Приложение 1

УТВЕРЖДЕН

приказом от 14 декабря 2012 г. № 150

Форма

**ДОГОВОР №\_\_\_\_\_\_**

**об обмене электронными документами между участниками юридически значимого электронного документооборота**

|  |  |
| --- | --- |
| г. Пермь | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
|  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(*полное наименование главного распорядителя средств бюджета Пермского муниципального района, сельских поселений)*

именуемый в дальнейшем “Субъект отчетности”, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и Финансово-экономическое управление администрации муниципального образования «Пермский муниципальный район», именуемое в дальнейшем «Организатор», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании Положения, с другой стороны, в дальнейшем именуемые «Участники», заключили настоящий Договор о нижеследующем:

1. Термины и определения

В настоящем Договоре применяются следующие термины и определения:

Аккредитованный удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06 апреля 2011г.№ 63-ФЗ «Об электронной подписи» (далее – Федеральный закон 63-ФЗ), и получившие аккредитацию.

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона 63-ФЗ.

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) – лицо, которому в установленном Федеральным законом 63-ФЗ порядке выдан сертификат ключа проверки электронной подписи.

Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (Журнал поэкземплярного учета СКЗИ) – документ, содержащий данные о выданных уполномоченным сотрудникам ключевых документах.

Квалифицированный сертификат ключа проверки электронной подписи (Сертификат) – сертификат ключа проверки электронной подписи, выданный УЦ или доверенным лицом УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ электронной подписи (закрытый ключ, ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Комплекс – программный комплекс «СКИФ», разработанный ОАО «Финтех» (далее – разработчик), предназначенный для автоматизации процессов формирования, приема, передачи, обработки и хранения форм отчетности.

Ключевой документ –ключевой носитель, содержащий ключ электронной подписи, а при необходимости – контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключа электронной подписи.

Организатор– Финансово-экономическое управление администрации муниципального образования «Пермский муниципальный район», осуществляющее прием от Субъекта отчетности, обработку и хранение форм отчетности.

Правила подписания – настроечный параметр Комплекса, позволяющий установить права на подписание электронных документов электронной подписью.

Регламент применения электронной подписи(Регламент) – документ, определяющий порядок и технические аспекты осуществления юридически значимого электронного документооборота.

Реестр сертификатов – перечень сертификатов Уполномоченных сотрудников Участников.

Список отозванных сертификатов – документ, содержащий список серийных номеров сертификатов, которые в определенный момент времени были отозваны, либо действие которых было приостановлено.

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

Сотрудник – пользователь, имеющий имя и пароль для входа в Комплекс и наделенный полномочиями для работы в Комплексе.

Средства криптографической защиты информации (СКЗИ) – аппаратные и(или) программные средства, обеспечивающие применение электронной подписи (создание, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи), и (или) шифрование при осуществлении электронного документооборота, а также обеспечивающие защиту информации по утвержденным стандартам и сертифицированные в соответствии с действующим законодательством.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверкаэлектронной подписи, создание ключа электронной подписи, ключа проверки электронной подписи.

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

Субъект отчетности – главный распорядитель средств бюджета Пермского муниципального района, администрации сельских поселений Пермского муниципального района, осуществляющий формирование и передачу форм отчетности Организатору.

Уполномоченный сотрудник – сотрудник, наделенный полномочиями по подписанию электронной подписью электронных документов в соответствии с утвержденным регламентом, для которого УЦ выпущен сертификат ключа проверки электронной подписи, отмеченный в Журнале поэкземплярного учета СКЗИ как получивший ключевой носитель. Уполномоченный сотрудник назначается приказом Участника.

Участник – юридическое лицо, принимающее участие в юридически значимом электронном документообороте.

Усиленная квалифицированная электронная подпись (ЭП) – вид электронной подписи, которая соответствует следующим признакам:

электронная подпись получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

электронная подпись позволяет определить лицо, подписавшее электронный документ;

электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

электронная подпись создается с использованием средств электронной подписи;

ключ проверки электронной подписи указан в Сертификате;

для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом 63-ФЗ.

Экспертная комиссия – комиссия, разрешающая конфликтные ситуации, связанные с использованием юридически значимого электронного документооборота.

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

Электронный документ– отчет,в котором информация представлена   
в электронной форме в формате Комплекса. Юридическая значимость электронного документа подтверждается ЭП.

Юридически значимый электронный документооборот (ЮЗЭД) – документооборот на базе Комплекса, в котором участники ЮЗЭД совершают действия по передаче и приему документов в электронной форме, удостоверенных ЭП, и несут ответственность за совершение либо несовершение этих действий.

1. Предмет договора

2.1. НастоящийДоговор определяет условия и порядок передачи и приема юридически значимых электронных документов между Участниками на базе Комплекса.

2.2. Договор определяет права и обязанности Участников, возникающие при осуществлении ЮЗЭД на базе Комплекса с учетом обеспечения информационной безопасности.

1. Общие положения

3.1.Участники осуществляют передачу и прием юридически значимых электронных документов на базе Комплекса по телекоммуникационным каналам связи. ЮЗЭД осуществляется с применением усиленной квалифицированной электронной подписи.

3.2. С целью обеспечения авторства, целостности и конфиденциальности электронных документов при информационном взаимодействии Участники используют сертифицированные СКЗИ.

3.3. Используемые при информационном взаимодействии Участников электронные документы с ЭП, сформированной Участниками средствами СКЗИ, имеют равную юридическую силу с документами на бумажном носителе, подписанными соответствующими собственноручными подписями Уполномоченных сотрудников Участников. При этом для их ЭП соблюдены следующие условия:

сертификаты изданы УЦ и не утратили силу (действуют) на момент проверки или на момент подписания электронного документа;

ЭП используетсяв соответствиисо сведениями, указанными в Сертификате.

3.4. Участники признают, что используемые при ЮЗЭД в Комплексе СКЗИ, реализующие функции создания ЭП, достаточны для подтверждения следующего:

электронный документ исходит от Субъекта отчетности, его составившего (подтверждение авторства отправленного электронного документа);

электронный документ не претерпел изменений в процессе передачи (подтверждение целостности и подлинности электронного документа).

1. Права и обязанности Участников
   1. Организатор обязан:
      1. Обеспечить функционирование Комплекса, а также обеспечить другой необходимой информацией для предоставления Субъекту отчетности возможности передачи юридически значимых электронных документов Организатору.
      2. При внесении изменении в Регламент провести настройки на серверной части Комплекса.
      3. Немедленно уведомить Субъекта отчетности любым доступным способом в случаях выявления:
         1. ошибок в работе Комплекса при работе с ЭП (подписания ЭП, проверки ЭП и др.);
         2. ошибок, возникающих в связи с попытками нарушения информационной безопасности.
      4. Вести актуальный реестр сертификатов Уполномоченных сотрудников Участников на основе принятых сертификатов и списка отозванных сертификатов от Субъекта отчетности.
      5. При условии соответствия электронных документов, признакам и требованиям к юридически значимым электронным документам, указанным в Регламенте (Приложение1 к настоящему Договору), принять от Субъекта отчетности электронный документдля дальнейшей проверки в соответствии с приказами Организатора.
      6. Предоставить Субъекту отчетности перечень форм отчетности, подписываемых ЭП, в соответствии с федеральным и региональным законодательством.
   2. Организатор имеет право:

4.2.1. В случае несоответствия электронного документа признакам и требованиям к юридически значимым электронным документам отказать Субъекту отчетности в приеме электронного документа с указанием мотивированной причины отказа.

4.2.2. Приостановить осуществление ЮЗЭД при:

4.2.2.1. несоблюдении субъектом отчетности требований по передаче ЭД и обеспечению информационной безопасности в соответствии с настоящим договором;

4.2.2.2. разрешении спорных ситуаций;

4.2.2.3. выполнении неотложных аварийных и ремонтно-восстановительных работ Комплекса.

4.2.3. На урегулирование вопросов в случае возникновения конфликтных ситуаций.

4.2.4. Вносить изменения в Регламент в соответствии с требованиями разработчика Комплекса.

* 1. Субъект отчетности обязан:

4.3.1. Обеспечить функционирование Комплекса на рабочем месте Субъекта отчетности, установить СКЗИ, указанные Организатором, на компьютерах Уполномоченных сотрудников для обеспечения работоспособности ЮЗЭД.

4.3.2. Обеспечить всеми необходимыми средствами (сертифицированные СКЗИ, сертификаты, ключевые носители и т.д.), Уполномоченных сотрудников Субъекта отчетности.

4.3.3. Выполнятьтребования УЦ в соответствии с регламентом УЦ и другими документами, регламентирующими процесс взаимодействия УЦ и пользователей услуг УЦ.

