МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ПРИКАЗ

29.06.2022 № 1285

г. Новосибирск

Об организации работы со средствами криптографической защиты информации в министерстве образования Новосибирской области

В соответствии с Приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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», приказом Федеральной службы безопасности Российской Федерации 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», в целях обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в министерстве образования Новосибирской области с использованием средств криптографической защиты информации (далее – Министерство, СКЗИ), организации учета, хранения и эксплуатации применяемых в Министерстве СКЗИ **п р и к а з ы в а ю :**

1. Назначить ответственной за эксплуатацию СКЗИ в Министерстве Галушко Галину Александровну, консультанта отдела организации управления и кадровой работы организационно-правового управления министерства образования Новосибирской области.

2. Утвердить прилагаемые:

1) Инструкцию ответственного за эксплуатацию СКЗИ в Министерстве;

2) Перечень лиц, допущенных к работе с СКЗИ в Министерстве;

3) Инструкцию пользователя СКЗИ Министерства;

4) Перечень лиц, имеющих доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и

парольной информации СКЗИ;

5) Порядок доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ;

6) форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

7) форму Журнала учета хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

9) Правила эксплуатации средств криптографической защиты информации в Министерстве;

3. Признать утратившими силу:

приказ министерства образования Новосибирской области от 07.05.2018 № 1093 «Об утверждении инструкций и журналов, касающихся использования средств криптографической защиты информации»;

приказ министерства образования Новосибирской области от 16.05.2018 № 1205 «О доступе работников министерства в помещения, в которых ведется обработка информации ограниченного доступа, и расположены средства криптографической защиты информации»;

приказ министерства образования Новосибирской области от 13.12.2018 № 3236 «О внесении изменений в приказ министерства образования Новосибирской области от 07.05.2018№ 1093»;

приказ министерства образования Новосибирской области от 14.12.2021 № 2815 «О внесении изменений в приказ министерства образования Новосибирской области от 16.05.2018 № 1205»

приказ министерства образования Новосибирской области от 30.12.2021 № 2953 «О внесении изменений в приказ министерства образования Новосибирской области от 07.05.2018№ 1093»;

4. Контроль за исполнением настоящего приказа оставляю за собой.

Министр С.В. Федорчук

Галушко Г.А.
238-73-41

начальник отдела организации
управления и кадровой работы
организационно-правового управления
министерства образования
Новосибирской области Силакова Е.Е.

начальник организационно-правового
управления министерства образования
Новосибирской области Тарасик Т.М.

Рассылка: организационно-правового управления

[--] На контроль

[+] Для размещения на сайте Минобразования Новосибирской области и в ГИС НСО «Электронная демократия»

с «22» июня по «29» июня 2022 года *даты начала и окончания приема заключений независимой антикоррупционной экспертизы размещения НПА (не менее 7 дней).*

[+] для НПА: 1) Прокуратура Новосибирской области – 1экз.;
2) Главное Управление Министерства юстиции Российской Федерации по Новосибирской области – 1экз.;
3) Законодательное Собрание Новосибирской области – 1экз.;
4) Министерство юстиции Новосибирской области – 1 экз.;
5) Размещается на сайте Минобразования Новосибирской области;
6) На официальное опубликование на www.nsopravo.ru

[--] для НПА на официальное размещение (опубликование) www.pravo.gov.ru

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 29.06.2022_№_1285__

ИНСТРУКЦИЯ
ответственного за эксплуатацию средств криптографической защиты информации в министерстве образования Новосибирской области
(далее – Инструкция)

I. Общие положения

1. Инструкция определяет основные обязанности и права ответственного за эксплуатацию средств криптографической защиты информации в министерстве образования Новосибирской области (далее – СКЗИ, Министерство).

2. Ответственный за эксплуатацию СКЗИ назначается приказом государственного автономного учреждения дополнительного профессионального образования Новосибирской области «Новосибирский институт повышения квалификации и переподготовки работников образования».

3. Ответственный за эксплуатацию СКЗИ получает указания непосредственно от министра образования Новосибирской области (далее – министр) или иного уполномоченного министром лица и подотчетно ему.

4. Ответственный за эксплуатацию СКЗИ отвечает за организацию, обеспечение функционирования и безопасности СКЗИ, применяемых в Министерстве, в том числе предназначенных для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), обрабатываемой в информационных системах Министерства.

5. В своей деятельности ответственный за эксплуатацию СКЗИ руководствуется действующими нормативными правовыми актами в сфере (области) применения шифровальных (криптографических) средств, эксплуатационной и технической документацией на СКЗИ, приказами Министерства по вопросам эксплуатации СКЗИ и Инструкцией.

