



ВОЛОГОДСКАЯ ОБЛАСТЬ
ГОРОД ЧЕРЕПОВЕЦ
МЭРИЯ
ФИНАНСОВОЕ УПРАВЛЕНИЕ
РАСПОРЯЖЕНИЕ

16.08.2018 № 39

О безбумажной технологии документооборота
с главными распорядителями, получателями
средств городского бюджета, муниципальными
бюджетными и автономными учреждениями города

В целях реализации Соглашения №8 между финансовым управлением мэрии и муниципальным казенным учреждением «Финансово-бухгалтерский центр» о передаче функций по ведению бюджетного учета исполнения городского бюджета, казначейского исполнения городского бюджета, осуществлению проверки и обработки сводной бюджетной (бухгалтерской) отчетности, технической подготовке документов (материалов) к исполнению расходной части городского бюджета и информации об организациях в целях ведения реестра участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса, техническому ведению реестра источников доходов городского бюджета, ведению реестра администрируемых доходов, осуществлению мониторинга показателей финансово-хозяйственной деятельности муниципальных унитарных предприятий в рамках оперативного контроля от 28 марта 2017 года и обеспечения безбумажной технологии документооборота с главными распорядителями, получателями средств городского бюджета, муниципальными бюджетными и автономными учреждениями города Череповца в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место»:

1. Утвердить типовую форму Соглашения об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» (Приложение 1).

2. Утвердить типовую форму Дополнительного соглашения к Соглашению об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» (далее – Дополнительное соглашение) (Приложение 2).

3. Утвердить типовую форму Соглашения о расторжении Соглашения об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» (Приложение 3).

4. Утвердить Порядок проведения электронных платежных документов учреждений, подписанных электронной подписью в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» (Приложение 4).

5. Муниципальному казенному учреждению «Финансово-бухгалтерский центр», муниципальному бюджетному учреждению «Центр муниципальных информационных ресурсов и технологий» обеспечить заключение Соглашений об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» с главными распорядителями, получателями средств городского бюджета, муниципальными бюджетными и автономными учреждениями города Череповца (далее – учреждения) в соответствии с утвержденной типовыми формой, при изменении организационной структуры учреждений обеспечить заключение Дополнительного соглашения в соответствии с утвержденной типовой формой.

6. Признать утратившими силу приказы финансового управления мэрии:

- от 03.12.2015 № 51 «Об утверждении типовых форм Соглашений» за исключением пункта 4;

- от 28.10.2016 № 58 «О внесении изменений в приказ финансового управления мэрии от 03.12.2015 № 51».

7. Заместителю начальника сводного бюджетного отдела - главному бухгалтеру финансового управления мэрии (Н.Ю. Ефремова) довести настоящее распоряжение до главных распорядителей средств городского бюджета, муниципального казенного учреждения «Финансово-бухгалтерский центр», муниципального бюджетного учреждения «Центр муниципальных информационных ресурсов и технологий».

8. Главным распорядителям средств городского бюджета руководствоваться настоящим распоряжением и довести его до подведомственных учреждений.

Заместитель мэра города,
начальник финансового управления мэрии

А.В. Гуркина

УТВЕРЖДЕНА
распоряжением
финансового управления
мэрии
от 16.08.2018 № 39
(приложение 1)

Типовая форма

Соглашение №

об обмене электронными платежными документами в автоматизированной системе
«Бюджет», автоматизированной системе «Удаленное рабочее место»

г. Череповец

«___» _____ 20__ г.

Муниципальное казенное учреждение «Финансово-бухгалтерский центр»
(далее - МКУ «ФБЦ»), в лице директора _____,
действующего на основании Устава учреждения, муниципальное бюджетное
учреждение «Центр муниципальных информационных ресурсов и технологий» (далее
- МБУ «ЦМИРиТ»), именуемое в дальнейшем Администратор информационной
безопасности, в лице директора _____, действующего на
основании Устава учреждения, и

(полное наименование организации)

(далее - Клиент) - участник обмена электронными платежными документами (далее -
ЭПД), в лице _____,

(Ф.И.О., должность)

действующий

на

основании

_____, (при совместном
упоминании в тексте именуемые - Стороны), заключили настоящее трехстороннее
Соглашение о нижеследующем:

1. Предмет Соглашения

1.1. Настоящее Соглашение определяет условия и порядок обмена
электронными платежными документами с применением средств электронной
подписи между МКУ «ФБЦ» и Клиентом в автоматизированной системе «Бюджет»,
автоматизированной системе «Удаленное рабочее место» (далее - АС «Бюджет», АС
«УРМ»), а также устанавливает права и обязательства Сторон по обеспечению
информационной безопасности при обмене ЭПД.

1.2. С целью обмена ЭПД в МКУ «ФБЦ» и у Клиента установлены
автоматизированные рабочие места (далее - АРМ), оснащенные сертифицированными
средствами электронной подписи CryptoPro CSP. На указанных АРМ также
установлены: в МКУ «ФБЦ» - программный модуль «Сервер обмена данными и
синхронизации удаленных рабочих мест» программного комплекса АС «Бюджет»
(далее - «УРМ» сервер), у Клиента - удаленное рабочее место АС «УРМ».

Техническое сопровождение и администрирование «УРМ» сервера осуществляет Администратор информационной безопасности.

2. Общие положения

2.1. Термины, используемые в Соглашении, имеют следующие значения:

клиент - участник обмена электронными платежными документами, использующий УРМ (удаленное рабочее место) клиента для обмена ЭПД с АС «Бюджет»;

автоматизированная система «Бюджет» (АС «Бюджет») - центральная часть системы финансового электронного документооборота, установленная в МКУ «ФБЦ», предназначенная для комплексной автоматизации деятельности МКУ «ФБЦ» и Клиента;

автоматизированная система «Удаленное рабочее место» (АС «УРМ») - клиентская часть системы финансового электронного документооборота, реализующая функции создания и обработки ЭПД, а также приема-передачи ЭПД по телекоммуникационным каналам связи;

автоматизированное рабочее место обмена ЭПД (АРМ обмена ЭПД) - комплекс программных и аппаратных средств, используемых Сторонами для обмена ЭПД;

администратор информационной безопасности АС «Бюджет», АС «УРМ» (Администратор информационной безопасности) - полномочное лицо, назначенное приказом директора МБУ «ЦМИРиТ», исполняющее и контролирующее выполнение требований информационной безопасности при осуществлении обмена ЭПД с Клиентом;

администратор АРМ Клиента - полномочное лицо, назначенное Клиентом для обеспечения бесперебойной эксплуатации программных и аппаратных средств АРМ Клиента, проведения мероприятий по защите информации, хранению и учету ЭПД, взаимодействия с Администратором информационной безопасности по техническим вопросам и вопросам обеспечения безопасности информации;

программное обеспечение «Сервер обмена данными» (СОД) - серверная часть системы удаленного документооборота, обеспечивающая взаимодействие клиентского программного обеспечения АС «УРМ» с АС «Бюджет»;

система защищенного документооборота МКУ «ФБЦ» (СЗД ФБЦ) - комплексная информационная структура, созданная для обеспечения обмена ЭПД между участниками обмена. Система включает в свой состав АС «Бюджет», АС «УРМ», СОД, «КриптоПРО»;

