УТВЕРЖДАЮ
Директор МБОУ «Луковниковская СОШ им. вице-адмирала В.А.Корнилова»
Приказ № 40 от 24.03.2023 года

_____/ О.М.Васильева
М.П.

ИНСТРУКЦИЯ

по обращению с сертифицированными ФСБ России средствами криптографической защиты информации в Автоматизированной системе управления сферой образования Тверской области

1 Общие положения

1.1 Инструкция по обращению с сертифицированными ФСБ России средствами криптографической защиты информации (далее – СКЗИ) в Автоматизированной системе управления сферой образования Тверской области (далее – АСУ СО ТО) Государственного бюджетного учреждения «Центр информатизации образования Тверской области» (далее – Учреждение) регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации ограниченного доступа.

1.2 К СКЗИ относятся:

1.2.1 Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.2.2 Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

1.2.3 Средства электронной подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием

открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи.

1.2.4 Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.2.5 Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

1.2.6 Ключевые документы (независимо от вида носителя ключевой информации).

1.3 В настоящей Инструкции используются следующие понятия и определения:

1.3.4 Доступ к информации – возможность получения информации и ее использования.

1.3.5 Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

1.3.6 Ключевой документ – физический носитель определенной структуры, содержащий криптоключи.

1.3.7 Компрометация криптоключа – утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

1.3.8 Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

1.3.9 Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

1.3.10 Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

1.3.11 Модель угроз – перечень возможных угроз.

1.3.12 Пользователь криптосредства – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.3.13 Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.4 Для обеспечения безопасности информации ограниченного доступа в АСУ СО ТО должны использоваться сертифицированные в системе сертификации ФСБ России

криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.5 Класс криптосредства определяется в соответствии с приказом ФСБ России от 10 июля 2014 г. № 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».

2 Организационная структура

2.2 Безопасность обработки информации в АСУ СО ТО с использованием криптосредств организует и обеспечивает Администратор безопасности АСУ СО ТО.

3 Обязанности пользователей криптосредств

3.2 Пользователи криптосредств допускаются к работе с ними только после ознакомления под подпись с настоящей Инструкцией, Инструкцией о порядке учета и выдачи СКЗИ, электронной цифровой подписи, эксплуатационно-технической документации и ключевых документов, Инструкцией по обращению с сертифицированными ФСБ России СКЗИ, другими документами, регламентирующими организацию и обеспечение безопасности информации.

3.3 При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

3.4 Пользователи криптосредств обязаны:

3.4.4 Не нарушать конфиденциальность закрытых ключей.

3.4.5 Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

3.4.6 Не допускать вывод закрытых ключей на дисплей (монитор) ПЭВМ или принтер.

3.4.7 Не допускать записи на ключевой документ посторонней информации.

3.4.8 Не допускать установки ключевых документов в другие ПЭВМ.

3.4.9 Обеспечить конфиденциальность информации о криптосредствах, других мерах защиты.

3.4.10 Точно соблюдать требования к к обеспечению безопасности криптосредств и ключевых документов к ним.

3.4.11 Хранить ключевые документы к криптосредствам в защищаемых хранилищах.

3.4.12 Сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей.

3.4.13 Своевременно выявлять и сообщать администратору безопасности АСУ СО ТО о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.

3.4.14 Немедленно уведомлять администратора безопасности АСУ СО ТО и принимать меры по предупреждению нарушения конфиденциальности защищаемой информации при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности информации ограниченного доступа.

3.5 Администратор безопасности АСУ СО ТО обязан:

3.5.4 Осуществлять поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним.

3.5.5 Осуществлять контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией.

3.5.6 Осуществлять учет Пользователей криптосредств.

3.5.7 Надежно хранить эксплуатационную и техническую документацию к криптосредствам, ключевые документы, носители дистрибутивов криптосредств, бумажные и машинные носители информации.

3.5.8 Проводить расследования и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации.

3.5.9 Осуществлять разработку и принимать меры по предотвращению возможных негативных последствий нарушений.

4 Действия с СКЗИ

4.2 Порядок учета и выдачи ключевых документов, СКЗИ, эксплуатационной и технической документации определен в Инструкции о порядке учета и выдачи СКЗИ, электронной подписи, эксплуатационно-технической документации и ключевых документов в Автоматизированной системе управления сферой образования Тверской области.

