

4.1.7. Предоставить стороне перечень форм отчетности, подписываемых ЭП, в соответствии с федеральным и региональным законодательством.

4.2. Организатор имеет право:

4.2.1. В случае несоответствия электронного документа признакам и требованиям к юридически значимым электронным документам, отказать стороне в приеме электронного документа с указанием мотивированной причины отказа.

4.2.2. Приостановить осуществление ЮЗЭД при:

несоблюдении стороной требований по передаче электронных документов и обеспечению информационной безопасности в соответствии с настоящим соглашением;

разрешении спорных ситуаций;

выполнении неотложных аварийных и ремонтно-восстановительных работ системы.

4.2.3. На урегулирование вопросов в случае возникновения конфликтных ситуаций.

4.2.4. В соответствии с требованиями законодательства Российской Федерации в одностороннем порядке произвести изменения настоящего соглашения (включая все приложения к соглашению) и настроить серверную часть системы в целях выполнения условий обновленного регламента.

4.3. Сторона обязана:

4.3.1. Обеспечить функционирование аппаратно-программного комплекса клиентской части уполномоченных сотрудников стороны для обеспечения работоспособности ЮЗЭД.

4.3.2. Выполнять требования УЦ в соответствии с регламентом УЦ и другими документами, регламентирующими процесс взаимодействия УЦ и пользователей услуг УЦ.

4.3.3. Обеспечить всеми необходимыми средствами (сертифицированные СКЗИ, квалифицированные сертификаты, ключевые носители и считывателями информации т.д.), Уполномоченных сотрудников Стороны.

4.3.4. Передавать организатору электронные документы, оформленные в соответствии с регламентом.

4.3.5. В целях обеспечения безопасности обработки и передачи юридически значимых электронных документов:

соблюдать требования, изложенные в разделе 5 настоящего соглашения, и требования положения о порядке работы со средствами криптографической защиты информации, утвержденного приказом организатора;

соблюдать требования эксплуатационной документации на используемые СКЗИ;

прекращать использование ЭП в случае компрометации ключа ЭП и немедленно любым доступным способом информировать организатора и УЦ об указанном факте;

хранить ключевой документ в месте, исключающем доступ неуполномоченных лиц и /или возможность его повреждения.

4.3.6. В случае невозможности исполнения обязательств по настоящему соглашению немедленно известить организатора о приостановлении исполнения обязательств.

4.3.7. В случае невозможности использования ЭП сторона оформляет и передает организатору документы на бумажном носителе и в электронном виде в формате системы.

4.3.8. При возникновении споров, связанных с принятием или непринятием электронных документов, подписанных ЭП, входящих в перечень юридически значимых электронных документов, руководствоваться разделом 8 настоящего соглашения.

4.3.9. Заменить сертификат ключа ЭП в порядке, предусмотренном для его оформления согласно регламенту УЦ, в следующих случаях:

смены уполномоченных сотрудников стороны, наделенных полномочием подписи электронных документов;

изменения данных, идентифицирующих уполномоченного сотрудника стороны;

смены ключей ЭП;

в иных случаях, прекращающих действие сертификата.

4.3.10. Немедленно уведомить организатора любым доступным способом в случаях:

возникновения угрозы использования (копирования) иными лицами ключа ЭП, принадлежащего уполномоченному сотруднику стороны;

утраты ключевого документа уполномоченного сотрудника стороны;

изменения состава уполномоченных сотрудников стороны, обладающих правом использования ключей ЭП.

4.3.11. Обеспечить подписание и хранение отчетности в электронном виде в соответствии с установленными организатором требованиями;

4.3.12. Обеспечить идентичность показателей отчетных форм, представленных Организатору в электронном виде, показателям отчетности на бумажных носителях.

4.4. Сторона имеет право на урегулирование вопросов в случае возникновения конфликтных ситуаций.

Раздел 5. Безопасность эксплуатации средств криптографической защиты

5.1. Дистрибутивы СКЗИ, эксплуатационная и техническая документация к СКЗИ хранятся у ответственного за эксплуатацию СКЗИ сотрудника участника. Ключи ЭП хранятся у уполномоченных сотрудников. Хранение осуществляется в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих безконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.2. Ключевые документы с неработоспособными ключами ЭП ответственный за эксплуатацию СКЗИ сотрудник участника принимает у уполномоченного сотрудника. Неработоспособные ключевые документы подлежат уничтожению.

