П-145/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся
Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей
Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«29» октября 2019г.

Приказ № 522 о/д от 29.10.2019

Инструкция
по обращению со средствами криптографической защиты информации

1. Общие положения

1.1. Средство криптографической защиты информации (далее – СКЗИ) предназначено для подписания электронных документов и сообщений ЭЦП с целью подтверждения подлинности информации, ее авторства и шифрования этих документов при передаче по открытым каналам связи для обеспечения конфиденциальности.

1.2. ЭЦП может использоваться только для защиты информации в соответствии со сведениями, указанными в сертификате ключа ЭЦП.

1.3. Указанные СКЗИ должны использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

1.4. Данные Правила не исключают выполнения требований и рекомендаций эксплуатационно-технической документации на используемые СКЗИ.

2. Работа с СКЗИ

2.1. Для работы с СКЗИ привлекаются уполномоченные лица, назначенные соответствующим приказом ректора. Должностные лица, уполномоченные эксплуатировать СКЗИ, получать и использовать ключи ЭЦП обязаны:

2.1.1. Не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах.

2.1.2. Сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями.

2.1.3. Соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ.

2.1.4. Сообщать в орган криптозащиты, организации выдавшей ЭЦП (далее — ОКЗ) о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним.

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

2.1.6. Немедленно уведомлять ОКЗ 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.

2.2. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях уполномоченных лиц должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

Техническое обслуживание такого оборудования и смена криптоключей осуществляются при отсутствии лиц, не допущенных к работе с данными СКЗИ. На время отсутствия уполномоченных лиц указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае, в учреждении должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

2.3. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых дискет, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы.

2.4. Пользователь несет ответственность за то, что на компьютере, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование программных СКЗИ. На рабочем месте, где установлено СКЗИ программное обеспечение должно быть лицензионным.

2.5. При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

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

2.7. Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведут органы криптографической защиты и обладатели конфиденциальной информации.

2.8. Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

2.9. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета.

2.10. Такая передача между пользователями СКЗИ должна быть санкционирована соответствующим органом криптографической защиты.

2.11. Обладатель конфиденциальной информации с согласия органа криптографической защиты может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета.

2.12. Уполномоченным лицам не допускается:

2.12.1. Разглашать конфиденциальную информацию, к которой был допущен Пользователь.

2.12.2. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным.

2.12.3. Выводить ключевую информацию на дисплей и принтер.

2.12.4. Вставлять ключевой носитель в дисковод ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в дисководы других ПЭВМ.

2.12.5. Записывать на ключевом носителе постороннюю информацию.

2.12.6. Вносить какие-либо изменения в программное обеспечение СКЗИ.

2.12.1. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

3. Действия в случае компрометации ключей

3.1. Под компрометацией криптоключей понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

3.2. К компрометации ключей относятся следующие события:

3.2.1. Утрата носителей ключа.

3.2.2. Утрата иных носителей ключа с последующим обнаружением.

3.2.3. Увольнение работников, имевших доступ к ключевой информации.

3.2.4. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.

3.2.5. Нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов.

3.2.6. Утрата ключей от сейфов в момент нахождения в них носителей ключевой информации.

3.2.7. Утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением.

3.2.8. Доступ посторонних лиц к ключевой информации.

3.2.9. Другие события утери доверия к ключевой документации.

3.3. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

3.4. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать руководству.

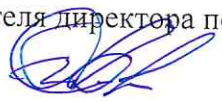
3.5. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.6. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации.

Действующие и резервные ключевые документы, предназначенные для применения

в случае компрометации действующих криптоключей, должны храниться во внутреннем отсеке сейфа в различных конвертах.

Разработчик:
заместителя директора по общим вопросам



_____/ Ю.Ю. Алексеев /

Лист
ознакомления с «Инструкцией по обращению со средствами криптографической защиты информации»

№ п/п	ФИО	Должность	Подпись, дата