4.3.4. Назначить сотрудника, ответственного за эксплуатацию СКЗИ и ведение Журнала поэкземплярного учета СКЗИ, Уполномоченных сотрудников, имеющих право на работу в Комплексе.

4.3.5. Передавать Организатору электронные документы, оформленные в соответствии с Регламентом.

4.3.6. В целях обеспечения безопасности обработки и передачи юридически значимых электронных документов:

4.3.6.1. соблюдать требования, изложенные в разделе 5 настоящего Договора, и требования Положения о порядке работы со средствами криптографической защиты информации, утвержденного приказом Организатора;

4.3.6.2. соблюдать требования эксплуатационной документации на используемые СКЗИ;

4.3.6.3. прекратить использование ЭП в случае компрометации ключа и немедленно любым доступным способом информировать Организатора и УЦ об указанном факте;

4.3.6.4. хранить ключевой документ в месте, исключающем доступ неуполномоченных лиц и/или возможность его повреждения.

4.3.7. В случае невозможности исполнения обязательств по настоящему Договору немедленно известить Организатора о приостановлении обязательств.

4.3.8. В случае невозможности использования ЭП Субъект отчетности оформляет и передает Организатору документы на бумажном носителе и в электронном виде в формате Комплекса.

4.3.9. При возникновении споров, связанных с принятием или непринятием электронных документов, подписанных ЭП, входящих в перечень юридически значимых электронных документов, руководствоваться Порядком разбора конфликтных ситуаций, утвержденным приказом Организатора. Способ разрешения конфликтных ситуаций устанавливает Организатор.

4.3.10. По первому требованию предоставить Организатору заверенные печатью и подписями Уполномоченных сотрудников Субъекта отчетности электронные документы, распечатанные по формам отчетности, входящие в перечень юридически значимых электронных документов.

4.3.11. Заменить Сертификат в порядке, предусмотренном для его оформления согласно регламенту УЦ в следующих случаях:

4.3.11.1. смены Уполномоченных сотрудников Субъекта отчетности, наделенных полномочием подписи электронных документов;

4.3.11.2. изменения данных, идентифицирующих Уполномоченного сотрудника Субъекта отчетности;

4.3.11.3. смены ключей ЭП;

4.3.11.4. в иных случаях, прекращающих действие сертификата.

4.3.12. Немедленно уведомить Организатора любым доступным способом в случаях:

4.3.12.1. возникновения угрозы использования (копирования) иными лицами ключа ЭП, принадлежащего Уполномоченному сотруднику Субъекта отчетности;

4.3.12.2. утраты ключевого документа Уполномоченного сотрудника Субъекта отчетности;

4.3.12.3. изменения состава Уполномоченных сотрудников Субъекта отчетности, обладающих правом использования ключей ЭП;

* 1. Субъект отчетности имеет право:

4.4.1. требовать от Организатора принятия от Субъекта отчетности электронных документов.

4.4.2. на урегулирование вопросов в случае возникновения конфликтных ситуаций.

1. Безопасность эксплуатации средств криптографической защиты информации в Комплексе

5.1. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету.

5.2. Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет ответственный за эксплуатацию СКЗИ сотрудник Участника в Журнале поэкземплярного учета СКЗИ, по форме, утвержденной приказом Организатора. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их эксплуатация.

5.3. Единицей поэкземплярного учета ключей ЭП считается ключевой носитель многократного использования. В случае, когда один и тот же ключевой носитель многократно используют для записи ключей ЭП, то каждый раз он подлежит отдельной регистрации.

5.4. Все выдаваемые экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключей ЭП должны быть выданы под расписку в Журнале поэкземплярного учета СКЗИ Уполномоченным сотрудникам, которые несут персональную ответственность за их сохранность.

5.5. Дистрибутивы СКЗИ, эксплуатационная и техническая документация к СКЗИ хранятся у ответственного за эксплуатацию СКЗИ сотрудника Участника. Ключи ЭП хранятся у Уполномоченных сотрудников. Хранение осуществляется в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.6. Ключевые документы с неработоспособными ключами ЭП ответственный за эксплуатацию СКЗИ сотрудник Участника принимает у Уполномоченного сотрудника под роспись в Журнале поэкземплярного учета СКЗИ. Неработоспособные ключевые документы подлежат уничтожению.

5.7. В Комплексе используется СКЗИ с открытым распределением ключей.

5.8. Электронный документ может быть подписан ЭП с использованием только того ключа ЭП, для которого выдан сертификат Уполномоченного сотрудника.

5.9. Для подписи электронного документа Уполномоченный сотрудник использует свой собственный закрытый ключ. Проверка подлинности ЭП осуществляется Уполномоченным сотрудником с использованием открытого ключа.

5.10. Уполномоченный сотрудник не может подписать электронный документ ЭП, если истек срок действия закрытых ключей. Уполномоченный сотрудник не может проверить ЭП электронного документа в случае истечения срока действия Сертификата, необходимого для выполнения соответствующей операции.

5.11. Реализованные в СКЗИ алгоритмы шифрования и ЭП гарантируют невозможность восстановления закрытых ключей Уполномоченного сотрудника по его открытым ключам.

5.12. При выявлении сбоев или отказов Уполномоченный сотрудник обязан сообщить о факте их возникновения ответственному за эксплуатацию СКЗИ сотруднику Участника и представить ему ключевой документ для проверки его работоспособности. Проверку работоспособности ключевого документа ответственный за эксплуатацию СКЗИ сотрудник Участника выполняет в присутствии Уполномоченного сотрудника.

5.13. В случае, если ключевой документ потерял работоспособность, то Субъект отчетности организует получение Уполномоченным сотрудником ключевого документа.

5.14. Уполномоченному сотруднику запрещается:

5.14.1. осуществлять несанкционированное копирование ключей ЭП;

5.14.2. разглашать содержимое ключевого документа или передавать сами ключевые документы лицам, к ним не допущенным, оставлять без присмотра ключевой документ, выводить содержимое ключевого документа на дисплей или принтер;

5.14.3. вставлять ключевые документы в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания других аппаратных средств;

5.14.4. записывать на ключевой документ постороннюю информацию, использовать ключевой документ на неисправных устройствах считывания информации;

5.14.5. вносить какие-либо изменения в программное обеспечение СКЗИ.

1. Порядок ввода в действие юридически значимого электронного документооборота на базе Комплекса
   1. Субъект отчетности в соответствии с документацией к Комплексу устанавливает СКЗИ на компьютерах Уполномоченных сотрудников.
   2. Уполномоченные сотрудники Субъекта отчетности получают от УЦ средства ЭП: сертификаты, закрытые ключи, открытые ключи.
   3. Организатор выдает Субъекту отчетности под роспись настоящий Договор в 2-х экземплярах, подписанный Организатором.
   4. Субъект отчетности в течение одного рабочего дня после получения средств ЭП предоставляет Организатору:

подписанный экземпляр настоящего Договора;

копию приказа о назначении Уполномоченных сотрудников и сотрудника, ответственного за эксплуатацию СКЗИ и ведение Журнала поэкземплярного учета СКЗИ, заверенную руководителем Субъекта отчетности;

заявление на внесение в реестр Комплекса сертификатов уполномоченных сотрудников по форме согласно приложению 2 к настоящему Договору;

полученные от УЦ Сертификаты Уполномоченных сотрудников Субъекта отчетности в электронном виде и на бумажном носителе (копии, заверенные руководителем Субъекта отчетности);

* 1. Организатор после предоставления Субъектом отчетности документов, указанных в пункте 6.4 настоящего Договора, в течение одного рабочего дня вводит в действие СертификатыУполномоченных сотрудников Субъекта отчетности (вносит в реестр Комплекса).
  2. Участники приступают к осуществлению ЮЗЭД после принятия от Субъекта отчетности документов, указанных в пункте 6.4. настоящего Договора.

1. Ответственность Участников
   1. Участники несут ответственность за действия своих Уполномоченных сотрудников при осуществлении ЮЗЭД в рамках настоящего Договора.
   2. Субъект отчетности несет ответственность за содержание всех ЭД, подписанных ЭП Уполномоченных сотрудников.
   3. За неисполнение или ненадлежащее исполнение Участниками своих обязательств по настоящему Договору Участники несут ответственность в соответствии с законодательством Российской Федерации.
   4. Участник не отвечает за неисполнение или ненадлежащее выполнение своих обязательств по настоящему Договору, если это было вызвано действиями (бездействием) другого Участника.
   5. При использовании телекоммуникационных каналов связи и передачи данных Участники не несут ответственности за возможные временные задержки при доставке юридически значимых электронных документов, произошедшие не по их вине.
   6. Ответственность (включая размер ответственности), возлагаемая на Участника, определяется правилами системы электронного документооборота в соответствии с действующим законодательством Российской Федерации.
2. Разрешение конфликтных ситуаций

8.1. Все споры и разногласия, которые могут возникнуть в связи с применением, нарушением, толкованием настоящего Договора, признанием недействительным настоящего Договора или его части, Участники будут стремиться разрешить, используя переговоры и механизмы урегулирования споров и разногласий.