уникальный идентификатор для доступа к СОД - имя (login) пользователя, присваиваемое Клиенту администратором информационной безопасности в соответствии с правилами, установленными документацией СОД;

пароль (password) - секретный набор символов, предназначенный для подтверждения личности и полномочий Клиента в АС «УРМ» финансового электронного документооборота;

ключи аутентификации - совокупность имени и пароля Клиента, используемых Клиентом для получения доступа к ресурсам СОД;

электронная подпись (ЭП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

носитель ключевой информации - съемное электронное устройство, защищенное пин-кодом (e-Token или ru-Token) и предназначенное для записи и хранения на нем ключа ЭП;

удостоверяющий центр - юридическое лицо или индивидуальный предприниматель либо государственный орган, осуществляющие функции по созданию и выдаче сертификата ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

средства ЭП - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП;

сертификат ключа проверки ЭП - документ на бумажном носителе или электронный документ, который включает в себя ключ ЭП и выдается удостоверяющим центром для подтверждения подлинности ЭП и идентификации Клиента;

квалифицированный сертификат ключа проверки ЭП (далее - сертификат) - сертификат ключа проверки ЭП, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи;

владелец сертификата ключа проверки электронной подписи (Владелец СКП) - лицо, которому в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», выдан сертификат ключа проверки ЭП;

законодательство - нормативно-правовые акты РФ и субъекта РФ, иные правовые акты;

компрометация ключа ЭП - событие, определенное Владельцем СКП как ознакомление неуполномоченным лицом (лицами) с его закрытым ключом ЭП, хищение, подмена, утеря, копирование носителя ключа ЭП, а также все случаи подозрения на то, что указанные события могли иметь место;

электронный платежный документ (ЭПД) - электронный документ, являющийся основанием для совершения операций по лицевым счетам, открытым Клиенту в финансовом управлении мэрии города Череповца (далее - финансовое управление мэрии), ведение которых осуществляется в МКУ «ФБЦ» на основании соглашения, заключенного между финансовым управлением мэрии и МКУ «ФБЦ», подписанный электронной подписью и имеющий равную юридическую силу с платежным документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным оттиском печати.

2.2. МКУ «ФБЦ» и Клиент при обмене используют следующие типы ЭПД:

- уведомление об утверждении лимитов бюджетных обязательств на текущий финансовый год с поквартальным распределением и плановый период;
- уведомление об изменении лимитов бюджетных обязательств на текущий финансовый год с поквартальным распределением и плановый период;
- платежное поручение.

2.3. Стороны признают юридическую силу ЭПД, подписанных ЭП (при положительном результате проверки ЭП), равной юридической силе документов на бумажном носителе, оформленных в соответствии с требованиями законодательства, при одновременном соблюдении следующих условий:

- сертификат ключа проверки ЭП, относящийся к этой ЭП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность ЭП в ЭПД;
- ЭП используется в соответствии со сведениями, указанными в сертификате;
- электронный документ не претерпел изменений при информационном взаимодействии сторон (подтверждение целостности и подлинности документа).

2.4. Обмен ЭПД между МКУ «ФБЦ» и Клиентом осуществляется с использованием средств телекоммуникаций, а при невозможности их использования осуществляется переход на обмен документами на бумажных носителях. О переходе на обмен документами на бумажных носителях Клиент извещает МКУ «ФБЦ» письменно.

2.5. ЭПД порождает обязательства Сторон по настоящему Соглашению, если он надлежащим образом оформлен передающей Стороной, подписан ЭП, передан по АС «Бюджет», АС «УРМ» и принимающей Стороной получен, проверен и принят к исполнению. Свидетельством того, что ЭПД принят к исполнению, является соответствующее изменение статуса документа в АС «УРМ», АС «Бюджет».

2.6. Если по какой-либо причине Клиент не может своевременно доставить электронные документы в МКУ «ФБЦ» по АС «УРМ», то он доставляет эти документы на бумажном носителе, оформленные в соответствии с Положением Банка России от 19.06.2012 № 383-П «О правилах осуществления перевода денежных средств», приказом финансового управления мэрии от 06.12.2011 № 53 «Об утверждении порядка составления и ведения сводной бюджетной росписи, лимитов бюджетных обязательств городского бюджета и бюджетных росписей главных распорядителей бюджетных средств (главных администраторов источников финансирования дефицита городского бюджета), подписанные уполномоченными лицами, заверенные подписями ответственных лиц и скрепленные оттиском печати, включенных в карточку образцов подписей и оттиска печати.

2.7. Клиент согласует с МКУ «ФБЦ» и Администратором информационной безопасности дату начала обмена ЭПД, кандидатуры и количество лиц, имеющих право подписи ЭПД, путем оформления заявления о готовности Клиента к обмену ЭПД в системе АС «УРМ», оформленному в соответствии с Приложением 1 к настоящему Соглашению (далее - заявление о готовности Клиента к обмену ЭПД). Заявление о готовности Клиента к обмену ЭПД составляется в 3 (трех) экземплярах.

3. Использование ЭП при обмене ЭПД и управление ключевой системой

3.1. Стороны признают, что:

внесение изменений в ЭПД после его подписания ЭП дает отрицательный результат проверки ЭП;

каждая Сторона несет ответственность за сохранность своих ключей ЭП и за действия персонала при использовании АРМ.

3.2. Для подписания ЭПД и проверки ЭП Стороны используют средства защиты информации в соответствии с принятыми нормативными правовыми актами по защите информации и признают их достаточными для подтверждения подлинности ЭПД.

3.3. Управление ключевой информацией осуществляют Администратор информационной безопасности, уполномоченные лица удостоверяющих центров и администратор АРМ Клиента.

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

3.5. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения.

3.6. Учет носителей ключевой информации осуществляет администратор АРМ Клиента по соответствующим учетным формам.

3.7. Обеспечение требований по организации хранения и использования носителей ключевой информации.

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

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

3.7.3. Не разрешается:

производить несанкционированное копирование носителей ключевой информации;

знакомить или передавать носители ключевой информации лицам, к ним не допущенным;

выводить ключи ЭП или аутентификации 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.

3.8. Порядок работы с ключами ЭП Клиента.

3.8.1. Изготовление и сертификацию ключей ЭП для Клиента осуществляет один из поставщиков услуг удостоверяющих центров, сведения о котором содержатся в едином государственном реестре сертификатов ключей ЭП удостоверяющих центров, имеющее единое пространство доверия сертификатов ключей ЭП с Удостоверяющим центром «Информационные системы «Кристал».

3.8.2. Порядок выдачи, замены, уничтожения ключей ЭП, в том числе в случае их компрометации, обмена сертификатами ключей ЭП, определяется поставщиком услуг удостоверяющих центров.

3.8.3. Срок действия ключей ЭП определяется поставщиком услуг удостоверяющих центров.

3.8.4. После получения ключей ЭП Клиент обязан в течение двух рабочих дней предоставить сертификат открытого ключа ЭП, в виде файла в формате X.509 с расширением «.cer», Администратору информационной безопасности.

Для этого на адрес электронной почты techsupport@cherepovetscity.ru Клиент направляет заявку на регистрацию сертификата (оформленную в соответствии с Приложением 2 к настоящему Соглашению) с вложенным файлом сертификата открытого ключа ЭП.

