



**Департамент финансов
Администрации городского округа город Рыбинск**

П Р И К А З

от 08.11.2017

№ 89 -дф

Об утверждении правил, типовых форм и образцов документов, регулирующих обмен электронными документами с использованием электронной подписи

В целях организации взаимодействия органов местного самоуправления, муниципальных казенных, бюджетных и автономных учреждений, муниципальных казенных и унитарных предприятий, которым открыты лицевые счета в Департаменте финансов Администрации городского округа город Рыбинск, с Департаментом финансов Администрации городского округа город Рыбинск, **ДЕПАРТАМЕНТ ФИНАНСОВ АДМИНИСТРАЦИИ ГОРОДСКОГО ОКРУГА ГОРОД РЫБИНСК ПРИКАЗЫВАЕТ:**

1. Утвердить прилагаемые Правила обмена электронными документами с использованием электронной подписи.
2. Утвердить прилагаемую типовую форму Инструкции о порядке использования сертификата ключа электронной подписи.
3. Утвердить прилагаемый образец приказа о назначении ответственных лиц.
4. Утвердить прилагаемую типовую форму Договора об обмене электронными документами.
5. Электронный документооборот Департамента финансов Администрации городского округа город Рыбинск с учреждениями с применением электронной подписи в автоматизированных системах АС «Бюджет» и УРМ АС «Бюджет» осуществлять на основании заключенного Договора об обмене электронными документами в соответствии с Правилами обмена электронными документами с использованием электронной подписи.
6. Разместить настоящий приказ на официальном сайте Администрации городского округа город Рыбинск на странице «Департамент финансов» в разделе «Документы» (подраздел «Информация для ГРБС»).

7. Контроль за исполнением настоящего приказа возложить на заместителя директора Департамента финансов Администрации городского округа город Рыбинск.

Директор
Департамента финансов

Н.Н. Петухова

УТВЕРЖДЕНЫ
приказом Департамента финансов
Администрации городского округа
город Рыбинск
от 08.11.2017 № 89-дф

ПРАВИЛА ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ

Глава 1. Общие положения

Статья 1. Сфера действия настоящих правил

1. Настоящие Правила обмена электронными документами с использованием электронной подписи (далее – Правила) определяют порядок обмена электронными документами с применением электронной подписи при осуществлении взаимодействия органов местного самоуправления, муниципальных казенных, бюджетных и автономных учреждений, муниципальных казенных и унитарных предприятий (далее – Организаций), которым открыты лицевые счета в Департаменте финансов Администрации городского округа город Рыбинск, с Департаментом финансов Администрации городского округа город Рыбинск (далее – Департамент финансов) в автоматизированных системах АС «Бюджет» и УРМ АС «Бюджет».

2. При подготовке, обработке и передаче между Департаментом финансов и Организацией электронных документов Организации должны руководствоваться настоящими Правилами.

3. Электронные документы, оформленные в соответствии с настоящими Правилами, признаются равнозначными документам на бумажных носителях, подписанным собственноручными подписями уполномоченных лиц Организаций и Департамента финансов, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

4. Настоящие Правила не регулируют вопросы обмена электронными сообщениями, не являющимися электронными документами в соответствии с договором об обмене электронными документами (далее – Договор), заключаемого между Организациями и Департаментом финансов (далее – Стороны).

Статья 2. Основные понятия, используемые в настоящих правилах

В настоящих Правилах используются следующие понятия:

автоматизированное рабочее место – установленные в Департаменте финансов и устанавливаемые в Организации программное обеспечение и технические средства, включая средства криптографической защиты информации, предназначенные для работы в системе электронного документооборота;

администратор автоматизированного рабочего места Организации - сотрудник Организации, отвечающий за обеспечение бесперебойной эксплуатации программного обеспечения и технических средств автоматизированного рабочего места Организации, осуществляющий контроль мероприятий по защите информации, хранение и учет электронных документов, взаимодействие с Департаментом финансов по техническим вопросам и вопросам обеспечения безопасности информации;

администратор безопасности информации Департамента финансов - лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена электронными документами Департамента финансов с Организацией;

электронная подпись - информация в электронной форме, которая присоединена к подписываемой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

квалифицированный сертификат ключа проверки электронной подписи (далее - **Сертификат**) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи;

удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей;

аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи»;

владелец Сертификата - физическое лицо, на имя которого удостоверяющим центром выдан Сертификат;

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

ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

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

электронной подписи;

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

- сертификат, относящийся к этой электронной подписи, издан удостоверяющим центром, и не утратил силу (действует) на момент проверки или на момент подписания электронного документа,
- подтверждена подлинность этой электронной подписи в электронном документе,
- электронная подпись используется в соответствии со сведениями, указанными в Сертификате;

