

**ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ЗАБАЙКАЛЬСКИЙ ЦЕНТР ГОСУДАРСТВЕННЫХ ЗАКУПОК»
ПРИКАЗ**

от «03»мая 2017 г.

г. Чита

№ 28/ПД

**Об утверждении порядка доступа к информации,
содержащейся в АИС «Госзаказ»**

В соответствии с п.6 Порядка функционирования и использования государственной информационной системы Забайкальского края «Автоматизированная информационная система «Государственный заказ», утвержденного постановлением Правительства Забайкальского края от 12 декабря 2016 года № 446

ПРИКАЗЫВАЮ:

1. Утвердить порядок доступа к информации, содержащейся в автоматизированной информационной системе «Государственный заказ» (прилагается).

2. Начальнику отдела организационно-методического и нормативного сопровождения Жигалиной Е.А. осуществить ознакомление заказчиков Забайкальского края путем размещения настоящего приказа на официальном сайте учреждения.

Директор ГКУ «ЗабГосЗакуп»



А.Н. Лескова

ПРИЛОЖЕНИЕ

УТВЕРЖДЕН
приказом ГКУ «ЗабГосЗакуп»
от 03.05.2017 № 28/ПД

ПОРЯДОК доступа к информации, содержащейся в автоматизированной информационной системе «Государственный заказ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Термины и определения

Автоматизированное рабочее место Заказчика (далее – АРМ Заказчика) - рабочее место, обеспечивающее возможность удаленного on-line взаимодействия Оператора и Заказчика, включая наличие в нем программного обеспечения (далее - ПО) и технических средств, в том числе средств криптографической защиты информации (далее – СКЗИ).

Администратор АРМ Заказчика - сотрудник Заказчика, отвечающий за обеспечение бесперебойной эксплуатации ПО, СКЗИ и технических средств АРМ Заказчика, контроль мероприятий по защите информации, хранение и учет электронных документов (далее - ЭД), взаимодействие с Оператором по техническим вопросам и вопросам обеспечения безопасности информации.

Администратор безопасности информации Оператора (далее – администратор безопасности информации) - лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена ЭД с Заказчиком.

АИС «Госзаказ» - государственная информационная система «Автоматизированная информационная система «Государственный заказ Забайкальского края».

Владелец сертификата ключа подписи - должностное лицо, на имя которого удостоверяющим центром Федерального казначейства (далее - УЦ ФК) выдан сертификат ключа проверки электронной подписи (далее - Сертификат) и которое владеет соответствующим ключом электронной подписи.

Заказчик - государственные заказчики Забайкальского края, к которым относятся Законодательное Собрание Забайкальского края, Избирательная комиссия Забайкальского края, Контрольно-счетная палата Забайкальского края (в случае реализации пункта 4 Порядка взаимодействия государственного казенного учреждения «Забайкальский центр государственных закупок» с заказчиками, осуществляющими закупки для обеспечения нужд Забайкальского края, муниципальных нужд,

утвержденного постановлением Правительства Забайкальского края от 17.12.2013 № 544), исполнительные органы государственной власти Забайкальского края, Территориальный фонд обязательного медицинского страхования Забайкальского края, казенные учреждения, действующие от имени Забайкальского края, уполномоченные принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени Забайкальского края, и бюджетные учреждения Забайкальского края, осуществляющие закупки за счет субсидий, предоставленных из бюджетной системы Российской Федерации, и иных средств, государственные унитарные предприятия, муниципальные заказчики, к которым относятся муниципальные органы, муниципальные казенные учреждения, действующие от имени муниципального образования, уполномоченные принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени муниципального образования, и муниципальные бюджетные учреждения, осуществляющие закупки за счет субсидий, предоставленных из бюджетов бюджетной системы Российской Федерации, и иных средств, за исключением случаев, предусмотренных частями 2 и 3 статьи 15 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», муниципальные унитарные предприятия.

Закрытый ключ аутентификации - уникальная последовательность символов, известная владельцу Сертификата открытого ключа аутентификации (Администратору АРМ Заказчика) и предназначенная для аутентификации Заказчика на стороне Оператора с последующим установлением защищенного канала связи при информационном взаимодействии с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи).