3.8.5. После получения сертификата ключа проверки ЭП Клиента, Администратор информационной безопасности в течение одного рабочего дня проводит его регистрацию в хранилище сертификатов сервера обмена данными, о чем уведомляет Клиента по представленным в заявке контактам для обратной связи.

4. Условия участия в обмене ЭПД, основания для приостановления (прекращения) участия в обмене ЭПД

4.1. Для участия в обмене ЭПД Клиент выполняет следующие действия:

4.1.1. Назначает лиц, ответственных за осуществление обмена ЭПД с МКУ «ФБЦ», с представлением в МКУ «ФБЦ» документов, подтверждающих назначения и полномочия указанных лиц:

администратор АРМ клиента;
владельцы ключей ЭП.

4.1.2. По согласованию с Администратором информационной безопасности, клиент самостоятельно комплектует АРМ необходимыми аппаратными, системными, сетевыми и телекоммуникационными средствами.

4.1.3. За свой счет приобретает, устанавливает и обеспечивает работоспособность средств криптографической защиты информации и ЭП.

4.1.4. Оплачивает средства связи и каналы связи для организации обмена ЭПД.

4.1.5. Передает Администратору информационной безопасности сертификаты ключей проверки ЭП (пункт 3.8.4) для регистрации их в СОД.

4.2. Для участия Клиента в обмене ЭПД администратор информационной безопасности выполняет следующие действия:

4.2.1. Оказывает консультации по вопросам организации доступа к СЗД ФБЦ и обмена ЭПД с СОД.

4.2.2. Присваивает Клиенту уникальный идентификатор для доступа к СОД.

4.2.3. Регистрирует сертификаты ключей проверки ЭП Клиента.

4.3. Основаниями для приостановления участия Клиента в обмене ЭПД являются следующие условия:

4.3.1. Несоблюдение Клиентом требований к обмену ЭПД и обеспечению информационной безопасности при обмене ЭПД, предусмотренных действующим законодательством и условиями настоящего Соглашения.

4.3.2. Получение от Клиента письменного заявления с просьбой о приостановлении его участия в обмене ЭПД.

4.3.3. Компрометация ключей проверки ЭП или аутентификации Клиента.

4.3.4. Изменение Клиентом места своего нахождения.

4.3.5. Иные основания, предусмотренные действующим законодательством.

4.4. О факте приостановления участия Клиента в обмене ЭПД МКУ «ФБЦ» незамедлительно уведомляет Стороны письменно с указанием нарушения пунктов данного Соглашения, даты начала и срока приостановления участия в обмене ЭПД.

4.5. В случае, предусмотренном пунктом 4.3.3 настоящего Соглашения, обмен ЭПД с Клиентом приостанавливается с момента установления Сторонами факта компрометации ключей ЭП или аутентификации Клиента, при этом МКУ «ФБЦ» незамедлительно уведомляет Клиента о приостановлении обмена ЭПД. При этом Стороны руководствуются Приложением 3 к настоящему Соглашению (для служебного пользования) и Приложением 4 к настоящему Соглашению (для служебного пользования).

4.6. Участие Клиента в обмене ЭПД возобновляется после устранения причин его приостановления. О возобновлении участия Клиента в обмене ЭПД МКУ «ФБЦ» письменно уведомляет Стороны. В случае изменения Клиентом места своего нахождения участие в обмене ЭПД возобновляется после совершения Сторонами действий, предусмотренных пунктами 4.1. - 4.2. настоящего Соглашения.

4.7. Основанием для прекращения участия Клиента в обмене ЭПД является расторжение настоящего Соглашения в случаях, предусмотренных пунктом 10.5.

5. Права и обязанности МКУ «ФБЦ»

5.1. При обмене ЭПД МКУ «ФБЦ» имеет следующие права:

5.1.1. Отказать в регистрации Клиента в качестве участника обмена ЭПД в случае невыполнения им условий участия, предусмотренных настоящим Соглашением, а также отказывать Клиенту в приеме ЭПД с указанием причины отказа.

5.1.2. Приостанавливать обмен ЭПД при наличии оснований, предусмотренных пунктом 4.3. настоящего Соглашения.

5.1.3. Запрашивать при необходимости у Клиента копии ЭПД на бумажном носителе.

5.1.4. Вносить изменения в Соглашение, в том числе: изменять порядок обмена ЭПД, перечень ЭПД, используемых при обмене, с уведомлением Клиента письменно не позднее 10 рабочих дней до вступления изменений в силу с указанием даты вступления указанных изменений в силу.

5.1.5. Осуществлять контроль ЭПД, полученных от Клиента, и сообщать Клиенту об обнаруженных ошибках и причинах невозможности исполнения ЭПД.

5.2. При обмене ЭПД МКУ «ФБЦ» обязано:

5.2.1. Передать Администратору информационной безопасности течение 2 (двух) рабочих дней после получения от Клиента заявление о готовности Клиента к обмену ЭПД для настройки аппаратных и программных средств на прием ЭПД от Клиента в 3 (трех) экземплярах.

5.2.2. Направить Клиенту в течение 2 (двух) рабочих дней после получения от Администратора информационной безопасности согласованное заявление о готовности Клиента к обмену ЭПД.

5.2.3. Осуществлять прием ЭПД с подлинной ЭП.

6. Права и обязанности Клиента

6.1. При обмене ЭПД Клиент имеет следующие права:

6.1.1. Составлять и направлять в МКУ «ФБЦ», а также получать от МКУ «ФБЦ» ЭПД в соответствии с перечнем ЭПД, предусмотренным настоящим Соглашением.

6.1.2. Обращаться к Администратору информационной безопасности по вопросам доступа в СЗД ФБЦ.

6.1.3. Обращаться в МКУ «ФБЦ» с заявлением о предоставлении копий ЭПД, хранимых МКУ «ФБЦ».

6.1.4. Обращаться в Удостоверяющий центр за подтверждением подлинности ЭП в отношении выданных Удостоверяющим центром сертификатов ключей проверки ЭП.

6.1.5. Инициировать разрешение спора в отношении исполненных ЭПД.

6.1.6. Соблюдать требования по эксплуатации средств криптографической защиты.

6.2. При обмене ЭПД Клиент обязан:

6.2.1. Использовать для передачи ЭПД исключительно программное обеспечение АС «УРМ».

6.2.2. Предоставить МКУ «ФБЦ» заявление о готовности к обмену ЭПД в 3 (трех) экземплярах.

6.2.3. Приказом (распоряжением) назначить лиц, уполномоченных работать на АРМ обмена ЭПД и подписывать ЭП электронные платежные документы.

6.2.4. Информировать незамедлительно МКУ «ФБЦ» и Администратора информационной безопасности о прекращении, возобновлении полномочий ответственного лица на право подписи ЭПД письменно с указанием причины.

6.2.5. Предоставлять представителям Согласительной комиссии доступ в помещение, где размещается АРМ Клиента для проведения проверок соблюдения Клиентом условий настоящего Соглашения.

6.2.6. Обеспечивать сохранность, целостность и работоспособность АРМ Клиента.

6.2.7. Информировать стороны о неисправностях в работе АРМ Клиента и по запросам, письменно подтверждать наличие этих событий с указанием обстоятельств, при которых они возникли.

6.2.8. Незамедлительно информировать МКУ «ФБЦ» и Администратора информационной безопасности в случае обнаружения факта компрометации (в том числе утери) ключа ЭП или аутентификации, а также обо всех случаях технических неисправностей, и других обстоятельств, препятствующих обмену ЭПД.