5.3. В Системе используется СКЗИ с открытым распределением ключей.

5.4. Электронный документ может быть подписан ЭП с использованием только того ключа ЭП, для которого выдан сертификат уполномоченного сотрудника.

5.5. Для подписи электронного документа уполномоченный сотрудник использует свой собственный закрытый ключ. Проверка подлинности ЭП осуществляется уполномоченным сотрудником с использованием открытого ключа.

5.6. Уполномоченный сотрудник не может подписать электронный документ ЭП, если истек срок действия закрытых ключей. Уполномоченный сотрудник не может проверить ЭП электронного документа в случае истечения срока действия Сертификата, необходимого для выполнения соответствующей операции.

5.7. Реализованные в СКЗИ алгоритмы шифрования и ЭП гарантируют невозможность восстановления закрытых ключей уполномоченного сотрудника по его открытым ключам.

5.8. При выявлении сбоев или отказов уполномоченный сотрудник обязан сообщить о факте их возникновения ответственному за эксплуатацию СКЗИ сотруднику участника, и предоставить ему ключевой документ для проверки его работоспособности. Проверку работоспособности ключевого документа ответственный за эксплуатацию СКЗИ сотрудник участника выполняет в присутствии уполномоченного сотрудника.

5.9. В случае, если ключевой документ потерял работоспособность, то сторона организует получение уполномоченным сотрудником ключевого документа.

5.10. Уполномоченному сотруднику запрещается:

осуществлять несанкционированное копирование ключей ЭП;

разглашать содержимое ключевого документа или передавать сами ключевые документы лицам, к ним не допущенным, оставлять без присмотра ключевой документ, выводить содержимое ключевого документа на дисплей или принтер;

вставлять ключевые документы в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания других аппаратных средств;

записывать на ключевой документ постороннюю информацию, использовать ключевой документ на неисправных устройствах считывания информации;

вносить какие-либо изменения в программное обеспечение СКЗИ.

Раздел 6. Порядок ввода в действие юридически значимого электронного документооборота на базе системы

6.1. Сторона в соответствии с документацией к системе устанавливает СКЗИ на компьютерах уполномоченных сотрудников.

6.2. Уполномоченные сотрудники стороны получают от УЦ средства ЭП: сертификаты, закрытые ключи, открытые ключи.

6.3. Сторона предоставляет организатору:

заявление о присоединении к настоящему соглашению по форме согласно приложению №1 к настоящему соглашению;

заявление на внесение в реестр системы сертификатов уполномоченных сотрудников по форме согласно приложению № 2 к настоящему соглашению;

копию приказа о назначении уполномоченных сотрудников, заверенную руководителем стороны;

полученные от УЦ сертификаты уполномоченных сотрудников стороны в электронном виде.

6.4. Организатор, после представления стороной документов указанных в пункте 6.3. настоящего соглашения, в течение одного дня вводит в действие сертификаты уполномоченных сотрудников стороны (вносит в реестр системы).

6.5. Участники приступают к эксплуатации юридически значимого электронного документооборота после принятия организатором от стороны документов, указанных в пункте 6.3. настоящего соглашения.

Раздел 7. Ответственность сторон

7.1. Участники несут ответственность за действия своих уполномоченных сотрудников при осуществлении ЮЗЭД в рамках настоящего соглашения.

7.2. Сторона несет ответственность за содержание всех электронных документов, подписанных ЭП уполномоченных сотрудников.

7.3. За неисполнение или ненадлежащее исполнение участниками своих обязательств по настоящему соглашению участники несут ответственность в соответствии с законодательством Российской Федерации.

7.4. Участники не отвечают за неисполнение или ненадлежащее выполнение своих обязательств по настоящему соглашению, если это было вызвано действиями (бездействием) другого участника.

7.5. При использовании телекоммуникационных каналов связи и передачи данных Участники не несут ответственности за возможные временные задержки при доставке юридически значимых электронных документов, произошедшие не по их вине.

Раздел 8. Разрешение конфликтных ситуаций

8.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения ЭД, а также использованием в данных документах ЭП.

