Управление финансов и муниципальных закупок
города Димитровграда Ульяновской области

ПРИКАЗ

03 марта 2020 года **№ 10-О/Д**

О юридически значимом электронном документообороте в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области

Руководствуясь Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», постановлением Правительства Российской Федерации от 09.02.2012 N 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи», пунктом 2 распоряжения Правительства Российской Федерации от 20.07.2011 N 1275-р, в целях формирования в городе Димитровграде элементов инфраструктуры интегрированной информационной системы управления общественными финансами «Электронный бюджет» посредством увеличения доли юридически значимого электронного документооборота в общем объеме документооборота в области финансово-хозяйственной деятельности, п р и к а з ы в а ю:

1. Установить юридически значимый электронный документооборот между Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области и главными распорядителями бюджета города Димитровграда (далее – участники юридически значимого электронного документооборота) в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области.

2. Утвердить:

2.1. Форму соглашения об обмене электронными документами между Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области и участниками юридически значимого электронного документооборота (приложение N 1).

2.2. Регламент применения электронной подписи участниками юридически значимого электронного документооборота в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (приложение N 2).

2.3. Инструкцию о порядке работы со средствами криптографической защиты информации в автоматизированной системе «СКИФ-БП» Управления

финансов и муниципальных закупок города Димитровграда Ульяновской области (приложение N 3).

2.4. Форму заявления на внесение в реестр автоматизированной системы «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области сертификатов уполномоченных сотрудников (приложение N 4).

2.5. Порядок разбора конфликтных ситуаций при осуществлении юридически значимого электронного документооборота в автоматизированной системы «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (приложение N 5).

2.6. Порядок предоставления электронных документов из автоматизированной системы «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области по обращениям заинтересованных лиц (приложение N 6).

2.7. Карту рисков юридически значимого электронного документооборота в автоматизированной системы «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (приложение N 7).

3. Главным распорядителям бюджетных средств города Димитровграда в срок до 01.04.2020 перейти на юридически значимый электронный документооборот в автоматизированной системе «СКИФ-БП».

4. Отделу учета и отчетности Управления финансов и муниципальных закупок города Димитровграда Ульяновской области в срок до 25.03.2020 обеспечить подписание соглашений об обмене электронными документами между Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области и участниками юридически значимого электронного документооборота – главными распорядителями средств бюджета города Димитровграда Ульяновской области на юридически значимый электронный документооборот в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области.

5. Контроль за исполнением настоящего Приказа оставляю за собой.

Начальник Управления Н.В. Галактионов

Приложение N 1
к приказу
Управления финансов и
муниципальных закупок
города Димитровграда
Ульяновской области
от 03марта 2020 г. N10-ОД

форма

СОГЛАШЕНИЕ
об обмене электронными документамимежду
Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области и участником юридически значимого электронного документооборота

г. Димитровград «___» _____ 20__ г.

Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области в лице _____, действующего на основании _____, именуемое в дальнейшем «Организатор», с одной стороны, и _____
_____
_____
(полное наименование организации в соответствии с учредительным документом)
в лице _____
(должность, ФИО)
_____,
действующего на основании _____,
именуем_____ в дальнейшем «Клиент», с другой стороны, вместе именуемые Стороны, заключили соглашение о нижеследующем:

1. Термины и понятия, используемые в настоящем Соглашении

1.1. Такие термины и понятия, как "аккредитованный удостоверяющий центр" (далее - УЦ), "квалифицированный сертификат ключа проверки электронной подписи" (далее - сертификат), "ключ электронной подписи" (далее - ключ), "усиленная квалифицированная электронная подпись" (далее - ЭП) и "электронный документ", используемые в настоящем Соглашении, применяются в том же значении, что и в Федеральном законе от 06.04.2011 N 63-ФЗ "Об электронной подписи".

1.2. Автоматизированная система«СКИФ-БП»Управления финансов и муниципальных закупок города Димитровграда Ульяновской области – автоматизированнаясистема для принятия, формирования и свода бюджетной (бухгалтерской) отчетности, направляемые главными распорядителями бюджетных средств города Димитровграда в Ульяновской области (далее - Система).

Клиентская часть Системы - аппаратно-программный комплекс,

предназначенный для хранения, обработки и передачи данных по телекоммуникационным каналам связи с рабочих машин уполномоченных сотрудников на серверную часть Систем.

Компрометация ключа - утрата доверия к тому, что ключ используется исключительно уполномоченным сотрудником и исключительно по назначению.

Организатор – Управлениефинансов и муниципальных закупок города Димитровграда Ульяновской области, являющееся стороной ЮЗЭД (в лице уполномоченных сотрудников) на базе Системы, а также организатором ЮЗЭД в Системе, осуществляющим функции по хранению на своём оборудовании базы данных и конфигурации серверной части Системы, по настройке Системы на серверных станциях.

Регламент применения электронной подписи участниками юридически значимого электронного документооборота (далее - Регламент) - утвержденный Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области документ, определяющий статусы электронных документов, на которых происходит наложение ЭП.

Реестр Системы– справочникСистемы, в котором хранится перечень сертификатов ключей проверки электронной подписи уполномоченных сотрудников.

Средства криптографической защиты информации (далее - СКЗИ) - аппаратно-программный комплекс, выполняющий функцию по созданию ЭП и сертифицированный в соответствии с законодательством.

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

Уполномоченный сотрудник - сотрудник, наделенный полномочиями по подписанию ЭП электронных документов, определенных Регламентом.

Управление финансов и закупов – Управлениемфинансов и муниципальных закупок города Димитровграда Ульяновской области

Участник (и) - Организатор и (или) Сторона (при участии в ЮЗЭД).

Юридически значимый электронный документооборот (далее - ЮЗЭД) - документооборот на базе Системы, в котором стороны совершают действия по принятию к исполнению документов в электронной форме, удостоверенных ЭП, и при этом несут ответственность за совершение либо несовершение этих действий.

2. Предмет соглашения

2.1. Настоящее Соглашение регулирует обмен электронными документами (далее - ЭД) в рамках ЮЗЭД, подписанными электронной подписью (далее - ЭП), в Системе между Управлением финансов и закупок и участником, а также устанавливает обязательства Сторон по обеспечению информационной безопасности.

2.2. Областью применения ЭП является исключительно электронный документооборот между Управлением финансов и закупок и Стороной с использованием Системы.

2.3. С целью обеспечения авторства и целостности электронных документов при информационном взаимодействии Стороны используют сертифицированные СКЗИ.

2.4. Стороны признают, что СКЗИ, которые используются при обмене юридически значимыми электронными документами в Системах и реализуют функции создания ЭП, достаточны для подтверждения следующего:

1) электронный документ сформирован уполномоченным сотрудником одной из Сторон, наложившим ЭП (подтверждение авторства электронного документа);

2) электронный документ не претерпел изменений после формирования на момент проверки ЭП (подтверждение целостности и подлинности электронного документа).

2.5. Стороны признают, что ЭП в ЭД равнозначна собственноручной подписи Клиента, наделенного правом подписи финансовых документов, заверенной оттиском печати, в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа проверки электронной подписи, относящийся к этой электронной подписи, 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 не нарушает область применения, указанную в сертификате ключа подписи.

3. Общие принципы обмена ЭД

3.1. Участники самостоятельно выбирают юридическое лицо, оказывающее услуги Удостоверяющего центра.

3.2. Стороны несут ответственность за обеспечение конфиденциальности собственных ключей ЭП в соответствии с действующим законодательством.

3.3. Стороны принимают на себя обязательства:

- использовать для формирования и проверки ЭП в ЭПД сертифицированные средства криптографической защиты;
- принимать в обработку ЭД с подтвержденной подлинностью ЭП, без подтверждения на бумажном носителе;
- не принимать в обработку ЭД без ЭП или имеющий отрицательный результат проверки ЭП;
- немедленно прекратить прием и передачу ЭД в случае получения информации о компрометации ключа ЭП;
- самостоятельно отслеживать сроки действия сертификатов ключей ЭП и своевременно производить их замену и отзыв;
- в случае компрометации ключей ЭП сообщить об этом в Управление финансов и закупок для приостановки их действия в Системе.

