**П**

**Приложение № 4**

к Распоряжению Комитета финансов администрации

Кировского муниципального района

 Ленинградской области

№ 21 от «26» марта 2019 г.

**Положение о порядке работы**

**со средствами криптографической защиты информации**

**в автоматизированной системе «АЦК-Финансы»**

**Комитета финансов администрации Кировского**

 **муниципального района Ленинградской области**

1. **Термины и определения, используемые в настоящем положении**

Термины и определения, используемые в настоящем Порядке, перечислены

в Приложении № 1 к распоряжению Комитета финансов администрации Кировского муниципального района Ленинградской области от 26.03.2019г №21.

**2. Общие положения**

Настоящее положение регламентирует работу с СКЗИ в части относящейся к использованию ЭП и СЭП при осуществлении ЮЗЭД в Системе.

**3. Работа с СКЗИ**

3.1. При работе с материальными носителями должны соблюдаться требования «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13.06.2001 г. № 152, муниципальных нормативных правовых актов Комитета финансов администрации Кировского муниципального района Ленинградской области и настоящего Положения.

3.2. 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).

3.3. Внесение Сертификатов Уполномоченных сотрудников Участников в реестр Системы осуществляется Администратором безопасности информации Организатора на основании «Заявления на внесение в реестр системы сертификатов Уполномоченных сотрудников[[1]](#footnote-1)».

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

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

3.6. 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.

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

3.8. 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.

3.9. 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.

3.10. 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 уведомить Организатора, а так же УЦ по телекоммуникационным каналам связи.

В максимально короткие сроки, но не более 1 рабочего часа 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 № 5 к Распоряжению № 21 от «26» марта 2019 г. [↑](#footnote-ref-1)