6.2.9. Использовать АРМ Клиента только в целях, установленных настоящим Соглашением, без права передачи третьим лицам или копирования.

6.2.10. Обеспечивать доступ к АРМ Клиента только уполномоченным сотрудникам.

6.2.11. Соблюдать порядок обмена ЭПД.

6.2.12. При обмене ЭПД использовать ЭПД, предусмотренные пунктом 2.2 настоящего Соглашения.

6.2.13. Поддерживать за собственный счет в рабочем состоянии свои программно-технические средства, используемые при проведении обмена ЭПД в соответствии с настоящим Соглашением.

6.2.14. Выполнять рекомендации по информационной безопасности при использовании средств и ключей ЭП согласно Приложению 3 к настоящему Соглашению.

7. Права и обязанности Администратора информационной безопасности

7. При исполнении функций Администратор информационной безопасности обязан:

7.1. В течение 2 (двух) рабочих дней после получения от МКУ «ФБЦ» письменного заявления о готовности Клиента к обмену ЭПД, настроить аппаратные и программные средства на прием ЭПД от Клиента.

7.2. Направить в МКУ «ФБЦ» 2 (два) экземпляра согласованного заявления о готовности Клиента к обмену ЭПД в течение 2 (двух) рабочих дней после настройки аппаратных и программных средств на прием ЭПД от Клиента.

7.3. Устанавливать актуальные обновления АС «Бюджет», включая АС «УРМ», устанавливать актуальные файлы сервера проверки достоверности.

7.4. Обеспечить хранение ЭПД в соответствии со следующими требованиями: входящие ЭПД хранятся совместно со справочниками сертификатов ЭП, используемыми для подтверждения их подлинности;

сроки хранения ЭПД должны соответствовать срокам хранения, установленным для расчетных документов на бумажных носителях;

архив ЭПД должен обеспечивать оперативный доступ к ЭПД и возможность распечатки их копий на бумажном носителе.

7.5. Хранить программные средства, предназначенные для проверки правильности ЭП, а также документацию на эти средства в течение сроков хранения ЭПД, для подтверждения подлинности которых использовались (могут использоваться) указанные средства.

7.6. Обеспечивать бесперебойное функционирование аппаратно-программных средств, необходимых для приема и обработки ЭПД Клиента.

7.7. Своевременно информировать Стороны обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену ЭПД в установленном порядке.

8. Конфиденциальность

Сведения о ключевой информации, паролях доступа к СЗД МКУ «ФБЦ» и СОД, материалы работы Согласительной комиссии не подлежат передаче третьим лицам, за исключением установленных законодательством случаев.

9. Ответственность Сторон и риски убытков

9.1. Клиент несет ответственность за содержание любого ЭПД, подписанного его ЭП.

9.2. МКУ «ФБЦ» несет ответственность:

9.2.1. За своевременное принятие в обработку ЭПД «Клиента», прошедших проверку ЭП.

9.2.2. За непринятие мер в случае выявления факта компрометации ключа ЭП Клиента.

9.3. МКУ «ФБЦ» не несет ответственности за ошибочное списание средств со счетов Клиента и зачисление средств на счет другого получателя, если ошибка вызвана неправильным указанием Клиентом в ЭПД, подписанном ЭП, реквизитов банка плательщика (получателя), счета плательщика (получателя), наименования плательщика (получателя) или суммы платежа.

9.4. Администратор информационной безопасности несет ответственность за функционирование аппаратно-программных комплексов СЗД ФБЦ.

9.5. В случае возникновения ущерба Сторона, не исполнившая (ненадлежащим образом исполнившая) обязательства по настоящему Соглашению, несет ответственность перед другой Стороной.

При отсутствии доказательств неисполнения (ненадлежащего исполнения) Сторонами обязательств по настоящему Соглашению риск убытков несет Сторона, подписавшая ЭП ЭПД, исполнение которого повлекло за собой убытки.

9.6. МКУ «ФБЦ» и Администратор информационной безопасности не несет ответственности в случае невозможности осуществления обмена ЭПД с Клиентом, если это вызвано неисправностями используемых Клиентом программно-аппаратных средств и каналов связи, предоставленных третьими лицами.

9.7. Ответственность за ущерб, возникший вследствие нарушения конфиденциальности, несет Сторона, допустившая нарушение.

9.8. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств по настоящему Соглашению, если таковое явилось следствием обстоятельств непреодолимой силы, возникших после вступления в силу настоящего Соглашения, в результате событий чрезвычайного характера, которые не могли быть предвидены и предотвращены разумными мерами.

10. Срок действия Соглашения и прочие условия

10.1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу со дня его подписания.

10.2. Разрешение споров в отношении ЭПД, проводится Сторонами в порядке согласно Приложению 5 к настоящему Соглашению (для служебного пользования).

10.3. Внесение изменений в Соглашение оформляется в виде Дополнительного соглашения.

10.4. В случае принятия правового акта по вопросам, регулируемым настоящим Соглашением, соответствующие положения Соглашения утрачивают юридическую силу в части, противоречащей положениям правового акта.

10.5. МКУ «ФБЦ» вправе расторгнуть Соглашение в следующих случаях:

10.5.1. В случае закрытия лицевых счетов Клиента по основаниям, предусмотренным Порядками открытия и ведения лицевых счетов главных распорядителей и получателей средств городского бюджета, муниципальным бюджетным и автономным учреждениям и проведения кассовых операций со средствами данных учреждений, утвержденных приказами (распоряжениями) финансового управления мэрии.

10.5.2. В случае несогласия Клиента с изменениями к настоящему Соглашению, вносимыми МКУ «ФБЦ» в порядке, предусмотренном пунктом 5.1.4 настоящего Соглашения.

10.5.3. В случае нарушения Клиентом требований к обмену ЭПД, требований к обеспечению информационной безопасности при обмене ЭПД, предусмотренных законодательством и условиями настоящего Соглашения.

10.6. Расторжение Соглашения оформляется в виде Соглашения о расторжении Соглашения об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место».

10.7. Стороны обязуются уведомлять друг друга об изменении своего местонахождения, а также об изменении иных реквизитов, имеющих существенное значение для определения юридического статуса и идентификации Сторон.

10.8. Права и обязанности Сторон по настоящему Соглашению не могут быть переуступлены или переданы третьим лицам.