4. Права и обязанности Сторон

4.1. Управление финансов и закупок обязано:

- обеспечивать бесперебойное функционирование своей части аппаратно-программных средств, необходимых для формирования ЭД Клиента;
- вести актуальный реестр Системы;

- прекратить использование сертификатов уполномоченных сотрудников участников в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о факте компрометации ключа.

- принять и обработать электронный документ с действительной ЭП в соответствии с Регламентом;

4.2. Клиент обязан:

- в целях обеспечения безопасности обработки и передачи юридически значимых электронных документов соблюдать требования эксплуатационной документации на используемые СКЗИ, не допускать появления на рабочих местах Систем компьютерных вирусов, прекращать использование скомпрометированного ключа ЭП и немедленно информировать Управление финансов и закупок о факте компрометации ключа;

- использовать для формирования ЭД исключительно программное обеспечение, рекомендованное или предоставленное Управлением финансов и закупок;

- хранить материальные носители, содержащие ключи уполномоченных сотрудников, в месте, исключающем доступ неуполномоченных лиц и (или) возможность повреждения материальных носителей;

- немедленно известить Управление финансов и закупок о приостановлении исполнения своих обязанностей в случае невозможности исполнения обязательств по настоящему Соглашению;

- руководствоваться порядком разрешения конфликтных ситуаций, утвержденным Управлением финансов и закупок, при возникновении споров, связанных с принятием или непринятием, исполнением или неисполнением электронных документов, подписанных ЭП;

- заменить сертификат в порядке, предусмотренном для его оформления правилами УЦ, в следующих случаях: смены уполномоченных сотрудников, обладающих правом подписи электронных документов, изменения данных, идентифицирующих уполномоченного сотрудника, смены ключей, в иных случаях, прекращающих действие сертификата;

- немедленно уведомить Управление финансов и закупок любым доступным способом о компрометации ключа, об изменении состава уполномоченных сотрудников Стороны, обладающих правом использования ключей, об ошибках в работе Системы, возникающих при работе с ЭП (подписание ЭП, проверка ЭП и др.), об ошибках, возникающих в связи с попытками нарушения информационной безопасности.

4.3. Управление финансов и закупок имеет право:

- рекомендовать Клиенту оптимальные условия подключения к АЦК;

- отключить Клиента от Системы при нарушениях рекомендаций по информационной безопасности при использовании ключей ЭП.

- приостановить прием ЭД в случаях нарушения или ненадлежащего выполнения Клиентом условий настоящего Соглашения;

- запрашивать у Клиента при необходимости копии ЭД на бумажном носителе;

- соблюдать требования законодательства при использовании ключей ЭП;

- инициировать разрешение спора в отношении ЭД.

4.4. Клиент имеет право:

- обращаться в Управление финансов и закупок с запросами по проблемам обмена ЭПД;
- обращаться в Управление финансов и закупок с запросами по уточнению стадий обработки отправленных ЭД с ЭП;
- инициировать разрешение спора в отношении ЭД.

5. Порядок подключения к ЮЗЭД

5.1. Сторона в течение пяти рабочих дней после подписания настоящего Соглашения производит настройкуклиентской части Систем (при необходимости выполнения настроек) на рабочих местах уполномоченных сотрудников.

5.2. Управление финансов и закупок на основании представленного Стороной заявления на внесение в реестр Системы сертификатов уполномоченных сотрудников в течение двух рабочих дней вводит в действие сертификаты уполномоченных сотрудников Стороны.

6. Ответственность Сторон

6.1. Клиент несет ответственность за достоверность реквизитов и содержание каждого ЭД, подписанного ЭП Клиента.

6.2. Управление финансов и закупок несет ответственность:

- за функционирование Системы;
- за своевременное принятие в обработку ЭД Клиента, прошедших проверку ЭП;
- за непринятие мер в случае выявления факта неправомерного использования ЭП Клиента.

6.3. Ответственность за ущерб, возникший вследствие компрометации ключей ЭП, несет Сторона, допустившая нарушение.

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

6.5. Управление финансов и закупок не несет ответственности в случае невозможности формирования ЭД Клиентом, если это вызвано неисправностями используемых Клиентом программно-аппаратных средств и каналов связи, предоставленных третьими лицами.

6.6. 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 невозможно предвидеть и предотвратить разумными мерами.

7. Срок действия и порядок прекращения действия Соглашения

7.1. Настоящее Соглашение вступает в силу со дня его подписания и действует бессрочно.

7.2. Управление финансов и закупок вправе расторгнуть настоящее Соглашение в одностороннем порядке в случае нарушения Клиентом требований к форматам ЭД, требований информационной безопасности, предусмотренных действующим законодательством и условиями настоящего Соглашения, если данное нарушение повлекло ущерб для Управление финансов и закупок или в случае неоднократного нарушения указанных требований и условий Клиентом независимо от последствий.

7.3. Клиент вправе расторгнуть настоящее Соглашение в одностороннем порядке после направления в Управление финансов и закупок письменного уведомления не позднее, чем за 30 календарных дней до даты расторжения Соглашения.

7.4. Расторжение настоящего Соглашения не влияет на обязательства Сторон по исполнению ЭД, принятых до даты расторжения Соглашения.

8. Прочие условия

Во всем остальном, что не урегулировано настоящим Соглашением, Стороны руководствуются действующим законодательством.

9. Адреса и реквизиты Сторон

Организатор	**Сторона**
Управление финансов и муниципальных закупок города Димитровграда Ульяновской области Юридический и почтовый адрес: Россия, 433508, г. Димитровград, ул. Хмельницкого, д. 93. ИНН 7302032650, КПП 730201001	_____ _____ _____ Юридический адрес: _____ _____ _____ Почтовый адрес: _____ _____ _____ ИНН _____ КПП _____
_____ _____ (должность) _____ _____ (подпись) (ФИО)	_____ _____ (должность) _____ (подпись) (ФИО)
М.П.	М.П.

Приложение N 2
к приказу
Управления финансов и
муниципальных закупок
города Димитровграда
Ульяновской области
от 03 марта 2020 г. N10-ОД

РЕГЛАМЕНТ
Применения электронной подписи участниками юридически значимого электронного документооборота в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области

1. Общие положения

1.1. Регламент применения электронной подписи участниками юридически значимого электронного документооборота в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (далее -Система) определяет порядок и технические аспекты использования юридически значимого электронного документооборота в Системе, статусы электронных документов, на которых происходит наложение ЭП в электронном документе на определенном статусе.

1.2. Такие термины и понятия, как «аккредитованный удостоверяющий центр» (далее - УЦ), «квалифицированный сертификат ключа проверки электронной подписи» (далее - сертификат), «ключ электронной подписи» (далее - ключ), «усиленная квалифицированная электронная подпись» (далее - ЭП) и «электронный документ», используемые в настоящем Регламенте, применяются в том же значении, что и в Федеральном законе от 06.04.2011 N 63-ФЗ "Об электронной подписи".

Иные термины и понятия, используемые в настоящем Регламенте:

Организатор –Управление финансов и муниципальных закупок, являющееся стороной ЮЗЭД (в лице уполномоченных сотрудников) на базе Системы, а также организатором ЮЗЭД в Системе, осуществляющим функции по хранению на своем оборудовании базы данных и конфигурации серверной части Систем, по настройке Систем на серверных станциях.

Отозванный сертификат - сертификат, который отозван из обращения.

Правила подписания – настроечныйпараметр Системы, позволяющий установить права на подписание электронных документов ЭП для определенных ролей на определенных статусах.

