ФИНАНСОВОЕ УПРАВЛЕНИЕ АДМИНИСТРАЦИИ
АСБЕСТОВСКОГО ГОРОДСКОГО ОКРУГА

ПРИКАЗ
ПО ОСНОВНОЙ ДЕЯТЕЛЬНОСТИ

20 апреля 2020 г. № 38

Об организации электронного документооборота с использованием электронных подписей при исполнении бюджета Асбестовского городского округа

В соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 06.04.2011 № 63-ФЗ «Об электронной подписи», решением Думы Асбестовского городского округа от 24.10.2013 № 28/22 «Об утверждении Положения о Финансовом управлении администрации Асбестовского городского округа», в целях совершенствования процесса исполнения бюджета Асбестовского городского округа,

ПРИКАЗЫВАЮ:

1. Утвердить Порядок электронного документооборота с использованием электронных подписей при исполнении бюджета Асбестовского городского округа (прилагается).

2. Отделу казначейского исполнения бюджета (А.В. Савину):

1) организовать работу в соответствии с Порядком электронного документооборота с использованием электронных подписей при исполнении бюджета Асбестовского городского округа;

2) довести настоящий приказ до главных распорядителей бюджетных средств Асбестовского городского округа и органов, осуществляющих полномочия учредителей в отношении подведомственных учреждений.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Финансового управления
администрации Асбестовского
городского округа С.Г. Валова

Утвержден
приказом Финансового управления
администрации Асбестовского
городского округа
от 20.04.2020 № 38

Порядок электронного документооборота с использованием электронных подписей при исполнении бюджета Асбестовского городского округа

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящий Порядок электронного документооборота с использованием электронных подписей при исполнении бюджета Асбестовского городского округа (далее - Порядок) устанавливает общие принципы осуществления электронного документооборота между Финансовым управлением администрации Асбестовского городского округа (далее - Финансовое управление) и главными распорядителями, получателями средств бюджета Асбестовского городского округа, муниципальными бюджетными и автономными учреждениями Асбестовского городского округа, лицевые счета которым открыты в Финансовом управлении.

1.2 Термины и определения, используемые в настоящем порядке:

Автоматизированное рабочее место (далее - АРМ) - установленные программное обеспечение (далее - ПО) и технические средства, включая средства криптографической защиты информации (далее - СКЗИ), предназначенные для работы в системе электронного документооборота.

Администратор АРМ - сотрудник организации, отвечающий за обеспечение бесперебойной эксплуатации ПО и технических средств АРМ, контроль мероприятий по защите информации, хранение и учет электронных документов, взаимодействие по техническим вопросам и вопросам обеспечения безопасности информации.

Электронный документ (далее - ЭД) - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром (далее - УЦ), аккредитованным федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, выдан сертификат ключа подписи (далее - Сертификат), и которое владеет соответствующим закрытым ключом подписи, позволяющим с помощью средств электронной подписи создавать свою ЭП в ЭД (подписывать ЭД).

Закрытый ключ подписи - уникальная последовательность символов, известная владельцу Сертификата и предназначенная для создания в электронных документах ЭП с использованием средств ЭП, а также для аутентификации владельца с последующим установлением защищенного (шифрованного) канала связи при информационном взаимодействии с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи).

Компрометация закрытого ключа подписи - событие, определенное владельцем Сертификата, как ознакомление неуполномоченным лицом (лицами) с его закрытым ключом подписи, хищение, утеря носителя закрытого ключа подписи, несанкционированное копирование или другие причины появления у владельца Сертификата сомнений в сохранении тайны закрытого ключа подписи.

Корректная электронная подпись - ЭП лица, имеющего право подписи соответствующего документа, и для этой ЭП соблюдены следующие условия:

- сертификат ключа подписи (далее - Сертификат), относящийся к этой ЭП, издан УЦ и не утратил силу (действует) на момент проверки или на момент подписания ЭД;

- подтверждена подлинность этой ЭП в ЭД.

Носитель ключевой информации - материальный носитель информации, содержащий закрытый ключ подписи и аутентификации.

Открытый ключ подписи - уникальная последовательность символов, соответствующая закрытому ключу подписи, доступная сторонам электронного документооборота и предназначенная для подтверждения подлинности ЭП в ЭД, а также для подтверждения подлинности владельца Сертификата при его аутентификации с последующим установлением защищенного (шифрованного) канала связи с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи).

Отправитель - юридическое лицо, которое само непосредственно направляет или от имени которого направляется ЭД.

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

Получатель - юридическое лицо, которому ЭД отправлен самим отправителем или от имени отправителя.

Пользователи - лица сторон электронного документооборота, осуществляющие формирование, подписание, отправку/получение,

проверку, хранение и учет ЭД и/или обеспечивающие эксплуатацию ПО и технических средств АРМ.

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

Сертификат ключа подписи (Сертификат) - документ на бумажном носителе или ЭД, заверенный ЭП УЦ, который включает в себя открытый ключ подписи владельца Сертификата.

Уполномоченное лицо - лицо, имеющее право подписи ЭД.