II. Обязанности ответственного за эксплуатацию СКЗИ

6. Ответственный за эксплуатацию СКЗИ обязан:

1) соблюдать требования приказов Министерства по вопросам эксплуатации СКЗИ, а также приказов Министерства, устанавливающих порядок обработки и обеспечения безопасности защищаемой информации;

2) знать и обеспечивать реализацию норм действующего законодательства Российской Федерации в сфере (области) применения шифровальных

(криптографических) средств, в том числе обработки и обеспечения безопасности защищаемой информации с использованием СКЗИ;

3) обеспечивать исполнение принятых Министерством обязательств в соответствии с заключенными соглашениями, касающимися обеспечения функционирования и порядка эксплуатации СКЗИ;

4) контролировать соблюдение условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;

5) обеспечивать поддержание в актуальном состоянии приказов Министерства по вопросам эксплуатации СКЗИ, Перечень лиц, допущенных к работе с СКЗИ в Министерстве, и лиц, имеющих доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ;

6) обеспечивать надежное хранение эксплуатационной и технической документации к СКЗИ, ключевых документов;

7) осуществлять ведение Журнала учёта хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

8) вести поэкземплярный учет используемых в Министерстве СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета СКЗИ);

9) обеспечивать пломбирование (опечатывание) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ;

10) организовывать установку, настройку, ввод в эксплуатацию и вывод из эксплуатации СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ;

11) контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) и фиксировать факт уничтожения/вывода из эксплуатации в Журнале учета СКЗИ;

12) организовывать обучение и проводить инструктаж пользователей СКЗИ по правилам работы с СКЗИ;

13) контролировать оформление и при необходимости оформлять Заключение о допуске пользователя СКЗИ к самостоятельной работе;

14) контролировать исполнение пользователями СКЗИ требований Инструкции пользователя СКЗИ Министерства, а также требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации в пределах своей компетенции;

15) соблюдать требования к обеспечению безопасности информации, обрабатываемой в Министерстве, безопасности СКЗИ и ключевых документов к ним;

16) не разглашать информацию, к которой он допущен, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;

17) инициировать проведение проверок по фактам ставших известными попыток посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним, о фактах утраты или недостачи СКЗИ, ключевых документов к ним, личных печатей, ключей от хранилищ (сейфов, металлических шкафов, ящиков индивидуального пользования), помещений, в которых размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, и о других фактах, которые свидетельствуют о возможной компрометации криптографических ключей и могут привести к нарушению конфиденциальности информации ограниченного доступа, при необходимости в случае подтверждения факта компрометации криптографических ключей обеспечивать информирование всех заинтересованных участников информационного обмена о факте компрометации ключевой информации;

18) обеспечить выведение из действия криптоключей, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ;

19) осуществлять координацию и контроль действий пользователей СКЗИ по восстановлению скомпрометированных криптоключей;

20) организовывать проведение служебных расследований по фактам компрометации криптоключей, а также в целях выявления причин нарушения требований безопасности функционирования СКЗИ;

21) обобщать результаты всех видов контроля за организацией и обеспечением порядка использования СКЗИ в Министерстве, анализировать причины выявленных нарушений, разрабатывать меры по их профилактике и предотвращению возможных негативных последствий подобных нарушений, контролировать выполнение рекомендаций, содержащихся в актах проверок контролирующих организаций;

22) сдать своему непосредственному руководителю СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы, личную печать, ключи от хранилищ и помещений, в которые допущен ответственный за эксплуатацию СКЗИ, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

III. Права ответственного за эксплуатацию СКЗИ

7. Ответственный за эксплуатацию СКЗИ имеет право:

1) знакомиться с приказами Министерства, регламентирующими процессы обработки защищаемой информации;

2) требовать от работников Министерства соблюдения требований законодательства Российской Федерации, приказов Министерства в области применения шифровальных (криптографических) средств, в том числе обработки и обеспечения безопасности защищаемой информации с использованием СКЗИ;

3) требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения возложенных на него обязанностей;

4) получать доступ к информации, материалам, техническим средствам, и в помещения, необходимый для надлежащего исполнения своих прав и обязанностей;

5) проходить обучение по вопросам, связанным с исполнением возложенных на него обязанностей в области обеспечения учета, хранения и эксплуатации СКЗИ;

6) проводить проверки соблюдения в Министерстве условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ;

7) требовать прекращения пользователями СКЗИ обработки информации с использованием СКЗИ в случае установления фактов нарушения правил эксплуатации СКЗИ или нарушения функционирования СКЗИ;

8) вносить предложения министру образования Новосибирской области по вопросам использования СКЗИ, по устранению выявленных нарушений правил эксплуатации СКЗИ и предупреждению подобного рода нарушений.