Роль – совокупностьправ уполномоченных сотрудников при работе в Системе, с использованием которых уполномоченные сотрудники подписывают

электронные документы ЭП.

Средства криптографической защиты информации (далее - СКЗИ) - аппаратно-программный комплекс, выполняющий функцию по созданию ЭП, а также обеспечивающий защиту информации по утвержденным стандартам и сертифицированный в соответствии с законодательством Российской Федерации.

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

Сторона – юридическое лицо (участник ЮЗЭД в лице уполномоченных сотрудников), заключившее соглашение об обмене электронными документами с Организатором.

Уполномоченный сотрудник – сотрудникучастника, наделенный полномочиями по подписанию ЭП электронных документов, определенных Регламентом.

Участник(-и) - Организатор и (или) Сторона (при участии в ЮЗЭД).

Юридически значимый электронный документооборот (далее - ЮЗЭД) - документооборот на базе Системы, в котором участники совершают действия по принятию к исполнению документов в электронной форме, удостоверенных ЭП, и при этом несут ответственность за совершение либо несовершение этих действий.

2. Средства применения ЭП

2.1. При работе с ЮЗЭД принимаются и признаются сертификаты, изданные УЦ.

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

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

2.3. В качестве средства ЭП используются СКЗИ, сертифицированные в соответствии с законодательством, а также совместимые с Системой (согласно требованиям Системы) и обеспечивающие:

- реализацию функций создания ЭП в электронном документе с использованием ключа;

- подтверждение подлинности ЭП в электронном документе с использованием сертификата.

2.4. ЭП хранится отдельно от электронных документов. Формат ЭП определяется рекомендациями RFC 3852 "CryptographicMessageSyntax (CMS)", с учетом использования криптографических алгоритмов ГОСТ 28147-89, ГОСТ Р

34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94, в соответствии с RFC 4490 "Usingthe GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 AlgorithmswithCryptographicMessageSyntax (CMS)".

3. Программное обеспечение, в котором происходит функционирование ЮЗЭД

3.1. Функционирование ЮЗЭД происходит на базе Системы.

3.2. Организатор оставляет за собой право обновлять версию Системы с дальнейшей эксплуатацией ЮЗЭД на обновленной версии без предварительных уведомлений Стороны, если такие изменения не повлекут существенных изменений Систем.

4. Перечень электронных документов, включенных в ЮЗЭД

4.1. Электронные документы, которые будут считаться юридически значимыми при условии подписания их ЭП (в случае выполнения всех установленных законодательством условий равнозначности ЭП собственноручной и с учетом требований заключенных участниками соглашений об обмене электронными документами) – «Формы бюджетной (бухгалтерской) отчетности учреждений».

4.2. Требования к составу подписываемых полей юридически значимых электронных документов определяет Организатор. Сторона имеет право быть ознакомленной с составом подписываемых полей юридически значимых электронных документов.

5. Контроль за правилами подписания электронных документов

5.1. Контроль за правилами подписания электронных документов осуществляется Организатором организационными мерами, а также техническими средствами Системы (использование правил проверки в Системе). Способ контроля за правилами подписания определяется Организатором.

5.2. Правила подписания электронных документов представлены в таблице.

п/п	Наименование документа	Статус	Роль уполномоченного сотрудника
.	Формы бюджетной (бухгалтерской) отчетности главных распорядителей бюджетных средств города Димитровграда	Проверен	ГРБС - Главный бухгалтер
		Закрыт для редактирования	Управление финансов и закупок - Исполнитель
		Подпи	ГРБС - Главный бухгалтер,

	Ульяновской области	сан	Руководитель, Руководитель финансово-экономической службы (при наличии)
		Согласован	Управление финансов и закупок – Главный бухгалтер,Руководитель финансово-экономической службы
.	Формы сводной бухгалтерской отчетности государственных (муниципальных) бюджетных и автономных учреждений	Проверен	ГРБС - Главный бухгалтер
		Закрыт для редактирования	Управление финансов и закупок - Исполнитель
		Подписан	ГРБС - Главный бухгалтер, Руководитель, Руководитель финансово-экономической службы (при наличии)
		Согласован	Управление финансов и закупок – Главный бухгалтер,Руководитель финансово-экономической службы
.	Формы бюджетной отчетности об исполнении консолидированного бюджета города Димитровграда	Проверен Закрыт для редактирования Согласован	Управление финансов и закупок – Исполнитель
		Подписан	Управление финансов и закупок – Главный бухгалтер,Руководитель финансово-экономической службы, Руководитель
.	Формы консолидированной бухгалтерской отчетности государственных (муниципальных)	Проверен Закрыт для редактирования	Управление финансов и закупок – Исполнитель

	бюджетных и автономных учреждений города Димитровграда	Согласован	
		Подписан	Управление финансов и закупок – Главный бухгалтер,Руководитель финансово-экономической службы, Руководитель

5.3. Уполномоченные сотрудники участников обязаны подписывать юридически значимые электронные документы своей электронной подписью строго в соответствии с правилами подписания. В противном случае электронные документы не считаются юридически значимыми.

Приложение N 3
к приказу
Управления финансов и
муниципальных закупок
города Димитровграда
Ульяновской области
от 03 марта 2020 г. N10-ОД

ИНСТРУКЦИЯ
О порядке работы со средствами криптографической защиты информации в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области

1. Общие положения

1.1. Такие термины и понятия, как «аккредитованный удостоверяющий центр» (далее - УЦ), «ключ электронной подписи» (далее - ключ), «усиленная квалифицированная электронная подпись» (далее - ЭП) и «электронный документ», используемые в настоящей Инструкции, применяются в том же значении, что и в Федеральном законе от 06.04.2011 N 63-ФЗ «Об электронной подписи».

1.2. Иные термины и понятия, используемые в настоящей Инструкции:

«СКИФ-БП» - автоматизированная система для принятия, формирования и свода бюджетной (бухгалтерской) отчетности, направляемые главными распорядителями средств бюджета города Димитровграда Ульяновской области (далее - Система).

Компрометация ключа – утратадоверия к тому, что ключ используется исключительно уполномоченным сотрудником и исключительно по назначению.

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

Организатор –Управление финансов и муниципальных закупок города Димитровграда Ульяновской области, являющееся стороной ЮЗЭД (в лице уполномоченных сотрудников) на базе Системы, а также организатором ЮЗЭД в Системе, осуществляющим функции по хранению на своем оборудовании базы данных и конфигурации серверной части Системы, по настройке Системы на серверных станциях.

Средства криптографической защиты информации (далее - СКЗИ) - аппаратно-программный комплекс, выполняющий функцию по созданию ЭП, а также обеспечивающий защиту информации по утвержденным стандартам и сертифицированный в соответствии с законодательством.

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

Уполномоченный сотрудник – сотрудникучастника, наделенный полномочиями по подписанию ЭП электронных документов, определенных утвержденным Организатором регламентом, определяющим статусы электронных документов, на которых происходит наложение ЭП в электронном документе на определенном статусе.

Участник – юридическоелицо, принимающее участие в ЮЗЭД.

Юридически значимый электронный документооборот (далее - ЮЗЭД) - документооборот на базе Системы, в котором участники совершают действия по принятию к исполнению документов в электронной форме, удостоверенных ЭП, и при этом несут ответственность за совершение, либо несовершение этих действий.

2. Работа с СКЗИ

2.1. Для работы с СКЗИ в ЮЗЭД допускаются только уполномоченные сотрудники участников. Уполномоченные сотрудники участников несут персональную ответственность за сохранность СКЗИ (в том числе хранение в тайне ключей ЭП).

Уполномоченный сотрудник участника несет ответственность за отсутствие на компьютере, на котором осуществляется эксплуатация ЮЗЭД, посторонних программ (вирусов и т.д.), способствующих нарушению функционирования ЮЗЭД.