8.2. В случаях, когда конфликтная ситуация не урегулирована в результате переговоров и работы Экспертной комиссии, созданной в соответствии с Порядком разбора конфликтных ситуаций, утвержденным приказом Организатора, то Участники обращаются в Арбитражный суд.

1. Форс-мажорные обстоятельства
   1. Участник не несет ответственности в случае невыполнения, несвоевременного или ненадлежащего выполнения какого-либо обязательства по настоящему Договору, если указанное невыполнение, несвоевременное или ненадлежащее выполнение обусловлены исключительно наступлением и/или действием следующих обстоятельств (далее – форс-мажорные обстоятельства): обстоятельств непреодолимой силы; сбоев, неисправностей и отказов оборудования; сбоев и ошибок программного обеспечения; сбоев, неисправностей и отказов системы связи, энергосбережения, кондиционирования и других систем жизнеобеспечения, которые Участник не мог ни предвидеть, ни предотвратить.
   2. Участник, надлежащее исполнение обязательств которого оказалось невозможным в силу влияния форс-мажорных обстоятельств, в течение 3 (трех) рабочих часов после их наступления информирует другого Участника о наступлении этих обстоятельств и об их последствиях любым доступным способом и принимает все возможные меры с целью максимально ограничить отрицательные последствия, вызванные указанными форс-мажорными обстоятельствами.
   3. Неизвещение или несвоевременное извещение другого Участника Участником, надлежащее исполнение обязательств которого оказалось невозможным в силу влияния форс-мажорных обстоятельств, о наступлении этих обстоятельств влечет за собой утрату права ссылаться на эти обстоятельства.
   4. Наступление форс-мажорных обстоятельств влечет увеличение срока исполнения обязательств по настоящему Договору на период их действия, если Участники не договорились об ином.
2. Порядок внесения изменений в договор
   1. В случае принятия нормативного акта уполномоченным государственным органом по вопросам, регулируемым настоящим Договором, соответствующие положения Договора подлежат изменению по инициативе одного из Участников.
   2. Все изменения и дополнения к настоящему Договору действительны в том случае, если они оформлены в письменном виде и подписаны уполномоченными представителями Участников, за исключением изменений внесенных в приложения к настоящему Договору. Об изменениях и дополнениях к приложению настоящего Договора Организатор уведомляет Субъект отчетности в одностороннем порядке.
3. Срок действия Договора

11.1. Настоящий Договор вступает в силу с момента его подписания Участниками. Конечным сроком Договор не ограничивается.

11.2. Настоящий Договор может быть расторгнут по письменному соглашению Участников.

1. Заключительные положения

12.1. Настоящий Договор составлен на 15 листах в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждогоУчастника.

12.2. Приложения 1 и 2 к настоящему Договору являются его неотъемлемой частью.

1. Прочее

13.1 Расторжение настоящего Договора не влияет на действительность и порядок действия юридически значимых электронных документов, подписанных ЭП Уполномоченных сотрудников Участников до даты расторжения настоящего Договора.

1. Приложения

14.1. Приложение 1. Регламент осуществления ЮЗЭД с применением электронной подписи.

14.2. Приложение 2. Заявление на внесение в реестр Комплекса сертификатов уполномоченных сотрудников.

1. Адреса, банковские реквизиты и подписи Участников

|  |  |  |
| --- | --- | --- |
| СУБЪЕКТ ОТЧЕТНОСТИ |  | ОРГАНИЗАТОР |
|  |  | Финансово-экономическое управление администрации муниципального образования «Пермский муниципальный район» |
| \_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/  М.П. |

Приложение 1

к Договору №\_\_

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**РЕГЛАМЕНТ  
осуществления ЮЗЭД с применением электронной подписи**

1. Общие сведения

Настоящий Регламент определяет порядок и технические аспекты использования ЮЗЭД при передаче и приеме электронных документов от Субъекта отчетности, являющегося главным распорядителем средств бюджета Пермского муниципального района и бюджетов сельских поселений Пермского муниципального района.

1. Средства применения электронной подписи

При работе с ЮЗЭД принимаются и признаются сертификаты, изданные УЦ. Выбор УЦ при работе с Комплексом осуществляется Организатором.

Сертификат признается изданным УЦ, если подтверждена подлинность ЭП Уполномоченного лица УЦ, которым подписан сертификат Уполномоченного сотрудника Участника.

Идентификационные данные, занесенные в сертификат, однозначно идентифицируют владельца сертификата и соответствуют идентификационным данным владельца сертификата, зарегистрированным УЦ.

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

Местом публикации списков отозванных сертификатов принимается адрес информационного ресурса, определенный в регламенте или других актах УЦ.

В качестве средств ЭП, используются СКЗИ, сертифицированные в соответствии с действующим законодательством, а также совместимые с Комплексом (согласно требованиям Комплекса) и обеспечивающие следующее:

Реализацию функций создания ЭП в электронном документе с использованием ключа;

подтверждение с использованием сертификата подлинности ЭП в электронном документе;

создание ключей и сертификатов ЭП.

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)».

1. Программное обеспечение, в котором происходит функционирование юридически значимого электронного документооборота

Функционирование ЮЗЭД происходит на базе Комплекса.

1. Перечень электронных документов, включенных в юридически значимый электронный документооборот

Электронными документами, которые будут считаться юридически значимыми при условии подписания их ЭП (в случае выполнения всех условий равнозначности ЭП собственноручной в соответствии с Федеральным законом 63-ФЗ) и с учетом остальных требований настоящего Договора, являются формы бюджетной и сводной бухгалтерской отчетности мупниципальных автономных и бюджетных учреждений, установленные соответствующими приказами Министерства финансов Российской Федерации, Федерального казначейства, а также дополнительные формы бюджетной и бухгалтерской отчетности, установленные соответствующими приказами Организатора (далее – формы отчетности).

1. Правила подписания электронных документов

5.1. Право электронной подписи электронного документа принадлежит Уполномоченным сотрудникам.

5.2. Субъект отчетности после проведения в Комплексе функциональных этапов по вводу данных, проведения расчетов, контроля по логической увязке данных в формах отчетности (внутридокументный, междокументный контроль) устанавливает статус «Утвержден» и подписывает утвержденные формы отчетности. Каждая форма отчетности должна содержать две ЭП: первая подпись – руководитель главного распорядителя средств бюджета Пермского муниципального района, бюджета сельских поселений Пермского муниципального района, либо лицо, исполняющее его обязанности, вторая подпись – главный бухгалтер главного распорядителя средств бюджета Пермского муниципального района, бюджета сельских поселений Пермского муниципального района либо лицо, исполняющее его обязанности.

5.3. Уполномоченные сотрудники Субъекта отчетности обязуются подписывать юридически значимые электронные документы своей электронной подписью строго в соответствии с правилами подписания, в ином случае электронные документы не считаются юридически значимыми.

1. Контроль правил подписания юридически значимых электронных документов

6.1. Контроль правил подписания юридически значимых электронных документов осуществляется организационными мерами, также допускается контроль техническими средствами Комплекса (использование правил проверки в Комплексе). Способы контроля правил подписания определяются Организатором.

Приложение 2

к Договору №\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

ФЭУ Пермского муниципального района

ЗАЯВЛЕНИЕ

на внесение в реестр Комплекса сертификатов уполномоченных сотрудников

« \_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(полное наименование главного распорядителя средств бюджета Пермского муниципального района, бюджетов сельских поселений)

в соответствии с условиями Договора об обмене электронными документами между участниками юридически значимого электронного документооборота № \_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. просит для осуществления электронного документооборота внести в реестр Комплекса сертификат(ы) уполномоченного(ых) сотрудника(ов) Участника со следующими регистрационными данными:

№

Должность

Фамилия

Имя

Отчество

E-mail

Серийный номер сертификата электронной подписи

Название Роли (Руководитель или Главный бухгалтер)

Подпись уполномоченного сотрудника Стороны

Настоящим Участник,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(полное наименование главного распорядителя средств бюджета Пермского муниципального района, бюджетов сельских поселений)

заявляет, что любые действия, которые будут совершены владельцем(ми) сертификата(ов) на основании сертификата(ов) являются действиями, совершаемыми владельцем(ами) сертификата(ов) от имени Участника, по его указанию и связаны с участием в обмене юридически значимыми электронными документами в программном комплексе «СКИФ».

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Фамилия И.О./ М.П.

Приложение 2

УТВЕРЖДЕН

приказом от 14 декабря 2012 г. №\_\_\_

ПОЛОЖЕНИЕ

о порядке работы со средствами криптографической защиты информации

1. Термины и определения

Аккредитованный удостоверяющий центр (УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (далее - Федеральный закон 63-ФЗ), и получившие аккредитацию.