11. Местонахождение и реквизиты сторон

Муниципальное казенное учреждение «Финансово-бухгалтерский центр»:

162608, Вологодская область, город Череповец,

пр-кт Строителей, дом 4, корпус А телефон 50 05 84

ИНН 3528238825 КПП 352801001

р/сч 40204810200000000066

УФК по Вологодской области (Финупр/МКУ «Финансово-бухгалтерский центр» л/с 807.12.001.1)

Наименование банка: Отделение Вологда город Вологда БИК 041909001

Директор МКУ «Финансово-бухгалтерский центр»

_____/_____
(подпись) (расшифровка подписи)

Муниципальное бюджетное учреждение «Центр муниципальных информационных ресурсов и технологий»:

162622, Вологодская область, город Череповец,

улица Набережная, дом 29, корпус Д телефон 55 15 25

ИНН 3528073450 КПП 352801001

р/сч 40701810000091000286

УФК по Вологодской области (Финупр/МБУ «ЦМИРиТ» л/сч 801.20.001.1)

Наименование банка: Отделение Вологда город Вологда БИК 041909001

Директор МБУ «Центр муниципальных информационных ресурсов и технологий»

_____/_____
(подпись) (расшифровка подписи)

Клиент:

_____/_____
(подпись) (расшифровка подписи)

ЗАЯВЛЕНИЕ

(наименование организации)

(юридический адрес)

выражает готовность к электронному обмену платежными документами, подписанными электронной подписью, в системе удаленных рабочих мест АС «Бюджет» на основании следующего:

1. АРМ обмена ЭПД (№ системного блока _____), установлен в кабинете № _____ по адресу: _____

кабинет № _____ находится на _____ этаже здания и соответствует рекомендациям, установленным Приложением 3 к Соглашению № _____ от «_____» _____ 20__ г.

2. Ответственные за осуществление электронного обмена лица:

_____ Владелец СКП;
(Ф.И.О., должность)

_____ доверенное лицо;
(Ф.И.О., должность)

_____ Администратор АРМ Клиента.
(Ф.И.О., должность)

назначены _____ от «_____» _____ 20__ г. № _____
(указать каким документом)

3. На АРМ обмена ЭПД имеются:

приложения 1, 2, 3 к Соглашению № _____ от «_____» _____ 20__ г.;
Регламент Удостоверяющего центра;
журнал учета и приема-передачи ключевого носителя.

4. Канал передачи данных от АРМ Клиента «УРМ» - сервер для обмена ЭПД настроен.

5. Просим открыть права на ввод и отправку данных по интерфейсам относительно лицевых счетов (указать из списка необходимые типы документов):

Лицевой счёт	Интерфейс	Счет финансового органа
XXX.XX.XXX.X	Платежные поручения	
XXX.XX.XXX.X	Роспись по ПБС	
XXX.XX.XXX.X	ПОФ по ПБС (расходы)	
XXX.XX.XXX.X	СБР (расходы)	
XXX.XX.XXX.X	Лимиты (уведомления)	
XXX.XX.XXX.X	Кассовый план (расходы)	
XXX.XX.XXX.X	Сметы по ПД, субсидии БУ, АУ	

XXX.XX.XXX.X	Внутренние платежи за платные услуги	
.....		
.....		

Руководитель Клиента

(подпись)

(расшифровка подписи)

М.П.

«_____» _____ 20____ года

Согласовано:

Директор МКУ «ФБЦ»

(подпись)

(расшифровка подписи)

М.П.

«_____» _____ 20____ года

Директор МБУ «ЦМИРиТ» _____

(подпись)

(расшифровка подписи)

М.П.

«_____» _____ 20____ года

**Форма заявки
на установку сертификата открытого ключа электронной подписи.**

Прошу заменить сертификат в связи _____

указать причину

Сертификат открытого ключа ЭП прилагается.

Наименование организации, где меняется сертификат:

ИНН организации: _____

Код пользователя*:

Контактное лицо для связи - Ф.И.О., телефон, адрес электронной почты с кем можно связаться в случае возникновения вопросов по замене сертификата:

* Код пользователя можно посмотреть в УРМ → настройки → редактор настроек → строка: Код пользователя

Рекомендации по информационной безопасности при использовании средств и ключей ЭП

1. Рекомендации по размещению средств ЭП.

1.1. Размещение, охрана и специальное оборудование помещения, в котором установлены средства ЭП, должны обеспечивать сохранность информации, невозможность неконтролируемого проникновения в эти помещения.

1.2. Эти помещения должны находиться в контролируемой зоне, иметь прочные входные двери, на которые устанавливаются надёжные замки. Двери и окна помещений оборудуются охранной сигнализацией. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п. окна помещений рекомендуется оборудовать внутренними (раздвижными) решётками.

1.3. Для хранения ключей ЭП в помещениях рекомендуется устанавливать надёжные металлические хранилища, оборудованные внутренними замками с двумя экземплярами ключей.

1.4. По окончании рабочего дня помещение, в котором установлены средства ЭП и хранилища с ключами ЭП, рекомендуется закрывать и ставить под сигнализацию, извещатели которой могут выходить на посты ведомственной или военизированной охраны. Порядок охраны устанавливается на местах.

1.5. Рекомендуется двери помещений во время работы с ключами ЭП держать закрытыми, присутствие посторонних лиц, не имеющих доступа к ключевой информации, исключить.

1.6. Хранение ключей ЭП допускается в одном хранилище с другими документами, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним.

1.7. Для размещения средств ЭП рекомендуется использовать внутренние помещения здания (не граничащие с наружными стенами). Средства ЭП рекомендуется размещать, возможно, ближе к центру помещения и на удалении от наружных стен и стен, смежных с помещениями, где возможно пребывание посторонних лиц, не допущенных к информации ограниченного доступа.

1.8. В помещении, где размещаются средства ЭП, рекомендуется ограничивать применение электро -, радио - и другой аппаратуры.

Внешние модемы следует устанавливать в пределах контролируемой зоны на расстоянии не менее 1 м от средств ЭП.

2. Руководство по применению паролей.

2.1. Общие положения.

2.1.1. Пароль является средством защиты доступа к средствам вычислительной техники и информационным ресурсам и представляет собой символьную последовательность (буквенную, цифровую или смешанную), предъявляемую пользователем в ответ на соответствующий запрос. При положительном результате проверки достоверности предъявленного пользователем пароля:

система управления доступом предоставляет пользователю закрепленные за ним права доступа;

пользователь регистрируется встроенными средствами регистрации (если они имеются).

2.1.2. Пароль эффективен как средство защиты только при правильном его использовании. Пользователи несут полную ответственность за правильность использования паролей, которыми они владеют.

2.1.3. Пароль принадлежит только одному пользователю и применяется для его персонального доступа к средствам вычислительной техники и информационным ресурсам.

2.2. Использование паролей.

Правильное использование пароля заключается в выполнении следующих требований:

пароль должен быть известен только его владельцу;

запрещается сообщать пароль кому бы то ни было;

пользователь должен принять все меры для того, чтобы исключить возможность разглашения принадлежащего ему пароля;

символьная последовательность, составляющая пароль, должна иметь такую длину и содержание, чтобы нельзя было узнать её по её части или владея косвенной информацией о ней, а также нельзя было просто подобрать. Например, нельзя применять пароли, состоящие из одних и тех же или чередующихся символов. Не рекомендуется применять в качестве паролей общеупотребительные слова, основывать пароли на общеизвестных ассоциациях. Длина паролей, используемых для включения компьютера должна быть не менее 8 символов. Длина паролей, используемых для доступа к средствам ЭП должна быть не менее 8 символов;

не следует использовать один и тот же пароль для различных учётных записей; пароли, используемые для доступа к средствам ЭП, должны периодически меняться. Периодичность смены пароля должна быть не реже, чем раз в квартал. В случае разглашения пароля он должен заменяться немедленно; пароли, используемые для доступа к компьютеру, заменяются в случае разглашения.

2.3. Резервирование паролей.

2.3.1. По решению руководителя Клиента, либо руководителя структурного подразделения Клиента (далее - руководитель) может применяться резервирование некоторых паролей, таких, как пароли администраторов серверов и автоматизированных систем, пароли ответственных должностных лиц, пароли отдельных пользователей, выполняющих важные функции, единственно возможные пароли.