2.2. При обнаружении на компьютере, на котором осуществляется эксплуатация ЮЗЭД, посторонних программ (вирусов и т.д.), эксплуатация ЮЗЭД на этом компьютере должна прекратиться с дальнейшей организацией мероприятий по анализу и ликвидации посторонних программ и возможных последствий.

2.3. Запрещается:

- разглашать содержимое материальных носителей, содержащих ключи ЭП, или передавать сами материальные носители лицам, к ним не допущенным, выводить данные, содержащиеся на материальном носителе, на дисплей и принтер;

- вставлять материальный носитель, содержащий ключи ЭП, в дисковод или USB-считыватель компьютера уполномоченного сотрудника и других лиц при проведении работ, не связанных с эксплуатацией ЮЗЭД;

- записывать на материальный носитель, содержащий ключи ЭП, постороннюю информацию;

- вносить какие-либо изменения в программное обеспечение СКЗИ;

- использовать бывшие в работе материальные носители (правило не

распространяется на носитель типа RuToken и eToken).

Уполномоченный сотрудник несет ответственность за проведение в полном объеме организационных и технических мероприятий, обеспечивающих соблюдение указанных выше правил.

3. Действия в случае компрометации ключей

3.1. К событиям, связанным с компрометацией ключей, относятся следующие:

- утрата материальных носителей, содержащих ключи ЭП;

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

- разглашение содержимого материальных носителей, содержащих ключи ЭП;

- несанкционированное копирование содержимого материальных носителей, содержащих ключи ЭП;

- увольнение сотрудников, имевших доступ к материальным носителям, содержащим ключи ЭП;

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

- возникновение подозрений на утечку содержимого материальных носителей, содержащих ключи ЭП, или ее искажение в Системе;

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

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

- любые другие виды разглашения содержимого материальных носителей, содержащих ключи ЭП, в результате которых ключи могут стать доступными посторонним лицам и (или) процессам.

3.2. Уполномоченный сотрудник участника самостоятельно определяет факт компрометации ключа и оценивает значение этого события. Мероприятия по розыску и локализации последствий компрометации ключа организует и осуществляет Организатор с участием уполномоченного сотрудника участника (владельца скомпрометированного ключа).

В случае установления факта компрометации ключа уполномоченный сотрудник участника обязан незамедлительно прекратить эксплуатацию ЮЗЭД в Системах и уведомить Организатора, а также доверенный УЦ по телекоммуникационным каналам связи.

В течение 30 (тридцати) рабочих минут после поступления сообщения о компрометации ключа Организатор обеспечивает прекращение использования в ЮЗЭД соответствующего сертификата уполномоченного сотрудника.

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

Приложение N 4
к приказу
Управления финансов и
муниципальных закупок
города Димитровграда
Ульяновской области
от 03 марта 2020 г. N10-ОД

форма

ЗАЯВЛЕНИЕ
на внесение в реестр автоматизированной системы «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области сертификатовуполномоченных сотрудников

«___»_____ 20___г.

_____
_____ (далее - Сторона),
(полное наименование организации в соответствии с учредительным документом)

в соответствии с условиями Соглашения от _____ № _____ об обмене электронными документами, заключённого между Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (далее - Организатор) и Стороной, просит Организатора для осуществления юридически значимого электронного документооборота внести в реестр системы «СКИФ-БП» сертификат (ы) уполномоченного (ых) сотрудника (ов) Стороны со следующими регистрационными данными:

№ п/п	Должность	ФИО	Серийный номер сертификата электронной подписи *	Роль уполномоченного сотрудника **	Подпись уполномоченного сотрудника
1.					
2.					

Настоящим Стороназаявляет, что любые действия, которые будут совершенывладельцем(-ми) сертификата(-ов) Стороны на основании указанного(-ых)сертификата(-ов) являются действиями, совершаемыми владельцем(-ами)сертификата(-ов) от имени Стороны, по указанию Стороны и связаны с участиемв обмене юридически значимыми электронными документами в системе «СКИФ-БП».

Электронная(-ые) копия(-и) сертификата(-ов) уполномоченного(-ых)сотрудника(-ов) представлена Организатору

_____
(указывается способ предоставления)

_____ _____ _____
(должность руководителя Стороны) (подпись)(ФИО)
М.П.

_____
* При получении сертификатов электронных подписей через доверенное лицо Организатора поле может не заполняться.
** Указывается в соответствии с Управления финансов и муниципальных закупок города Димитровграда Ульяновской области Регламентом применения электронной подписи участниками юридически значимого электронного документооборота в

автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области

Приложение N 5
к приказу
Управления финансов и
муниципальных закупок
города Димитровграда
Ульяновской области
от 03 марта 2020 г. N10-ОД

ПОРЯДОК
Разбора конфликтных ситуаций при осуществлении юридически значимого электронного документооборота в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области

1. Общие положения

1.1. Настоящий Порядок определяет правила разбора конфликтных ситуаций, возникающих между Управлением финансов и муниципальных закупок города Димитровграда Ульяновской областии участниками юридически значимого электронного документооборота в ходе подписания электронных документов электронной подписью при осуществлении юридически значимого электронного документооборота в автоматизированной системе«СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (далее - Системы).

1.2. Такие термины и понятия, как «аккредитованный удостоверяющий центр» (далее - УЦ), «квалифицированный сертификат ключа проверки электронной подписи» (далее - сертификат), «ключ электронной подписи» (далее - ключ), «усиленная квалифицированная электронная подпись» (далее - ЭП) и «электронный документ», используемые в настоящем Порядке, применяются в том же значении, что и в Федеральном законе от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Иные термины и понятия, используемые в настоящем Порядке.

Альбом электронных документов – документ, предназначенный для детализированного описания реквизитного состава электронных документов, подписываемых ЭП при осуществлении ЮЗЭД в Системе.

Аттестат соответствия – документустановленной формы, подтверждающий соответствие используемых программных и аппаратных средств требованиям законодательства Российской Федерации в области защиты информации.

Инициатор – участник, инициирующий конфликтную ситуацию, связанную с необходимостью проверки юридической значимости электронного документа.

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

Область применения сертификата – параметрсертификата, определяющий перечень электронных документов, возможных для подписания при помощи данного сертификата.

Организатор - Управление финансов и муниципальных закупок города Димитровграда Ульяновской области, являющееся стороной ЮЗЭД (в лице уполномоченных сотрудников) на базе Системы, а также организатором ЮЗЭД в Системе, осуществляющим функции по хранению на своем оборудовании базы данных и конфигурации серверной части Системы, по настройке Системы на серверных станциях.

Ответчик – участник, привлекаемый в качестве предположительного нарушителя прав инициатора.

Отозванный сертификат – сертификат, который отозван из обращения.

Регламент применения электронной подписи участниками юридически значимого электронного документооборота (далее - Регламент) - утвержденный Организатором документ, определяющий статусы электронных документов, на которых происходит наложение ЭП в электронном документе на определенном статусе.

Средства криптографической защиты информации (далее - СКЗИ) - аппаратно-программный комплекс, выполняющий функцию по созданию ЭП, а также обеспечивающий защиту информации по утвержденным стандартам и сертифицированный в соответствии с законодательством.

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

Сторона – юридическоелицо (участник ЮЗЭД в лице уполномоченных сотрудников), заключившее соглашение об обмене электронными документами с Организатором.

Уполномоченный сотрудник – сотрудник участника, наделенный полномочиями по подписанию ЭП электронных документов, определенных Регламентом.

Участник(-и) - Организатор и (или) Сторона (при участии в ЮЗЭД).

Целостность программного обеспечения - отсутствие изменений в коде программного обеспечения при его эксплуатации.

Экспертная комиссия - комиссия, разрешающая конфликтные ситуации, связанные с использованием ЮЗЭД.

Юридически значимый электронный документооборот (далее - ЮЗЭД) - документооборот на базе Систем, в котором участники совершают действия по принятию к исполнению документов в электронной форме, удостоверенных ЭП, и при этом несут ответственность за совершение либо несовершение этих действий.