8.2. Конфликтные ситуации разрешаются (урегулируются) сторонами в рабочем порядке путем обмена письменными обращениями, сбором рабочих совещаний, привлечения экспертов.

8.3. В случае невозможности разрешения конфликтной ситуации в рабочем порядке стороны разрешают конфликтную ситуацию в судебном порядке, в соответствии с законодательством Российской Федерации.

Раздел 9. Форс-мажорные обстоятельства

9.1. Участник не несет ответственность в случае невыполнения, несвоевременного или ненадлежащее исполнения какого-либо обязательства по настоящему соглашению, если указанное невыполнение, несвоевременное или ненадлежащее исполнение обусловлены исключительно наступлением и/или действием следующих обстоятельств (далее – форс-мажорные обстоятельства): обстоятельств непреодолимой силы; сбоев, неисправностей и отказов оборудования; сбоев и ошибок программного обеспечения; сбоев, неисправностей и отказов системы связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения, которые участник не мог ни предвидеть, ни предотвратить.

9.2. Сторона, надлежащее исполнение обязательств которой оказалось невозможным в силу влияния форс-мажорных обстоятельств, в течение 3 рабочих часов после их наступления информирует организатора о наступлении этих обстоятельств и об их последствиях любым доступным способом, и принимает все возможные меры с целью максимально ограничить отрицательные последствия, вызванные указанными форс-мажорными обстоятельствами.

9.3. Не извещение или несвоевременное извещение организатора стороной, надлежащее исполнение обязательств которого оказалось невозможным в силу влияния форс-мажорных обстоятельств, о наступлении этих обстоятельств, влечет за собой утрату права ссылаться на эти обстоятельства.

9.4. Наступление форс-мажорных обстоятельств влечет увеличение срока исполнения обязательств по настоящему соглашению на период их действия, если участники не договорились об ином.

9.5. Наступление форс-мажорных обстоятельств является достаточным условием для предоставления стороной организатору документов, входящих в перечень электронных документов, в соответствии с утвержденным регламентом применения ЭП участниками ЮЗЭД в системе, и оформленных надлежащим образом, на бумажном носителе.

Раздел 10. Порядок внесения изменений в соглашение

10.1. Все изменения и дополнения к настоящему соглашению, включая приложения к нему, производятся организатором в одностороннем порядке.

Изменения и дополнения вступают в силу в сроки, определенные организатором.

10.2. Изменения и дополнения в настоящее соглашение доводятся организатором до сведения стороны в течение 10 календарных дней с даты вступления их в силу, путем направления последнему соответствующего уведомления по телекоммуникационным каналам связи. Датой уведомления считается дата отправления стороне соответствующего уведомления.

10.3. Сторона вправе потребовать расторжения или изменения соглашения, если соглашение хотя и не противоречит законодательству Российской Федерации, но лишает эту сторону прав, обычно предоставляемых по соглашениям (договорам) такого вида, исключает или ограничивает ответственность другой стороны за нарушение обязательств либо содержит другие явно обременительные для присоединившейся стороны условия, которые она исходя из своих разумно понимаемых интересов не приняла бы при наличии у нее возможности участвовать в определении условий соглашения.

Раздел 11. Срок действия соглашения

11.1. Настоящее соглашение вступает в силу с момента передачи организатору, подписанного стороной заявления о присоединении. Соглашение заключается на неопределенный срок.

11.2. Участник вправе расторгнуть настоящее соглашение, письменно уведомив другого участника за 1 месяц. Соглашение считается расторгнутым по истечении 1 месяца со дня получения такого уведомления.

Раздел 12. Прочие условия

12.1. Настоящее соглашение хранится у организатора.

12.2. Заявление о присоединении к настоящему соглашению оформляется в 2-х экземплярах, имеющих одинаковую юридическую силу: один экземпляр хранится у каждого участника.

12.3. Все приложения, а также изменения и дополнения к настоящему соглашению являются его неотъемлемой частью.

К настоящему соглашению прилагаются и являются неотъемлемой частью:

приложение № 1 – Заявление о присоединении к соглашению об обмене электронными документами;

приложение № 2 – Заявление на внесение в реестр программного комплекса «Бюджет – WEB» сертификатов уполномоченных сотрудников;

приложение № 3 – Регламент применения электронной подписи и использования средств криптозащиты информации участниками юридически значимого документооборота в программном комплексе «Бюджет – WEB».