носитель ключевой информации - материальный носитель информации, содержащий ключ подписи или аутентификации;

отправитель - юридическое лицо в системе электронного документооборота, которое само непосредственно направляет или от имени которого направляется электронный документ;

подтверждение подлинности электронной подписи в электронном документе - положительный результат проверки принадлежности электронной подписи в электронном документе владельцу Сертификата и отсутствия искажений в подписанном данной электронной подписью электронном документе;

получатель - юридическое лицо, которому электронный документ отправлен самим отправителем или от имени отправителя;

пользователи – лица, уполномоченные от имени Организации или от имени Департамента финансов осуществлять формирование, подписание, отправку/получение, проверку, хранение и учет электронных документов или/и обеспечивающие эксплуатацию программного обеспечения и технических средств автоматизированного рабочего места;

программное обеспечение - совокупность программ и программных документов, необходимых для их эксплуатации;

уполномоченное лицо - лицо, имеющее право подписи электронного документа.

Статья 3. Регулирование в отношениях при электронном документообороте.

Электронный документооборот между Департаментом финансов и Организацией регулируется следующими документами:

- договором об обмене электронными документами;
- технической документацией на автоматизированное рабочее место Организации, включая документацию на средства криптографической защиты информации;

нормативными правовыми актами Российской Федерации, Ярославской области, муниципального образования городской округ город Рыбинск.

Статья 4. Порядок и условия допуска Организации к осуществлению электронного документооборота с Департаментом финансов

1. Организация допускается к осуществлению электронного

документооборота после выполнения следующих мероприятий:

заключения Договора с Департаментом финансов;

назначения администратора(ов) автоматизированного рабочего места Организации;

наличие необходимого для осуществления электронного документооборота программного обеспечения, в том числе средств криптографической защиты информации;

установки программного обеспечения на автоматизированное рабочее место Организации;

проведения Департаментом финансов инструктажа Пользователей Организации работе с автоматизированным рабочим местом Организации;

получения, в случае использования средств криптографической защиты информации для защиты каналов связи и аутентификации при доступе в систему электронного документооборота, в установленном порядке ключевой документации;

регистрации Пользователей Организации в аккредитованном удостоверяющем центре и получения в установленном порядке Сертификатов.

2. Организация обеспечивает защиту автоматизированного рабочего места Организации от несанкционированного доступа в соответствии с требованиями нормативных документов и законодательства Российской Федерации.

3. Пользователи Организации:

несут персональную ответственность за безопасность ключевой информации, в том числе ключа электронной подписи и ключа проверки электронной подписи, и обязаны обеспечивать ее сохранность, неразглашение и нераспространение;

должны быть ознакомлены под роспись с документами, регулирующими электронный документооборот, определенными настоящими Правилами.

Глава 2. Электронные документы

Статья 5. Требования, предъявляемые к электронным документам

1. Электронные документы считаются надлежащим образом оформленными при условии их соответствия законодательству Российской Федерации, настоящим Правилам, а также иным документам, регулирующим электронный документооборот.

2. Электронные документы, не отвечающие требованиям, предъявляемым к электронным документам настоящими Правилами, рассматриваются Департаментом финансов и Организацией как электронные документы, не имеющие юридической силы.

Статья 6. Использование электронной подписи в электронном документе

1. Электронный документ может быть подписан только электронной подписью уполномоченных лиц Департамента финансов или Организации, для которых аккредитованным удостоверяющим центром изданы действующие Сертификаты.

2. Прекращение действия Сертификатов уполномоченных лиц Департамента финансов или Организации не влияет на юридическую силу и действительность

электронных документов, которыми Департамент финансов или Организация обменивались до прекращения действия Сертификатов.

Статья 7. Использование электронного документа

1. Электронные документы, подписанные корректными электронными подписями уполномоченных лиц Департамента финансов или Организации, имеют равную юридическую силу с документами, представленными на бумажных носителях, подписанных собственноручными подписями уполномоченных лиц Департамента финансов или Организации, и не могут быть оспорены только на том основании, что они выполнены в электронном виде.

2. Электронные документы могут иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего электронного документа осуществляется воспроизводство содержания документа вместе с электронной подписью.

3. Все экземпляры электронного документа являются подлинниками данного электронного документа.

Статья 8. Представление сведений, содержащихся в электронном документе, на бумажном носителе.

1. Сведения, содержащиеся в электронном документе, могут быть представлены (распечатаны) на бумажном носителе. В этом случае их соответствие электронному документу должно быть заверено собственноручной подписью и отметкой об ЭЦП лиц, уполномоченных Департаментом финансов или Организацией, являющимся отправителем или получателем электронного документа.