Ключ ЭП - уникальная последовательность символов, предназначенная для создания ЭП.

Компрометация ключа ЭП - событие, определенное владельцем Сертификата как ознакомление неуполномоченным лицом (лицами) с его ключом ЭП (например: хищение, утеря носителя ключа ЭП, несанкционированное копирование или другие события, повлекшие за собой нарушение конфиденциальности ключа ЭП).

Корректная ЭП - ЭП уполномоченного лица при выполнении следующих условий:

- Сертификаты, относящиеся к этим ЭП, изданы УЦ ФК и не утратили силу (действуют) на момент подписания ЭД;
- подтверждена подлинность этих ЭП в ЭД, при наличии достоверной информации о моменте подписания ЭД;
- ЭП используется в соответствии со сведениями, указанными в Сертификате.

Оператор - государственное казенное учреждение «Забайкальский центр государственных закупок».

Открытый ключ (сертификат) аутентификации - уникальная последовательность символов, соответствующая закрытому ключу аутентификации, доступная Сторонам и предназначенная для подтверждения подлинности Заказчика при его аутентификации на стороне Оператора, с последующим установлением защищенного (шифрованного) канала связи при информационном взаимодействии в АИС «Госзаказ» между Сторонами с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи). Принадлежность открытого ключа аутентификации владельцу подтверждается Сертификатом открытого ключа аутентификации, изданным Администратором безопасности информации Оператора.

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

Пользователь информации (далее – Заказчик) - государственные заказчики Забайкальского края, а также муниципальные районы Забайкальского края, работающие по Соглашению между Забайкальским краем и муниципальным районом Забайкальского края об определении поставщиков (подрядчиков, исполнителей).

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

Сертификат ключа проверки электронной подписи (далее – Сертификат) - электронный документ или документ на бумажном носителе, выданный УЦ ФК по заявлению должностного лица Заказчика и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Сертификат открытого ключа аутентификации - электронный документ, который включает в себя открытый ключ аутентификации владельца. Сертификат открытого ключа аутентификации издается Администратором безопасности информации Оператора для обеспечения аутентификации Заказчика на стороне Оператора с последующим установлением защищенного (шифрованного) канала связи при информационном взаимодействии в АИС «Госзаказ» между Сторонами с использованием СКЗИ (для защиты информации при ее передаче по открытым каналам связи).

Электронный документ (далее – ЭД) - информация в электронной форме, подписанная электронной подписью, равнозначный документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

ЭДО в АИС «Госзаказ» - электронный документооборот в государственной информационной системе «Автоматизированная информационная система «Государственный заказ Забайкальского края».

Уполномоченное лицо - лицо, имеющее право электронной подписи ЭД.

Удостоверяющий центр Федерального казначейства (далее – УЦ ФК) - функциональная группа структурного подразделения, должностные лица Управления Федерального казначейства, осуществляющие выполнение функций по созданию и выдаче сертификата, а также иные функции предусмотренные Федеральным законом «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ.

1.2. Предмет регулирования

1.2.1. Настоящий Порядок устанавливает общие требования к обеспечению доступа пользователей к информации, содержащейся в АИС «Госзаказ», а также общие принципы осуществления электронного документооборота в АИС «Госзаказ» между пользователями.

1.3. Документы, регулирующие ЭДО в АИС «Госзаказ»

1.3.1. ЭДО в АИС «Госзаказ» регулируется следующими документами:

- документацией пользователя и администратора АРМ Заказчика;
- документацией на СКЗИ;
- настоящим порядком;
- законодательными и другими нормативными правовыми актами Российской Федерации.

1.4. Порядок и условия допуска Заказчика к осуществлению документооборота в АИС «Госзаказ»

1.4.1 Заказчик допускается к осуществлению документооборота в АИС «Госзаказ» после выполнения им следующих мероприятий:

- ознакомления с настоящим порядком;
- назначения администратора(ов) АРМ Заказчика;
- получения в УЦ УФК необходимого сертифицированного ПО, в том числе СКЗИ (исключая общесистемное и офисное ПО);
- регистрации Пользователей Заказчика в УЦ УФК и получения в установленном порядке Сертификатов;
- получения у Оператора необходимого для осуществления ЭДО ПО;
- установки необходимого для осуществления ЭДО ПО, в том числе антивирусного ПО и СКЗИ, на АРМ Заказчика.

