

ИНСТРУКЦИЯ
ответственного пользователя средств
криптографической защиты информации
государственного бюджетного профессионального
образовательного учреждения Краснодарского края
«Успенский техникум механизации и
профессиональных технологий»

1. Общие положения

1.1. Ответственный пользователь средств криптографической защиты информации (далее - СКЗИ) обладает функциональной ролью (определенным набором функций, требований, прав и обязанностей), назначаемой работником государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация).

1.2. Ответственный пользователь СКЗИ назначается приказом директора образовательной организации.

1.3. На время отсутствия ответственного пользователя СКЗИ (отпуск, болезнь, прочее) его обязанности исполняет лицо, назначенное в установленном порядке приказом директора образовательной организации. Данное ответственное лицо наделяется правами и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.4. Ответственный пользователь СКЗИ в своей работе руководствуется следующими нормативными правовыми актами и организационно-распорядительными документами в области обработки и защиты информации:

1.4.1 инструкцией 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 Федерального агентства правительственной связи и информации Российской Федерации (далее – ФАПСИ) от 13 июня 2001 г. № 152;

1.4.2 приказом Федеральной службы безопасности Российской Федерации (далее – ФСБ России) от 10 июля 2014 г. № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

1.4.3 положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66;

1.4.4 методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденными руководством 8 Центра ФСБ России от 31 марта 2015 г. № 149/7/2/6-432;

1.4.5 политикой использования средств криптографической защиты информации в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – Политика СКЗИ образовательной организации);

1.4.6 настоящей инструкцией ответственного пользователя средств криптографической защиты информации государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – Инструкция);

1.4.7 иными организационно-распорядительными документами, правовыми актами образовательной организации.

1.5. Иные должностные лица образовательной организации по мере необходимости могут быть ознакомлены с основными положениями настоящей Инструкции.

1.6. В случае увольнения, ответственный пользователь СКЗИ обязан передать директору все СКЗИ, эксплуатационную и техническую документации к ним, ключевые документы, ключи от помещений и хранилищ, которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы.

2. Обязанности в части учета и хранения средств криптографической защиты информации эксплуатационной и технической документации к ним, а также ключевых документов

2.1. Ответственный пользователь СКЗИ в части учета и хранения средств криптографической защиты информации эксплуатационной и технической документации к ним, а также ключевых документов, должен руководствоваться пунктом 3 Политики СКЗИ Техникума и обязан:

2.1.1 вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, а также ключевых документов, в соответствии с утвержденной Формой поэкземплярного учета;

2.1.2 выдавать пользователям экземпляры СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы исключительно под расписку в журнале поэкземплярного учета;

2.1.3 вести аппаратный журнал, в котором учитываются криптоключи, которые вводят и хранят в СКЗИ на весь срок их действия (а также разовые криптоключи) – например, сохраненный в реестре сертификат электронной подписи или набор ключей (dst-файл), который используется для первичной инициализации СКЗИ;

2.1.4 вести журнал учета хранилищ СКЗИ и ключей от них;

2.1.5 хранить дистрибутивы СКЗИ, эксплуатационную и техническую документацию к ним с соблюдением условий, исключающих несанкционированный доступ к ним;

2.1.6 обеспечить безопасное раздельное хранение действующей и резервной ключевой информации;

2.1.7 передавать СКЗИ и криптографические ключи в соответствии с требованиями, установленными Политикой СКЗИ образовательной организации.

3. Обязанности в части использования СКЗИ

3.1. Ответственный пользователь СКЗИ в части использования средств криптографической защиты информации обязан:

3.1.1 обеспечивать размещение средств криптографической защиты информации строго в соответствии с требованиями Политики СКЗИ образовательной организации;

3.1.2 производить опечатывание/опломбирование программно-аппаратных средств криптографической защиты информации и установку пароля для входа в базовую систему ввода-вывода (BIOS) (при наличии технической возможности), а также следить за сохранностью защитных печатей (пломб);

3.1.3 производить периодический контроль сохранности СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок;

3.1.4 при подозрении о возможности компрометации ключевой информации оперативно осуществлять процедуру смены ключей (в соответствии с установленным порядком);

3.1.5 перед передачей АРМ, на котором установлено программное средство криптографической защиты информации, в ремонт – обеспечить удаление ключевой информации с данного АРМ или изъятие жестких дисков;

3.1.6 при организации и обеспечении работы с СКЗИ и криптографическими ключами руководствоваться формулярами к соответствующим СКЗИ;

3.1.7 участвовать в служебных проверках по фактам нарушения требований по обращению с СКЗИ.

