|  |  |
| --- | --- |
|  | Приложение 3 |
|  | к Приказу финансового управления администрации Еткульского |
|  | от 14.09. 2023 г. № 24-од |
|  |  |

Положение

о порядке работы со средствами криптографической

защиты информации автоматизированной системе «АЦК-Финансы»

1. Термины и определения, используемые в настоящем положении

Система - автоматизированная система «АЦК-Финансы».

Администратор безопасности информации – сотрудник, на которого возложены обязанности по обеспечению выполнения предусмотренных мер защиты информации в администрации Еткульского муниципального района Челябинской области.

Аккредитованный удостоверяющий центр (далее – УЦ) – удостоверяющий центр, прошедший аккредитацию в соответствии с действующим законодательством.

Квалифицированный сертификат ключа проверки электронной подписи (далее – Сертификат) – электронный документ или документ на бумажном носителе, выданный УЦ или доверенным лицом УЦ либо Федеральным органом исполнительной власти (уполномоченным в сфере использования электронной подписи) и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа.

Ключ электронной подписи (далее – Ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи.

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

Компрометация ключа – утрата доверия к тому, что Ключ используется только конкретным Уполномоченным сотрудником и только по назначению.

Материальный носитель ключевой информации (далее – материальный носитель) – материальный объект, используемый для записи и хранения информации, необходимой для подписания электронных документов ЭП.

Организатор – администрация Еткульского муниципального района Челябинской области, являющаяся организатором ЮЗЭД на базе Системы.

Регламент применения электронной подписи участниками юридически значимого электронного документооборота (далее – Регламент[[1]](#footnote-1)) – утвержденный Организатором документ, определяющий статусы электронных документов, на которых происходит наложение ЭП в электронном документе.

Реестр Системы – справочник Системы, в котором хранится перечень сертификатов Уполномоченных сотрудников Участников.

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

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

Сторона – юридическое лицо, участник ЮЗЭД, заключившее соглашение об обмене электронными документами между финансовым управлением администрацией Еткульского муниципального района и Участником юридически значимого электронного документооборота.

Удостоверяющий центр – юридическое лицо, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

Уполномоченный сотрудник – служащий или сотрудник Участника, наделенный полномочиями, по подписанию ЭП электронных документов в соответствии с утвержденным Регламентом.

Усиленная квалифицированная электронная подпись (далее – ЭП) –электронная подпись, соответствующая требованиям Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи», предъявляемым к электронной подписи данного вида.

Участник – юридическое лицо (Сторона или Организатор), принимающее участие в юридически значимом электронном документообороте на базе Системы.

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

Юридически значимый электронный документооборот(далее – ЮЗЭД) – документооборот, осуществляемый на базе Системы, в котором  электронный документ, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью, при этом Уполномоченные лица совершают  действия по формированию, утверждению (подписанию ЭП), проверке,  принятию к исполнению документов в электронной форме, удостоверенных ЭП, а также иные юридически значимые действия с электронными документами.

2. Общие положения

Настоящее положение регламентирует порядок работы с СКЗИ.

3. Работа с СКЗИ

3.1. При работе с СКЗИ должны соблюдаться требования «Инструкции об организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», утвержденную приказом Федерального агентства правительственной связи и информации (ФАСПИ) при Президенте Российской Федерации от 13.06.2001 г. № 152, иных нормативно – правовых документов финансового управления администрации Еткульского муниципального района и настоящего Положения.

3.2. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, материальные носители подлежат регистрации в соответствующих журналах поэкземплярного учета.

3.3. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, материальные носители, должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

3.4. Хранение инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к СКЗИ, и материальных носителей в запираемых шкафах (ящиках, хранилищах) должно производиться в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.5. Для работы с СКЗИ в ЮЗЭД допускаются только Уполномоченные сотрудники Участников. Уполномоченные сотрудники Участников несут персональную ответственность за сохранность СКЗИ (в том числе хранение в тайне ключей ЭП, неразглашение и нераспространение).

3.6. Внесение Сертификатов Уполномоченных сотрудников Участников в реестр Системы осуществляется Администратором безопасности информации Организатора на основании «Заявления на внесение в реестр системы сертификатов Уполномоченных сотрудников»[[2]](#footnote-2) и копии приказа (распоряжения), определяющего перечень Уполномоченных сотрудника Участника.