2. Порядок разбора конфликтных ситуаций

2.1. Под конфликтной ситуацией понимается ситуация, которая может быть вызвана следующими разногласиями между участниками:

– оспаривание факта отправления и (или) получения электронного документа;

– оспаривание времени отправления и (или) получения электронного документа;

– оспаривание содержания отправленного (полученного) электронного документа;

– оспаривание идентичности экземпляров электронного документа и (или)

подлинника и копии электронного документа на бумажном носителе;

– оспаривание целостности электронного документа;

– оспаривание идентификации лица, подписавшего электронный документ ЭП;

– оспаривание полномочий лица, подписавшего электронный документ ЭП;

– оспаривание действительности и правомочности использования сертификата, использованного для подписания электронного документа;

– иные случаи возникновения конфликтных ситуаций в ходе обмена электронными документами.

2.2. Разрешая конфликтные ситуации, участники исходят из следующего.

В соответствии с законодательством документ в электронном виде, подписанный ЭП в Системе, является документом, имеющим юридическую силу, аналогичным бумажному документу, подписанному подписью и заверенному печатью.

Электронный документ порождает обязательства участника перед другим участником, если документ оформлен надлежащим образом, подписан ЭП в Системе и доставлен другому участнику. При этом ЭП используется в соответствии со сведениями, указанными в сертификате, а сертификат отправителя является действующим или являлся действующим на момент подписания документа.

Математические свойства алгоритма ЭП должны соответствовать стандартам, существующим в Российской Федерации. Участник признает, что разбор конфликтной ситуации в отношении авторства, целостности и подлинности электронного документа, заключается в доказательстве подписания конкретного электронного документа на конкретном ключе ЭП.

Электронный документ может иметь неограниченное количество экземпляров. Для создания дополнительного экземпляра существующего электронного документа копирование этого электронного документа должно быть выполнено со всеми ЭП. Все экземпляры электронного документа являются подлинниками данного электронного документа.

Разрешение конфликтных ситуаций осуществляется несколькими способами (в зависимости от уровня эскалации конфликтной ситуации), а именно:

- в рабочем порядке (без создания Экспертной комиссии);

- с созданием Экспертной комиссии и участием разработчика программного обеспечения Системы;

- в претензионном порядке;

- в судебном порядке.

2.3. Разрешение конфликтных ситуаций в рабочем порядке

В случае возникновения обстоятельств, свидетельствующих, по мнению одного из участников, о возникновении конфликтной ситуации, данный участник (инициатор) незамедлительно извещает других заинтересованных участников любым доступным способом о возможном возникновении и (или) наличии конфликтной ситуации, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также о ее предполагаемых причинах.

Участники, которым была направлена информация (извещение в произвольной форме) о конфликтной ситуации и которые должны участвовать в ее разрешении, обязаны проверить наличие указанных в извещении обстоятельств

и по необходимости принять меры по разрешению конфликтной ситуации со своей стороны.

Ответчик извещает доступным способом инициатора о результатах проверки и при необходимости - о мерах, принятых для разрешения конфликтной ситуации, в течение одного рабочего дня с момента получения уведомления от инициатора.

Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если инициатор удовлетворен информацией, содержащейся в извещениях ответчика, не имеет к нему претензий и информация представлена в надлежащий срок.

Разрешение конфликтных ситуаций в рабочем порядке допускаются в тех случаях, когда действия, являющиеся причиной конфликта, не наносят существенный ущерб участникам.

2.4. Разрешение конфликтных ситуаций с созданием Экспертной комиссии

2.4.1. Экспертная комиссия создается с целью разрешения конфликтных ситуаций, возникающих в ходе обмена электронными документами в Системах в тех случаях, когда разрешение конфликтных ситуаций в рабочем порядке не представляется возможным по следующим причинам:

- действия, являющиеся конфликтными, наносят существенный ущерб участникам;

- действия, являющиеся конфликтными, не наносят существенный ущерб участникам, но инициатор не удовлетворен результатами разрешения конфликтной ситуации в рабочем порядке.

2.4.2. Формирование Экспертной комиссии

В случае если конфликтная ситуация не была разрешена в рабочем порядке, инициатор не позднее трех рабочих дней после возникновения конфликтной ситуации направляет ответчику заявление о разногласиях[1] (далее - Заявление) и предложение о создании Экспертной комиссии (далее - Предложение).

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

Заявление о разногласиях в обязательном порядке должно содержать следующую информацию:

- уникальный идентификатор электронного документа[2];

- название класса электронного документа и его номер в Системах;

- дата Заявления;

- номер Заявления (если ведется журнал заявлений о разногласиях);

- обстоятельства, на которых основаны заявленные требования и сведения о подтверждающих их доказательствах;

- дата и время подписания (по системному журналу);

- нормы законодательных и иных нормативных правовых актов, положения соглашения между участниками, на основании которых выставляется требование.

К Заявлению должны быть приложены следующие документы:

---

[1]До подачи Заявления инициатору необходимо убедиться в целостности установленного на его технических средствах программного обеспечения, в том числе средств ЭП, а также в том, что не было произведено несанкционированных действий относительно программного обеспечения, и в том, что на его технических средствах не установлено вредоносного или шпионского программного обеспечения.

[2]Определяется через интерфейс Системы

- файл, содержащий электронный документ, а также ЭП этого электронного документа [3];

- файл, содержащий вложение электронного документа, а также ЭП этого вложения электронного документа[4];

- файлы, содержащие сертификаты ключей ЭП, которыми был подписан электронный документ и вложения.

Предложение должно содержать следующую информацию:

- предполагаемая дата (не позднее трех рабочих дней со дня отправления Заявления), время и место сбора Экспертной комиссии;

- список предлагаемых для участия в работе Экспертной комиссии представителей инициатора, с указанием ФИО, должностей, контактной информации (телефон, электронная почта, факс).

Заявление и Предложение составляются в произвольной форме на бумажном носителе, подписываются должностными лицами инициатора, уполномоченными участвовать в разрешении конфликтной ситуации, и передаются ответчику способом, подтверждающим вручение корреспонденции.

2.4.3. Предполагаемые место и дата сбора Экспертной комиссии

Не позднее чем на третий рабочий день после получения Заявления и Предложения участниками, участвующими в разрешении конфликтной ситуации, должна быть сформирована Экспертная комиссия.

Состав Экспертной комиссии, время и место ее работы утверждается руководителями (иными уполномоченными лицами) участвующих в разрешении конфликтной ситуации участников.

Срок работы Экспертной комиссии - пять рабочих дней. В исключительных случаях срок работы Экспертной комиссии может быть продлен, но не более чем на тридцать рабочих дней.

Если участники не договорятся об ином, то в состав Экспертной комиссии входит равное количество уполномоченных лиц участников, участвующих в разрешении конфликтной ситуации.

В состав Экспертной комиссии могут включаться специалисты служб обеспечения информационной безопасности участников, уполномоченные сотрудники участников, представители юридических служб участников, а также представители органов, осуществляющих государственное регулирование и контроль в соответствующих сферах деятельности и уполномоченные сотрудники УЦ (по согласованию).

По инициативе любого из участников, участвующих в разрешении конфликтной ситуации, к работе Экспертной комиссии могут привлекаться независимые эксперты.

Лица, входящие в состав Экспертной комиссии, должны обладать знаниями и опытом работы с электронными документами, в области организации и обеспечения информационной безопасности при обмене электронными документами, иметь соответствующий допуск к необходимым для проведения работы Экспертной комиссии документам и программно-техническим средствам.

Председатель Экспертной комиссии назначается по согласованию участников. Если согласование не достигнуто, то председатель Экспертной комиссии

---

[3]Выгружается из Системы

[4]Выгружается из Системы

назначается простым большинством голосов по результатам открытого голосования членов Экспертной комиссии.