1.4.2. Заказчик несет ответственность за:

- защиту АРМ АИС «Госзаказ» и носителей ключевой информации от несанкционированного доступа в соответствии с требованиями нормативных документов и законодательства Российской Федерации;

- ознакомление пользователей Заказчика с документами, регулируемыми ЭДО в АИС «Госзаказ»;

- проведения инструктажа Пользователей Заказчика по работе с АРМ Заказчика и требованиям по безопасности информации при работе в АИС «Госзаказ».

1.4.3. Пользователи Заказчика несут персональную ответственность за безопасность ключевой информации, в том числе ключей ЭП и ключей аутентификации, и обязаны обеспечивать ее конфиденциальность.

1.5. Применение настоящего порядка доступа, а также внесение изменений

1.5.1. Настоящий порядок применяется ко всем пользователям АИС «Госзаказ».

1.5.2. Изменения и дополнения в настоящий порядок вносятся в установленном порядке.

2. ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ

2.1. Требования, предъявляемые к ЭД

2.1.1. ЭД, сформированные в АИС «Госзаказ» и подписанные надлежащим количеством корректных ЭП, имеют юридическую силу наравне с бумажными документами, подписанными собственноручными подписями.

2.1.2. ЭД считаются надлежащим образом оформленными при условии их соответствия законодательству Российской Федерации, а также документам, регулирующим ЭДО в АИС «Госзаказ».

2.1.3. ЭД, не отвечающие требованиям, предъявляемым к ЭД настоящими Правилами, рассматриваются Сторонами как ЭД, не имеющие юридической силы.

2.2. Использование ЭП в ЭД

2.2.1. ЭД может быть подписан только ЭП уполномоченных лиц Сторон, для которых УЦ УФК изданы действующие Сертификаты.

2.2.2. Прекращение действия Сертификатов уполномоченных лиц Сторон не влияет на юридическую силу ЭД, которыми Стороны обменивались до прекращения действия Сертификатов.

2.3. Использование ЭД

2.3.1. ЭД, подписанный надлежащим количеством корректных ЭП уполномоченных лиц Сторон, имеет равную юридическую силу с документом, представленным на бумажном носителе, подписанном собственноручными подписями уполномоченных лиц Сторон, и не может быть оспорен только на том основании, что он выполнен в электронном виде.

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

2.3.3. Все экземпляры ЭД являются подлинниками данного ЭД.

2.4. Представление сведений, содержащихся в ЭД, на бумажном носителе

2.4.1. Сведения, содержащиеся в ЭД, могут быть представлены (распечатаны) на бумажном носителе. В этом случае их соответствие ЭД должно быть заверено Оператором или Заказчиком в установленном порядке.

3. ОРГАНИЗАЦИЯ ЭДО В АИС «ГОСЗАКАЗ»

Организация ЭДО в АИС «Госзаказ» осуществляется в соответствии с Порядком взаимодействия государственного казенного учреждения «Забайкальский центр государственных закупок» с заказчиками, осуществляющими закупки для обеспечения нужд Забайкальского края, муниципальных нужд, утвержденным постановлением Правительства Забайкальского края от 17.12.2013 № 544 «О некоторых вопросах реализации Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Общие требования обеспечения защиты информации в АИС «Госзаказ»

4.1.1. В случае обмена конфиденциальной информацией организационно-технические меры по защите и доступу к ней регламентируются законодательством Российской Федерации, нормативными актами, регулирующими вопросы информационной безопасности.

4.2. Управление ключевой информацией

4.2.1 Управление ключевой информацией осуществляют администраторы безопасности информации, уполномоченные лица УЦ ФК и администраторы АРМ Заказчика.

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

4.2.3. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения. При обращении с ними должны выполняться 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 при Президенте Российской Федерации от 13.06.2001 № 152, и настоящего порядка.

4.2.4. Учет носителей ключевой информации осуществляют администраторы безопасности информации и администраторы АРМ Заказчика по соответствующим учетным формам.

4.2.5. Требования по организации хранения и использования носителей ключевой информации.