2. Программы, осуществляющие представление сведений, содержащихся в электронных документах на бумажных носителях, являются составной частью программного обеспечения, используемого в системе электронного документооборота.

Глава 3. Электронный документооборот

Статья 9. Организация электронного документооборота

Электронный документооборот включает:

формирование электронных документов и их электронной подписи с использованием ключей электронной подписи соответствующих уполномоченных лиц Сторон;

отправку и доставку электронных документов;

проверку подлинности электронной подписи в доставленном электронном документе;

подтверждение получения электронного документа;

отзыв электронного документа;

учет электронных документов (регистрацию входящих и исходящих электронных документов);

хранение электронных документов;
создание дополнительных экземпляров электронных документов;
создание представлений (распечатывание) электронных документов в бумажном виде.

Статья 10. Формирование электронного документа и их электронная подпись

Формирование электронных документов и их электронная подпись осуществляется согласно документам, регулирующим электронный документооборот, определенный настоящими Правилами.

Статья 11. Отправка и доставка электронных документов

1. В отношениях между отправителем и получателем электронный документ считается исходящим от отправителя, если электронный документ отправлен лицом, уполномоченным действовать от имени отправителя в отношении данного электронного документа.

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

3. Документы от Организации принимаются Департаментом финансов круглосуточно.

Статья 12. Проверка подлинности доставленного электронного документа

1. Проверка подлинности электронного документа включает:

проверку электронного документа на соответствие документам, регулирующим электронный документооборот, определенный настоящими Правилами;

проверку подлинности электронной подписи в электронном документе.

2. В случае положительного результата проверки подлинности электронного документа данный электронный документ принимается к исполнению (передается на последующий контроль, проверку корректности содержания). В противном случае данный электронный документ к исполнению не принимается.

3. Не принятые к исполнению электронные документы сохраняются на случай разрешения относительно них конфликтных ситуаций.

Статья 13. Подтверждение получения электронного документа

Подтверждение получения электронного документа (уведомление) производится в автоматическом режиме.

Статья 14. Отзыв электронного документа

1. Организация вправе отозвать отправленный электронный документ.

2. Электронный документ должен быть отозван отправителем до начала его обработки (исполнения) получателем.

Статья 15. Учет электронных документов

1. Учет электронных документов осуществляется путем ведения электронных журналов учета в автоматизированном рабочем месте Организации.
2. Срок хранения электронных журналов учета определяется сроком хранения учитываемых электронных документов.

Статья 16. Хранение электронных документов

1. Электронные документы должны храниться с сохранением всех реквизитов (полей), включая все электронные подписи. Допускается хранение электронных документов в виде последовательности всех полей электронного документа (включая все электронные подписи) в записи базы данных.
2. Срок хранения электронного документа должен соответствовать сроку хранения соответствующих документов на бумажных носителях.
3. Хранение электронного документа должно сопровождаться хранением соответствующих электронных журналов учета, Сертификатов, подтверждений о доставке электронного документа, а также программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки электронной подписи хранимых электронных документов.

Глава 4. Обеспечение информационной безопасности**Статья 17. Общие требования обеспечения защиты информации в системе электронного документооборота**

В случае обмена конфиденциальной информацией Организация должна выполнять 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 N 152 (далее - Инструкция N 152).

Статья 18. Управление ключевой информацией

1. Управление ключевой информацией осуществляют администраторы безопасности информации, уполномоченные лица удостоверяющего центра и администраторы автоматизированного рабочего места Организации.
2. Ключевая информация содержит сведения конфиденциального характера, хранится на, учтенных в установленном порядке, носителях ключевой информации и не подлежит передаче третьим лицам.
3. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения. При обращении с ними должны выполняться требования Инструкции N 152, иных документов, регламентирующих порядок обращения с информацией ограниченного распространения в органах исполнительной власти, и настоящих Правил.
4. Учет носителей ключевой информации осуществляют администраторы безопасности информации.

Статья 19. Требования по организации хранения и использования носителей ключевой информации

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

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

3. Не разрешается:

производить несанкционированное копирование носителей ключевой информации;

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

выводить ключи электронной подписи на дисплей или принтер;

вставлять носитель ключевой информации в считывающее устройство других компьютеров;

оставлять носитель ключевой информации без присмотра на рабочем месте;

записывать на носитель ключевой информации посторонние файлы.

Статья 20. Порядок действий при компрометации ключей электронной подписи или проверки электронной подписи

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

2. При компрометации ключа электронной подписи или проверки электронной подписи уполномоченное лицо Организации немедленно прекращает его использование и незамедлительно сообщает об этом администратору автоматизированного рабочего места Организации, а тот, в свою очередь, администратору безопасности информации.