2.3.2. Для резервирования пароля:

лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него может быть также вложен лист темной бумаги. Конверт заклеивается. На конверте владелец пароля указывает свою должность, фамилию и инициалы, наименование информационного средства, которое защищается этим паролем, текущие дату и время, при необходимости - другие данные, и заверяет запись личной подписью;

конверт передаётся для хранения руководителю или лицу, им для этого назначенному, и учитывается в специальном разделе Журнала учёта средств защиты информации. Учётный номер (сквозной по журналу) проставляется ответственным за хранение на конверте.

2.3.3. Конверты с паролями хранятся в сейфе. Ответственный за хранение не реже чем один раз в неделю проверяет их наличие по журналу учёта.

2.3.4. При замене пароля конверт передаётся владельцу пароля, который уничтожает лист с резервным паролем, о чем делается запись в журнале учёта. Новый резервный пароль подготавливается к хранению в порядке указанном в пункте 2.3.2.

настоящих требований. Новый конверт учитывается в журнале учёта отдельной позицией.

2.3.5. Вскрытие конверта с паролем производится по решению руководителя подразделения в случае необходимости использования прав доступа его владельца в отсутствие самого владельца, если иными способами получить доступ невозможно. Для вскрытия конверта назначается комиссия не менее чем из трёх сотрудников подразделения. О вскрытии конверта комиссией составляется акт, утверждаемый руководителем подразделения, который по окончании работы комиссии хранится в документах руководителя или лица им назначенного.

2.3.6. С целью сохранения прав доступа, закреплённых за пользователем, которому принадлежал пароль, на время его отсутствия назначается сотрудник, который заменяет пароль владельца на свой собственный. По прибытии владельца ему возвращаются его права доступа, и он назначает новый пароль.

2.4. Для доступа к особо критичным средствам вычислительной техники и информации вместо пароля должны применяться средства сильной аутентификации (автоматическая выработка случайных паролей максимальной длины и их хранение на аппаратных носителях: touch-метогу, смарт-картах и т.п.).

3. Рекомендации по применению ЭП.

3.1. Использование ЭП в качестве аналога собственноручной подписи предполагает визуальный контроль владельцем СКП содержания электронного документа перед его подписанием и отправкой.

3.2. Владелец СКП может являться руководителем или сотрудником, которому от имени Клиента предоставлено право удостоверения соответствия электронных документов оригиналам.

При изменении реквизитов владельца ключа (смена руководителя организации, названия и т. д.), а также компрометации закрытого ключа требуется отозвать текущий сертификат и оформить новый.

3.3. В системах ЭПД использование ЭП должно осуществляться с соблюдением следующих принципов безопасности:

3.3.1. Сотрудники, имеющие права защиты (удостоверения содержания) электронных платёжных документов, назначаются приказами или распоряжениями руководства Клиента. При этом руководитель несет персональную ответственность за подбор указанных сотрудников. Эти сотрудники могут не быть должностными лицами, обладающими правами первой и второй подписи оригинальных платёжных документов (бумажных). Формирование (подготовка исходного текста) и отправка ЭПД может осуществляться как указанными лицами, так и другими сотрудниками, которым это поручено руководителем Клиента.

3.3.2. Основанием для защиты и передачи электронного платёжного документа по системе электронного документооборота является либо наличие полностью надлежаще оформленного и подписанного уполномоченными лицами соответствующего бумажного документа, либо наличие соответствующего электронного документа (или его заверенной распечатки), полученного с соблюдением пункта 3.1 настоящих требований.

3.4. Допускается назначение доверенного лица владельцем СКП, в случае если владельцем СКП является руководитель Клиента.

3.4.1 Доверенные лица имеют право подписи электронных документов ключом владельца при наличии распечаток этих документов на бумажном носителе, подписанных владельцем СКП и заверенных печатью Клиента. Владелец СКП (доверенное лицо), подписавший электронный документ, несет ответственность за содержание подписанного электронного платёжного документа.

3.4.2. Назначение доверенных лиц оформляется распоряжением руководителя Клиента, с указанием на право удостоверения подлинности электронных платежных документов (в соответствии с п. 3.2 настоящих рекомендаций).

3.4.3. Передача носителя с ключом ЭП от владельца СКП доверенному лицу и наоборот должна фиксироваться владельцем СКП в специально предназначенном для этого журнале. Данный журнал может оформляться в произвольном виде, но с обязательными полями: «тип носителя ЭП», «идентификатор ЭП», «дата и время передачи носителя», «фамилия, инициалы и подпись лица, принявшего носитель».

3.5. Основными угрозами при использовании ЭП для защиты систем электронного документооборота являются компрометация ключей ЭП отправителей электронных документов и внедрение в базы ключей проверки ЭП получателей электронных документов фальшивых или выведенных из действия сертификатов ключей проверки ЭП, а также нарушение целостности программного обеспечения, реализующего функции формирования и проверки ЭП.

3.6. В процессе всего периода использования и хранения ключей ЭП должна быть обеспечена их надежная защита от компрометации.

3.7. Носители ключей ЭП должны храниться в сейфах (металлических шкафах), а при нахождении носителей вне сейфов владельцы СКП (доверенные лица) должны принять необходимые меры, направленные на исключение компрометации ключа ЭП.

3.8. При хранении в сейфе (металлическом шкафу) коллективного пользования носитель ключа ЭП должен быть помещен в опечатанный конверт, пенал или другие средства, позволяющие обнаружить несанкционированный доступ к носителю ключа со стороны других пользователей сейфа.

3.9. Владелец СКП несет ответственность за соблюдение правил хранения носителя ключа ЭП и правильность его использования.

Порядок действий при компрометации ключа ЭП

1. Понятие компрометации применяется только к ключу ЭП и означает, что произошло нарушение безопасности хранения и использования ключа, в результате которого возникла вероятность несанкционированного его применения и нанесения тем самым ущерба.

2. Явной считается компрометация в одном из следующих случаев:

2.1. Ключ ЭП оказался доступен кому-либо, кроме его владельца.

2.2. Обнаружен случай подписания электронного документа экземпляром ЭП кем-либо, кроме его владельца.

3. Неявной считается компрометация в одном из следующих случаев:

3.1. Ключ ЭП был скопирован на жесткий диск или другой носитель, передан в локальной вычислительной или телекоммуникационной сети или иным образом, даже в случае последующего уничтожения, мог после этого оказаться восстановленным посторонним лицом.

3.2. Носитель ключа ЭП оказался доступен постороннему лицу без контроля со стороны владельца СКП.

3.3. У владельца СКП возникло подозрение, что ключ ЭП мог оказаться доступен кому - либо, кроме него самого.

4. Как явная, так и неявная компрометация ключа ЭП считается нарушением информационной безопасности и требует принятия немедленных мер по предотвращению возможного ущерба, при этом различий в принимаемых мерах для той и другой формы не делается.

В указанных выше случаях Клиент обязан незамедлительно сообщить письменно о компрометации ключа ЭП в Удостоверяющий центр и МКУ «ФБЦ».

5. МКУ «ФБЦ» приостанавливает прием ЭПД с ЭП Клиента до смены скомпрометированных ключей ЭП.