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального [закона](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ.

Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (журнал поэкземплярного учета СКЗИ) - документ, содержащий данные о выданных уполномоченным сотрудникам ключевых документах.

Квалифицированный сертификат ключа проверки электронной подписи (Сертификат) - сертификат ключа проверки электронной подписи, выданный УЦ или доверенным лицом УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Компрометация криптоключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Ключ электронной подписи (криптоключ, закрытый ключ, ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ - ключевой носитель, содержащий ключ электронной подписи, а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключа электронной подписи.

Пользователь СКЗИ (пользователь) - физическое лицо Участника, непосредственно допущенное к работе со средствами криптографической защиты информации.

Комплекс – программный комплекс «СКИФ», разработанный ОАО «Финтех» (далее – разработчик), предназначенный для автоматизации формирования, приема, передачи, обработки и хранения форм отчетности.

Средства криптографической защиты информации (СКЗИ) - аппаратные и(или) программные средства, обеспечивающие применение электронной подписи (создание, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи) и(или) шифрование при осуществлении электронного документооборота, а также обеспечивающие защиту информации по утвержденным стандартам и сертифицированные в соответствии с действующим законодательством.

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

Участник - юридическое лицо, принимающее участие в юридически значимом электронном документообороте.

Усиленная квалифицированная электронная подпись (ЭП) - вид электронной подписи, который соответствует следующим признакам:

электронная подпись получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

электронная подпись позволяет определить лицо, подписавшее электронный документ;

электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

ключ проверки электронной подписи указан в Сертификате;

для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ.

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

Электронный документ – отчет, в котором информация представлена   
в электронной форме в формате Комплекса. Юридическая значимость электронного документа подтверждается ЭП.

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

2. Общие положения

Настоящий документ регламентирует порядок работы со средствами криптографической защиты информации (СКЗИ) в соответствии с [Приказом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76221ECBA24B4AEE6647A7A0EB0VDV0F) ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", [Положением](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EEB32FB1A0BB6E722302B2D7372DE0AC255967F07F139AV9VBF) о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным Приказом ФСБ РФ от 09 февраля 2005 г. N 66.

3. Организация и обеспечение безопасности хранения

и применения СКЗИ

Ключевые документы или исходная информация для выработки ключевых документов изготавливаются УЦ или ответственным за эксплуатацию СКЗИ сотрудником Участника.

Пользователи СКЗИ обязаны:

не разглашать сведения о криптоключах;

соблюдать требования и рекомендации указанные производителем СКЗИ в сопроводительной документации;

сообщать ответственному за эксплуатацию СКЗИ сотруднику Участника, а также Организатору о ставших им известными попытках посторонних лиц получить сведения об используемых криптоключах или ключевых документах;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

при получении в пользование ключевого носителя изменить PIN-код пользователя. Изменение PIN-кода администратора производит ответственный за эксплуатацию СКЗИ сотрудник Участника;

немедленно уведомлять ответственного за эксплуатацию СКЗИ сотрудника Участника, а также организатора о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего инструктажа. Инструктаж включает в себя ознакомление с руководством пользователя СКЗИ, инструкцией по установке, настройке и эксплуатации СКЗИ, Регламентом УЦ. Инструктаж проводит ответственный за эксплуатацию СКЗИ сотрудник Участника и(или) УЦ.

4. Порядок обращения с СКЗИ и криптоключами к ним.

Мероприятия при компрометации криптоключей

Для организации и обеспечения безопасности хранения и применения ЭП следует использовать СКЗИ, предусматривающие запись ключей ЭП на электронные ключевые носители многократного (долговременного) использования (дискеты, компакт-диски (CD-ROM), Data Key, Smart Card, eToken, RuToken и т.п.).

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленной форме в соответствии с требованиями Положения ПКЗ-2005. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

[Журнал](#Par133) поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет ответственный за эксплуатацию СКЗИ сотрудник Участника по форме согласно приложению к настоящему Положению.

Все полученные ответственным за эксплуатацию СКЗИ сотрудником Участника экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета СКЗИ несущим персональную ответственность за их сохранность.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) ответственными за эксплуатацию СКЗИ сотрудниками Участника под расписку в соответствующих журналах поэкземплярного учета СКЗИ.

Пользователи СКЗИ хранят носители СКЗИ, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Аппаратные средства, с которыми осуществляется штатное функционирование, СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными из числа ответственных за эксплуатацию СКЗИ сотрудников Участника или пользователей СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

Для пересылки СКЗИ ключевые документы должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают ответственного за эксплуатацию СКЗИ сотрудника Участника или пользователя СКЗИ, для которого эти упаковки предназначены. На упаковках делают пометку "Лично". Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Оформленную таким образом упаковку, при предъявлении фельдсвязью дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

Полученные упаковки вскрывают только ответственный за эксплуатацию СКЗИ сотрудник Участника или пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от отправителя применять не разрешается.

Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению на месте эксплуатации.

Уничтожение криптоключей (исходной ключевой информации) производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, eTo-ken, RuToken и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в журнале поэкземплярного учета.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным за эксплуатацию СКЗИ сотрудником Участника под расписку в журнале поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом, пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников Участника, в том числе ответственного за эксплуатацию СКЗИ сотрудника. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делается отметка в журнале поэкземплярного учета СКЗИ.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают в УЦ и ФЭУ Пермского муниципального района. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей, пользователи СКЗИ обязаны сообщать в УЦ и ФЭУ Пермского муниципального района. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается соответствующим Регламентом оказания услуг УЦ.

5. Контроль за организацией и обеспечением безопасности

хранения и применения СКЗИ

Контроль за организацией и обеспечением безопасности хранения, эксплуатации, обработки и передачи по каналам связи информации с использованием СКЗИ - государственный контроль осуществляют уполномоченные федеральные органы. В ходе государственного контроля изучаются и оцениваются:

организация безопасности хранения, эксплуатации СКЗИ;

достигнутый уровень криптографической защиты информации;

условия использования СКЗИ.

Приложение

к Положению

о порядке работы со средствами

криптографической защиты

информации

ЖУРНАЛ

поэкземплярного учета СКЗИ, эксплуатационной и технической

документации к ним, ключевых документов

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N  п/п | Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов | Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов | Отметка о получении | | Отметка о выдаче | | Отметка о подключении   (установке) СКЗИ | | | Отметка об изъятии СКЗИ из  аппаратных средств, уничтожении  (утрате) ключевых документов | | | Примечание |
| От кого  получены | Дата и  номер  сопроводительного  письма | Ф.И.О.  пользо- вателя  СКЗИ | Дата и  расписка в получе  нии | Ф.И.О.  сотруд-  ников  пользователя  СКЗИ,  произведших подключение (установ- ку) | Дата  подключения (установ- ки) и  подписи  лиц, произвед ших  подключение  (установ- ку) | Номера  аппарат-  ных  средств,  в которые установ-  лены или  к которым подключены СКЗИ | Дата  изъятия  (уничто- жения,  утери) | Ф.И.О.  сотрудников пользователя  СКЗИ,  производивших изъятие  (уничтожение)/  Ф.И.О.  пользователя  СКЗИ,  утратившего | Номер  акта или расписка об унич- тожении  (утере) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

Приложение 3

УТВЕРЖДЕН

приказом от 14 декабря 2012 г. №\_\_\_

ПОРЯДОК

разбора конфликтных ситуаций

1. Термины и определения

Термины и определения, используемые в документе:

Аккредитованный удостоверяющий центр (УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (далее - Федеральный закон 63-ФЗ), и получившее аккредитацию.

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального [закона](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ.

Альбом электронных документов - документ, содержащий список электронных документов, включенных в юридически значимый электронный документооборот.

Аттестат соответствия - документ установленной формы, подтверждающий выполнение требований нормативных правовых актов в области защиты информации.

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) - лицо, которому в установленном Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ порядке выдан сертификат ключа проверки электронной подписи.

Доказательная база - информация в электронном и в бумажном виде, достаточная для разрешения конфликтных ситуаций.

Жизненный цикл электронного документа - существование электронного документа от момента формирования до момента передачи в архив или уничтожения.

Инициатор - юридическое лицо, инициирующее разбор конфликтной ситуации, связанной с необходимостью проверки юридической значимости электронного документа.

Квалифицированный сертификат ключа проверки электронной подписи (сертификат) - сертификат ключа проверки электронной подписи, выданный УЦ или доверенным лицом УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ электронной подписи (закрытый ключ, ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Область применения сертификата - параметр сертификата. Область применения сертификата определяет перечень электронных документов, возможных для подписания при помощи данного сертификата.

Ответчик - юридическое лицо, привлекаемое в качестве предполагаемого нарушителя прав Инициатора.