3. После получения от владельца Сертификата Организации сообщения о компрометации ключей электронной подписи или проверки электронной подписи администратор безопасности информации проверяет достоверность полученного сообщения. В случае подтверждения полученной информации, инициируется процедура отзыва или приостановления действия соответствующего Сертификата.

4. Дата и время, с которой Сертификат считается недействительным в системе электронного документооборота, устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанного в списке отозванных Сертификатов.

5. Уведомление о компрометации ключей электронной подписи или проверки электронной подписи должно быть подтверждено официальным уведомлением Организации о компрометации в письменном виде. Уведомление должно содержать идентификационные параметры Сертификата.

6. Использовать скомпрометированные ключи электронной подписи для подписи электронного документа и ключи проверки электронной подписи для

организации защищенного канала связи запрещается.

7. В случае компрометации ключа электронной подписи и отзыва соответствующего Сертификата с публикацией в списке отозванных сертификатов Организация изготавливает новые ключи электронной подписи или проверки электронной подписи.

8. Сертификат, соответствующий скомпрометированному ключу электронной подписи, хранится в установленном порядке в удостоверяющем центре для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением электронной подписи.

Статья 21. Отзыв сертификата ключа подписи

1. Удостоверяющий центр отзывает Сертификат Организации в следующих случаях:

в случае компрометации;

по заявлению в письменном виде владельца Сертификата, заверенному Организацией.

2. В случае отзыва или приостановления действия Сертификата пользователя Организации удостоверяющий центр обеспечивает публикацию списка отозванных сертификатов с указанием серийного номера Сертификата, даты, времени и причины аннулирования. Дата и время, с которых Сертификат считается недействительным, устанавливается равной дате и времени отзыва или приостановления действия Сертификата, указанных в списке отозванных сертификатов.

Глава 5. Порядок разрешения конфликтных ситуаций и споров в связи с осуществлением электронного документооборота

Статья 22. Возникновение конфликтных ситуаций в связи с осуществлением электронного документооборота.

1. В связи с осуществлением электронного документооборота возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также использования в данных документах электронной подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

оспаривание факта отправления и/или получения электронного документа;

оспаривание времени отправления и/или получения электронного документа;

оспаривание содержания отправленного/полученного электронного документа;

оспаривание подлинности экземпляров электронного документа;

оспаривание целостности электронного документа;

оспаривание идентичности лица, заверившего электронный документ электронной подписью;

оспаривание полномочий лица, заверившего электронный документ электронной подписью.

2. Конфликтные ситуации разрешаются (урегулируются) Сторонами в

рабочем порядке и/или по итогам работы комиссии по разрешению конфликтной ситуации (далее - Комиссия).

3. В случае невозможности разрешения конфликтной ситуации в рабочем порядке и/или по итогам работы Комиссии Стороны разрешают конфликтную ситуацию в претензионном порядке либо направляют имеющиеся разногласия на рассмотрение вышестоящих органов либо суда в порядке, установленном законодательством Российской Федерации.

Статья 23. Уведомление о конфликтной ситуации

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

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.

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

Статья 24. Разрешение конфликтной ситуации в рабочем порядке

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

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

Статья 25. Формирование Комиссии по разрешению конфликтной ситуации

1. В случае, если конфликтная ситуация не была разрешена в рабочем порядке, Сторона-инициатор должна не позднее чем в течение трех рабочих дней после возникновения конфликтной ситуации направить уведомление о конфликтной ситуации (далее - Уведомление) и предложение о создании комиссии по разрешению конфликтной ситуации (далее - Предложение) Стороне-ответчику.

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

3. Уведомление должно содержать информацию с указанием фамилий, имен, отчеств, должностей и контактной информации должностных лиц Стороны-

инициатора, уполномоченных в разрешении конфликтной ситуации.

4. Предложение должно содержать информацию о предлагаемом месте, дате и времени сбора комиссии, но не позднее трех рабочих дней со дня отправления Предложения, список предлагаемых для участия в работе Комиссии представителей Стороны-инициатора с указанием фамилий, имен, отчеств, должностей, при необходимости исполняемых при обмене электронными документами функциональных ролей (администратор, администратор безопасности и т.п.), их контактной информации (телефон, факс, электронная почта).

5. Уведомление и Предложение составляются на бумажном носителе, подписываются должностными лицами Стороны-инициатора, уполномоченными в разрешении конфликтной ситуации, и передаются Стороне-ответчику в установленном порядке, обеспечивающем подтверждение вручения корреспонденции.