IV. Ответственность

8. Ответственный за эксплуатацию СКЗИ несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

1) неисполнение либо ненадлежащее исполнение возложенных на него обязанностей;

2) превышение, злоупотребление или неправильное использование предоставленных полномочий, предусмотренных Инструкцией;

3) нарушение законодательства Российской Федерации, приказов Министерства, устанавливающих порядок работы с СКЗИ;

4) применение к Министерству штрафных санкций по вине ответственного за эксплуатацию СКЗИ;

5) совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от _29.06.2022_№ 1285__

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации министерства образования Новосибирской области (далее – Инструкция)

I. Общие положения

1. Инструкция определяет права и обязанности пользователей средств криптографической защиты информации (далее – СКЗИ).
2. Пользователями СКЗИ являются работники (сотрудники) министерства образования Новосибирской области (далее – Министерство), включенные в Перечень лиц, допущенных к работе с СКЗИ в Министерстве, утвержденный приказом Министерства.
3. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами в сфере (области) применения шифровальных (криптографических) средств, приказами Министерства по вопросам эксплуатации СКЗИ, Инструкцией и проходит обучение правилам работы с СКЗИ.
4. Пользователь считается допущенным к СКЗИ после оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе.
5. Инструктаж по правилам работы с СКЗИ и оформление Заключения о допуске пользователя СКЗИ к самостоятельной работе осуществляют уполномоченные сотрудники организаций, осуществляющих ввод в эксплуатацию СКЗИ или ответственный за эксплуатацию СКЗИ в Министерстве.
6. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИ от несанкционированного использования, а также за сохранность полученных под расписку в соответствующем журнале СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

II. Обязанности и права пользователя СКЗИ

7. Пользователь СКЗИ обязан:
1) соблюдать требования по обеспечению безопасности функционирования СКЗИ;
2) обеспечить конфиденциальность информации ограниченного распространения, доступной ему по роду выполняемых функциональных обязанностей, в том числе сведений о криптоключах;
3 обеспечить хранение ключевых документов, эксплуатационной и

технической документации, дистрибутивов СКЗИ, опечатываемых тубусов (пеналов) в надежно запираемых шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;

5) сообщать ответственному за эксплуатацию СКЗИ о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

6) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать ответственному за эксплуатацию СКЗИ в Министерстве, а при его отсутствии руководителю соответствующего структурного подразделения СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы, ключевые носители, личные печати;

7) сдать имеющиеся у него ключи от замков хранилищ ответственному за эксплуатацию СКЗИ, а при его отсутствии руководителю соответствующего структурного подразделения при увольнении, либо при назначении другого лица ответственным за хранилище;

8) сдать имеющиеся у него ключи от помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) ответственному за эксплуатацию СКЗИ, а при его отсутствии руководителю соответствующего структурного подразделения при увольнении или переводе в иное структурное подразделение;

9) немедленно уведомлять своего непосредственного руководителя и ответственного за эксплуатацию СКЗИ о компрометации криптоключей, фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от Помещений, хранилищ, личных печатей, удостоверений, пропусков и о других фактах, которые могут привести к разглашению защищаемой информации, а также о причинах и условиях возможной утечки таких сведений;

10) незамедлительно прекратить применение скомпрометированных криптоключей (обмен электронными документами/формирование электронной подписи и пр.) и обеспечить вывод из действия криптоключей, в отношении которых возникло подозрение в компрометации, а также действующих совместно с ними других криптоключей;

11) немедленно прекратить работу с СКЗИ в случае обнаружения на рабочей станции посторонних программ (в том числе вредоносного программного обеспечения), о произошедшем известить ответственного за эксплуатацию СКЗИ и ответственного за защиту информации в Министерстве;

12) в пределах своей компетенции предоставлять по требованию ответственного за эксплуатацию СКЗИ информацию, необходимую при проведении служебных расследований по фактам компрометации криптоключей, а также в целях выявления причин нарушения требований безопасности функционирования СКЗИ.

8. Пользователю СКЗИ запрещается:

1) осуществлять несанкционированное и безучётное копирование ключевой информации;

2) хранить ключевые носители вне хранилищ и помещений, гарантирующих их сохранность и конфиденциальность ключевой информации;

3) передавать ключевые носители лицам, к ним не допущенным;

4) во время работы оставлять ключевые носители без присмотра (например, на рабочем столе или в разъеме системного блока персонального компьютера);

5) выводить ключевую информацию на печать, дисплей монитора или иное средство визуализации данных;

6) записывать на ключевые носители постороннюю информацию;

7) вносить какие-либо изменения в программное обеспечение СКЗИ;

8) устанавливать и эксплуатировать стороннее программное обеспечение, которое может нарушить функционирование СКЗИ.

9) использовать бывшие ранее в работе ключевые носители для записи новой ключевой информации без предварительного гарантированного уничтожения ранее хранящейся на них информации;

10) использовать ключевые носители, выведенные из действия;

11) передавать кому-либо ключи от хранилищ и Помещений, а также личные печати кроме как в случаях, предусмотренных Инструкцией.