Отозванный сертификат - сертификат, который отозван из обращения.

Регламент применения электронной подписи (Регламент) - документ, определяющий статусы электронных документов, на которых происходит наложение электронной подписи в электронном документе.

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

Комплекс – программный комплекс «СКИФ», разработанный ОАО «Финтех» (далее – разработчик), предназначенный для автоматизации формирования, приема, передачи, обработки и хранения форм отчетности.

Средства криптографической защиты информации (СКЗИ) - аппаратные и(или) программные средства, обеспечивающие применение электронной подписи (создание, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи) и (или) шифрование при осуществлении электронного документооборота, а также обеспечивающие защиту информации по утвержденным стандартам и сертифицированные в соответствии с действующим законодательством.

Статус электронного документа - атрибут электронного документа, идентифицирующий его состояние по определенному признаку.

Сотрудник - пользователь, имеющий имя и пароль для входа в Комплекс и наделенный полномочиями для работы в Комплексе.

Уполномоченный сотрудник - сотрудник, наделенный полномочиями по подписанию электронной подписью электронных документов в соответствии с утвержденным Регламентом, для которого УЦ выпущен сертификат ключа проверки электронной подписи.

Участник - юридическое лицо, принимающее участие в юридически значимом электронном документообороте.

Усиленная квалифицированная электронная подпись (ЭП) - вид электронной подписи, которая соответствует следующим признакам;

электронная подпись получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

электронная подпись позволяет определить лицо, подписавшее электронный документ;

электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

электронная подпись создается с использованием средств электронной подписи;

ключ проверки электронной подписи указан в сертификате;

для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ.

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

Цепочка доверия - последовательность взаимосвязанных (доверенных) сертификатов, возникающая при проверке ключа ЭП.

Экспертная комиссия - комиссия, разрешающая конфликтные ситуации, связанные с использованием юридически значимого электронного документооборота.

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

Электронный документ – отчет, в котором информация представлена в электронной форме в формате Комплекса. Юридическая значимость электронного документа подтверждается ЭП.

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

2. Назначение документа

2.1. Настоящий документ определяет порядок разрешения конфликтных ситуаций, связанных с использованием ЮЗЭД на базе Комплекса. Использование ЮЗЭД подразумевает под собой подписание ЭП электронных документов на базе Комплекс.

2.2. Настоящий документ предназначен для Участников, в том числе для Инициаторов, Ответчиков, а также для членов Экспертных комиссий.

3. Порядок разрешения конфликтных ситуаций

3.1. Общие положения

3.1.1. В ходе обмена юридически значимыми электронными документами между Участниками могут возникать конфликтные ситуации в части установления авторства и/или подлинности электронных документов, нарушения правил использования СКЗИ. Возможны возникновения разногласий в следующих ситуациях:

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, заверившего электронный документ ЭП;

оспаривание полномочий лица, заверившего электронный документ ЭП;

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

иные случаи возникновения конфликтных ситуаций в ходе обмена электронными документами.

3.1.2. Разрешая конфликтные ситуации, Участники исходят из того, что:

в соответствии с действующим законодательством документ в электронном виде, заверенный ЭП в Комплексе, является документом, имеющим юридическую силу, аналогичным бумажному документу, снабженному подписью и печатью;

электронный документ порождает обязательства Участника перед другими Участниками, если документ оформлен надлежащим образом, подписан ЭП в Комплексе и доставлен другому Участнику. При этом ЭП используется в соответствии со сведениями, указанными в сертификате, а сертификат отправителя является действующим;

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.

3.1.3. Разрешение конфликтных ситуаций может осуществляться несколькими способами (в зависимости от уровня эскалации конфликтной ситуации), а именно:

Участник, инициировавший разбор, и Ответчик разрешают конфликтную ситуацию в рабочем порядке (без создания Экспертной комиссии);

Участник, инициировавший разбор, и Ответчик разрешают конфликтную ситуацию с созданием Экспертной комиссии и привлечением разработчиков программного обеспечения Комплекса;

претензионный порядок разрешения конфликтной ситуации;

Участник, инициировавший разбор, и Ответчик разрешают конфликтную ситуацию в судебном порядке.

3.2. 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 ответственного сотрудника 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. Информация, полученная от Инициатора по телефону или в ином устном обращении, регистрируется ответственным сотрудником в журнале регистрации извещений о разборе конфликтной ситуации. Инициатор обязан продублировать извещение в письменном виде.

Ответчик, которому была направлена информация (извещение в свободной форме) о конфликтной ситуации, и который должен участвовать в ее разрешении, обязан проверить наличие указанных в извещении обстоятельств и принять меры по разрешению конфликтной ситуации со своей стороны.

Ответчик письмом извещает Инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения конфликтной ситуации.

Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если Инициатор удовлетворен информацией, содержащейся в извещениях Ответчика, и не имеет к ней претензий.

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

3.3. Разрешение конфликтной ситуации с созданием Экспертной комиссии

В случае если конфликтная ситуация не была разрешена в рабочем порядке, Инициатор может направить Ответчику заявление о разногласиях в свободной форме с предложением создать Экспертную комиссию.

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

действия, являющиеся конфликтными, наносят существенный ущерб;

действия, являющиеся конфликтными, не наносят существенный ущерб, но Участник, инициировавший разбор, не удовлетворен информацией, полученной от Ответчика в процессе разрешения конфликтной ситуации в рабочем порядке.

3.3.1. Формирование заявления о разногласиях

При возникновении разногласий Инициатор, заявляющий о разногласии, направляет Ответчику заявление о разногласиях<1> в свободной форме.

--------------------------------

<1> До подачи заявления Участнику, инициировавшему разбор конфликтной ситуации, необходимо убедиться в целостности установленного на его технических средствах программного обеспечения, в том числе средств ЭП. Инициатор обязан убедиться в том, что не было произведено несанкционированных действий относительно программного обеспечения. А также удостовериться в том, что на его технических средствах не установлено вредоносное или шпионское программное обеспечение.

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 составляется в свободной форме на бумажном носителе, подписывается должностными лицами Инициатора, уполномоченными участвовать в разрешении конфликтной ситуации, и передаются Ответчику.

Заявление о разногласиях в обязательном порядке должно содержать следующую информацию:

уникальный идентификатор электронного документа [<2>](#Par277);

название класса электронного документа и его номер в Комплексе;

дата заявления;

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

нормы законодательных и иных нормативных правовых актов, на основании которых выставляется требование (в том числе договор об обмене электронными документами между Участниками юридически значимого электронного документооборота);

предложение создать Экспертную комиссию;

перечень документов (составляющих доказательную базу при конфликтной ситуации для судебных разбирательств), прилагаемых к заявлению о разногласии. В состав указанных документов должны быть включены:

файл, содержащий электронный документ, а также ЭП этого электронного документа [<3>](#Par287);

файл, содержащий вложение электронного документа, а также ЭП этого вложения электронного документа [<4>](#Par291);

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

3.3.2. Предполагаемое место и дата сбора Экспертной комиссии

Не позднее чем на третий рабочий день после получения заявления о разногласиях Участниками, участвующими в разрешении конфликтной ситуации, должна быть сформирована Экспертная комиссия.

Экспертная комиссия формируется на основании приказа Министерства финансов Пермского края. Приказ устанавливает состав Экспертной комиссии, время, место и срок ее работы.

--------------------------------

<2> Определяется через интерфейс Комплекса.

<3> Выгружается из Комплекса.

<4> Выгружается из Комплекса.

Устанавливается срок работы Экспертной комиссии - 5 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 включаются представители отдела автоматизации Министерства финансов Пермского края, а также исполнители электронных документов, являющиеся подписантами с использованием ЭП в Комплексе.

В состав Экспертной комиссии могут быть включены представители юридических служб Участников, представители органов, осуществляющих государственное регулирование и контроль соответствующих видов деятельности.

По инициативе любого из Участников, участвующих в разрешении конфликтной ситуации, к работе Экспертной комиссии для проведения технической экспертизы привлекаются уполномоченные сотрудники УЦ и(или) иные независимые эксперты.

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

Председатель Экспертной комиссии назначается по согласованию Участников.

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

3.3.3. Права и полномочия Экспертной комиссии

Экспертная комиссия имеет право получать доступ к необходимым для ее работы документальным материалам Участников, в том числе нормативным правовым актам по обмену электронными документами, архивам электронных документов.

Экспертная комиссия имеет право на ознакомление с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета электронных документов Участников.

Экспертная комиссия имеет право на ознакомление с условиями и порядком эксплуатации программных и технических средств обмена электронными документами Участников.

Экспертная комиссия имеет право на ознакомление с условиями и порядком изготовления, использования и хранения Участниками ключей, иной конфиденциальной информации, а также материальных носителей, необходимых для работы средств обмена электронными документами.