6. Уведомление и Предложение могут быть составлены и направлены в форме электронного документа. При этом факт их доставки должен быть подтвержден.

Статья 26. Формирование комиссии по разрешению конфликтной ситуации, ее состав

1. Не позднее чем на третий рабочий день после получения Предложения Сторонами, участвующими в разрешении конфликтной ситуации, должна быть сформирована Комиссия.

2. Комиссия формируется на основании совместного приказа Сторон. Приказ устанавливает состав Комиссии, время и место ее работы.

3. Устанавливается тридцатидневный срок работы Комиссии. В исключительных случаях срок работы Комиссии по согласованию Сторон может быть дополнительно продлен не более чем на тридцать дней.

4. Если Стороны не договорятся об ином, в состав Комиссии входит равное количество уполномоченных лиц каждой из Сторон, участвующих в разрешении конфликтной ситуации.

5. В состав Комиссии назначаются представители служб информационно-технического обеспечения и служб обеспечения информационной безопасности, а также представители подразделений - исполнителей электронного документа.

6. В состав Комиссии могут быть включены представители юридических служб Сторон, представители органов, осуществляющих регулирование и контроль соответствующих видов деятельности.

7. Независимо от соглашения Сторон в состав Комиссии должен входить хотя бы один уполномоченный представитель удостоверяющего центра.

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

9. Лица, входящие в состав Комиссии, должны обладать необходимыми знаниями и опытом работы в области подготовки и исполнения электронных

документов, построения и функционирования системы электронного документооборота, организации и обеспечения информационной безопасности при обмене электронными документами, должны иметь соответствующий допуск к необходимым для проведения работы Комиссии документальным материалам и программно-техническим средствам.

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

Статья 27. Задачи, права и полномочия комиссии по разрешению конфликтной ситуации

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

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

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

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

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

6. Комиссия имеет право получать объяснения от должностных лиц Сторон, обеспечивающих обмен электронными документами.

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

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

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

Статья 28. Протокол работы комиссии по разрешению конфликтной ситуации

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

2. Протокол работы Комиссии должен содержать следующие данные:

состав Комиссии с указанием сведений о фамилиях, именах, отчествах, местах работы, занимаемых должностях, допусках к необходимым работам, при необходимости исполняемых при обмене электронными документами

функциональных ролях, контактной информации и квалификации каждого из членов комиссии;

краткое изложение обстоятельств, свидетельствующих, по мнению Стороны-инициатора, о возникновении и/или наличии конфликтной ситуации;

установленные Комиссией фактические обстоятельства;

мероприятия, проведенные Комиссией для установления наличия, причин возникновения и последствий возникшей конфликтной ситуации, с указанием даты, времени и места их проведения;

выводы, к которым пришла Комиссия в результате проведенных мероприятий;

подписи всех членов комиссии.

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

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

Статья 29. Акт по итогам работы комиссии по разрешению конфликтной ситуации

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

состав Комиссии;

дату и место составления Акта;

даты и время начала и окончания работы Комиссии;

фактические обстоятельства, установленные Комиссией;

краткий перечень мероприятий, проведенных Комиссией;

выводы, к которым пришла Комиссия в результате проведенных мероприятий;

подписи членов Комиссии;

в случае наличия - особое мнение члена или членов Комиссии.

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

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

Статья 30. Разрешение конфликтной ситуации по итогам работы комиссии

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

2. В срок не более трех рабочих дней со дня окончания работы Комиссии

Стороны на основании выводов Комиссии принимают меры по разрешению конфликтной ситуации и извещают другие Стороны о принятых мерах.

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

4. В случае, если конфликтная ситуация признается Сторонами разрешенной, то в срок не позднее пяти рабочих дней со дня окончания работы Комиссии Стороны оформляют решение об урегулировании конфликтной ситуации (далее - Решение).

5. Решение составляется Сторонами в форме документа на бумажном носителе по одному экземпляру каждой Стороне. Решение подписывается уполномоченными в разрешении конфликтной ситуации лицами Сторон и утверждается руководителями Сторон либо их заместителями.

Статья 31. Претензионный порядок разрешения конфликтной ситуации

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

2. Претензия должна содержать:

изложение существа требований Стороны-инициатора;

при возможности денежной оценки претензии - ее сумму и расчет;

изложение фактических обстоятельств, на которых основываются требования Стороны-инициатора и доказательства, подтверждающие их, со ссылкой на соответствующие нормы законодательства и нормативных правовых актов;

сведения о работе Комиссии и, в случае, если Комиссия работала в связи с рассматриваемой конфликтной ситуацией, копии материалов работы Комиссии, независимо от выводов Комиссии, согласия или несогласия с этими выводами Стороны-инициатора;

иные документы, имеющие значение, по мнению Стороны-инициатора;

перечень прилагаемых к Претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по Претензии.

