



Министерство образования и молодежной политики
Свердловской области

Государственное автономное профессиональное образовательное учреждение
Свердловской области

«Екатеринбургский техникум химического машиностроения»

Инструкция пользователя СКЗИ

Рассмотрено
на заседании Совета
ГАПОУ СО «ЕТХМ»
Протокол № 3,
от « 31 » января 2020 г.

№ 24 - о/д от « 03 » февраля 2020 г.



**ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ
ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) В ГОСУДАРСТВЕННОМ
АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ
УЧРЕЖДЕНИИ СВЕРДЛОВСКОЙ ОБЛАСТИ
«ЕКАТЕРИНБУРГСКИЙ ТЕХНИКУМ ХИМИЧЕСКОГО
МАШИНОСТРОЕНИЯ»**

Екатеринбург
2020 г.

Введено в действие с 03.02.2020 г.

1. Общие положения

1.1. Настоящая Инструкция разработана на основании:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказа ФАПСИ от 13.06.2001 № 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».

1.2. Инструкция определяет основные обязанности, права и ответственность пользователя средств криптографической защиты информации (далее - пользователь, СКЗИ).

1.3. Пользователями СКЗИ являются сотрудники образовательной организации, в силу своих функциональных обязанностей участвующие в процессах работы со средствами криптографической защиты информации, из числа которых приказом руководителя образовательной организации назначается ответственное лицо.

1.4. Допуск пользователей к работе со СКЗИ осуществляется по приказу руководителя образовательной организации только после соответствующего обучения.

1.5. Организация обучения и контроль допуска пользователей к СКЗИ возлагаются на ответственное лицо.

1.6. К обучению пользователей с санкции руководителя образовательной организации могут быть привлечены сторонние лица и организации на основании договоров об оказании услуг.

1.7. Перед началом работ пользователь/ответственное лицо обязан изучить настоящую Инструкцию и ознакомиться с ответственностью за выполнение требований Инструкции по организации хранения, учета и использования СКЗИ под подпись.

1.8. В своей деятельности пользователь/ответственное лицо руководствуется настоящей Инструкцией, Инструкцией по порядку использования и организации работы со средствами криптографической защиты информации и действующим законодательством в сфере защиты конфиденциальной информации.

1.9. Пользователь/ответственное лицо несёт персональную ответственность за выполнение настоящей Инструкции в установленном законом порядке.

2. Организация работы

2.1. Помещения, в которых установлены СКЗИ и/или хранятся криптографические ключи (далее - спецпомещения), должны исключать возможность неконтролируемого доступа и использования СКЗИ посторонними лицами, а также наблюдения посторонними лицами за проходящими в спецпомещениях работами.

2.2. В спецпомещениях устанавливаются надежно запираемые шкафы/ячейки, оборудованные приспособлениями для опечатывания.

2.3. Каждому пользователю выделяется индивидуальный шкаф/ячейка, ключ и средство опечатывания.

2.4. Резервные ключи от индивидуальных шкафов/ячеек передаются ответственному лицу.

2.5. Ключи и средства опечатывания хранятся в условиях, исключающих доступ посторонних лиц.

3. Обязанности пользователя

Пользователь обязан:

3.1. Соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ, руководствуясь Инструкцией по порядку использования и организации работы со средствами криптографической защиты информации.

3.2. Выполнять криптографические операции используя только действующие криптографические ключи.

3.3. Незамедлительно сообщать о фактах утраты СКЗИ, криптографических ключей, 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.

3.4. Периодически проверять сохранность оборудования и целостность печатей на оборудовании.

3.5. При выявлении нарушений сохранности оборудования, целостности печатей/пломб, сбоев или отказов в работе программно-аппаратного обеспечения незамедлительно сообщить ответственному лицу и предоставить ему носители криптографических ключей для проверки их работоспособности.

3.6. Сообщать ответственному лицу о попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним.

3.7. Сдать установочный комплект СКЗИ, эксплуатационную и

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

Пользователю запрещается:

3.8. Производить несанкционированное копирование ключевых документов и ключевых носителей.

3.9. Знакомить посторонних с ключевыми документами, или передавать указанные документы лицам, не имеющим соответствующего допуска.

3.10. Оставлять носители ключевой информации без присмотра на рабочем месте.

3.11. Оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации.

3.12. Записывать на носители ключевой информации посторонние файлы.

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

3.14. Вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя и/или в устройство, не предназначенной для работы с ключевыми носителями.

3.15. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

4. Обязанности ответственного лица

Ответственное лицо обязано:

4.1. Обеспечивать конфиденциальность всей информации ограниченного распространения, в том числе сведения о криптографических ключах.

4.2. Не допускать снятия копий с ключевых документов, записи посторонней информации на ключевой носитель.

4.3. Получать от пользователей носители ключевой информации при их длительном отсутствии, увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

4.4. Получать от пользователей носители ключевой информации по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

4.5. Вести поэкземплярный учет СКЗИ и криптографических ключей в специальном журнале учета/реестре образовательной организации установленной формы.