9. Пользователь СКЗИ имеет право:

1) знакомиться с локальными актами Министерства, регламентирующими процессы обработки и обеспечения безопасности защищаемой информации;

2) требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения возложенных на него обязанностей;

3) получать доступ к информации, материалам, техническим средствам, и в помещения, необходимый для надлежащего исполнения своих прав и обязанностей;

4) проходить обучение по вопросам, связанным с исполнением возложенных на него обязанностей в области эксплуатации СКЗИ;

5) уничтожать использованные непосредственно им (предназначенные для него) ключевые документы с обязательным уведомлением ответственного за эксплуатацию СКЗИ, если иное не предусмотрено эксплуатационной и технической документацией на СКЗИ, договорами или соглашениями, заключенными с организациями, осуществлявшими ввод в эксплуатацию СКЗИ;

6) вносить предложения министру образования Новосибирской области по вопросам использования СКЗИ, по устранению выявленных нарушений правил эксплуатации СКЗИ и предупреждению подобного рода нарушений.

III. Ответственность

10. Пользователь СКЗИ несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

1) неисполнение либо ненадлежащее исполнение возложенных на него обязанностей;

2) превышение, злоупотребление или неправильное использование предоставленных полномочий, предусмотренных Инструкцией;

3) нарушение законодательства Российской Федерации, приказов Министерства, устанавливающих порядок работы с СКЗИ;

4) применение к Министерству штрафных санкций по вине пользователя СКЗИ;

5) совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

УТВЕРЖДЕН
приказом Минобразования
Новосибирской области
от 29.06.2022_№_1285___

ПОРЯДОК
доступа в помещения, где размещены используемые средства криптографической защиты информации, хранятся средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации
(далее – Порядок)

I. Общие положение

1. Порядок регламентирует условия и порядок осуществления доступа в помещения министерства образования Новосибирской области (далее – Министерство), где размещены используемые средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) в целях обеспечения сохранности СКЗИ и носителей ключевой, аутентифицирующей и парольной информации СКЗИ, а также организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

2. Порядок разработан в соответствии с требованиями Приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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», приказа Федеральной службы безопасности Российской Федерации 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».

II. Порядок доступа в помещения

3. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

4. Должно обеспечиваться постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода.

5. По окончании рабочего дня Помещения опечатываются либо должны быть активированы соответствующие технические устройства, сигнализирующие о несанкционированном вскрытии Помещений.

6. Установленный режим охраны Помещений должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящего Порядка. Правила допуска работников (сотрудников) Министерства, а также посетителей в Помещения в рабочее и нерабочее время должны учитывать специфику и условия работы конкретных пользователей СКЗИ.

7. Доступ в Помещения в рабочее (служебное) время имеют работники, включенные в Перечень лиц, имеющих доступ в помещения, где размещены используемые средства криптографической защиты информации, хранятся средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации (далее – Перечень лиц, имеющих доступ в Помещения), утвержденный приказом Министерства.

8. В нерабочее (неслужебное) время пребывание вышеуказанных работников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных министром образования Новосибирской области.

9. Нахождение в Помещениях лиц, не включенных в Перечень лиц, имеющих доступ в Помещения (посетителей), возможно только в присутствии работников (сотрудников) Министерства, включенных в Перечень лиц, имеющих доступ в Помещения. Время нахождения посетителей в Помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в Помещении.

10. Ключи от входных дверей Помещений учитывают и выдают работникам (сотрудникам) Министерства, включенным в Перечень лиц, имеющих доступ в Помещения, под расписку в Журнале учета хранилищ средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета хранилищ).

11. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в Помещения посторонних лиц, или в случае утраты ключа от Помещения о случившемся должно быть немедленно сообщено непосредственному руководителю соответствующего структурного подразделения, ответственному за эксплуатацию СКЗИ и министру образования Новосибирской области. При необходимости вызываются работники правоохранительных органов и принимаются меры по охране места происшествия до их прибытия (Помещения не вскрываются, работники (сотрудники) Министерства и посетители в Помещения не допускаются). Дальнейшие действия определяются характером произошедшего инцидента.

12. По результатам анализа случившегося, необходимо дать оценку возможности компрометации хранящихся ключевых и других документов, составить акт об обнаружении признаков, указывающих на возможное

проникновение посторонних лиц в Помещения Министерства (типовая форма Акта об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в помещения Министерства, приведена в Приложении к Порядку) и принять при необходимости меры к локализации последствий компрометации информации и к замене скомпрометированных криптоключей.

