МИНИСТЕРСТВО СОЦИАЛЬНОЙ ПОЛИТИКИ СВЕРДЛОВСКОЙ ОБЛАСТИ

ТЕРРИТОРИАЛЬНЫЙ ОТРАСЛЕВОЙ ИСПОЛНИТЕЛЬНЫЙ ОРГАН ГОСУДАРСТВЕННОЙ ВЛАСТИ СВЕРДЛОВСКОЙ ОБЛАСТИ - УПРАВЛЕНИЕ СОЦИАЛЬНОЙ ПОЛИТИКИ МИНИСТЕРСТВА СОЦИАЛЬНОЙ ПОЛИТИКИ СВЕРДЛОВСКОЙ ОБЛАСТИ № 21
(УПРАВЛЕНИЕ СОЦИАЛЬНОЙ ПОЛИТИКИ № 21)

ПРИКАЗ

26.07.2022 № 2341

г. Нижний Тагил

Об утверждении Положения по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации территориального отраслевого исполнительного органа государственной власти Свердловской области – Управления социальной политики Министерства социальной политики Свердловской области №21

С целью обеспечения безопасности информации с помощью средств криптографической защиты в соответствии с требованиями Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Положение по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации территориального отраслевого исполнительного органа государственной власти Свердловской области – Управления социальной политики Министерства социальной политики Свердловской области №21 (далее – Положение)(прилагается).
2. Руководителям структурных подразделений территориального отраслевого исполнительного органа государственной власти Свердловской области – Управления социальной политики Министерства социальной политики Свердловской области №21 обеспечить соблюдение требований положения
3. Контроль за выполнением требований настоящего приказа оставляю за собой.

Начальник управления Пануш Л.Ю.

Приложение № 1
к приказу территориального
отраслевого исполнительного
органа государственной власти
Свердловской области –
Управления социальной политики
Министерства социальной
политики Свердловской области
№21.
от 26.07.2022 № 2341

ПОЛОЖЕНИЕ

по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации территориального отраслевого исполнительного органа государственной власти Свердловской области – Управления социальной политики Министерства социальной политики Свердловской области №21

Содержание

Глава 1. Общие положения

1. Положение по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации территориального отраслевого исполнительного органа государственной власти Свердловской области – Управления социальной политики Министерства социальной политики Свердловской области №21 (далее —Положение) определяет порядок организации и проведения работ по обеспечению безопасности персональных данных и информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (далее – защищаемая информация) в территориальном отраслевом исполнительном органе государственной власти Свердловской области – Управлении социальной политики Министерства социальной политики Свердловской области №21 (далее — Управление социальной политики №21) с использованием средств криптографической защиты информации.

2. Настоящее Положение разработано на основании:

1) Федерального закона от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) Федерального закона от 27 июля 2006 №152-ФЗ «О персональных данных»;

3) постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4) 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»;

5) приказа Федеральной службы безопасности (далее — ФСБ России) Российской Федерации от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

6) 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»;

7) Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России 31.03.2015 №149/7/2/9-432).

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

1) 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;

2) 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;

3) средства электронной подписи;

4) 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;

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

6) 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.

Глава 2. Структура ответственных лиц

4. Структуру ответственных лиц по направлению организации и обеспечения криптографической защиты информации в Управлении социальной политики №21 составляют:

1) ответственный пользователь СКЗИ;

2) пользователи СКЗИ.

5. Ответственный пользователь СКЗИ назначается руководителем Управления социальной политики №21.

6. Перед допуском к работе ответственный пользователь СКЗИ знакомится с нормативными правовыми документами, регулирующими организацию и обеспечение криптографической защиты информации, с настоящим Положением и правовыми актами Управления социальной политики №21, регламентирующими защиту информации с помощью СКЗИ в Управлении социальной политики №21.

Ответственный пользователь СКЗИ несет ответственность за соответствие проводимых в Управлении социальной политики №21 мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по

каналам связи защищаемой информации с использованием СКЗИ требованиям действующего законодательства, эксплуатационной и технической документации к СКЗИ и требованиям настоящего Положения, а также за обеспечение эксплуатации СКЗИ в Управлении социальной политики №21.

