УТВЕРЖДАЮ
Директор МАОУ СОШ № 31
_____ Е.В. Иванова
« 22» сентября 2023г.

Инструкция
по обеспечению безопасности эксплуатации сертифицированных средств криптографической защиты информации (СКЗИ)

1. Общие положения.

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ в муниципальном автономном общеобразовательном учреждении города Калининграда средней общеобразовательной школы № 31 (далее – МАОУ СОШ № 31).

1.2. Настоящая Инструкция разработана на основе законодательства Российской Федерации, а также:

- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 9 февраля 2005 г. № 66;
- 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 июня 2001 г. № 152.

1.3. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом №____ от «___»_____202_г. назначен Ответственный за организацию эксплуатации и обеспечения безопасности СКЗИ (далее по тексту – Ответственный за эксплуатацию).

1.4. Ответственный за эксплуатацию СКЗИ осуществляет:

- поэкземплярный учет предоставленных пользователю СКЗИ, эксплуатационной и технической документации к ним;
- контроль над соблюдением условий использования СКЗИ;
- расследования и составления заключения по фактам нарушения условий использования СКЗИ;
- разработку и принятия мер по предотвращению возможных последствий таких нарушений.

1.5. Ответственные пользователи СКЗИ (далее по тексту – Пользователи) назначаются приказом по МАОУ СОШ № 31.

1.6. Пользователь СКЗИ обязан:

- не разглашать конфиденциальную информацию, к которой допущен, в том числе сведения о криптографических ключах;
- соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ;
- незамедлительно уведомлять Ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи 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.

1.7. Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения.

1.8. Обучение Пользователей правилам работы с СКЗИ осуществляет Ответственный за эксплуатацию СКЗИ ***или с помощью привлечения сторонних организаций, имеющих соответствующие лицензии.***

1.9. Текущий контроль, обеспечение безопасного функционирования СКЗИ возлагается на Ответственного за эксплуатацию СКЗИ.

1.10. Ответственный за эксплуатацию СКЗИ и Пользователи СКЗИ должны быть ознакомлены с настоящей Инструкцией под роспись.

достоверность дистрибутива СКЗИ;

- На ПЭВМ не должны устанавливаться средства разработки ПО и отладчики;
- После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения в соответствии с документацией;

3.9. Программное обеспечение, устанавливаемое на ПЭВМ с СКЗИ не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

3.10. При организации работ по защите информации от НСД необходимо учитывать следующие требования:

- необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:
- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 года.

3.11. Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

3.12. Средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

3.13. Администратор информационной безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии ОС;
- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;
- на ПЭВМ должна быть установлена только одна операционная система;
- правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т. п.);
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

3.14. Необходимо предусмотреть меры, максимально ограничивающие доступ к

- работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- изменять настройки, установленные программой установки СКЗИ или администратором;
- использовать синхропосылки, вырабатываемые не средствами СКЗИ;
- обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ;
- осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

4. Изготовление и плановая смена криптографических ключей.

4.1. При формировании закрытого криптографического ключа одновременно выполняется формирование открытого ключа, который передается в электронной форме в Удостоверяющий центр в виде запроса на сертификат.

4.2. Удостоверяющий центр формирует Пользователю сертификат в соответствии с Регламентом Удостоверяющего центра, который Пользователь получает в электронном и бумажном виде.

4.3. Плановую смену криптографических ключей следует проводить не менее, чем за две недели до истечения срока действия сертификата (и соответствующего закрытого ключа) Пользователя.

4.4. Переход на новые криптографические ключи и установку новых сертификатов Пользователь выполняет самостоятельно, в соответствии с эксплуатационной документацией на СКЗИ.

5. Действия при компрометации криптографических ключей.

5.1. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

5.2. В случае возникновения обстоятельств, указанных в п.5.1 настоящей Инструкции, Пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации Ответственному за эксплуатацию СКЗИ.

5.3. Смена криптографических ключей проводится в соответствии с соответствующими положениями Регламента Удостоверяющего центра.

5.4. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

5.5. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в Разделе 6 настоящей Инструкции.

Приложение № 1

Утверждаю

_____

_____

«____»_____20__г.

АКТ №_____
об уничтожении криптографических ключей и ключевых документов.

г. _____ **«____»_____20__г.**

Комиссия в составе:
Председателя: _____, членов комиссии:
_____

_____

произвела уничтожение криптографических ключей и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)	Примечание
1	2	3	4	5	6	7	8

Всего уничтожено (_____) криптографических ключей на (_____) ключевых носителях. Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем их стирания в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/
_____ /_____/
_____ /_____/