12.4. Расторжение настоящего соглашения не влияет на действительность и порядок действия электронных документов, подписанных ЭП уполномоченных сотрудников участников, до даты его расторжения.

Раздел 13. Адрес и реквизиты организатора:

Министерство финансов Свердловской области

Юридический адрес: 620000, Свердловская область, г. Екатеринбург, пр. Ленина, д. 34;

Почтовый адрес: 620000, Свердловская область, г. Екатеринбург, пр. Ленина, д. 34;

ИНН 6661004608

КПП 667101001

ЛС 02622009880

р/с 40201810400000100001

Банк Уральское ГУ Банка России г. Екатеринбург

БИК 046577001

Приложение № 1
к соглашению об обмене электронными документами

ЗАЯВЛЕНИЕ
о присоединении к соглашению об обмене электронными документами

_____
(наименование организации, включая организационно-правовую форму)
в лице _____
(должность)
_____,
(фамилия, имя, отчество)
действующего на основании_____

В соответствии со статьей 428 Гражданского Кодекса Российской Федерации полностью и безусловно присоединяется к Соглашению об обмене электронными документами.

С соглашением об обмене электронными документами и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Руководитель организации стороны_____/ Фамилия И.О./

М.П.

ИНН _____
Реквизиты _____
(Р/с банка, наименование, БИК, К/с банка)
_____
_____
юридический адрес_____
_____
почтовый адрес_____
_____

Приложение № 2
К соглашению об обмене
электронными документами

ЗАЯВЛЕНИЕ
на внесение в реестр программного комплекса «Бюджет – WEB» сертификатов уполномоченных сотрудников

«___»_____ 20____

_____
_____(далее – сторона),
(полное наименование организации в соответствии с учредительным документом)

в соответствии с условиями соглашения об обмене электронными документами, утвержденного приказом Министерства финансов Свердловской области от «____»_____2017 № _____, на основании приказа (распоряжения) от «___»_____20__ года №_____, просит организатора для осуществления юридически значимого электронного документооборота внести в реестр программного комплекса «Бюджет – WEB» сертификат (-ы) уполномоченного (-ых) сотрудника (-ов) стороны со следующими регистрационными данными:

	Должность	ФИО	E-mail	Серийный номер сертификата электронной подписи	Подпись уполномоченного сотрудника стороны
Руководитель					
Главный бухгалтер					

Настоящим сторона заявляет, что любые действия, которые будут совершены владельцем(-ми) сертификата(-ов) стороны на основании указанного(-ых) сертификата(-ов) являются действиями, совершаемыми владельцем(-ами) сертификата(-ов) от имени стороны, по указанию стороны и связаны с участием в обмене юридически значимыми электронными документами в программного комплекса «Бюджет – WEB».

Электронная (-ые) копия (-и) сертификата (-ов) уполномоченного (-ых) сотрудника (-ов) представлены организатору _____

_____
(указывается способ предоставления)

_____ _____ _____
(должность руководителя стороны) (подпись) (Ф.И.О.)

М.П.

Приложение № 3
К соглашению об обмене
электронными документами

РЕГЛАМЕНТ
применения электронной подписи и использования средств криптозащиты информации участниками юридически значимого документооборота в программном комплексе «Бюджет – WEB»

Раздел 1. Общие положения

1.1. Настоящий регламент определяет порядок и технические аспекты использования юридически значимого электронного документооборота в системе.

Раздел. 2 Средства применения электронной подписи

2.1. При работе с юридически значимым электронным документооборотом принимаются и признаются сертификаты, изданные УЦ.

Сертификат признается изданным УЦ, если подтверждена подлинность ЭП уполномоченного лица УЦ, которым подписан сертификат уполномоченного сотрудника участника.

Идентификационные данные, занесенные в сертификат, однозначно идентифицируют владельца сертификата и соответствуют идентификационным данным владельца сертификата, зарегистрированным УЦ.

2.2. Для определения статуса сертификата используется список отозванных сертификатов, издаваемый и публикуемый УЦ в порядке и с периодичностью, определяемой УЦ.