13. При утрате ключа от входной двери в Помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей, соответствующие сведения вносятся в Журнал учета хранилищ. Порядок размещения СКЗИ, хранения ключевых и других документов в Помещении, от которого утрачен ключ, до замены замка или изменения секрета замка устанавливает руководитель соответствующего структурного подразделения Министерства по согласованию с ответственным за эксплуатацию СКЗИ, при этом должны быть обеспечены условия, исключающие бесконтрольный доступ, а также непреднамеренное уничтожение СКЗИ, ключевых и иных документов.

14. В случае возникновения нештатной ситуации (в том числе событий чрезвычайного характера) необходимо в обязательном порядке известить о случившемся ответственного за эксплуатацию СКЗИ и министра образования Новосибирской области.

15. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка Информации и расположены средства СКЗИ, возлагается на сотрудников структурных подразделений, уполномоченных на обработку персональных данных в Министерстве, а также руководителей структурных подразделений Министерства.

16. Сотрудники аварийно-спасательных служб, врачи «скорой помощи» допускаются в Помещения в сопровождении министра образования Новосибирской области, руководителя соответствующего структурного подразделения, сотрудников Министерства, включенных в Перечень лиц, имеющих доступ в Помещения, или сотрудников службы охраны.

ПРИЛОЖЕНИЕ
к Порядку доступа в помещения, где размещены используемые средства криптографической защиты информации, хранятся средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации

ТИПОВАЯ ФОРМА

АКТ № _____
об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в помещения министерстве образования Новосибирской области

«__» _____ 20___ г.

_____
(должность, фамилия, имя, отчество должностного лица)

в связи с обнаружением _____
_____

в присутствии:
_____
_____
(должность, фамилии, имена, отчества иных лиц, присутствовавших при осмотре)

произведен осмотр помещения (в котором ведется обработка информации ограниченного доступа (в том числе персональных данных) и размещены используемые средства криптографической информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ[1]), расположенного по адресу:
_____

В ходе осмотра обнаружено:
_____
_____
_____

Подписи лиц, принимавших участие (присутствовавших) при проведении осмотра:

_____	_____	_____
(должность)	(подпись)	(ФИО (отчество при наличии))
_____	_____	_____
(должность)	(подпись)	(ФИО (отчество при наличии))

[1] Уточнить, оставить нужное

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от _29.06.2022__№ 1285_

ФОРМА

ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. (отчество при наличии) пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. (отчество при наличии) лиц, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. (отчество при наличии) лиц, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 29.06.2022__№_1285__

ФОРМА

ЖУРНАЛ
учета хранилищ средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование помещения, хранилища (сейф, металлический шкаф, ящик индивидуального пользования, тубус (пенал))	Местонахождение (подразделение, номер кабинета)	Что находится (документы, изделия)	Ф.И.О. (отчество при наличии) ответственного за помещение/хранилище
1	2	3	4	5

Количество комплектов ключей от помещения, хранилища и их номера[2]	Расписка о получении ключа (ФИО (отчество при наличии), номер комплекта ключей, подпись получившего ключ, дата получения ключа), тубуса(пенала) (ФИО (отчество при наличии), номер печати, подпись получившего тубус (пенал), дата получения тубуса (пенала))	Расписка о возврате ключа (ФИО (отчество при наличии), номер комплекта ключей, подпись принявшего ключ, дата возврата ключа), тубуса (пенала) (ФИО (отчество при наличии), номер печати, подпись принявшего тубус (пенал), дата возврата тубуса (пенала))	Примечание
6	7	8	9

[2] Для тубусов (пеналов) в графе ставится прочерк

УТВЕРЖДЕНЫ
приказом Минобразования
Новосибирской области
от 29.06.2022 № 1285

ПРАВИЛА
эксплуатации средств криптографической защиты информации в министерстве образования Новосибирской области

I. Общие положения

Настоящие Правила эксплуатации средств криптографической защиты информации в министерстве образования Новосибирской области (далее – Правила) определяют порядок учета, обеспечения сохранности, вывода из эксплуатации и уничтожения средств криптографической защиты информации (далее – СКЗИ), а также порядок действий сотрудников министерства образования Новосибирской области (далее – Министерство) при компрометации криптографических ключей.

2. В Правилах применяются следующие термины и определения:

электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

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

закрытый ключ – криптоключ, который хранится пользователем системы в тайне;

ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию;

ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.);

компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и

ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

ответственный за эксплуатацию СКЗИ – сотрудник, осуществляющий организацию учета, хранения и эксплуатации СКЗИ, в том числе обеспечения работ по техническому обслуживанию СКЗИ и управлению криптографическими ключами;

пользователи СКЗИ – сотрудники Министерства, непосредственно допущенные к работе с СКЗИ;

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, ограждающие конструкции охраняемого здания, охраняемой части здания.