Экспертная комиссия имеет право получать объяснения от должностных лиц Участников, обеспечивающих обмен электронными документами.

Экспертная комиссия вправе 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.

3.3.4. Порядок работы Экспертной комиссии

Ответчик обязан в период работы Экспертной комиссии представить Инициатору и Экспертной комиссии ответы по каждому вопросу, изложенному в заявлении о разногласиях.

В ответах Ответчика на каждое требование должны содержаться документально обоснованные ответы или даны ссылки на доказательства, которые могут быть представлены в ходе работы Экспертной комиссии.

Любая сторона в ходе работы Экспертной комиссии может внести ходатайства об изменении или дополнении своих требований или возражений.

Экспертная комиссия в любой момент может затребовать от сторон предоставления документов, вещественных или иных доказательств в устанавливаемый Экспертной комиссией срок.

Рассмотрение спора производится на основании всех представленных документов, доказательств.

В том случае, если обстоятельства требуют подтверждения факта подлинности ЭП в электронном документе, Экспертная комиссия проводит экспертизу по подтверждению подлинности ЭП.

Для проведения экспертизы по подтверждению подлинности ЭП привлекаются уполномоченные сотрудники УЦ.

Технический порядок проведения экспертизы определяется эксплуатационной документацией на данное специализированное программное обеспечение.

3.3.5. Проверка подлинности электронных документов

Для проверки подлинности электронного документа необходимо:

проверить наличие данного электронного документа в Комплексе;

получить электронный документ и ЭП для проведения анализа, при этом документ и ЭП выгружают из Комплекса в виде файла: документ и подпись в виде файла в формате xml.

Проверка осуществляется посредством поиска уникального идентификатора, указанного в заявлении о разногласиях.

При установлении факта отсутствия данного электронного документа в Комплексе делается вывод об отсутствии причин конфликтной ситуации. При установлении факта присутствия электронного документа в Комплексе необходимо продолжить разрешение конфликтной ситуации в соответствии с настоящим Порядком.

3.3.6. 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 уполномоченным сотрудником УЦ. Экспертиза осуществляется с использованием применяемого средства ЭП и специализированного программного обеспечения, используемого УЦ для разрешения конфликтных ситуаций.

Для проведения экспертизы подлинности ЭП в электронном документе необходимо:

определить сертификат, необходимый для проверки ЭП;

проверить подлинность ЭП электронного документа с использованием сертификата;

в случае если при наложении ЭП используется штамп времени, проверить статус сертификата на момент подписания.

При установлении факта неподтверждения подлинности ЭП делается вывод об отсутствии причин конфликтной ситуации.

При установлении факта подлинности ЭП делается вывод о продолжении разрешения конфликтной ситуации в соответствии с настоящим Порядком.

3.3.7. Проверка организационных аспектов

После подтверждения подлинности ЭП в представленном электронном документе проводится проверка организационных аспектов электронного документа.

3.3.7.1. При проверке на соответствие положениям Регламента в Комплексе проверяются следующие условия:

соответствие полномочий уполномоченного сотрудника на подписание электронного документа ЭП в соответствии с Регламентом;

соответствие личности должностного лица, подписавшего документ, информации, указанной в сертификате, который был представлен Экспертной комиссии.

При проверке соответствия полномочий уполномоченного сотрудника на подписание электронного документа ЭП в соответствии с Регламентом проверяется:

соответствие представленного электронного документа описанию класса (описание классов документов приведено в документации к Комплексу);

возможность подписания ЭП электронных документов данного класса;

возможность подписания ЭП на заданном статусе жизненного цикла электронного документа;

присутствие электронного документа данного класса в перечне юридически значимых электронных документов;

время и дата подписания электронного документа (по времени системного журнала).

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

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

3.3.7.2. Правомерность использования копий СКЗИ и Комплекса в соответствии с условиями лицензионных соглашений.

При установлении факта правомерности использования СКЗИ и Комплекса, а также при наличии остальных подтверждающих фактов делается вывод о правомерности претензий Инициатора, зафиксированных в заявлении о разногласиях.

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

3.3.7.3. Корректность использования копий СКЗИ и Комплекса в соответствии с документацией на используемые программные и аппаратные средства и аттестатами соответствия.

При установлении факта корректного использования СКЗИ и Комплекса, а также при наличии остальных подтверждающих фактов делается вывод о правомерности претензий Инициатора, зафиксированных в заявлении о разногласиях.

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

3.3.7.4. Правомерность подписания электронного документа Уполномоченным сотрудником Участника на основании приказов о наделении сотрудника правом подписи электронных документов определенных классов.

При установлении факта правомерного подписания электронного документа сотрудником Участника, а также при наличии остальных подтверждающих фактов делается вывод о правомерности претензий Инициатора, зафиксированных в заявлении о разногласиях.

При установлении факта неправомерного подписания Электронного документа сотрудником Участника делается вывод об отсутствии причин конфликтной ситуации.

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

При установлении факта использования сертификатов в соответствии с областью применения, а также при наличии остальных подтверждающих фактов делается вывод о правомерности претензий Инициатора, зафиксированных в заявлении о разногласиях.

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

3.3.8. Оформление результатов работы Экспертной комиссии

3.3.8.1. Протокол работы Экспертной комиссии

Все действия, предпринимаемые Экспертной комиссией для выяснения фактических обстоятельств, а также выводы, сделанные Экспертной комиссией, заносятся в протокол работы Экспертной комиссии.

Протокол работы Экспертной комиссии должен содержать следующие данные:

состав Экспертной комиссии с указанием фамилии, имени, отчества, места работы, занимаемой должности, при необходимости исполняемой при обмене электронными документами функциональной роли, 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.

3.3.8.2. Акт по итогам работы Экспертной комиссии

По итогам работы Экспертной комиссии составляется акт, который должен содержать следующую информацию:

краткое изложение выводов Экспертной комиссии;

принятое решение Экспертной комиссии;

состав Экспертной комиссии;

дату и место составления акта;

дату и время начала и окончания работы Экспертной комиссии;

перечень мероприятий, проведенных Экспертной комиссией;

собственноручные подписи членов Экспертной комиссии;

указание на особое мнение члена (членов) Экспертной комиссии, в случае наличия такового.

Акт составляется в форме документа в свободной форме на бумажном носителе в 2 экземплярах и выдается Инициатору и Ответчику.

3.3.9. 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 позднее 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 форме документа на бумажном носителе и выдается по одному экземпляру каждому Участнику. Решение подписывается уполномоченными в разрешении конфликтной ситуации лицами Участников и утверждается руководителями Участников.

4. Претензионный порядок разрешения конфликтной ситуации

Претензионный порядок разрешения конфликтной ситуации применяется:

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;

в случае если один из Участников считает, что его права в связи с обменом электронными документами были нарушены.

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 нормативные акты;

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 Участника, инициирующего претензионный порядок разрешения конфликтной ситуации;

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 свободной форме, подписывается руководителем Инициатора, заверяется печатью Инициатора. Претензия и прилагаемые к ней документы направляются в адрес Ответчика. Участник, в адрес которого направлена претензия, 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 разделом претензионного порядка и может рассматриваться в качестве отказа в удовлетворении требований претензии.

5. Разрешение конфликтных ситуаций в судах

Разрешение конфликтных ситуаций в судах допускается в тех случаях, когда разрешение конфликтных ситуаций в рабочем порядке, с созданием Экспертной комиссии, или в претензионном порядке не привело к разрешению конфликтной ситуации.

Разрешение конфликтных ситуаций в судах проводится в порядке, установленном законодательством Российской Федерации.