Местом публикации списков отозванных сертификатов является адрес информационного ресурса, определенный в регламенте или других актах УЦ.

2.3. В качестве средства ЭП используются СКЗИ, сертифицированные в соответствии с действующим законодательством Российской Федерации, а также совместимые с системой (согласно требованиям системы) и обеспечивающие:

реализацию функций создания ЭП в электронном документе с использованием ключа;

подтверждение подлинности ЭП в электронном документе с использованием сертификата;

создание ключей и сертификатов ЭП.

Раздел 3. Программное обеспечение, на базе которого происходит функционирование юридически значимого электронного документооборота

3.1. Функционирование юридически значимого электронного документооборота происходит на базе системы.

3.2. Организатор оставляет за собой право обновлять версию системы, с дальнейшей эксплуатацией юридически значимого электронного документооборота на обновленной версии без уведомления стороны, если такие изменения не повлекут существенных изменений механизма подписания электронного документа или изменения правил подписания и проверки ЭП.

Раздел 4. Перечень Электронных документов, включенных в юридически значимый электронный документооборот

4.1. Электронными документами, которые будут считаться юридически значимыми при условии подписания их ЭП (в случае выполнения всех условий равнозначности ЭП собственноручной в соответствии с Федеральным законом № 63-ФЗ), и с учетом остальных требований настоящего соглашения, являются формы бюджетной и сводной бухгалтерской отчетности государственных (муниципальных) автономных и бюджетных учреждений, отчеты по сети, штатам и контингентам получателей бюджетных средств, состоящих на бюджете субъекта Российской Федерации и бюджетах муниципальных образований (далее – формы отчетности), установленные соответствующими приказами Министерства финансов Российской Федерации, Федерального казначейства, а также дополнительные формы бюджетной и бухгалтерской отчетности, установленные нормативными документами Министерства финансов Российской Федерации, Федерального казначейства и Министерства финансов Свердловской области (далее – нормативными документами):

Раздел 5. Правила направления и подписания электронных документов

5.1. Сотрудник стороны после проведения в системе функциональных этапов по вводу/загрузке данных, проведения расчетов, контроля по логической увязке данных в формах отчетности (внутридокументный, междокументный контроль) устанавливает статус «Готов к проверке».

5.2. Уполномоченный сотрудник подписывает утвержденные формы отчетности.

Каждая форма отчетности должна содержать две ЭП:

подпись руководителя стороны;

подпись главного бухгалтера стороны.

5.3. Уполномоченные сотрудники участников обязаны подписывать юридически значимые электронные документы своей ЭП строго в соответствии с правилами подписания, в противном случае электронные документы не признаются юридически значимыми документами.

5.4. Форма отчетности, подписанная ЭП стороны, проверяется организатором на соответствие требованиям, установленным нормативными документами.

5.5. В случае выявления несоответствия форм отчетности требованиям нормативных документов, проверяемая форма отчетности переводится организатором в статус «На доработке».

Сторона в течение одного рабочего дня обязана предпринять необходимые меры для приведения формы отчетности в соответствие с установленными требованиями, после чего повторно переводит форму отчетности в состояние «Готов к проверке» и подписывает ЭП.

5.6. После проведения в системе расчетов, контроля по логической увязке данных в формах отчетности (внутридокументный, междокументный контроль) организатор переводит проверенные формы отчетности в следующие статусы:

состояние «Проверяется»;

состояние «Проверен»;

состояние «Утвержден».

Раздел 6. Контроль правил подписания юридически значимых электронных документов

6.1. Контроль правил подписания юридически значимых электронных документов осуществляется организационными мерами, также допускается контроль техническими средствами системы (использование правил проверки в системе). Способы контроля правил подписания определяются организатором.

УТВЕРЖДЕНО
приказом Министерства финансов
Свердловской области
от _____ № _____
«О переходе на юридически значимый
документооборот в программном
комплексе «Бюджет – WEB»

ПОЛОЖЕНИЕ
о порядке работы со средствами криптографической защиты информации в программном комплексе «Бюджет – WEB»

1. Термины и определения

Система – программный комплекс «Бюджет – WEB», правообладатель компания ООО «Кейсистем» (далее – разработчик), предназначенный для автоматизации процесса формирования, приема, передачи, обработки и хранения форм отчётности.

