СОГЛАСОВАНО:
На заседании Управляющего Совета
ГБОУ школа-интернат №2 г.о.Жигулевск
Протокол №_3__ от «_26_» _03__ 2024г.

УТВЕРЖДАЮ:
Приказ №296 от 03.04.2024г.

Директор ГБОУ школа-интернат №2 г.о.Жигулевск

_____А.Р. Будинец

ЭП

C=RU, O=ГБОУ ШКОЛА-ИНТЕРНАТ №2, CN=Андрей Романович Будинец, E=so_cu_gscou2zhg@samara.edu.ru
00a520f8c4e7a66a33
2024.04.03 16:08:53+04'00'

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты

государственного бюджетного общеобразовательного учреждения Самарской области «Школы-интерната № 2 для обучающихся с ограниченными возможностями здоровья городского округа Жигулевск»

Жигулевск, 2024г.

1. Общие положения

1.1. Положение разработано в целях организации и проведении работ по обеспечению безопасности конфиденциальной информации с использованием средств криптографической защиты в государственном бюджетном общеобразовательном учреждении Самарской области «школа-интернат №2 для обучающихся с ограниченными возможностями здоровья городского округа Жигулевск» (далее – школа-интернат).

1.2. Настоящее положение разработано для практического применения пользователями средств криптографической защиты информации (далее - СКЗИ) в школе-интернате на основании приказа ФАПСИ РФ 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», утвержденных руководством 8 Центра ФСБ России 21.02.2008 №149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»», приказа ФСБ России от 10.07.2014 №378 «Об утверждении Состава 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».

1.3. В школе-интернате определяются должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

1.4. В школе-интернате разрабатываются нормативные и распорядительные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ.

2. Термины и определения

В настоящем положении применены следующие термины с соответствующими определениями:

- ***Средства криптографической защиты конфиденциальной информации,*** сертифицированные ФСБ, именуются - СКЗИ. К СКЗИ относятся криптографические алгоритмы преобразования информации, программные средства, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи включая СКЗИ, защиту от несанкционированного доступа к информации и навязывания ложной информации, включая средства имитозащиты и «электронной подписи».
- ***Пользователи СКЗИ*** - физические и юридические лица, непосредственно допущенные к работе с СКЗИ.
- ***Криптографический ключ (криптоключ)*** - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.
- ***Ключевая информация*** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.
- ***Ключевой носитель*** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.
- ***Ключевой документ*** - физический носитель определенной

структуры, содержащий ключевую информацию, а при необходимости - контрольную, служебную и технологическую информацию.

- ***Компрометация криптоключей*** - хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

3. Порядок обращения с конфиденциальной информацией

3.1. При работе с конфиденциальной информацией сотрудники, допущенные к самостоятельной работе с СКЗИ, обязаны соблюдать следующие правила:

- информация, полученная сотрудниками при регистрации пользователя, является конфиденциальной и не подлежит разглашению третьим лицам;
- конфиденциальная информация, полученная сотрудниками, в результате выполнения должностных обязанностей в процессе работы с СКЗИ, должна сохраняться в тайне;
- содержание закрытых ключей СКЗИ и ключевых документов должно сохраняться в тайне;
- носители ключевой информации, ключевые документы и инсталлирующие СКЗИ носители должны храниться в шкафах (ящиках, хранилищах) индивидуального пользования, учтённых в соответствующем журнале учета сейфов, металлических шкафов, спецхранилищ и ключей от них в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.2. Не допускается:

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер; вставлять ключевой носитель в 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;

- записывать на ключевом носителе постороннюю информацию; вносить какие-либо изменения в программное обеспечение СКЗИ и ключевую информацию; модифицировать содержимое ключевых носителей; использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования; снимать несанкционированные копии с ключевых носителей; знакомить кого-либо с содержанием ключевых носителей или передавать кому-либо ключевые носители.

4. Требования по размещению СКЗИ и режиму охраны

4.1. Помещения, в которых размещаются программно-технические средства со встроенными СКЗИ, являются спецпомещениями и должны обеспечивать конфиденциальность проводимых работ.

4.2. Размещение спецпомещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

4.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

4.4. Входные двери спецпомещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

4.5. Окна и двери спецпомещений, как правило, оборудуются охранной

сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

4.6. Размещение технических средств в спецпомещениях должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отображается, через окна.

4.7. Системные блоки ПЭВМ с СКЗИ оборудуются средствами контроля вскрытия (опломбируются).

4.8. Ремонт и/или последующее использование системных блоков не в целях применения СКЗИ осуществляется после удаления с них программного обеспечения СКЗИ.

5. Требования по обеспечению безопасности СКЗИ и ключевой информации

5.1. Ключевые и инсталляционные носители с программным обеспечением СКЗИ берутся на поэкземплярный учет в выделенных для этих целей журналах поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. Учет и хранение ключевых носителей поручается ответственному за эксплуатацию СКЗИ. Для хранения ключевых носителей выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.

5.2. Хранение ключевых и инсталляционных носителей с ПО СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

5.3. Рабочие (актуальные) и резервные ключевые носители хранятся раздельно, с обеспечением условия невозможности их одновременной компрометации.

6. Порядок допуска к самостоятельной работе с СКЗИ

6.1. К самостоятельной работе с СКЗИ допускаются лица, принятые на работу в школу-интернат в соответствии с приказом директора на основании заключенных с ними трудовых договоров и назначенные на должности, выполнение обязанностей по которым связано с изготовлением, хранением и использованием СКЗИ.

6.2. Сотрудники допускаются к самостоятельной работе с СКЗИ после их специальной подготовки (обучения) по утвержденным программам по правилам работы с СКЗИ, не содержащей сведений, составляющих государственную тайну и сдачи зачета на допуск к самостоятельной работе с СКЗИ. Документом, подтверждающим должную специальную подготовку допускаемого и возможность его допуска к самостоятельной работе с СКЗИ является заключение к самостоятельной работе с СКЗИ, составленное комиссией школы-интерната, на основании принятого зачета по программе подготовки (обучения).

6.3. Программа подготовки к самостоятельной работе с СКЗИ содержит:

- ознакомление с нормами действующего законодательства Российской Федерации, регулирующими отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; защите информации, прав субъектов, участвующих в информационных процессах и информатизации; использовании электронной подписи в электронных документах; ответственности за нарушение указанных норм;
- ознакомление с нормативными актами органов государственного управления Российской Федерации, определяющими порядок разработки, производства, реализации, использования СКЗИ; регламентирующими вопросы взаимодействия участников информационного обмена с

использованием СКЗИ; изучение должностных инструкций, положений о структурных подразделениях, других локальных нормативных актов министерства по вопросам производственной деятельности, связанной с хранением и использованием СКЗИ; изучение эксплуатационно-технической документации на СКЗИ; приобретение практических навыков выполнения работ, предусмотренных обязанностями по занимаемой должности.

6.4. Методика подготовки к сдаче зачета на допуск к самостоятельной работе с СКЗИ должна предусматривать формы самостоятельного изучения и освоения программного материала сотрудником.

Пользователи, допущенные к работе с СКЗИ, регистрируются в журнале учета обучения пользователей СКЗИ.