4.6. Контролировать соблюдение правил хранения криптографических ключей, ключей от помещений, хранилищ, личных печатей.

4.7. Контролировать соблюдение правил работы со СКЗИ и криптографическими ключами.

4.8. Обеспечивать соответствие спецпомещений изложенным выше требованиям.

4.9. Организовывать и контролировать обучение пользователей.

4.10. Проводить расследования по факту недостачи или утраты СКЗИ, криптографических ключей, ключей от помещений, хранилищ, личных печатей и в других случаях, которые могут привести к разглашению защищаемой информации.

4.11. Останавливать работу пользователей в случаях обнаружения неисправностей программно-аппаратного обеспечения, правил работы со СКЗИ и криптографическими ключами.

Ответственному лицу запрещается:

4.12. Осуществлять несанкционированное копирование криптографических ключей.

4.13. Допускать использование ключевых носителей на других рабочих местах или для использования в целях, не относящихся к работе.

4.14. Допускать хранение ключевых носителей вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

4.15. Допускать передачу ключевых носителей каким лицам, не имеющим соответствующих прав.

4.16. Допускать использование в спецпомещениях личных технических средств, позволяющих осуществлять копирование ключевой информации.

4.17. Допускать разглашение содержимого ключевых носителей и вывод ключевой информации на дисплей или принтер.

4.18. Допускать использование носителей криптографических ключей на устройствах считывания в режимах, не предусмотренных штатным режимом работы СКЗИ.

4.19. Вносить какие-либо изменения в программно-аппаратное обеспечение СКЗИ.

4.20. Допускать к работе со СКЗИ и криптографическими ключами пользователей, не прошедших специальное обучение.

4.21. Допускать в спецпомещения лиц, не имеющих соответствующих прав.

5. Права пользователя

Пользователь имеет право:

5.1. Осуществлять доступ к программно-аппаратному обеспечению СКЗИ, индивидуальному шкафу/ячейке в пределах предоставленных

полномочий и в соответствии с закрепленными за ним обязанностями.

5.2. Хранить выданные ему носители ключевой информации, ключи и средства опечатывания индивидуального шкафа/ячейки с соблюдением условий, исключающих доступ посторонних лиц.

5.3. Обращаться к техническим специалистам, ответственному лицу и руководству образовательной организации за необходимой технической и методической помощью.

5.4. Участвовать в анализе ситуаций, касающихся функционирования закрепленных за ним СКЗИ.

5.5. Знакомиться с проектами решений руководства организации, касающимися его деятельности.

5.6. Вносить на рассмотрение руководства предложения по совершенствованию работы СКЗИ.

6. Права ответственного лица

Ответственное лицо имеет право:

6.1. Требовать от сотрудников ГАПОУ СО «ЕТХМ» выполнения положений действующего законодательства и локальных нормативных актов по обеспечению информационной безопасности.

6.2. Требовать от пользователей своевременного информирования о возникновении сбоев в работе СКЗИ и/или инцидентов, связанных с нарушением правил доступа и правил работы со СКЗИ и криптографическими ключами.

6.3. Давать пользователям обязательные для выполнения указания по работе со СКЗИ и криптографическими ключами.

6.4. Хранить дистрибутивы СКЗИ, эксплуатационную и техническую документацию к СКЗИ, инструкции, учебные материалы, резервные копии ключей от индивидуальных шкафов/ячеек пользователей.

6.5. Принимать на хранение ключевые носители, ключи и средства опечатывания индивидуальных шкафов/ячеек пользователей.

6.6. Инициировать и проводить служебные расследования:

- по фактам нарушения установленных требований работы со СКЗИ и криптографическими ключами, правил эксплуатации технических средств, правил работы в спецпомещениях;

- в случаях компрометации/подозрения на компрометацию криптографических ключей.

6.7. С санкции руководителя образовательной организации привлекать сотрудников к проведению плановых и внеочередных работ по обеспечению требований настоящей Инструкции и Инструкции по порядку использования и организации работы со средствами криптографической защиты информации, установке и модернизации программных и аппаратных средств.

6.8. Вести переписку со сторонними организациями по вопросам, входящим в его компетенцию.

6.9. Участвовать в анализе ситуаций, касающихся функционирования СКЗИ.

6.10. Знакомиться с проектами решений руководства организации, касающимися его деятельности.

6.11. Вносить на рассмотрение руководства предложения по совершенствованию работы СКЗИ.

7. Ответственность

Пользователи несут ответственность:

7.1. За неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, - в пределах, определенных действующим трудовым законодательством Российской Федерации;

7.2. За причинение материального ущерба работодателю - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации;

7.3. За правонарушения, совершенные в процессе осуществления своей деятельности, - в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

Разработал:

Заместитель директора по УПР

Н.В. Катанэ