Список

необходимых для разрешения конфликтной ситуации проверок

|  |  |  |
| --- | --- | --- |
| N | Наименование проверки | Результат проверки  (да/нет) |
| 1 | Проверка подлинности электронного документа |  |
| 1.1 | Проверка присутствия документа в Комплексе |  |
| 2 | Подтверждение подлинности ЭП |  |
| 2.1 | Успешно ли выполнена проверка ЭП с использованием  сертификатов, представленных Инициатором и УЦ? |  |
| 2.2 | Действителен ли сертификат, которым подписан конфликтный  документ на момент подписания? |  |
| 3 | Проверка организационных аспектов |  |
| 3.1 | Проверка на соответствие положениям Регламента в Комплексе |  |
| 3.1.1 | Соответствует ли представленный документ описанию класса? |  |
| 3.1.2 | Возможно ли подписание ЭП документов данного класса? |  |
| 3.1.3 | Подтверждена ли правомерность использования электронного  документа данного класса в ЮЗЭД в соответствии со списком электронных документов, включенных в альбом электронных  документов? |  |
| 3.1.4 | Соответствует ли время и дата подписания электронного  документа, указанные в системном журнале, времени и дате  подписания электронного документа, указанным в заявке о  разногласиях? |  |
| 3.1.5 | Соответствует ли личность должностного лица, подписавшего документ, информации, указанной в сертификате,  представленном Экспертной комиссии? |  |
| 3.2 | Прочие организационные аспекты |  |
| 3.2.1 | Подтверждена ли правомерность использования копий средств криптографической защиты информации и Комплекса в  соответствии с условиями лицензионных соглашений? |  |
| 3.2.2 | Подтверждена ли корректность использования копий средств  криптографической защиты информации и Комплекса в  соответствии с документацией на используемые программные  и аппаратные средства и аттестатами соответствия? |  |
| 3.2.3 | Правомерно ли подписание электронного документа  Уполномоченным сотрудником Участника на основании  приказов о наделении сотрудника правом подписи  электронных документов определенных классов? |  |
| 3.2.4 | Представлены ли доказательства признания цепочек доверия  на основании договоров на обслуживание сертификатов  ключей ЭП, договоров на оказание услуг УЦ? |  |

Приложение 4

УТВЕРЖДЕН

приказом от 14 декабря 2012 г. №\_\_\_

ПОРЯДОК

предоставления документов из программного комплекса «СКИФ» по запросу контролирующих органов

1. Термины и определения

Термины и определения, используемые в документе:

Квалифицированный сертификат ключа проверки электронной подписи (Сертификат) - сертификат ключа проверки электронной подписи, выданный удостоверяющим центром или доверенным лицом удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ электронной подписи (закрытый ключ, ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Комплекс – программный комплекс «СКИФ», разработанный ОАО «Финтех» (далее – разработчик), предназначенный для автоматизации формирования, приема, передачи, обработки и хранения форм отчетности.

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

Сотрудник - пользователь, имеющий имя и пароль для входа в Комплекс и наделенный полномочиями для работы в Комплексе.

Участник - юридическое лицо, принимающее участие в юридически значимом электронном документообороте.

Усиленная квалифицированная электронная подпись (ЭП) - вид электронной подписи, которая соответствует следующим признакам:

электронная подпись получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

электронная подпись позволяет определить лицо, подписавшее электронный документ;

электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

электронная подпись создается с использованием средств электронной подписи;

ключ проверки электронной подписи указан в Сертификате;

для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

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

Электронный документ – отчет, в котором информация представлена   
в электронной форме в формате Комплекса. Юридическая значимость электронного документа подтверждается ЭП.

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

2. Общие положения

Предоставление документов из Комплекса контролирующим органам происходит в целях осуществления муниципального контроля, в том числе муниципального финансового контроля в соответствии с действующим законодательством.

Настоящий Порядок определяет перечень и формат предоставляемых из Комплекса электронных документов для контролирующих органов при осуществлении ЮЗЭД.

3. Предоставление документов

3.1. Порядок формирования и содержание запроса

Контролирующие органы направляют запрос об истребовании документов Участнику в форме официального запроса, подписанного уполномоченным должностным лицом контролирующего органа.

3.2. Порядок подготовки ответа на запрос:

Подготовка ответа на запрос осуществляется Участниками в рамках своей компетенции.

Непосредственную подготовку ответа осуществляют сотрудники Участника, ответственные за работу с указанными в запросе электронными документами.

Ответ на запрос подписывается должностным лицом Участника и направляется в контролирующие органы. К ответу на запрос, в качестве приложения прикрепляются распечатанные документы или электронные документы, выгруженные из Комплекса, с отпечатанными реквизитами ЭП и Сертификатом должностного лица, подписавшего документ ЭП. До выгрузки документов с реквизитами ЭП ответственный сотрудник сектора информационных технологий Финансово-экономического управления администрации муниципального образования «Пермский муниципальный район» проводит настройку выгрузки ЭП в Комплексе.

4. Выгрузка электронных документов из Комплекса

4.1. Выгрузка электронных документов из Комплекса:

Для того чтобы выгрузить электронный документ из Комплекса, необходимо:

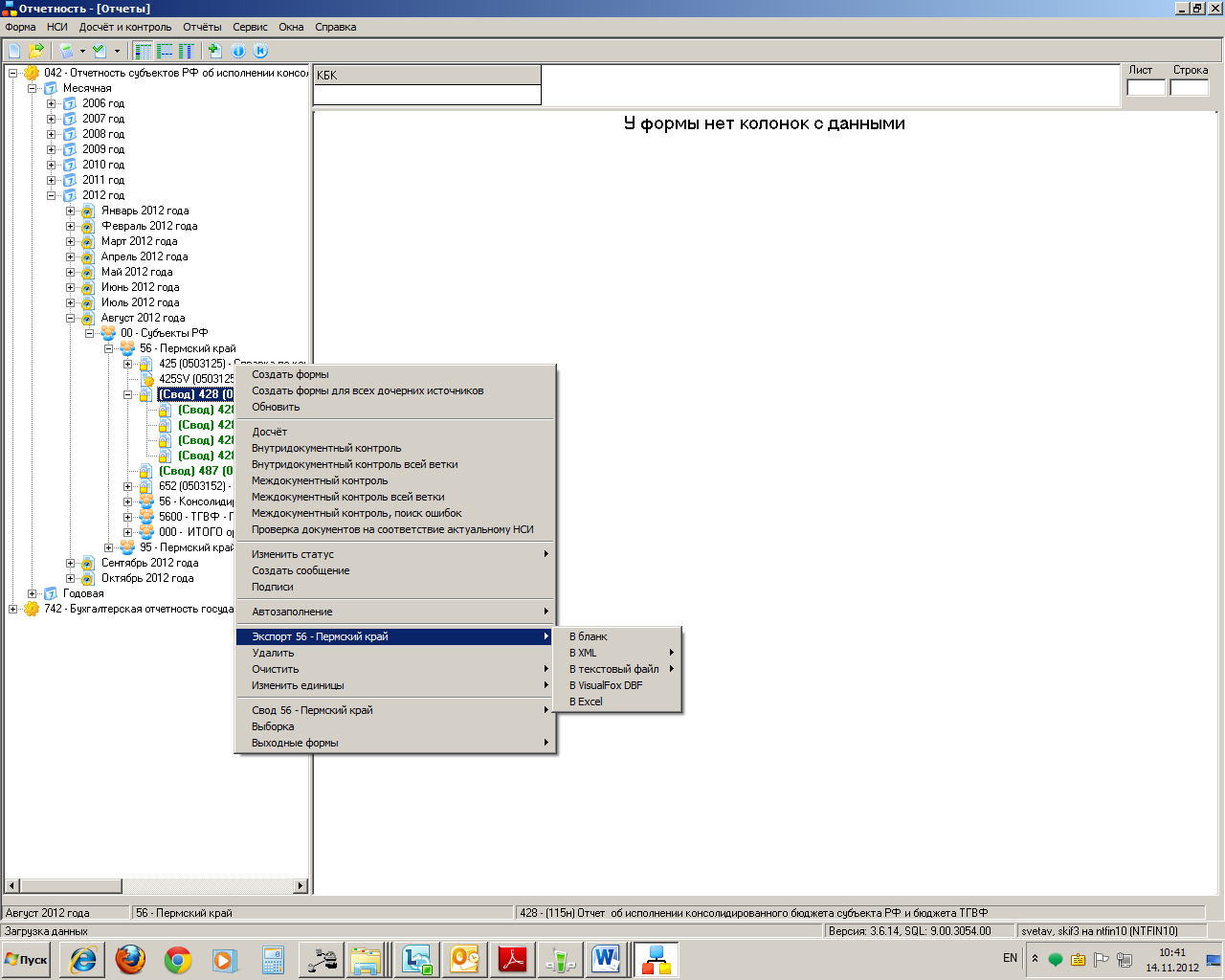
открыть список электронных документов, содержащий искомый документ;

выбрать запрашиваемый электронный документ;

открыть выгружаемый документ на редактирование одним щелчком мыши;

выбрать операцию «Экспорт» и необходимый формат выгрузки (см. рис. 1).

Рис.1



5. Перечень предоставляемых документов

К документам, предоставляемым из Комплекса по запросу контролирующих органов, относятся формы бюджетной отчетности и сводной бухгалтерской отчетности муниципальных бюджетных и автономных учреждений.

Приложение 5

УТВЕРЖДЕН

приказом от 14 декабря 2012 г. №\_\_\_

КАРТА

рисков электронного документооборота

1. Термины и определения

Термины и определения, используемые в документе:

Аккредитованный удостоверяющий центр (УЦ) - юридическое лицо, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (далее - Федеральный закон 63-ФЗ), и получившее аккредитацию.

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального [закона](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ.

Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (журнал поэкземплярного учета СКЗИ) - документ, содержащий данные о выданных уполномоченным сотрудникам ключевых документах.