7. Обеспечение эксплуатации СКЗИ представляет следующий комплекс мероприятий по:

1) установке и вводу в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам;

2) удалению и выводу из эксплуатации СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам;

3) проверке готовности СКЗИ к использованию с составлением заключений о возможности их эксплуатации;

4) обеспечению функционирования СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

5) созданию исходной ключевой информации, созданию из исходной ключевой информации криптографических ключей,

6) получению, распределению (выдаче), рассылке, учету и уничтожению ключевых документов;

7) плановой смене ключевой информации, а также смене ключевой информации в случае ее компрометации;

8) обучению пользователей СКЗИ работе с СКЗИ;

9) учету пользователей СКЗИ;

10) поэкземплярному учету используемых СКЗИ, эксплуатационной и технической документацией к ним;

11) контролю соблюдения пользователями СКЗИ условий использования СКЗИ, эксплуатационной и технической документации к ним, ключевых документов,

12) контролю ведения учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, пользователей СКЗИ;

13) проведению проверок по фактам нарушения условий криптографической защиты информации.

8. Пользователи СКЗИ –сотрудники Управления социальной политики №21, допущенные к работе с СКЗИ с целью выполнения их должностных обязанностей.

Пользователи СКЗИ знакомятся с документами, регламентирующими организацию и обеспечение криптографической защиты информации в Управлении социальной политики №21, под подпись и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

Пользователь СКЗИ обязан:

1) соблюдать конфиденциальность ключевой и парольной информации, информации о настройках, применяемых СКЗИ;

2) осуществлять эксплуатацию СКЗИ в соответствии с требованиями эксплуатационной документации;

3) не допускать снятия копий с ключевых документов;

4) не допускать записи на ключевой носитель посторонней информации;

5) не допускать установки ключевых документов на другие автоматизированные рабочие места (далее — АРМ);

6) хранить инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;

7) предусматривать раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей;

8) сообщать о ставших известными попытках получения сведений об используемых СКЗИ или ключевых документах лицами, не обладающими правом доступа к таким сведениям (любым лицом, за исключением ответственного пользователя СКЗИ в Управлении социальной политики №21);

9) немедленно уведомлять ответственного пользователя СКЗИ, руководство о фактах утраты СКЗИ, ключевых документов к ним, ключей от помещений, где размещены используемые СКЗИ, хранятся носители ключевой, (далее — помещения), хранилищ, личных печатей, предназначенных для опечатывания помещений (хранилищ), и о других фактах, которые могут привести к снижению уровня характеристик безопасности информации;

10) сдавать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

Глава 3. Требования к обеспечению безопасности хранения и обработки информации с использованием СКЗИ

9. Безопасность хранения и обработки информации с использованием СКЗИ достигается за счет:

1) соблюдения пользователями СКЗИ конфиденциальности ключевой и парольной информации, информации о настройках, применяемых СКЗИ;

2) точного выполнения пользователями СКЗИ требований к обеспечению безопасности информации;

3) надежного хранения эксплуатационной и технической документации к СКЗИ, ключевых документов;

4) своевременного выявления сотрудниками попыток получения сведений о защищаемой информации, об используемых СКЗИ или ключевых документах лицами, не обладающими правом доступа к таким сведениям;

5) принятия мер по предупреждению разглашения защищаемой информации при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и т.п.

10. Размещение, специальное оборудование, охрана и организация режима в помещениях, должны обеспечивать сохранность защищаемой информации, СКЗИ и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотр посторонними лицами ведущихся там работ.

Помещения должны удовлетворять требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ, иметь прочные входные двери с замками, гарантирующими надежное закрытие.

Окна помещений, расположенных на первых зданий и других мест откуда возможен просмотр извне должны быть оснащены жалюзи.

11. Обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях лиц, не имеющих права доступа в помещения, достигается путем:

1) оснащения помещений входными дверьми с замками;

2) обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода,

3) опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;

4) утверждения правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

5) утверждения перечня лиц, имеющих право доступа в помещения.

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

12. Ответственный пользователь СКЗИ осуществляет учет хранилищ[1] и ключей от них в журнале учета хранилищ и ключей от них. Форма журнала учета хранилищ и ключей от них приведена в Приложении №1.