2.4.4. Права Экспертной комиссии

Экспертная комиссия имеет право:

− получать доступ к необходимым для ее работы документам участников, в том числе к архивам электронных документов;

− знакомиться с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета электронных документов участников;

− знакомиться с условиями и порядком эксплуатации программных и технических средств обмена электронными документами участников;

− знакомиться с условиями и порядком изготовления, использования и хранения участниками ключей, иной конфиденциальной информации, а также материальных носителей, необходимых для работы средств обмена электронными документами;

− получать объяснения от должностных лиц участников, обеспечивающих обмен электронными документами;

− получать от участников любую иную информацию, относящуюся, по ее мнению, к разрешаемой конфликтной ситуации.

Для проведения необходимых проверок и документирования данных Экспертной комиссией могут применяться специальные программные и технические средства.

2.4.5. Порядок работы Экспертной комиссии

Ответчик обязан в период работы Экспертной комиссии представить инициатору и Экспертной комиссии документально обоснованные объяснения и (или) доказательства по каждому вопросу, изложенному в Заявлении.

Любая сторона в ходе работы Экспертной комиссии может вынести (в письменной форме) на рассмотрение Экспертной комиссии ходатайство об изменении или дополнении своих требований или возражений.

Экспертная комиссия может затребовать от сторон представление документов, вещественных или иных доказательств.

Рассмотрение спора производится на основании всех представленных документов и доказательств.

В том случае, если обстоятельства требуют подтверждения факта подлинности ЭП в электронном документе, Экспертная комиссия проводит экспертизу по подтверждению подлинности ЭП. Проведение экспертизы возлагается на уполномоченных сотрудников УЦ, входящих в состав Экспертной комиссии.

2.4.6. Оформление результатов работы Экспертной комиссии

Все действия, предпринимаемые Экспертной комиссией для выяснения фактических обстоятельств конфликтной ситуации, а также сделанные выводы заносятся в протокол работы Экспертной комиссии. По итогам работы Экспертной комиссии составляется акт.

2.4.6.1. Протокол работы Экспертной комиссии

Протокол работы Экспертной комиссии должен содержать следующую информацию:

- дату и место составления протокола;

- состав Экспертной комиссии с указанием фамилий, имен, отчеств, мест работы, занимаемых должностей, исполняемых при обмене электронными документами функциональных ролей, контактной информации и квалификации членов Экспертной комиссии;

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

- установленные Экспертной комиссией фактические обстоятельства;

- мероприятия, проводимые Экспертной комиссией для установления наличия, причин возникновения и последствий возникшей конфликтной ситуации, с указанием даты, времени и места их проведения;

- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;

- подписи всех членов Экспертной комиссии.

Выводы, к которым пришла Экспертная комиссия, должны основываться на положениях, дающих возможность проверить обоснованность и достоверность сделанных выводов на базе организационных, технических и практических данных.

Протокол должен быть составлен в форме документа на бумажном носителе в двух экземплярах, по одному для инициатора и ответчика. По обращению любого из членов Экспертной комиссии может быть выдана заверенная копия протокола.

2.4.6.2. Акт по итогам работы Экспертной комиссии

Акт, составленный по итогам работы Экспертной комиссии, должен содержать следующую информацию:

- дату и место составления акта;

- дату и время начала и окончания работы Экспертной комиссии;

- состав Экспертной комиссии;

- краткое изложение выводов Экспертной комиссии;

- принятое решение Экспертной комиссии;

- перечень мероприятий, проведенных Экспертной комиссией;

- указание на особое мнение члена Экспертной комиссии (при наличии);

- подписи всех членов Экспертной комиссии.

При наличии указания на особое мнение члена Экспертной комиссии к акту прилагается документ, составленный в произвольной форме и отражающий особое мнение члена Экспертной комиссии, не согласного с выводами Экспертной комиссии. Этот документ должен быть подписан членом Экспертной комиссии, чье мнение он отражает.

Акт должен быть составлен в форме документа на бумажном носителе в двух экземплярах, по одному для инициатора и ответчика. По обращению любого из членов Экспертной комиссии может быть выдана заверенная копия акта.

2.4.7. Разрешение конфликтной ситуации по итогам работы Экспертной комиссии

Акт Экспертной комиссии является основанием для принятия участниками, участвующими в разрешении конфликтной ситуации, решения по урегулированию конфликтной ситуации.

В срок не более трех рабочих дней со дня окончания работы Экспертной комиссии участники, участвующие в разрешении конфликтной ситуации, на

основании выводов Экспертной комиссии принимают меры по разрешению конфликтной ситуации.

Конфликтная ситуация признается разрешенной по итогам работы Экспертной комиссии, если участники, участвующие в разрешении конфликтной ситуации, удовлетворены выводами, полученными Экспертной комиссией, и не имеют претензий в связи с разрешаемой конфликтной ситуацией.

В случае если конфликтная ситуация признается разрешенной, участники, участвующие в разрешении конфликтной ситуации, в срок не позднее пяти рабочих дней со дня окончания работы Экспертной комиссии оформляют решение об урегулировании конфликтной ситуации.

Решение составляется участниками, участвующими в разрешении конфликтной ситуации, в произвольной форме в виде документа на бумажном носителе и выдается по одному экземпляру каждому участнику. Решение подписывается уполномоченными в разрешении конфликтной ситуации лицами участников и утверждается руководителями (иными уполномоченными лицами) участников.

2.5. Претензионный порядок разрешения конфликтных ситуаций

В случаях когда конфликтная ситуация не разрешена по итогам работы Экспертной комиссии, в случае прямого или косвенного отказа одного из участников от участия в работе Экспертной комиссии или если одним из участников, участвующим в разрешении конфликтной ситуации, создавались препятствия работе Экспертной комиссии, а также в случае если один из участников считает, что его права в связи с обменом электронными документами были нарушены, он обязан направить участнику, который, по его мнению, нарушил его права, претензию.

Претензия должна содержать:

- изложение требований инициатора;

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

- сведения о работе Экспертной комиссии и, в случае если Экспертная комиссия работала в связи с разрешаемой конфликтной ситуацией, копии материалов работы Экспертной комиссии независимо от выводов Экспертной комиссии/согласия или несогласия с этими выводами инициатора;

- иные документы, имеющие значение, по мнению инициатора;

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

Претензия составляется в форме документа на бумажном носителе в произвольной форме, подписывается руководителем (иным уполномоченным лицом) инициатора, заверяется печатью инициатора. Претензия и прилагаемые к ней документы направляются в адрес ответчика. Ответчик обязан 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 настоящим пунктом претензионного порядка и может рассматриваться в качестве отказа в удовлетворении требований претензии.

2.6. Разрешение конфликтных ситуаций в судебном порядке

В случае невозможности разрешения конфликтной ситуации в рабочем порядке, по итогам работы Экспертной комиссии и (или) в претензионном порядке участник вправе направить имеющиеся разногласия на рассмотрение суда в порядке, установленном законодательством Российской Федерации.

3. Процедуры проверки электронных документов

3.1. Проверка наличия электронных документов

Для проверки наличия электронного документа необходимо:

- получить электронный документ и ЭП для анализа (документ и ЭП могут быть получены из Систем в виде двух файлов: документ в виде файла в формате "txt", ЭП - в виде файла в формате "PKCS#7");

- проверить наличие данного электронного документа в Системе. Проверка осуществляется посредством поиска уникального идентификатора, указанного в Заявлении.

При этом могут быть сделаны следующие выводы:

- при отсутствии данного электронного документа в Системе, делается вывод об отсутствии причин конфликтной ситуации;

- при наличии электронного документа в Системе, необходимо продолжить разрешение конфликтной ситуации в соответствии с настоящим Порядком.

3.2. Подтверждение подлинности ЭП

Подтверждение подлинности ЭП в электронном документе - это положительный результат подтверждения сертифицированным средством ЭП принадлежности содержащейся в электронном документе ЭП ее владельцу и отсутствия искажения и подделки подписанного данной ЭП электронного документа.