6. Все электронные платежные документы, заверенные скомпрометированным ключом ЭП, принятые к обработке после установленного или предполагаемого времени возникновения (а не обнаружения) компрометации ключа ЭП, независимо от того, продолжается ли еще обработка этих документов или уже завершена, должны быть немедленно сверены по всему маршруту их движения в АС «УРМ».

7. Прием и исполнение ЭПД Клиента без ЭП продолжается только при предоставлении копий ЭПД на бумажном носителе в соответствии с пунктом 2.6. настоящего Соглашения.

8. После замены скомпрометированных ключей ЭП обмен ЭПД возобновляется в режиме определенным настоящим Соглашением.

Порядок разрешения споров

1. Для разрешения споров в отношении ЭПД, Стороны принимают следующий порядок:

1.1. Каждая из Сторон имеет право инициировать разрешение спора, связанного с электронным документом или группой электронных документов, отправленных или полученных Сторонами.

1.2. Инициирование разрешения спора осуществляет одна из Сторон путем направления другой Стороне уведомления (письма) за подписью уполномоченного лица, с изложением причин разногласия, в трехдневный срок с момента возникновения спора.

1.3. Стороны, по взаимному согласию, пытаются урегулировать разногласия путем ведения переговоров в срок не более семи календарных дней с момента получения уведомления (письма) одной из Сторон.

1.4. Разногласия, не урегулированные путем переговоров, разрешаются уполномоченными представителями Сторон в рамках Согласительной комиссии (далее - Комиссия).

2. Комиссия создается с целью разрешения разногласий при обмене ЭПД, установления фактических обстоятельств, послуживших основанием их возникновения, а также для проверки целостности и подтверждения подлинности ЭПД.

3. В состав комиссии должны входить уполномоченные представители сторон: МКУ «ФБЦ» (2 чел., в том числе директор);

Клиента (2 чел.);

Администратора информационной безопасности (2 чел.).

Члены комиссии от каждой Стороны назначаются приказами соответствующей Стороны. В случае необходимости, при согласии Сторон, для разрешения споров могут привлекаться независимые эксперты.

Оплата работы независимых экспертов осуществляется Стороной, направившей заявление о разногласиях.

4. Комиссия создается на срок до окончания решения спорной ситуации.

5. Стороны обязуются способствовать работе Комиссии и не допускать отказа от предоставления необходимых документов.

6. Стороны обязуются предоставить Комиссии возможность ознакомления с условиями и порядком работы своих АРМ обмена ЭПД.

7. При возникновении разногласий при обмене (в связи с обменом) ЭПД Сторона, заявляющая разногласие (МКУ «ФБЦ» или Клиент), обязана направить другой Стороне (Клиенту или МКУ «ФБЦ») заявление о разногласиях, подписанное уполномоченным должностным лицом, с подробным изложением причин разногласий и предложением создать Комиссию. Заявление должно содержать фамилии представителей Стороны, заявляющей разногласие, которые будут участвовать в работе Комиссии, место, время и дату сбора комиссии (не позднее 7 дней со дня отправления заявления).

До подачи заявления МКУ «ФБЦ» необходимо убедиться в неизменности используемой ключевой информации, а также отсутствии несанкционированных действий со стороны персонала, обслуживающего собственный АРМ.

8. Работа согласительной комиссии проходит в два этапа:

8.1. 1-й этап - подготовительный.

8.2. Комиссия сравнивает сертификат ключа подписи Клиента на бумажном носителе с распечаткой его электронного образа, находящегося в базе ключей проверки ЭП АС «Бюджет». При отрицательном результате сравнения дальнейшее рассмотрение разногласий не проводится.

8.3. Комиссия сравнивает сертификат ключа подписи Клиента со списком отозванных сертификатов (СОС). В случае совпадения реквизитов сертификата с реквизитами сертификата из СОС дальнейшее рассмотрение разногласий не проводится.

8.4. 2-й этап - проверка и анализ спорных документов, принятие решения по сути спора.

9. По итогам работы комиссии составляется акт, содержащий:
фактические обстоятельства, послужившие основанием возникновения разногласий;

порядок работы членов комиссии;

вывод о подлинности (не подлинности) оспариваемого ЭПД и его обоснование.

Акт составляется в трех экземплярах, подписывается всеми членами Комиссии. Члены Комиссии, не согласные с мнением большинства, подписывают акт с особым мнением, которое прикладывается к акту. Каждой из Сторон согласительная комиссия направляет по одному экземпляру акта для принятия решения.

10. В случае если на предложение МКУ «ФБЦ» о создании комиссии ответ Клиента не был получен, или получен отказ от участия в работе комиссии, или если Клиентом чинились препятствия работе Комиссии, Комиссия составляет акт в соответствии с пунктом 11.9. без участия Клиента. Один экземпляр акта направляется Клиенту.

11. В случае невозможности разрешения разногласий в рамках Согласительной комиссии Стороны передают их на рассмотрение Арбитражного суда Вологодской области в порядке, установленном законодательством.

УТВЕРЖДЕНА
распоряжением
финансового управления
мэрии
от 16.08.2018 № 39
(приложение 2)

Типовая форма

Дополнительное соглашение
к Соглашению об обмене электронными платежными документами в
автоматизированной системе «Бюджет», автоматизированной системе
«Удаленное рабочее место» № ____ от _____

г. Череповец

«__» _____ 20__ г.

Муниципальное казенное учреждение «Финансово-бухгалтерский центр»
(далее - МКУ «ФБЦ»), в лице директора _____, действующего
на основании Устава учреждения, муниципальное бюджетное учреждение «Центр
муниципальных информационных ресурсов и технологий» (далее - МБУ
«ЦМИРиТ»), именуемое в дальнейшем Администратор информационной
безопасности, в лице директора _____, действующего на
основании Устава учреждения, и

(полное наименование организации)

(далее - Клиент) – участник обмена электронными платежными документами (далее -
ЭПД), в лице _____,
(Ф.И.О., должность)

действующий на основании _____,
(при совместном упоминании в тексте именуемые – Стороны), заключили настоящее
трехстороннее Дополнительное Соглашение о нижеследующем:

1. В связи с _____
(реорганизацией, переименованием)

(полное наименование организации)
Стороны Соглашения, руководствуясь _____

(нормы ГК, иного нормативного правового акта)
договорились внести в Соглашение следующие изменения:

1.1. В преамбуле Соглашения слова

« _____
_____»

(полное наименование организации)
(далее - Клиент) - участник обмена электронными платежными документами (далее -
ЭПД), в лице _____
(Ф.И.О., должность)

действующий на основании _____,»

заменить словами

« _____
_____»

(полное наименование организации)

(далее - Клиент) - участник обмена электронными платежными документами (далее - ЭПД), в лице _____,

(Ф.И.О., должность)

действующий на основании _____,»

1.2. В разделе 11 Соглашения «Местонахождение и реквизиты сторон» наименование (реквизиты) «Клиента» изложить в следующей редакции:

_____.

2. С даты, следующей за днем подписания настоящего дополнительного соглашения, «Клиент» обязан использовать новый ключ электронной подписи.

3. Остальные условия Соглашения, не затронутые настоящим дополнительным соглашением, остаются неизменными.

4. Настоящее Дополнительное соглашение является неотъемлемой частью Соглашения об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» № ____ от _____, вступает в силу с даты его подписания сторонами, составлено в трех экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из сторон.