Юридически значимый электронный документооборот (ЮЗЭД) – документооборот на базе системы, в котором участники юридически значимого электронного документооборота совершают действия по принятию к исполнению документов в электронной форме, удостоверенных электронной подписью, и при этом несут ответственность за совершение, либо не совершение этих действий.

Организатор – Министерство финансов Свердловской области, участник и координатор юридически значимого электронного документооборота на базе системы, который осуществляет конфигурацию серверной части системы, а также настройку системы на серверных станциях.

Регламент применения электронной подписи участниками юридически значимого электронного документооборота (регламент) – утвержденный организатором документ, фиксирующий техническую сторону организации юридически значимого электронного документооборота.

Телекоммуникационные каналы связи – это совокупность технических и программных средств, посредством которых осуществляется передача и прием информации между объектами. Используемые каналы связи определяются организатором.

Квалифицированная электронная подпись (ЭП) – электронная подпись, соответствующая следующим признакам:

получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи, получивших (получившего) подтверждения соответствия требованиям, установленным Федеральным законом от 6 апреля 2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ);

позволяет определить лицо, подписавшее электронный документ;

позволяет обнаружить факт внесения изменений в электронный документ после его подписания;

ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

Электронный документ – документ, в котором информация представлена в электронной форме в формате системы. Юридическая значимость электронного документа подтверждается электронной подписью.

Ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.

Средства криптографической защиты информации (СКЗИ) – аппаратные и (или) программные средства, обеспечивающие применение ЭП (создание, проверка ЭП, создание ключа ЭП и ключа проверки ЭП), и (или) шифрование при осуществлении электронного документооборота, а также обеспечивающие защиту информации по утвержденным стандартам и сертифицированные в соответствии с действующим законодательством.

Нарушение конфиденциальности ключа ЭП – утрата доверия к тому, что ключ используется только конкретным уполномоченным сотрудником и только по назначению.

Материальный носитель – материальный объект, используемый для записи и хранения информации, необходимой для подписания электронных документов ЭП.

Удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронной подписи, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ, и получившие аккредитацию.

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона № 63-ФЗ.

Квалифицированный сертификат ключа проверки электронной подписи (сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром либо доверенным лицом аккредитованного удостоверяющего центра в форме, требования к которой утверждены приказом Федеральной Службы Безопасности Российской Федерации от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Владелец сертификата – лицо, которому в установленном Федеральным законом № 63-ФЗ порядке выдан сертификат ключа проверки ЭП.

Список отозванных сертификатов – электронный документ с электронной подписью удостоверяющего центра, включающий в себя список серийных

номеров сертификатов ключей проверки ЭП, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

Реестр Сертификатов – справочник системы, который содержит перечень сертификатов уполномоченных сотрудников участников.

Ключевой документ – ключевой носитель, содержащий ключ ЭП, а при необходимости – контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключа ЭП.

Сторона – юридическое лицо, принимающее участие в юридически значимом электронном документообороте (в лице уполномоченных сотрудников) на базе системы, присоединившееся к соглашению об обмене электронными документами и осуществляющее формирование и передачу форм отчетности организатору.

Участник – сторона или организатор (вместе – участники).

Сотрудник – пользователь, имеющий имя и пароль для входа в систему и наделенный полномочиями для работы в системе.

Уполномоченный сотрудник – руководитель участника (либо лицо, его замещающее), главный бухгалтер участника (либо лицо, его замещающее), наделенные полномочиями по подписанию электронной подписью электронных документов в системе.

В случае передачи полномочий по ведению бюджетного учета иному государственному учреждению (органу государственной власти) отчетность, подписывается руководителем субъекта отчетности, передавшего полномочия по ведению учета, и главным бухгалтером учреждения (органа власти), осуществляющего ведение бюджетного учета.

Уполномоченный сотрудник назначается приказом участника.

Раздел 2. Общие положения

2.1. Настоящий документ регламентирует порядок работы с СКЗИ в системе.

2.2. При работе с материальными носителями СКЗИ должны соблюдаться требования «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 Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации от 13.06.2001 № 152, Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной Службы Безопасности Российской Федерации от 09.02.2005 № 66, Федерального закона № 63-ФЗ, а также настоящего положения.