3. К шифровальным (криптографическим) средствам (средствам криптографической защиты информации (СКЗИ)), включая документацию на эти средства, относятся:

средства шифрования – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

средства имитозащиты – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

средства кодирования – средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

средства изготовления ключевых документов – аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

ключевые документы – электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

аппаратные шифровальные (криптографические) средства – устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

программные шифровальные (криптографические) средства – программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

программно-аппаратные шифровальные (криптографические) средства – устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

4. Правила в своем составе, терминах и определениях основываются на положения следующих нормативных правовых актов:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Приказ Федеральной службы безопасности Российской Федерации 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» (далее – Приказ ФСБ России от 10.07.2014 № 378);

Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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»;

иные нормативные правовые акты и методические документы по эксплуатации шифровальных (криптографических) средств.

5. В Министерстве подлежат использованию использоваться только СКЗИ, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации и имеющие сертификат Федеральной службы безопасности Российской Федерации.

6. Класс применяемых СКЗИ определяется в соответствии с Приказом ФСБ России от 10.07.2014 № 378, а также иными нормативными правовыми актами по эксплуатации шифровальных (криптографических) средств.

7. Для организации и обеспечения работ по учету, хранению и эксплуатации СКЗИ в Министерстве приказом назначается ответственный за эксплуатацию СКЗИ.

8. Ввод в эксплуатацию СКЗИ оформляется актом (типовая форма приведена в Приложении № 1 к Правилам). Акт ввода в эксплуатацию СКЗИ оформляют организации, осуществляющих поставку и ввод в эксплуатацию СКЗИ.

II. Порядок допуска пользователей к работе со средствами криптографической защиты информации

9. Для работы с СКЗИ допускаются сотрудники Министерства, включенные в Перечень лиц, допущенных к работе со средствами криптографической защиты информации в Министерстве (далее – Перечень лиц, допущенных к работе с СКЗИ).

10. Перечень лиц, допущенных к работе с СКЗИ, утверждается приказом Министерства.

11. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами по эксплуатации шифровальных (криптографических) средств, приказами Министерства по вопросам эксплуатации СКЗИ и проходит обучение правилам работы с СКЗИ.

12. Пользователь считается допущенным к СКЗИ после оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе.

13. Инструктаж по правилам работы с СКЗИ и оформление Заключения о допуске пользователя СКЗИ к самостоятельной работе осуществляют уполномоченные сотрудники организаций, осуществляющих поставку и ввод в эксплуатацию СКЗИ, или ответственный за эксплуатацию СКЗИ в Министерстве. Типовая форма Заключения о допуске пользователя СКЗИ к самостоятельной работе приведена в Приложении № 2 к Правилам.

III. Учет средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

14. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету.

15. Поэкземплярный учет СКЗИ ведет ответственный за эксплуатацию СКЗИ в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета СКЗИ). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

16. Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

17. Все экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются пользователям СКЗИ под расписку в Журнале учета СКЗИ.

18. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ не допускается.

IV. Обеспечение сохранности средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

19. Хранение ключевых документов, эксплуатационной и технической документации, дистрибутивов СКЗИ должно осуществляться в надежно запираемых шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

20. Ключевые носители могут храниться в тубусах (пеналах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

21. Замочные скважины вышеуказанных хранилищ, а также тубусы (пеналы) для хранения ключевых носителей должны быть оборудованы приспособлениями для опечатывания. Печати, предназначенные для опечатывания хранилищ и тубусов (пеналов), должны находиться у ответственных за эти хранилища/тубусы (пеналы).

22. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под роспись в Журнале учета СКЗИ пользователям СКЗИ, несущим персональную ответственность за их сохранность.

23. Порядок изготовления дубликатов, учета и хранения ключей для доступа к хранилищам (сейфам, металлическим шкафам, ящикам индивидуального пользования) и помещениям, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения):

несанкционированное изготовление дубликатов ключей запрещено;

количество комплектов ключей от Помещений и от замков хранилищ и их номера указываются в Журнале учета хранилищ средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета хранилищ);

в Журнале учета хранилищ отражается первичная выдача ключа от Помещений и хранилищ, возможная повторная выдача ключа (в случае смены замка и других обстоятельствах) и сдача ключа при увольнении сотрудника или смене должностных обязанностей (переводе в иное структурное подразделение).

ключи от хранилищ и (или) Помещений, сданные ответственному за эксплуатацию СКЗИ или руководителю соответствующего структурного подразделения, хранятся в сейфе.

24. Тубусы (пеналы), предназначенные для хранения ключевых носителей, подлежат учету в Журнале учета хранилищ.

25. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. Опечатывание производит ответственный за эксплуатацию СКЗИ либо лицо, проводившее ввод в эксплуатацию СКЗИ.