4. Порядок действий при компрометации криптоключей

4.1. При получении сообщения о компрометации ключа пользователя, ответственный пользователь СКЗИ ответным звонком уточняет факт

компрометации, и в случае его подтверждения немедленно приостанавливает действие ключа. При наличии резервных ключей, пользователь должен перейти на комплект резервных ключей. Если резервные ключи не были предусмотрены, для восстановления системы необходимо повторно произвести формирование ключа и обеспечить получение новых криптоключей пользователями системы.

5. Обязанности в части уничтожения СКЗИ

5.1. Ответственный пользователь СКЗИ в части уничтожения криптографических ключей должен руководствоваться Политикой СКЗИ образовательной организации и обязан:

5.1.1 участвовать в качестве члена комиссии от образовательной организации при уничтожении СКЗИ;

5.1.2 производить отметки об уничтожении СКЗИ в журнале поэкземплярного учета и техническом (аппаратном) журнале;

5.1.3 обеспечить сохранность Актов об уничтожении СКЗИ.

6. Взаимодействие с прочими ответственными лицами

6.1. Ответственный пользователь СКЗИ должен взаимодействовать со следующими ответственными лицами:

6.1.1. Со всеми пользователями СКЗИ образовательной организации в ходе разъяснения им возникающих вопросов по функционированию СКЗИ и порядка работы с ними;

6.1.2. С администратором информационных систем и администратором информационной безопасности при:

6.1.2.1 согласовании процессов установки средства криптографической защиты информации;

6.1.2.1 оказании помощи в выполнении ими своих служебных обязанностей;

6.1.3. С органом криптографической защиты информации (далее – ОКЗИ) при:

6.1.3.1 инструктаже пользователей СКЗИ;

6.1.3.2 проведении ОКЗИ проверки возможности допуска пользователей к самостоятельной работе с СКЗИ;

6.1.3.3 проведении ОКЗИ проверки о возможности эксплуатации СКЗИ;

6.1.3.4 разработки мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ;

6.1.3.5 расследовании и составлении заключений по фактам нарушения условий использования СКЗИ;

6.1.3.6 выполнении ОКЗИ иных работ по заключенному государственному контракту.

7. Права ответственного пользователя СКЗИ

7.1. Ответственный пользователь СКЗИ имеет право:

7.1.1 требовать от пользователей СКЗИ безусловного выполнения требований Политики СКЗИ образовательной организации;

7.1.2 требовать от пользователей СКЗИ представления письменных объяснений по фактам нарушений требований Политики СКЗИ образовательной организации;

7.1.3 вносить обоснованные предложения о привлечении к ответственности пользователей СКЗИ, допустивших нарушение установленных требований Политики СКЗИ образовательной организации;

7.1.4 требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав;

7.1.5 в рамках своих функциональных обязанностей инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности;

7.1.6 осуществлять плановые и внеплановые проверки пользователей СКЗИ, наличия ключевых документов и технической документации у пользователей (если таковые выдавались);

7.1.7 осуществлять, в рамках своей компетенции, взаимодействие с администратором информационной безопасности и администратором информационных систем;

7.1.8 осуществлять плановые и внеплановые проверки функционирования СКЗИ;

7.1.9 осуществлять, в рамках своей компетенции, взаимодействие с организациями-производителями СКЗИ;

7.1.10 при изменении состава СКЗИ получить профессиональную переподготовку, повышение квалификации и стажировку в порядке, установленном законодательством Российской Федерации.

8. Ответственность ответственного пользователя СКЗИ

8.1. Ответственный пользователь СКЗИ несет ответственность за:

8.1.1 ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, другими регламентирующими документами в соответствии с действующим законодательством Российской Федерации, трудовым законодательством Российской Федерации;

8.1.2 нарушение требований Политики СКЗИ образовательной организации;

8.1.3 за полноту и качество проводимых им работ по обеспечению функционирования СКЗИ, находящихся в зоне его ответственности;

8.1.4 правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

8.1.5 разглашение сведений конфиденциального характера и другой

защищаемой информации Техникума, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

С инструкцией ознакомлен:

Должность

ФИО