Удостоверяющий центр (УЦ) - аккредитованный федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, основной компонент инфраструктуры открытых ключей, осуществляющий выполнение целевых функций удостоверяющего центра.

1.3. Электронный документооборот (далее - ЭДО) осуществляется в Автоматизированном рабочем комплексе «Бюджет-СМАРТ ПРО» (далее - Бюджет-СМАРТ).

1.4. Электронный документооборот в Бюджет-СМАРТ между Финансовым управлением и главными распорядителями, получателями средств Асбестовского городского округа, муниципальными бюджетными и автономными учреждениями Асбестовского городского округа, лицевые счета которым открыты в Финансовом управлении (далее - Участники), регулируется следующими документами:

- настоящим Порядком;
- нормативными правовыми актами Российской Федерации.

1.5. Электронный документооборот в Бюджет-СМАРТ осуществляется после выполнения Участником всех следующих мероприятий:

- наделения ответственных лиц Участника (пользователей) правом электронной подписи при осуществлении электронного документооборота с Финансовым управлением в соответствии с приказом (распоряжением) Участника;
- назначения администратора(ов) АРМ Участника в соответствии с приказом (распоряжением) Участника;
- установки необходимого для осуществления ЭДО ПО (исключая общесистемное и офисное ПО), имен и паролей доступа к серверу ЭДО;
- установки ПО на АРМ Участника;
- наличия Сертификата ЭП.

1.6. Участник самостоятельно обеспечивает защиту АРМ Бюджет-СМАРТ от несанкционированного доступа в соответствии с требованиями нормативных документов и законодательства Российской Федерации.

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

1.8. Пользователи назначаются приказом (распоряжением) Участника.

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

2. ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ

2.1. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К ЭД

2.1.1. ЭД, сформированные в Бюджет-СМАРТ и подписанные надлежащим количеством корректных ЭП, имеют юридическую силу наравне с бумажными документами, подписанными собственноручными подписями.

2.1.2. ЭД считаются надлежащим образом оформленными при условии их соответствия законодательству Российской Федерации, а также документам, регулирующими ЭДО в Бюджет-СМАРТ.

2.1.3. ЭД, не отвечающие требованиям, предъявляемым к ЭД настоящим Порядком, рассматриваются как ЭД, не имеющие юридической силы.

2.2. ИСПОЛЬЗОВАНИЕ ЭП В ЭД

2.2.1. ЭД должен быть подписан только ЭП уполномоченных лиц Участника для которых изданы действующие Сертификаты.

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

2.3. ПОДЛИННИК ЭД

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

2.3.2. Все экземпляры ЭД являются подлинниками данного ЭД.

2.4. КОПИИ ЭД НА БУМАЖНОМ НОСИТЕЛЕ

2.4.1. Копии ЭД могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью уполномоченных лиц Финансового управления или Участника, являющихся отправителем или получателем электронного документа.

2.4.2. Копии ЭД на бумажном носителе должны соответствовать требованиям законодательства Российской Федерации и государственным стандартам.

2.4.3. ЭД и его копии на бумажном носителе должны быть аутентичными.

2.5. ИСПОЛЬЗОВАНИЕ СВЕДЕНИЙ НА БУМАЖНОМ НОСИТЕЛЕ

2.5.1. Сведения, представленные на бумажном носителе, принимаются к обработке в Бюджет-СМАРТ в случае возникновения у одной из сторон электронного документооборота обстоятельств непреодолимой силы, к которым в том числе относятся перебои связи, электроэнергии, аварии коммунальных сетей.

3. ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

3.1. ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

3.1.1. Электронный документооборот включает:

- формирование ЭД и ЭП с использованием закрытых ключей подписи соответствующих уполномоченных лиц;
- отправку и доставку ЭД;
- проверку подлинности ЭП в доставленном ЭД:
- отзыв ЭД;
- исполнение ЭД;
- хранение ЭД (ведение архивов ЭД);
- создание бумажных копий ЭД (при необходимости).

3.2. ФОРМИРОВАНИЕ ЭД И ЭП

3.2.1. Формирование ЭД и ЭП осуществляется согласно документам, регулирующим ЭДО в Бюджет-СМАРТ, определенным настоящим Порядком.

3.3. ПРОВЕРКА ПОДЛИННОСТИ ДОСТАВЛЕННОГО ЭД

3.3.1. Проверка подлинности ЭД включает:

- проверку ЭД на соответствие документам, регулирующим ЭДО в Бюджет-СМАРТ, определенным настоящим Порядком;
- проверку подлинности всех ЭП в ЭД;
- проверку статуса соответствующих Сертификатов на момент подписания или приема соответствующего ЭД.

3.3.2. В случае положительного результата проверки подлинности ЭД, данный ЭД принимается к исполнению. В противном случае данный ЭД к

исполнению не принимается, документу будет присвоен аналитический признак «Забракован» с указанием причины непринятия ЭД к исполнению.

3.3.3. Не принятые к исполнению ЭД сохраняются на случай возможной необходимости разрешения в отношении них конфликтных ситуаций.