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

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

удовлетворении требований Претензии.

Статья 32. Разрешение конфликтной ситуации судами

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

УТВЕРЖДЕНА
приказом Департамента финансов
Администрации городского округа
город Рыбинск
от 08.11.2017 № 89-дф

Типовая форма

ИНСТРУКЦИЯ О ПОРЯДКЕ ИСПОЛЬЗОВАНИЯ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

1. Владелец сертификата ключа проверки электронной подписи (далее «Владелец сертификата») обязан обеспечить конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих ему ключей электронных подписей без его согласия.

2. Владелец сертификата обязан не использовать ключи электронной подписи, если ему известно, что эти ключи скомпрометированы. Под компрометацией ключа понимается утрата доверия к тому, что используемый ключ недоступен посторонним лицам. К событиям, связанным с компрометацией ключа, относятся следующие:

- утрата ключевых носителей;
- утрата ключевых носителей ключа с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей с последующим обнаружением;
- доступ посторонних лиц к ключевой информации;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе, когда ключевой носитель вышел из строя и не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- и т.п.

3. Владелец сертификата обязан немедленно требовать приостановления действия сертификата ключа проверки электронной подписи при наличии событий и случаев, предусмотренных 2 данной Инструкции, а также оснований полагать, что конфиденциальность ключей электронных подписей нарушена.

4. Владелец сертификата обязан применять сертификат ключа проверки электронной подписи только в соответствии с областями действия сертификата

ключа проверки электронной подписи. В случае несоблюдения данного требования применение сертификата ключа проверки электронной подписи признается неправомерным.

5. Владелец сертификата обязан соблюдать правила использования ПО СКЗИ, содержащиеся в требованиях приказа ФАПСИ N 152 от 13.06.2001 "Об Утверждении 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".

Владелец сертификата обязан выполнять иные требования, предусмотренные Федеральным законом от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

С настоящей инструкцией ознакомлен, согласен и обязуюсь выполнять.

_____/_____
" ____ " _____ 20__ г.

УТВЕРЖДЕН
приказом Департамента финансов
Администрации городского округа
город Рыбинск
от 08.11.2017 № 89-дф

Образец

ПРИКАЗ О НАЗНАЧЕНИИ ОТВЕТСТВЕННЫХ ЛИЦ

(наименование организации)

(дата подписания приказа)

(номер приказа)

О назначении ответственных лиц

В соответствии с Договором об обмене электронными документами между Департаментом финансов Администрации городского округа город Рыбинск и _____, приказываю:

1. Наделить правом электронной подписи электронных документов следующих сотрудников:

п/п	Ф.И.О.	Подразделение, должность	Перечень подписываемых документов

2. Возложить функции и обязанности Администратора безопасности по организации, обеспечению и контролю мероприятий по защите информации при обмене электронными документами на **Ф.И.О.**, наделить его соответствующими правами и полномочиями.

3. Возложить функции и обязанности Администратора автоматизированного рабочего места обмена электронными документами (далее - АРМ ЭД), по организации и обеспечению надежной бесперебойной эксплуатации программно-технических средств АРМ ЭД на **Ф.И.О.**, наделить его соответствующими правами и полномочиями.

4. Назначенные в п.п. 1 - 3 настоящего приказа сотрудники несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе обмена информацией между Департаментом финансов Администрации городского округа город Рыбинск и _____;
- обеспечение конфиденциальности ключей электронных подписей;
- соблюдение правил эксплуатации средств АРМ ЭД и средств электронной

подписи.

5. Копию настоящего приказа представить в Департамент финансов Администрации городского округа город Рыбинск.

6. Сертификаты пользователей ЭЦП Организации посылаются Администратором информационной безопасности Организации на почтовый ящик **esp@dfagogr.ru**.

7. Сертификаты на новых пользователей ЭЦП, сопровождаются копией приказа «О назначении пользователей ЭЦП» на бумажном носителе в Департамент финансов Администрации городского округа город Рыбинск.

8. Контроль за выполнением настоящего приказа _____.

Руководитель

УТВЕРЖДЕН
приказом Департамента финансов
Администрации городского округа
город Рыбинск
от 08.11.2017 № 89-дф

Типовая форма

Договор об обмене электронными документами
№ _____ от _____ 201__ г.

Департамент финансов Администрации городского округа город Рыбинск, именуемый в дальнейшем «Департамент финансов», в лице _____, действующего на основании _____, с одной стороны, и _____, именуем _____ в дальнейшем «Организация», в лице _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», заключили настоящий договор (далее - Договор) о нижеследующем.