Подтверждение подлинности ЭП выполняется путем проведения экспертизы. Экспертиза подлинности ЭП в электронном документе выполняется только УЦ.

При этом могут быть сделаны следующие выводы:

- при неподтверждении УЦ подлинности ЭП делается вывод об отсутствии причин конфликтной ситуации;

- при подтверждении УЦ подлинности ЭП, а также при наличии остальных подтверждающих фактов делается вывод о правомерности претензий инициатора, зафиксированных в Заявлении.

3.3. Проверка организационных аспектов

3.3.1. Соответствие положениям Регламента:

1) соответствие полномочий подписанта на подписание электронного документа ЭП в соответствии с Регламентом, а именно:

а) соответствие представленного документа описанию класса документов согласно документации к Системе;

б) возможность подписания ЭП электронных документов данного класса;

в) возможность подписания ЭП на заданном статусе жизненного цикла электронного документа;

г) присутствие документа данного класса в альбоме электронных документов, используемых при осуществлении ЮЗЭД в Системе;

2) время и дата подписания электронного документа (по времени системного

журнала);

3) соответствие личности должностного лица, подписавшего электронный документ, информации, указанной в сертификате.

При установлении факта соответствия между Регламентом и ЭП в электронном документе, времени и даты подписания электронного документа, указанных в системном журнале, времени и дате подписания электронного документа, указанным в Заявлении, а также при наличии остальных подтверждающих фактов делается вывод о правомерности претензий инициатора, зафиксированных в Заявлении.

При установлении факта несоответствия между Регламентом и ЭП в электронном документе, времени и даты подписания электронного документа, указанных в системном журнале, времени и дате подписания электронного документа, указанным в Заявлении делается вывод об отсутствии причин конфликтной ситуации.

3.3.2. Правомерность использования копий СКЗИ и копий Системы в соответствии с условиями лицензионных соглашений об их использовании

При установлении факта правомерности использования копий СКЗИ и копий Системы делается вывод о правомерности претензий инициатора, зафиксированных в Заявлении.

При установлении факта неправомерности использования копий СКЗИ и копий Системы делается вывод об отсутствии причин конфликтной ситуации.

3.3.3. Корректность использования СКЗИ и Системы в соответствии с документацией на используемые программные и аппаратные средства и аттестатами соответствия

При установлении факта корректного использования СКЗИ и Системы делается вывод о правомерности претензий инициатора, зафиксированных в Заявлении.

При установлении факта некорректного использования СКЗИ и Системы делается вывод об отсутствии причин конфликтной ситуации.

3.3.4. Правомерность подписания электронного документа уполномоченным сотрудником на основании Регламента и заявления участника на внесение в реестр Системы сертификатов уполномоченных сотрудников

При установлении факта правомерного подписания электронного документа уполномоченным сотрудником делается вывод о правомерности претензий инициатора, зафиксированных в Заявлении.

При установлении факта неправомерного подписания электронного документа уполномоченным сотрудником делается вывод об отсутствии причин конфликтной ситуации.

3.3.5. Доказательства корректности условий использования сертификатов в соответствии с областью применения сертификатов

При установлении факта использования сертификатов в соответствии с областью применения сертификатов делается вывод о правомерности претензий инициатора, зафиксированных в Заявлении.

При установлении факта использования сертификатов не в соответствии с областью применения сертификатов делается вывод об отсутствии причин конфликтной ситуации.

Список необходимых для разрешения конфликтной ситуации проверок

N п/п	Наименование проверки	Успешность проверки (да/нет)
1.	Проверка подлинности электронного документа	
	Присутствие документа в Системе	
2.	Подтверждение подлинности ЭП	
2.1.	Успешное выполнение проверки ЭП с использованием сертификатов, представленных инициатором и УЦ	
2.2.	Действительность сертификата, которым подписан конфликтный документ на момент подписания	
3.	Проверка организационных аспектов	
3.1.	Проверка на соответствие положениям Регламента	
3.1.1.	Соответствие представленного документа описанию класса	
3.1.2.	Возможность подписания ЭП документов данного класса	
3.1.3.	Соответствие личности должностного лица, подписавшего документ, информации, указанной в сертификате, представленном Экспертной комиссии	
3.1.4.	Присутствие документа данного класса в альбоме электронных документов	
3.2.	Прочие организационные аспекты	
3.2.1.	Подтверждение правомерности использования копий СКЗИ и Системе в соответствии с условиями лицензионных соглашений	
3.2.2.	Подтверждение корректности использования копий СКЗИ и Системе в соответствии с документацией на используемые программные и аппаратные средства и аттестатами соответствия	
3.2.3.	Подтверждение правомерности использования электронного документа данного класса в ЮЗЭД в соответствии со списком электронных документов, включенных в альбом электронных документов	
3.2.4.	Наличие доказательств того, что сертификат, которым подписан электронный документ, выдан УЦ	
3.2.5.	Доказательства корректности условий использования сертификатов в соответствии с областью применения сертификатов	

Приложение N 6
к приказу
Управления финансов и
муниципальных закупок
города Димитровграда
Ульяновской области
от 03 марта 2020 г. N10-ОД

ПОРЯДОК
Представления Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области электронных документов из автоматизированной системы «СКИФ-БП»Управления финансов и муниципальных закупок города Димитровграда Ульяновской области по обращениям заинтересованных лиц

1. Настоящий Порядок определяет формат и перечень электронных документов, представляемых Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области из автоматизированной системы«СКИФ-БП»Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (далее - Управление, Системы) по обращениям заинтересованных лиц.

2. Такие термины и понятия, как «квалифицированный сертификат ключа проверки электронной подписи» (далее - сертификат), «усиленная квалифицированная электронная подпись» (далее - ЭП) и «электронный документ», используемые в настоящем Порядке, применяются в том же значении, что и в Федеральном законе от 06.04.2011 N 63-ФЗ «Об электронной подписи».

В целях настоящего Порядка также:

под заинтересованным лицом понимаются обратившиеся в Управление граждане или юридические лица, ответы на запросы которых требуют представления электронных документов, содержащихся в Системе;

под уполномоченным сотрудником понимается сотрудник Управления, наделенный полномочиями по подписанию ЭП электронных документов, определенных утвержденным Управлением регламентом, определяющим статусы электронных документов, на которых происходит наложение ЭП в электронном документе на определенном статусе.

3. В случае представления на обращение заинтересованного лица ответа в электронной форме к ответу в качестве приложения прикрепляются выгруженные из Системы электронные документы в формате «txt», файлы ЭП в формате «PRCS#7», а также электронные документы в формате «xls» или «xlsx» с реквизитами ЭП и сертификата уполномоченного сотрудника, подписавшего документ ЭП.

4. В случае представления на обращение заинтересованного лица ответа в печатной форме к ответу прилагаются бумажные копии выгруженных из Системы электронных документов, изготовленные в установленном Управлением порядке организации архива электронных документов, содержащихся в Системе.

5. Электронные документы, представляемыеУправлением из Системы по обращениям заинтересованных лиц: «Бюджетная (бухгалтерская) отчетность ГРБС, учреждений».

Приложение N 7
к приказу
Управления финансов и
муниципальных закупок
города Димитровграда
Ульяновской области
от 03 марта 2020 г. N10-ОД

КАРТА РИСКОВ
юридически значимого электронного документооборота в автоматизированной системе «СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области

1. Общие положения

1.1. Карта рисков юридически значимого электронного документооборота в автоматизированной системе«СКИФ-БП» Управления финансов и муниципальных закупок города Димитровграда Ульяновской области (далее - Карта рисков, Система) предназначена для описания вероятности возникновения рисков при осуществлении ЮЗЭД в Системе, мероприятий по их снижению, а также описания возможной степени причиненного ими ущерба.