3.4. ОТЗЫВ ЭД

3.4.1. ЭД может быть отозван (удален) Участником только до начала его обработки (исполнения) уполномоченным лицом Финансового управления.

3.5. ИСПОЛНЕНИЕ ПЛАТЕЖНЫХ ЭД

3.5.1. Платежные ЭД, подписанные ЭП до 12-30 часов текущего рабочего дня, считаются принятыми к обработке в текущем рабочем дне, после 12-30 часов текущего рабочего дня - в следующем рабочем дне.

В случае, если платежный ЭД не соответствует требованиям по оформлению и (или) к нему не приложены необходимые документы для осуществления операции по списанию, и (или) на момент обработки на счете Участника нет доступного остатка средств, документу будет присвоен аналитический признак «Забракован» с указанием причины в отказе принятия ЭД к исполнению в течение трех рабочих дней со дня поступления ЭД.

3.6. ХРАНЕНИЕ ЭД

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

3.6.2. Срок хранения ЭД 5 лет.

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

4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. УПРАВЛЕНИЕ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ

4.1.1. Управление ключевой информацией осуществляют администраторы безопасности информации, уполномоченные лица УЦ и администраторы АРМ Участника.

4.1.2. Ключевая информация содержит сведения конфиденциального характера, хранится на носителях ключевой информации и не подлежит передаче третьим лицам.

4.1.3. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения. При обращении с ними должны выполняться требования установленные настоящим Порядком регламентирующие порядок обращения с информацией ограниченного распространения.

4.1.4. Требования по организации хранения и использования носителей ключевой информации:

- порядок хранения и использования носителей ключевой информации должен исключать возможность несанкционированного доступа к ним;
- во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

4.1.5. Не разрешается:

- знакомить или передавать носители ключевой информации лицам, к ним не допущенным;
- выводить закрытые ключи подписи на дисплей или принтер;
- вставлять носитель ключевой информации в считывающее устройство других (чужих) компьютеров;
- оставлять носитель ключевой информации без присмотра на рабочем месте;

4.1.6. Порядок работы с ключами подписи:

- в Финансовое управление предоставляются действующие Сертификаты уполномоченных лиц в формате *.cer для идентификации электронной подписи;
- владельцы Сертификатов несут персональную ответственность за безопасность (сохранение в тайне) своих закрытых ключей подписи и обязаны обеспечивать их сохранность, неразглашение и нераспространение;
- срок действия Сертификата указывается в Сертификате. Владелец Сертификата получает право использования соответствующего закрытого ключа подписи для подписи ЭД в течение срока действия Сертификата;
- сертификат пользователя Участника доступен всем пользователям Бюджет-СМАРТ после опубликования его в справочнике сертификатов ключей подписи;
- за 5 рабочих дней до окончания срока действия Сертификата его владелец обязан предоставить в Финансовое управление новый Сертификат.

4.2. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ ЗАКРЫТЫХ КЛЮЧЕЙ ПОДПИСИ

4.2.1. К событиям, связанным с компрометацией закрытых ключей подписи, относятся хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых закрытые ключи

подписи могли стать доступными неуполномоченным лицам и (или) процессам.

4.2.2. При компрометации закрытого ключа подписи владелец соответствующего Сертификата Участника немедленно прекращает его использование и незамедлительно сообщает об этом в Финансовое управление.

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

4.2.4. Дата и время, с которой Сертификат считается недействительным в Бюджет-СМАРТ, устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанного в списке отозванных сертификатов.

4.2.5. Уведомление о компрометации закрытых ключей подписи должно быть подтверждено официальным уведомлением Участника о компрометации в письменном виде. Уведомление должно содержать идентификационные параметры Сертификата.

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

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

4.3. ОТЗЫВ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

4.3.1. Отзыв Сертификата Участника осуществляется в следующих случаях:

- в случае компрометации;
- по заявлению в письменном виде владельца Сертификата, заверенному Участником.

4.3.2. Дата и время, с которых Сертификат считается недействительным в Бюджет-СМАРТ, устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанных в списке отозванных сертификатов.

5. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭДО

5.1. УВЕДОМЛЕНИЕ О КОНФЛИКТНОЙ СИТУАЦИИ

5.1.1. В случае возникновения обстоятельств, свидетельствующих, по мнению одной из сторон электронного документооборота, о возникновении и/или наличии конфликтной ситуации, данная сторона (далее - Сторона-инициатор) незамедлительно извещает другую сторону любыми доступными способами, позволяющими получить подтверждение получения другой стороной извещения, о возможном возникновении и/или наличии конфликтной ситуации, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также ее предполагаемых причинах.

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

5.1.3. В тот же срок Стороны-ответчики извещают любыми доступными способами, позволяющими получить подтверждение получение Стороной-инициатором извещения, Сторону-инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации.

5.2. РАЗРЕШЕНИЕ КОНФЛИКТНОЙ СИТУАЦИИ СУДАМИ

5.2.1. В случае невозможности разрешения споров и разногласий по конфликтной ситуации в рабочем порядке, стороны электронного документооборота передают их на рассмотрение суда в порядке, установленном законодательством Российской Федерации.