3.7. Ответственность за корректность ввода сертификатов Уполномоченных сотрудников Участника в реестр Системы несет Организатор.

3.8. Организатор обеспечивает хранение Сертификатов Уполномоченных сотрудников Участника в течение срока хранения электронного документа.

3.9. Срок действия ключей ЭП и соответствующих Сертификатов определяется УЦ. После окончания срока действия Сертификата Уполномоченный сотрудник Участника теряет право использования ключей ЭП, соответствующих данному Сертификату. Для получения новых ключей Уполномоченный сотрудник Участника должен руководствоваться порядком получения новых ключей, установленным УЦ.

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

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

3.12. Категорически запрещается:

* разглашать содержимое материальных носителей, содержащих ключи ЭП, или передавать сами материальные носители лицам, к ним не допущенным, выводить данные, содержащиеся на материальном носителе, на дисплей и принтер;
* производить несанкционированное копирование носителей ключевой информации;
* вставлять материальный носитель, содержащий ключи ЭП, в дисковод или USB-считыватель компьютера Уполномоченного сотрудника и других лиц при проведении работ, не связанных с эксплуатацией ЮЗЭД;
* записывать на материальный носитель, содержащий ключи ЭП, постороннюю информацию;
* оставлять материальный носитель, содержащий ключи ЭП без присмотра на рабочем месте;
* вносить какие-либо изменения в программное обеспечение СКЗИ;
* использовать бывшие в работе материальные носители (правило не распространяется на носитель типа RuToken и eToken).

Уполномоченный сотрудник Участника несёт ответственность за проведение в полном объёме организационных и технических мероприятий, обеспечивающих соблюдение указанных выше правил.

4. Действия в случае компрометации ключей

4.1. К событиям, связанным с компрометацией ключей, относят следующие:

* утрата материальных носителей, содержащих ключи ЭП;
* потеря материальных носителей, содержащих ключи ЭП, с их последующим обнаружением;
* хищение материальных носителей, содержащих ключи ЭП;
* разглашение содержимого материальных носителей, содержащих ключи ЭП;
* несанкционированное копирование содержимого материальных носителей, содержащих ключи ЭП;
* увольнение сотрудников, имевших доступ к материальным носителям, содержащим ключи ЭП;
* нарушение правил хранения и уничтожения (после окончания срока действия материальных носителей, содержащих ключи ЭП);
* возникновение подозрений на утечку содержимого материальных носителей, содержащих ключи ЭП, или её искажение в Системе;
* нарушение печати на сейфе или замка сейфа, в котором хранятся материальные носители, содержащие ключи ЭП;
* невозможность достоверного установления того, что произошло с материальными носителями (в том числе случаи, когда материальный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошёл в результате несанкционированных действий злоумышленников);
* любые другие виды разглашения содержимого материальных носителей, содержащих ключи ЭП, в результате которых ключи могут стать доступными посторонним лицам и (или) процессам.

4.2. Уполномоченный сотрудник Участника самостоятельно определяет факт компрометации Ключа и оценивает значение этого события. Мероприятия по розыску и локализации последствий компрометации Ключа организует и осуществляет Организатор с участием Уполномоченного сотрудника Участника (владельца скомпрометированного Ключа).

В случае установления факта компрометации Ключа Уполномоченный сотрудник Участника обязан незамедлительно прекратить эксплуатацию ЮЗЭД в Системе и в течение 3-х часов уведомить об этом Организатора, а так же УЦ по телекоммуникационным каналам связи.

В течение 60 (шестидесяти) рабочих минут после поступления сообщения о компрометации Ключа Организатор обеспечивает прекращение использования в ЮЗЭД соответствующего Сертификата Уполномоченного сотрудника.

4.3. Дата и время, с которой Сертификат считается недействительным в Системе, устанавливается равной дате и времени прекращения использования в ЮЗЭД соответствующего Сертификата.

4.4. При получении электронного документа, подписанного скомпрометированным ключом ЭП, данный электронный документ считается недействительным.

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

Для получения новых ключей Уполномоченный сотрудник Участника должен руководствоваться порядком получения новых ключей, установленным УЦ.

1. Приложение 2 к Приказу от 14.09. 2023 г. № 24-од [↑](#footnote-ref-1)
2. Приложение 4 к Приказу от 14.09. 2023 г. № 24-од. [↑](#footnote-ref-2)