1.2. Такие термины и понятия, как «аккредитованный удостоверяющий центр» (далее - УЦ), «квалифицированный сертификат ключа проверки электронной подписи» (далее - сертификат), «ключ электронной подписи» (далее - ключ), «усиленная квалифицированная электронная подпись» (далее - ЭП) и «электронный документ», используемые в Карте рисков, применяются в том же значении, что и в Федеральном законеот 06.04.2011 N 63-ФЗ «Об электронной подписи».

Иные термины и понятия, используемые о Карте рисков:

Организатор - Управление финансов и муниципальных закупок города Димитровграда Ульяновской области, являющееся стороной ЮЗЭД (в лице уполномоченных сотрудников) на базе Системы, а также организатором ЮЗЭД в Системе, осуществляющим функции по хранению на своем оборудовании базы данных и конфигурации серверной части Системы, по настройке Системы на серверных станциях.

Средства криптографической защиты информации (далее – СКЗИ) – аппаратно-программный комплекс, выполняющий Функцию по созданию ЭП, а также обеспечивающий защиту информации по утвержденным стандартам и сертифицированный в соответствии с законодательством.

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

Сторона – юридическоелицо (участник ЮЗЭД в лице уполномоченных сотрудников), заключившее соглашение об обмене электронными документами с Организатором.

Уполномоченный сотрудник – сотрудникучастника, наделенный

полномочиями по подписанию ЭП электронных документов, определенных утвержденным Управлением финансов и муниципальных закупок города Димитровграда Ульяновской области регламентом, определяющим статусы электронных документов, на которых происходит наложение ЭП в электронном документе на определенном статусе.

Участник(-и) - Организатор и (или) Сторона (при участии в ЮЗЭД).

Юридически значимый электронный документооборот (далее - ЮЗЭД) - документооборот на базе Системы, в котором участники совершают действия по принятию к исполнению документов в электронной форме, удостоверенных ЭП, и при этом несут ответственность за совершение либо несовершение этих действий.

2. Классификация рисков

2.1. Риски, связанные с осуществлением ЮЗЭД в Системе, можно разделить по:

- типу (организационные и технические);
- источнику возникновения (внешние и внутренние).

Классификация рисков представлена в таблицах 3 и 4.

2.2. Вероятность реализации рисков, подверженность информационных активов Системы воздействию рисков.

С целью выделения групп близких по значимости рисков и подготовки полученных материалов для дальнейшего (например, количественного) анализа для каждого риска, выявленного в процессе анализа, экспертно оцениваются следующие показатели (присваиваются значения атрибутов):

- вероятность реализации риска;
- уровень подверженности информационного актива воздействию (существенность ущерба для Организатора).

Текстовые описания значений атрибутов приведены в таблицах 1 и 2.

Таблица 1

Значения атрибута «Вероятность реализации риска»

Вероятность	Описание
Высокая	Вероятна реализация риска один или несколько раз в течение календарного года
Средняя	Риск может быть реализован хотя бы один раз в течение двух-трех календарных лет
Низкая	Реализация риска в течение трех календарных лет маловероятна

Таблица 2

Значения атрибута «Уровень подверженности информационного актива воздействию»

Уровень подверженности воздействию	Существенность ущерба (конфиденциальность/целостность информационного актива)
5	Серьезные повреждения (например, повреждения, видимые снаружи и существенно влияющие на ход производственных процессов

	или существенно увеличивающие затраты) или полный выход актива из строя
4	Серьезные повреждения, не приводящие к полному выходу актива из строя (например, повреждения, не видимые снаружи, но существенно влияющие на ход производственных процессов или увеличивающие затраты)
3	Средние повреждения или ущерб (например, повреждения, влияющие на внутренние регламенты, увеличивающие затраты)
2	Незначительные повреждения или ущерб
1	Небольшие изменения информационного актива

Таблица 3

Организационные риски

	Источник возникновения	Описание	Вероятность реализации	Существенность ущерба	Меры по снижению риска
.	Внутренний/ Внешний	Компрометация ключа ЭП путем хищения носителей/копирования данных	высокая	4	Организация хранения материальных носителей, журналов выдачи. Использование некопируемых материальных носителей
.	Внутренний	Нарушение уполномоченным сотрудником правил использования СКЗИ	высокая	3	Ознакомление уполномоченного сотрудника под роспись в журнале ознакомления с пакетом документации по ЮЗЭД
.	Внутренний	Увольнение уполномоченного сотрудника, имевшего доступ к ключам ЭП	высокая	3	Подача заявления в УЦ на отзыв сертификата ЭП
.	Внутренний	Отказ от выполнения должностных обязанностей (в части использования ЭП) ввиду наличия риска компрометации ключа	средняя	4	Обучение персонала (ознакомление с законодательством, регламентирующим применение)
.	Внутренний	Несоответствие Систем требованиям ФСТЭК России в части защиты информации	средняя	5	Проведение аттестации Систем на соответствие классу защищенности 1Г. Обеспечение доступности информации

					об аттестате соответствия для всех заинтересованных в предоставлении гарантий физических и юридических лиц
.	Внутренний	Выгрузка в архивное хранение произведена неполностью, с нарушением целостности информации о цепочках доверия или с нарушением целостности документарных томов. Утрата документов или их реквизитов в процессе выгрузки	Высокая	4	Издание правового акта о регламенте хранения документов в архиве
.	Внутренний	Низкая степень значимости (важности) сертификата ключа подписи как документа для уполномоченного сотрудника	Высокая	4	Выдача бумажного оригинала сертификата, изготовленного на типографском бланке
.	Внутренний/ Внешний	Несанкционированный доступ к техническим средствам Систем (серверам, рабочим станциям пользователей и т.д.)	Средняя	5	Организация пропускного режима в помещения, где размещены технические средства Систем, а также в кабинеты, в которых расположены рабочие станции пользователей
.	Внутренний	Отказ от признания результатов экспертизы электронного документа одним из представителей конфликтующих сторон	Высокая	3	Издание порядка разбора конфликтных ситуаций, описывающего действия при разборе конфликтных ситуаций (в т.ч. претензионный порядок разрешения конфликтов)
0.	Внутренний	Разрешение конфликтов в суде	Средняя	5	Описание досудебного разбора конфликтов
1.	Внутренний	Доступ пользователей к не принадлежащим им	Высокая	3	Использование системы разграничения прав доступа, настройка

		объектам Систем			ролей пользователей
2.	Внутренний	Сопротивление сотрудников внедрению и использованию ЮЗЭД, неприятие новых методов работы	Высокая	4	Внедрение ЮЗЭД нормативным правовым актом Организатора. Организация обучения сотрудников
3.	Внутренний	Утечка конфиденциальной информации	Высокая	5	Разработка локальных актов о персональной ответственности сотрудников

Таблица 4

Технические риски

	Источник возникновения	Описание	Вероятность реализации	Существенность ущерба	Меры по снижению риска
.	Внешний	Перехват информации, передаваемой по каналам связи	Средняя	4	Защита протокола передачи данных между участниками и web-серверами путем организации https-доступа к web-серверу, SSL-шифрование трафика между участниками и web-серверами
.	Внешний	Несанкционированный доступ к серверам Систем	Средняя	5	Организация VPN сети. Расположение серверов в DMZ. Ограничение по портам доступа к серверам приложений Систем. Использование аппаратногобрэндмауэра
.	Внешний	Заражение компьютерными вирусами	Средняя	4	Организация антивирусной защиты
.	Внутренний	Нарушение целостности баз данных Систем	Высокая	5	Резервное копирование средствами используемых средств управления базами данных
.	Внутренний	Нехватка производственных мощностей серверов Систем	Низкая	3	Анализ планируемой нагрузки и наращивание мощностей в случае необходимости
	Внутрен	Утечка	Средн	4	Применение к

.	ний/ Внешний	ключей ЭП с рабочих станций пользователей	яя		рабочим станциям единой политики безопасности