26. При наличии технической возможности на время отсутствия пользователей СКЗИ аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ необходимо отключать от линии связи и убирать в опечатываемые хранилища.

27. Вскрытие аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ, оборудованных средствами контроля за их вскрытием, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного за эксплуатацию СКЗИ.

28. При необходимости передачи аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ в сторонние организации для проведения ремонтно-восстановительных или иных работ, осуществляется предусмотренная эксплуатационной и технической документацией к СКЗИ процедура изъятия (удаления программного обеспечения) СКЗИ из аппаратных средств, с которыми они функционировали, и уничтожение криптоключей (исходной ключевой информации), хранящейся в аппаратных СКЗИ.

V. Мероприятия при компрометации криптоключей

29. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, относятся следующие:

утрата (хищение) ключевых носителей с криптографическими ключами, в том числе с последующим их обнаружением;

возникновение подозрений относительно утечки информации или ее искажения (подмены, подделки);

нарушение целостности печатей на хранилищах СКЗИ и ключевых документов (если используется процедура опечатывания хранилищ);

утрата ключей от хранилищ СКЗИ и ключевых документов (при нахождении в них ключевых носителей с криптографическими ключами);

нарушение правил хранения криптографических ключей;

ошибки при совершении криптографических операций (например, отрицательный результат по результатам проверки электронной подписи);

несанкционированное и безучетное копирование ключевой информации;

увольнение (переназначение) работников, имевших доступ к ключевым

носителям;

передача секретных ключей по линиям связи в открытом виде;

временный доступ посторонних лиц к ключевым носителям,

другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

30. В случае возникновения любого из вышеперечисленных обстоятельств, пользователь СКЗИ обязан незамедлительно прекратить применение криптоключей, в отношении которых возникло подозрение в компрометации (обмен электронными документами/формирование электронной подписи и пр.), и информировать о факте возможной компрометации используемых криптоключей ответственного за эксплуатацию СКЗИ любым доступным способом. Пользователь СКЗИ обязан убедиться, что его сообщение получено и прочтено.

31. Решение о компрометации криптографических ключей принимает ответственный за эксплуатацию СКЗИ.

32. Криптоключи, которые были скомпрометированы или в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи подлежат выводу из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. Проведение мероприятий по выводу из действия криптоключей/отзыву сертификата ключа электронной подписи пользователя СКЗИ обеспечивается ответственным за эксплуатацию СКЗИ.

33. Сертификат скомпрометированного ключа электронной подписи, подлежит хранению ответственным за эксплуатацию СКЗИ в течение срока хранения электронных документов для проведения (в случае необходимости) расследований, связанных с применением электронной подписи.

VI. Порядок вывода из действия и уничтожения средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов, криптоключей (исходной ключевой информации) и ключевых носителей

34. Неиспользованные или выведенные из действия криптоключи и ключевые документы подлежат уничтожению.

35. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

36. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями

организации, производившей запись криптоключей (исходной ключевой информации).

37. Ключевые носители многократного использования после стирания (разрушения) хранимых на них криптоключей (исходной ключевой информации) подлежат возврату в организацию, предоставившую СКЗИ во временное пользование на основании заключенного договора, контракта или соглашения и (или) осуществлявшую ввод в эксплуатацию СКЗИ, либо по ее указанию могут быть уничтожены на месте.

38. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

39. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

40. Ключевые документы должны быть уничтожены в порядке и в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

41. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

42. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

43. Вывод из эксплуатации СКЗИ осуществляется в порядке, предусмотренном эксплуатационной и технической документацией на СКЗИ, согласно регламентам удостоверяющих центров, заключенным договорам и соглашениям, а также в соответствии с указаниями организаций, осуществлявших ввод в эксплуатацию средств криптографической защиты информации.

44. Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным за эксплуатацию СКЗИ. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими

(предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом ответственного за эксплуатацию СКЗИ.

45. По результатам уничтожения криптографических ключей, содержащихся на ключевых носителях, и ключевых документов оформляется Акт об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов (типовая форма Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов приведена в Приложении № 3 к Правилам).

46. После уничтожения ключевых документов и/или ключевых носителей, а также вывода из эксплуатации СКЗИ ответственный за эксплуатацию СКЗИ вносит необходимые отметки в Журнал учета СКЗИ.

VII. Размещение, специальное оборудование, охрана и организация режима доступа в помещения, где установлены СКЗИ или хранятся ключевые документы к ним

47. Размещение, специальное оборудование, охрана и организация режима в Помещениях, должны обеспечивать сохранность СКЗИ и носителей ключевой, аутентифицирующей и парольной информации СКЗИ, а также исключать возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

48. Обеспечение безопасности используемых СКЗИ, хранящихся СКЗИ и (или) носителей ключевой, аутентифицирующей и парольной информации СКЗИ от уничтожения, изменения, копирования, а также от иных неправомерных действий достигается в том числе установлением порядка доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждаемым приказом Министерства.