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

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

4.2.5.3. Не разрешается:

- производить несанкционированное копирование носителей ключевой информации;

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

- выводить ключи ЭП 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.

4.2.6. Порядок работы с ключами аутентификации для организации шифрованного канала связи.

4.2.6.1. В качестве ключей и сертификата аутентификации могут использоваться сертификаты, выданные удостоверяющим центром Федерального казначейства с наличием в их составе идентификатора «аутентификация клиента». Порядок получения плановой смены ключей и сертификатов, в указанном пункте описан в Регламенте удостоверяющего центра Федерального казначейства.

4.2.6.2. Мероприятия по обеспечению удаленного защищенного доступа к информационным ресурсам Оператора осуществляются администратором безопасности информации Оператора в соответствии с эксплуатационной документацией АИС «Госзаказ».

4.2.6.3. Передача сертификата открытого ключа аутентификации администратору АРМ Заказчика, действующего на основании доверенности, осуществляется любым доступным способом.

4.2.6.4. При плановой смене сертификата формирование нового комплекта ключей аутентификации осуществляет администратор АРМ Заказчика. Соответствующий запрос на смену сертификата аутентификации направляется администратору безопасности информации Оператора.

4.2.6.5. О всех случаях компрометации закрытых ключей аутентификации администратор АРМ Заказчика извещает администратора безопасности информации Оператора. В этом случае формируется новый комплект ключей аутентификации.

4.2.7. Порядок работы с ключами ЭП определяется Регламентом УЦ ФК.

4.2.8. Все работы, связанные с управлением списком отозванных сертификатов и поддержанием его в актуальном состоянии, обеспечиваются УЦ ФК.

4.3. Порядок действий при компрометации и отзыве ключей ЭП определяется Регламентом УЦ ФК.

4.4. Порядок действий при компрометации закрытых ключей аутентификации.

4.4.1. При компрометации закрытого ключа аутентификации уполномоченное лицо Заказчика немедленно прекращает его использование и незамедлительно сообщает об этом администратору АРМ Заказчика, а тот, в свою очередь, - администратору безопасности информации Оператора.

4.4.2. После получения от владельца Сертификата Заказчика сообщения о компрометации закрытого ключа аутентификации администратор безопасности информации Оператора проверяет достоверность полученного сообщения. В случае подтверждения полученной информации инициируется процедура отзыва или приостановления действия соответствующего Сертификата.

4.4.3. Уведомление о компрометации закрытых ключей аутентификации должно быть подтверждено официальным уведомлением Заказчика о компрометации в письменном виде.

4.4.4. Использовать скомпрометированные закрытые ключи аутентификации для организации защищенного канала связи запрещается.

4.4.5. В случае компрометации закрытого ключа аутентификации Заказчик установленным порядком изготавливает новые открытый и закрытый ключи аутентификации.

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

5.1 Возникновение конфликтных ситуаций в связи с осуществлением ЭДО в АИС «Госзаказ»

5.1.1. В связи с осуществлением ЭДО возможно возникновение конфликтных ситуаций, связанных с формированием, подтверждением получения ЭД, а также использования в документах ЭП. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- оспаривание факта отправления и/или получения ЭД;
- оспаривание времени отправления и/или получения ЭД;
- оспаривание содержания отправленного/полученного ЭД;
- оспаривание подлинности экземпляров ЭД;

- оспаривание целостности ЭД;
- оспаривание идентичности лица, заверившего ЭД ЭП;
- оспаривание полномочий лица, заверившего ЭД ЭП.

5.1.2. Конфликтные ситуации разрешаются (урегулируются) Сторонами в рабочем порядке и/или по итогам работы комиссии по разрешению конфликтной ситуации (далее - Комиссия).

5.1.3. 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.

5.2. Уведомление о конфликтной ситуации

5.2.1. 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.

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

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

5.3. Разрешение конфликтной ситуации в рабочем порядке

5.3.1. 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.

5.3.2. В случае если Сторона-инициатор не удовлетворена информацией, полученной от Сторон-ответчиков, для рассмотрения конфликтной ситуации формируется Комиссия. В состав Комиссии входит равное количество уполномоченных лиц каждой из Сторон, участвующих в разрешении конфликтной ситуации. По результатам работы Комиссии выносятся протокол.