Раздел 3. Обеспечение информационной безопасности при работе со средствами криптографической защиты информации

3.1. Для использования в работе СКЗИ в системе ЮЗЭД допускаются только уполномоченные сотрудники участников.

Уполномоченные сотрудники должны быть ознакомлены под роспись с настоящим регламентом, а также другими документами, регулирующими использование СКЗИ в системе ЮЗЭД.

3.2. Уполномоченный сотрудник обязан:

обеспечить сохранность персональных СКЗИ (в том числе хранить в тайне ключи ЭП);

не допускать в пределах своих полномочий появления на персональном компьютере, задействованном в ЮЗЭД, появления постороннего, в том числе вредоносного программного обеспечения;

при обнаружении постороннего, в том числе вредоносного программного обеспечения, немедленно прекратить эксплуатацию СКЗИ в системе ЮЗЭД, сообщить организатору о случившемся факте и принять незамедлительные меры для ликвидации вредоносного программного обеспечения и устранения возможных последствий его деятельности;

не разглашать содержимое материальных носителей, содержащих ключи;

не передавать материальные носители иным лицам;

не выводить данные, содержащиеся на материальном носителе, на монитор и печатающее устройство;

при осуществлении деятельности, не связанной с использованием СКЗИ при работе в системе ЮЗЭД, не помещать материальный носитель, содержащий ключи, в считывающие устройства персонального компьютера;

не записывать на материальный носитель, содержащий ключи, постороннюю информацию;

не вносить изменения в программное обеспечение СКЗИ;

не использовать в работе бывшие в употреблении материальные носители (за исключением носителей типа RuToken и eToken).

3.3. Уполномоченный сотрудник несет персональную ответственность за ненадлежащее исполнение указанных выше обязанностей в пределах своих полномочий.

Раздел 4. Действия в случае нарушения конфиденциальности ключей

4.1. К событиям, связанным с нарушением конфиденциальности ключей, относят следующие:

утрата материальных носителей, содержащих ключи;

потеря материальных носителей, содержащих ключи, с их последующим обнаружением;

хищение материальных носителей, содержащих ключи;

разглашение содержимого материальных носителей, содержащих ключи;

несанкционированное копирование содержимого материальных носителей, содержащих ключи;

увольнение сотрудников, имевших доступ к материальным носителям,

содержащим ключи;

нарушение правил хранения и уничтожения (после окончания срока действия) материальных носителей, содержащих ключи;

возникновение подозрений на утечку содержимого материальных носителей, содержащих ключи, или ее искажение в системе;

нарушение печати на сейфе или замка сейфа, в котором хранятся материальные носители, содержащие ключи;

невозможность достоверного установления того, что произошло с материальными носителями (в том числе случаи, когда материальный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошёл в результате несанкционированных действий злоумышленников);

любые другие виды разглашения содержимого материальных носителей, содержащих ключи, в результате которых ключи могут стать доступными посторонним лицам и (или) воздействию вредоносного программного обеспечения.

4.2. Уполномоченный сотрудник участника самостоятельно определяет факт нарушения конфиденциальности ключа и оценивает значение этого события. Мероприятия по розыску и локализации последствий нарушения конфиденциальности ключа осуществляются Стороной совместно с организатором с участием уполномоченного сотрудника участника (владельца утратившего конфиденциальность ключа).

В случае установления факта нарушения конфиденциальности ключа уполномоченный сотрудник участника обязан незамедлительно прекратить эксплуатацию ЮЗЭД в системе и в срок не более одного рабочего дня уведомить о факте нарушения организатора, а также УЦ по телекоммуникационным каналам связи.

В течение 30 рабочих минут после поступления сообщения о нарушения конфиденциальности ключа организатор обеспечивает прекращение использования в ЮЗЭД соответствующего сертификата уполномоченного сотрудника участника.

Возобновление работы уполномоченного сотрудника участника в ЮЗЭД происходит только после замены утратившего конфиденциальность ключа.

Получение ключей (при выпуске новых и замене старых, отозванных и скомпрометированных ключей) уполномоченными сотрудниками участника производится в порядке, установленном УЦ.