1. Предмет договора

1.1. Договор регулирует отношения между Сторонами по электронному документообороту, в соответствии с Правилами обмена электронными документами с использованием электронной подписи (далее - Правила), утвержденными приказом Департамента финансов Администрации городского округа город Рыбинск от _____. 201__ № _____.

1.2. Договор определяет права и обязанности Сторон, возникающие при осуществлении электронного документооборота (далее - ЭДО), с учетом обеспечения информационной безопасности.

1.3. Договор определяет условия и порядок обмена электронными документами (далее - ЭД) при осуществлении ЭДО между Сторонами в автоматизированных системах АС «Бюджет» и УРМ АС «Бюджет» (далее - СЭД).

2. Права и обязанности Сторон

2.1. При осуществлении обмена ЭД с использованием СЭД Стороны обязуются:

2.1.1. Руководствоваться законодательством Российской Федерации, нормативными актами Министерства финансов Российской Федерации, Федерального казначейства, эксплуатационной документацией на программное

обеспечение (далее - ПО) СЭД (включая средства криптографической защиты информации (далее - СКЗИ)), Правилами и настоящим Договором.

2.1.2. При компрометации ключей электронных подписей (далее - ключ электронной подписи) руководствоваться Правилами.

2.2. Стороны признают, что:

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

- сертификаты ключей проверки электронных подписей (далее - сертификаты), относящиеся к этим ЭП, изданы аккредитованным удостоверяющим центром и не утратили силу (действуют) на момент проверки или на момент подписания ЭД;

- подтверждена подлинность этих ЭП в ЭД;

- ЭП используется в соответствии со сведениями, указанными в сертификате.

2.2.2. Применяемые в СЭД сертифицированные СКЗИ и ЭП обеспечивают конфиденциальность, целостность и подлинность ЭД при осуществлении Сторонами обмена ЭД с использованием общедоступных каналов связи и нескомпрометированных ключей электронной подписи уполномоченных лиц.

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

Положения настоящего пункта подлежат применению к следующим ЭД (согласно описанию в СЭД):

- Кассовый план (расходы);
- Помесечные предельные объемы финансирования по ПБС;
- Помесечный кассовый план;
- Помесечные предельные объемы финансирования по ПБС (расходы);
- Роспись по ПБС (расходы);
- Сводная бюджетная роспись (расходы);
- Кассовый план (доходы);
- Кассовый план (источники);
- Роспись по администраторам источников финансирования (источники);
- Сведения БУ, АУ (ПФХД);
- Расход по платежным поручениям;
- Приход от прочих;
- Утверждение объемов финансирования;
- Распределение объемов финансирования;
- Уведомления по лимитам;
- Выписка по доходам, возврат доходов;
- Месячные отчеты организаций;
- Внутреннее казначейское уведомление;

- Внутренние платежи за платные услуги
- Расходное расписание;
- Уведомление об уточнении вида и принадлежности платежа;
- Договор;
- Контракт;
- Документ исполнения;
- Заявка на закупку;
- Внутренняя переброска.

Список документов может изменяться, в связи с изменением возможностей СЭД, путем заключения дополнительного соглашения к настоящему договору.

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

2.3. Департамент финансов обязуется:

2.3.1. Предоставить информацию о технических требованиях, предъявляемых к АРМ Организации, необходимых для подключения к СЭД.

2.3.2. Принимать и исполнять, оформленные должным образом, ЭД Организации СЭД в соответствии с настоящим Договором.

2.3.2.1. Обработать и отправить в Федеральное казначейство или Отделения Ярославль ЦБ платежные документы, согласно регламентов обмена с Федеральным казначейством и Отделением Ярославль ЦБ, не позднее следующего рабочего дня. Отправка может быть отменена при не прохождении документом контролей в автоматизированной системе АС «Бюджет», с указанием причины отклонения.

2.3.3. Предоставлять Организации актуальные справочники, используемые в СЭД и необходимые для подготовки ЭД.

2.3.4. При изменении порядка и/или правил обработки ЭД, при необходимости, своевременно предоставлять Организации модернизированное ПО для АРМ Организации с откорректированной технической документацией.

2.3.5. При техническом сбое организовать одно рабочее место с возможностью отправки документов с ЭЦП и сканирование документов в кабинете №108 по адресу: г. Рыбинск, Рабочая д.1.

Под техническим сбоем понимается:

выход из строя компьютера с СЭД;

выход из строя ПО СЭД;

выход из строя канала связи с Департаментом финансов.