Квалифицированный сертификат ключа проверки электронной подписи (Сертификат) - сертификат ключа проверки электронной подписи, выданный УЦ или доверенным лицом УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ электронной подписи (закрытый ключ, ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключевой документ - ключевой носитель, содержащий ключ электронной подписи, а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключа электронной подписи.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, и представляет собой коммерческую, служебную или личную тайны, охраняющиеся ее владельцем.

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Роль - совокупность прав сотрудников при работе в Комплексе, с использованием которых они подписывают электронные документы электронной подписью.

Комплекс – программный комплекс «СКИФ», разработанный ОАО «Финтех» (далее – разработчик), предназначенный для автоматизации формирования, приема, передачи, обработки и хранения форм отчетности.

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

Сотрудник - пользователь, имеющий имя и пароль для входа в Комплекс и наделенный полномочиями для работы в Комплексе.

Средства криптографической защиты информации (СКЗИ) - аппаратные и(или) программные средства, обеспечивающие применение электронной подписи (создание, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи) и (или) шифрование при осуществлении электронного документооборота, а также обеспечивающие защиту информации по утвержденным стандартам и сертифицированные в соответствии с действующим законодательством.

Уполномоченный сотрудник - сотрудник, наделенный полномочиями по подписанию электронной подписью электронных документов в соответствии с утвержденным Регламентом, для которого УЦ выпущен сертификат ключа проверки электронной подписи, отмеченный в журнале поэкземплярного учета СКЗИ как получивший ключевой носитель. Уполномоченный сотрудник назначается приказом Участника.

Участник - юридическое лицо, принимающее участие в юридически значимом электронном документообороте.

Усиленная квалифицированная электронная подпись (ЭП) - вид электронной подписи, который соответствует следующим признакам:

электронная подпись получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

электронная подпись позволяет определить лицо, подписавшее электронный документ;

электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

электронная подпись создается с использованием средств электронной подписи;

ключ проверки электронной подписи указан в Сертификате;

для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным [законом](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ.

Цепочка доверия - последовательность взаимосвязанных (доверенных) сертификатов, возникающая при проверке ключа ЭП.

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

Электронный документ – отчет, в котором информация представлена   
в электронной форме в формате Комплекса. Юридическая значимость электронного документа подтверждается ЭП.

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

2. Общие сведения

Настоящий документ предназначен для описания вероятности возникновения рисков и мероприятий по их снижению, а также возможной степени причиненного ущерба.

3. Классификация рисков

Риски, связанные с ведением электронного документооборота в Комплексе, можно разделить по типу: организационные и технические, а также по источнику возникновения: внешние и внутренние.

Классификация рисков представлена в [таблицах 3](#Par700) и [4](#Par818).

4. Вероятность реализации рисков, подверженность

информационных активов 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, оцениваются следующие показатели (значения атрибутов):

вероятность реализации риска;

уровень подверженности информационного актива воздействию (существенность ущерба для Финансово-экономического управления администрации муниципального образования «Пермский муниципальный район»).

Текстовые описания значений атрибутов приведены в [таблицах 1](#Par660) и [2](#Par674).

Таблица 1. Значения атрибута "Вероятность реализации риска"

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

Таблица 2. Значения атрибута "Уровень подверженности информационного актива воздействию"

|  |  |
| --- | --- |
| Уровень подверженности воздействию | Существенность ущерба конфиденциальность/целостность информационного актива) |
| 5 | Серьезные повреждения или полный выход информационного актива из строя (например, видимые снаружи и существенно влияющие на ход производственных процессов, существенно увеличивающие затраты) |
| 4 | Серьезные повреждения, не приводящие к полному выходу информационного актива из строя (например, не видимые снаружи, но существенно влияющие на ход производственных процессов, увеличивающие затраты) |
| 3 | Средние повреждения или ущерб (например, влияющие на  внутренние регламенты, увеличивающие затраты) |
| 2 | Незначительные повреждения или ущерб |
| 1 | Небольшие изменения информационного актива |

Таблица 3. Организационные риски

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N | Тип риска  (внутренний/ внешний) | Описание | Вероятность реализации | Сущест венность ущерба | Меры по снижению |
| 1 | Внутренний/  внешний | Компрометация ключа ЭП путем хищения  носителей/копирования данных | Высокая | 4 | Организация хранения  ключевых носителей и  документов, журналов  поэкземплярного учета  СКЗИ |
| 2 | Внутренний | Нарушение сотрудником  правил использования  СКЗИ | Высокая | 3 | Ознакомление сотрудника  под роспись с пакетом  документации по ЮЗЭД |
| 3 | Внутренний | Увольнение сотрудника,  имевшего доступ к  ключам ЭП | Высокая | 3 | Подача заявления в УЦ на отзыв Сертификата |
| 4 | Внутренний | Отказ от выполнения  должностных  обязанностей со ссылкой на нормы Федерального  [закона](consultantplus://offline/ref=3B533F8C38F7A26A189BB6DEB642D76223EDB122B6A6BB6E722302B2D7V3V7F) 63-ФЗ по части защиты ключа ЭП | Средняя | 4 | Проведение обучения  персонала с показом, что работа в Комплексе при ЮЗЭД  соответствует по защищенности локальному  рабочему месту, т.е. риска компрометации ключа ЭП нет |
| 5 | Внутренний | Несоответствие Комплекса  требованиям Федеральной службы по техническому  и экспортному контролю  по части защиты  информации | Низкая | 5 | Обеспечение доступности  информации об аттестате  соответствия для всех  заинтересованных лиц |
| 6 | Внутренний | Выгрузка в архивное  хранение произведена не полностью и(или) с  нарушением целостности  информации о цепочках  доверия или с  нарушением целостности  документарных томов.  Утрата документов или  их реквизитов в  процессе выгрузки | Высокая | 4 | Исполнение регламента  выгрузки документов на  архивное хранение и  хранения документов в  архиве |
| 7 | Внутренний | Низкая степень  значимости (важности)  Сертификата как документа для уполномоченных сотрудников | Высокая | 4 | Выдавать бумажный  оригинал Сертификата |
| 8 | Внутренний/  внешний | Несанкционированный доступ к техническим  средствам Комплекса  (серверам, рабочим  станциям пользователей  и т.д.) | Средняя | 5 | Организация пропускного  режима в помещения,  размещающие технические  средства системы,  кабинеты, в которых  расположены рабочие  станции пользователей |
| 9 | Внутренний | Отказ от признания  результатов экспертизы  электронного документа  одним из представителей конфликтующих сторон | Высокая | 3 | Разработка порядка  разбора конфликтных  ситуаций, описывающего  действия, находящиеся за пределами установления  авторства подписи |
| 10 | Внутренний | Разрешение конфликтов в суде | Средняя | 5 | Описание досудебного  разбора конфликтов |
| 11 | Внутренний | Длительная остановка  производственного процесса по причине  невозможности  проведения изъятия (выемки) документов  контролирующими органами (ситуация  рассматривается как экстренная для  организации) | Средняя | 5 | Описать порядок  предоставления  документов по запросу  контролирующих органов |
| 12 | Внутренний | Доступ пользователей к не принадлежащим им объектам Комплекса | Высокая | 3 | Использование системы  разграничения прав доступа, настройка ролей пользователей |
| 13 | Внутренний | Сопротивление персонала внедрению и  использованию ЮЗЭД,  неприятие новых методов работы | Высокая | 4 | Каждый этап внедрения  сопровождается  письменными  распоряжениями руководства. Организация обучения  сотрудников |
| 14 | Внутренний | Утечка конфиденциальной информации | Высокая | 5 | Назначение персональной  ответственности  сотрудников |

Таблица 4. Технические риски

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N | Тип риска | Описание | Вероятность реализации | Сущест венность ущерба | Меры по снижению |
| 1 | Внешний | Перехват информации,  передаваемой по каналам связи | Средняя | 4 | Защита протокола  передачи данных между клиентами и веб-серверами путем организации https-доступа к web-серверу, SSL-шифрование трафика между клиентами и веб- серверами |
| 2 | Внешний | Несанкционированный доступ к серверам  Комплекса | Средняя | 5 | Организация VPN-сети;  расположение серверов в DMZ;  ограничение по портам доступа к серверам  приложений Комплекса;  использование  аппаратного брандмауэра |
| 3 | Внутренний | Нарушение целостности  данных баз данных | Высокая | 5 | Резервное копирование  средствами используемых  СУБД (средств управления базами данных) |
| 4 | Внутренний/  внешний | Утечка ключей ЭП с рабочих станций  пользователей | Средняя | 4 | Применение к рабочим  станциям единой политики безопасности |
| 5 | Внешний | Заражение компьютерными вирусами | Средняя | 4 | Организация антивирусной защиты |
| 6 | Внутренний | Нехватка  производственных  мощностей серверов  Комплекса | Низкая | 3 | Анализ планируемой  нагрузки и наращивание  мощностей в случае  необходимости |