Местонахождение и реквизиты сторон

Муниципальное казенное учреждение «Финансово-бухгалтерский центр»:

162608, Вологодская область, город Череповец,
пр-кт Строителей, дом 4, корпус А телефон 50 05 84

ИНН 3528238825 КПП 352801001 р/сч 40204810200000000066

УФК по Вологодской области (Финупр/МКУ «Финансово-бухгалтерский центр» л/с 807.12.001.1)

Наименование банка: Отделение Вологда город Вологда БИК 041909001

Директор МКУ «Финансово-бухгалтерский центр»

_____/_____
(подпись) (расшифровка подписи)

Муниципальное бюджетное учреждение «Центр муниципальных информационных ресурсов и технологий»:

162622, Вологодская область, город Череповец,
улица Набережная, дом 29, корпус Д телефон 55 15 25

ИНН 3528073450 КПП 352801001 р/сч 40701810000091000286

УФК по Вологодской области (Финупр/МБУ «ЦМИРиТ» л/сч 801.20.001.1)

Наименование банка: Отделение Вологда город Вологда БИК 041909001

Директор МБУ «Центр муниципальных информационных ресурсов и технологий»

_____/_____
(подпись) (расшифровка подписи)

Клиент:

_____/_____
(подпись) (расшифровка подписи)

УТВЕРЖДЕНА
распоряжением
финансового управления
мэрии
от 16.08.2018 № 39
(приложение 3)

Типовая форма

Соглашение

о расторжении Соглашения об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» № ____ от _____

г. Череповец

«__» _____ 20__ г.

Муниципальное казенное учреждение «Финансово-бухгалтерский центр», в лице директора _____, действующего на основании Устава учреждения, муниципальное бюджетное учреждение «Центр муниципальных информационных ресурсов и технологий», именуемое в дальнейшем Администратор информационной безопасности, в лице директора _____, действующего на основании Устава учреждения, и

(полное наименование организации)

(далее - Клиент) – участник обмена электронными платежными документами (далее - ЭПД), в лице _____
(Ф.И.О., должность)

действующий на основании _____,
(при совместном упоминании в тексте именуемые – Стороны), заключили Соглашение о нижеследующем:

1. Расторгнуть Соглашение об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» № ____ от _____.

2. Стороны взаимных претензий не имеют, с даты подписания настоящего Соглашения не считают себя связанными какими-либо правами и обязанностями.

3. Настоящее Соглашение является неотъемлемой частью Соглашения об обмене электронными платежными документами в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» № ____ от _____, вступает в силу с даты его подписания сторонами, составлено в трех экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из сторон.

Местонахождение и реквизиты сторон

Муниципальное казенное учреждение «Финансово-бухгалтерский центр»:
162608, Вологодская область, город Череповец,
пр-кт Строителей, дом 4, корпус А телефон 50 05 84
ИНН 3528238825 КПП 352801001 р/сч 40204810200000000066

УФК по Вологодской области (Финупр/МКУ «Финансово-бухгалтерский центр» л/с 807.12.001.1)

Наименование банка: Отделение Вологда город Вологда БИК 041909001

Директор МКУ «Финансово-бухгалтерский центр»

_____/_____
(подпись) (расшифровка подписи)

Муниципальное бюджетное учреждение «Центр муниципальных информационных ресурсов и технологий»:

162622, Вологодская область, город Череповец,

улица Набережная, дом 29, корпус Д телефон 55 15 25

ИНН 3528073450 КПП 352801001

р/сч 40701810000091000286

УФК по Вологодской области (Финупр/МБУ «ЦМИРиТ» л/сч 801.20.001.1)

Наименование банка: Отделение Вологда город Вологда БИК 041909001

Директор МБУ «Центр муниципальных информационных ресурсов и технологий»

_____/_____
(подпись) (расшифровка подписи)

Клиент:

_____/_____
(подпись) (расшифровка подписи)

Порядок
проведения электронных платежных документов главных распорядителей,
получателей средств городского бюджета, муниципальных бюджетных и автономных
учреждений города, подписанных электронной подписью в автоматизированной
системе «Бюджет», автоматизированной системе «Удаленное рабочее место»

1. Главные распорядители, получатели средств бюджета, муниципальные бюджетные и автономные учреждения города (далее – получатели), переведенные на безбумажную технологию документооборота с применением электронной подписи (далее - ЭП) в автоматизированной системе «Бюджет», автоматизированной системе «Удаленное рабочее место» (далее – АС «Бюджет», АС «УРМ»), представляют в отдел исполнения городского бюджета и бюджетной отчетности муниципального казенного учреждения «Финансово-бухгалтерский центр» (далее – отдел МКУ «ФБЦ») подготовленные в АС «УРМ» электронные платежные документы, подписанные ЭП, без подтверждения на бумажном носителе.

2. Документы, указанные в пункте 1 настоящего Порядка принимаются отделом МКУ «ФБЦ» ежедневно в рабочие дни с 9 до 12 часов датой текущего рабочего дня, поступившие после 12 часов - датой следующего рабочего дня. При этом датой и временем поступления электронного платежного документа считается дата и время его создания, отображаемые в АС «Бюджет»

3. Отдел МКУ «ФБЦ» проверяет электронные платежные документы, подписанные ЭП на подлинность ЭП, не принимает в обработку электронные платежные документы, подписанные некорректной ЭП или без ЭП.

4. Внесение каких-либо изменений в электронные платежные документы, поступившие в отдел МКУ «ФБЦ» с ЭП, не допускается.

5. Электронные платежные документы, подписанные ЭП и имеющие положительный результат проверки на подлинность ЭП, представленные получателями, проверяются специалистами отдела МКУ «ФБЦ» в соответствии с Порядком санкционирования оплаты денежных обязательств главных распорядителей и получателей средств городского бюджета, Порядком открытия и ведения лицевых счетов муниципальным бюджетным и автономным учреждениям и проведения кассовых операций со средствами данных учреждений, установленными финансовым управлением мэрии.

6. В случае отрицательного результата проверки электронного платежного документа, подписанного ЭП, на соответствие требованиям, указанным в пункте 5 настоящего Порядка, отдел МКУ «ФБЦ» отказывает получателю в его проведении с указанием причины отклонения. Отказ оформляется в электронном образе платежного документа в АС «Бюджет».

7. Отдел МКУ «ФБЦ» включает прошедшие контроль электронные платежные документы, подписанные ЭП, в реестр платежных поручений.

8. При возникающих у получателей проблемах обмена электронными платежными документами в АС «УРМ» (отсутствие связи и т.п.) платежные документы принимаются на бумажных носителях, подписанные уполномоченными

лицами, заверенные подписями ответственных лиц и скрепленные оттиском печати, включенных в карточку образцов подписей и оттиска печати с представлением письменного обращения получателя о проведении платежа с указанием причины.

9. Отклонение платежных документов отделом МКУ «ФБЦ», подписанных ЭП, производится на основании обращений, подписанных уполномоченными лицами получателей, включенных в карточку образцов подписей и оттиска печати, с указанием причины.

10. После обработки выписок банка из Управления Федерального казначейства по Вологодской области отдел МКУ «ФБЦ» выдает получателям, осуществляющим электронный обмен платежными документами с применением ЭП, выписки из лицевого счета.