2.4. Департамент финансов имеет право:

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

2.4.2. Приостанавливать обмен ЭД при:

несоблюдении Организацией требований по передаче ЭД и обеспечению информационной безопасности, предусмотренных законодательством Российской Федерации и условиями настоящего Договора;

разрешении спорных ситуаций, а также для выполнения неотложных, аварийных и ремонтно-восстановительных работ на АРМ Департамента финансов.

2.4.3. Производить замену ПО СЭД.

2.5. Организация обязуется:

2.5.1. Использовать АРМ Организации исключительно в целях, предусмотренных настоящим Договором.

2.5.2. В течение 3-х дней со дня заключения настоящего Договора назначить приказом (образец приказа утвержден приказом Департамента финансов Администрации городского округа город Рыбинск от _____.____201__ № _____-дф) и предоставить его копию в Департамент финансов следующих лиц:

2.5.2.1. Лицо или несколько лиц, уполномоченных на подписание ЭП ЭД, исходящих от Организации;

2.5.2.2. Лицо, ответственное за выполнение функций и обязанностей Администратора безопасности по организации, обеспечению и контролю мероприятий по защите информации при обмене электронными документами;

2.5.2.3. Лицо, ответственное за выполнение функций и обязанностей Администратора АРМ обмена электронными документами по организации и обеспечению надежной бесперебойной эксплуатации программно-технических средств АРМ.

2.5.3. Передавать Департаменту финансов должным образом оформленные ЭД и получать от Департамента финансов электронные сообщения, подтверждающие получение и обработку ЭД.

2.5.4. Обеспечить конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия, ПО (в том числе СКЗИ и ключевой документации к ним).

2.5.5. Владельцев ЭП Организации под роспись ознакомить с Инструкцией о порядке использования сертификата ключа проверки электронной подписи, форма которой утверждена приказом Департамента финансов Администрации городского округа город Рыбинск от _____.____201__ № _____.

2.5.6. Исполнять требования по обеспечению информационной безопасности АРМ Организации, изложенные в Правилах.

2.5.7. Соблюдать требования предоставленной Департаментом финансов документации пользователя и администратора АРМ Организации.

2.6. Организация имеет право:

2.6.1. Требовать от Департамента финансов исполнения принятых от Организации ЭД при условии корректности содержания ЭД.

2.6.2. Требовать от Департамента финансов приостановления исполнения (обработки) всех ЭД в случаях компрометации ключей электронной подписи Организации.

3. Ответственность Сторон

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

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

3.3. Стороны не несут ответственности за возможные временные задержки

исполнения и/или искажения ЭД, возникающие по вине лиц, предоставляющих услуги связи для использования в СЭД.

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

3.5. Сторона не несет ответственность за убытки другой Стороны, возникшие вследствие несвоевременного сообщения о компрометации ключей электронной подписи представителями другой Стороны, участвующими в СЭД.

3.6. Организация несет ответственность за соблюдение требований предоставленной Департаменту финансов документации пользователя и администратора АРМ Организации.

3.7. В случае неработоспособности АРМ Организации, произошедшей по вине Организации, а также в случае необходимости переноса ПО АРМ Организации на другое аппаратное обеспечение Организация обязуется в срок не более 2-х рабочих дней обеспечить работоспособность АРМ Организации.

4. Порядок разрешения конфликтных ситуаций

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

4.2. В случае, если конфликтная ситуация не урегулирована в результате переговоров Сторон, создается Комиссия из представителей Сторон в соответствии с Правилами.

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

5. Срок действия договора, порядок его изменения и расторжения

5.1. Настоящий Договор заключается на 5 лет и вступает в силу со дня его подписания Сторонами.

5.2. В случае принятия нормативного акта уполномоченным государственным органом по вопросам, регулируемым настоящим Договором, соответствующие положения Договора подлежат изменению по инициативе одной из Сторон.

5.3. Настоящий договор может быть расторгнут по инициативе одной из Сторон с предварительным уведомлением об отказе от Договора другой стороны не позднее чем за 15 (пятнадцать) дней до предполагаемой даты расторжения.

5.4. Договор от [] № [] «Об обмене электронными документами, имеющими электронную цифровую подпись», заключенный между Сторонами, прекращает свое действие со дня вступления в силу настоящего

Договора.

6. Дополнительные условия

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

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

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

6.4. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

7. Адреса и реквизиты Сторон

Департамент финансов:

Организация:

Департамент финансов
Администрации городского округа
город Рыбинск
ИНН 7610070192, КПП 761001001
152900, Ярославская область,
г. Рыбинск, ул. Рабочая, д.1.
р/сч. 40204810100000000022
УФК по ЯО (ДФ АГОГР
02713001310) (ДФ АГОГР 13011300)
Отделение Ярославль г. Ярославль
БИК 047888001

_____/

М.П.

/