4.3 Уничтожение ключевых документов:

4.3.4 Ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются администратору безопасности АСУ СО ТО, или по его указанию уничтожаются на месте пользователями криптосредств.

4.3.5 Уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа.

4.3.6 Бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

4.3.7 Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 (десяти) суток после вывода их из действия (окончания срока действия).

4.3.8 Пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом Администратора безопасности АСУ СО ТО.

4.4 Уничтожение эксплуатационной и технической документации к криптосредствам:

4.4.4 Эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин.

5 Техническое обслуживание криптосредств

5.2 Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.3 На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

6 Опечатывание аппаратных средств

6.2 ПЭВМ, на которых установлены криптосредства, а также программно-аппаратные СКЗИ должны оборудоваться средствами контроля за их вскрытием (опечатываются, опломбируются). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

7 Организация режима помещений

7.2 Охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним, должны обеспечивать сохранность информации ограниченного распространения, криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в режимных помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.3 При оборудовании помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

7.4 Помещения выделяются с учетом размеров контролируемых зон. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

7.5 Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается в документе «Порядок доступа служащих в помещения, в которых ведется обработка информации ограниченного распространения».

7.6 Двери помещений должны закрываться на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

7.7 Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

8 Порядок доступа к хранилищам

8.2 Эксплуатация хранилищ:

8.2.4 Пользователи криптосредств хранят, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

8.2.5 Металлические хранилища должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

8.2.6 Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

8.3 При необходимости доступа к содержимому хранилища сотрудник, ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

8.4 По окончании работы сотрудник закрывает и опечатывает хранилище, за которое он ответственен.

8.5 Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за данные хранилища.

8.6 Порядок предоставления сотрудникам ключей для доступа к хранилищам:

8.6.4 Рабочий ключ от хранилища предоставляется сотруднику, ответственному за данное хранилище, под подпись в соответствующем администратором безопасности АСУ СО ТО.

8.6.5 Запасные экземпляры ключей от хранилищ хранятся в сейфе (хранилище) администратора безопасности АСУ СО ТО.

8.6.6 Запасные экземпляры ключей от сейфа администратора безопасности АСУ СО ТО передаются в опечатанном пенале под подпись в соответствующем журнале.

8.6.7 Ключи от хранилища не должны предоставляться сотрудникам, не ответственным за данные хранилища.

8.6.8 Изготовлять ключи от механического замка хранилищ имеет право только администратор безопасности АСУ СО ТО.

8.6.9 Ключи от механических замков хранилищ должны быть пронумерованы, учтены в соответствующем журнале.

8.6.10 При увольнении сотрудника, либо при назначении другого лица ответственным за хранилище данного сотрудника, сотрудник обязан сдать имеющиеся у него ключи от механического замка хранилища администратору безопасности АСУ СО ТО.

8.6.11 Сотрудникам запрещено передавать кому-либо ключи от хранилищ кроме как в случаях, предусмотренных настоящей Инструкцией.

8.7 Действия при несанкционированном проникновении или утрате ключей от хранилища:

8.7.4 При утрате ключа от хранилища замок данного хранилища необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Об утрате ключа сотрудник должен немедленно оповестить администратора безопасности АСУ СО ТО. Порядок хранения документов в хранилище, от

которого утрачен ключ, до изменения секрета замка устанавливает администратор безопасности АСУ СО ТО.

8.7.5 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилища посторонних лиц, о случившемся должно быть немедленно сообщено администратору безопасности АСУ СО ТО. Администратор безопасности АСУ СО ТО должен оценить возможность компрометации, хищения, подмены, порчи хранящихся документов и технических средств**,** составить акт и принять, при необходимости, меры к локализации последствий.

9 Контроль безопасности криптосредств

9.2 Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на администратора безопасности АСУ СО ТО в пределах его полномочий.

10 Ответственность за нарушение требований

10.2 Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

10.3 Администратор безопасности АСУ СО ТО несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки информации ограниченного доступа с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Лист ознакомления

№ п/п	Должность	Фамилия, Имя, Отчество	Дата ознакомления	Подпись