49. При оборудовании Помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

50. Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.

51. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие Помещений в нерабочее время. По окончании рабочего дня Помещения должны быть опечатаны, либо Помещения должны быть оборудованы соответствующими техническими устройствами, сигнализирующими об их несанкционированном вскрытии.

52. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Помещения.

53. На время отсутствия пользователей СКЗИ оборудование, функционирующее с СКЗИ, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые

хранилища. В противном случае пользователи СКЗИ по согласованию с ответственным за эксплуатацию СКЗИ обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

54. В Помещениях для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых хранилищ (в том числе индивидуального пользования), оборудованных приспособлениями для опечатывания. Ключи от этих хранилищ подлежат учету и хранению в порядке согласно настоящим Правилам.

55. В обычных условиях опечатанные хранилища могут быть вскрыты только самими ответственными за хранилища, указанными в Журнале учета хранилищ.

ПРИЛОЖЕНИЕ № 1
к Правилам эксплуатации средств криптографической защиты информации в министерстве образования Новосибирской области

ТИПОВАЯ ФОРМА

АКТ
ввода в эксплуатацию средств криптографической защиты информации

Настоящий акт составлен о том, что произведена установка и настройка изделия:

_____
Наименование средства криптографической защиты информации

Адрес: _____

Помещение: _____

Характеристики помещения	**Да**	**Нет**
Помещение находится в пределах контролируемой зоны		
Помещение оборудовано входной дверью с замком		
Помещение оснащено охранной сигнализацией		
Помещение оснащено пожарной сигнализацией		
Окна помещения защищены от просмотра извне		
Исключена возможность неконтролируемого проникновения или пребывания в помещении посторонних лиц		

Изделие: наименование средства криптографической защиты информации:

серийный номер дистрибутива: _____;

регистрационный (учетный) номер СКЗИ: _____;

размещено на аппаратном средстве (№ системного блока): _____

и в соответствии с эксплуатационной и технической документацией на СКЗИ (указывается наименование СКЗИ) введено в эксплуатацию.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы), место опечатывания (опломбирования) возможно контролировать визуально, номер(а) печати(ей) (пломбира(ов)): _____.

Дистрибутив СКЗИ (указывается наименование СКЗИ) учтен в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Первичный инструктаж по использованию СКЗИ проведен со специалистом:

_____

Ответственный за эксплуатацию СКЗИ: _____ _____
(подпись) (ФИО (отчество при наличии))

« » 20 г.

ПРИЛОЖЕНИЕ № 2
к Правилам эксплуатации средств криптографической защиты информации в министерстве образования Новосибирской области

ТИПОВАЯ ФОРМА

ЗАКЛЮЧЕНИЕ
о допуске пользователя СКЗИ к самостоятельной работе

_____
(ФИО (отчество при наличии), должность пользователя СКЗИ)

(далее – пользователь СКЗИ) в соответствии с 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 Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 (далее – Инструкция), прошел обучение правилам эксплуатации и обеспечения безопасности_____
(Наименование СКЗИ)

Пользователь СКЗИ обязуется:

не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе, сведения о криптоключах;

соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

сообщать ответственному за эксплуатацию СКЗИ о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от обязанностей, связанных с использованием СКЗИ;

немедленно уведомлять ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), 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.

Заключение: пользователь к самостоятельной работе с СКЗИ допущен.

Ответственный за
эксплуатацию СКЗИ: _____ _____
(подпись) (ФИО)

Пользователь СКЗИ: _____ _____
(подпись) (ФИО)

«____» _____ 20_ __ г.

ПРИЛОЖЕНИЕ № 3
к Правилам эксплуатации средств криптографической защиты информации в министерстве образования Новосибирской области

ТИПОВАЯ ФОРМА

АКТ № _____
об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов

«__» _____ 20___ г.

_____
(должность, фамилия, имя отчество (отчество при наличии) должностного лица)

произведено уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№ п/п	Наименование СКЗИ, ключевых документов	Номер (идентификатор) криптографического ключа, ключевого документа	Ф.И.О. (отчество при наличии) владельца ключа (документа)	Номер аппаратного средства	Примечание

Всего уничтожено криптографических ключей на ключевых носителях. Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи акта сверены с записями в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Узлы и детали аппаратных средств передать для дальнейшей эксплуатации.

Подписи лиц, принимавших участие (присутствовавших) при проведении уничтожения криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

_____ (должность)	_____ (подпись)	_____ (ФИО (отчество при наличии))
_____ (должность)	_____ (подпись)	_____ (ФИО (отчество при наличии))
_____ (должность)	_____ (подпись)	_____ (ФИО (отчество при наличии))