13. Спецпомещения[2] подлежат опечатыванию или оснащаются охранной сигнализацией, связанной со службой охраны здания. Исправность охранной сигнализации должна проверяться не реже одного раза в месяц ответственным пользователем СКЗИ с отметкой в журнале проверки работы средств охранной сигнализации.

Форма журнала проверки работы средств охранной сигнализации приведена в Приложении №2.

По окончании рабочего дня спецпомещения и установленные в них хранилища закрываются, спецпомешения оснащенные охранной сигнализацией ставятся на охрану посредством технических средств охраны, спецпомешения, оснащенные средствами опечатывания, и установленные в спецпомещениях хранилища опечатываются с записью в журнале опечатывания (вскрытия) помещений (хранилищ). Форма журнала опечатывания (вскрытия) помещений (хранилищ) приведена в Приложении №3.

14. Ответственный пользователь СКЗИ не реже 1 раза в месяц осуществляет контроль за вскрытием, опечатыванием спецпомещений и установленных в них хранилищ с обязательной отметкой в журнале опечатывания (вскрытия) хранилищ. Хранение ключей от хранилищ установленных в спецпомещениях ответственный пользователь СКЗИ осуществляет в специально выделенном хранилище.

---

1 Хранилища – это сейфы, шкафы индивидуального пользования, оборудованные приспособлениями для опечатывания замочных скважин, предназначенные для хранения носителей с дистрибутивами СКЗИ, документации к СКЗИ, ключевых носителей, машинных носителей с защищаемой информацией.

2 Спецпомещения – это помещения, предназначенные для выполнения должностных обязанностей ответственными пользователями СКЗИ.

15. При утрате ключа от входной двери в спецпомещение или от установленного в нем хранилища замок меняется или переделывается его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь СКЗИ.

В обычных условиях спецпомещения могут быть вскрыты только сотрудниками, имеющими право доступа в соответствующие спецпомещения.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещение ответственный пользователь СКЗИ немедленно сообщает ответственному пользователю СКЗИ или руководителю о случившемся, оценивает возможность компрометации хранящихся ключевых и других документов, составляет акт и принимает, при необходимости, меры к локализации последствий компрометации и к замене скомпрометированных криптоключей.

16. Ключи от дверей спецпомещений учитываются ответственным пользователем СКЗИ в журнале учета хранилищ и ключей от них.

Дубликаты ключей от спецпомещений хранятся у руководителя ответственного пользователя СКЗИ в сейфе.

17. Личные печати сотрудников, предназначенные для опечатывания спецпомещений и установленных в них хранилищ, должны находиться у сотрудников, ответственных за хранилища и/или работающих в спецпомещениях. Выдачу личных печатей сотрудникам осуществляет ответственный пользователь СКЗИ с отметкой в журнале учета личных печатей, предназначенных для опечатывания помещений (хранилищ).Форма журнала учета личных печатей, предназначенных для опечатывания помещений (хранилищ) приведена в Приложении №4.

18. Спецпомещения должны быть оснащены достаточным числом надежно запираемых хранилищ индивидуального пользования, оборудованных внутренними замками и приспособлениями для опечатывания замочных скважин или кодовыми замками. Ключи от этих хранилищ должны находиться у соответствующих ответственных пользователей СКЗИ либо храниться в специально выделенном для хранения ключей хранилище. Дубликаты ключей от хранилищ хранятся у руководителя ответственного пользователя СКЗИ в сейфе.

19. Техническое обслуживание СКЗИ в спецпомещениях и смена криптоключей осуществляется в отсутствие лиц, не допущенных к работе с данными СКЗИ.

20. Для криптографической защиты информации должны применяться только сертифицированные по требованиям Федеральной службы безопасности Российской Федерации СКЗИ.

21. Технические характеристики и состав программного обеспечения должны соответствовать требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ.

22. 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 визуально контролируемым. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства отключаются от линии связи и убираются в опечатываемые хранилища.

Глава 4. Регистрация и учет СКЗИ, ключевых документов и эксплуатационной и технической документации к ним

23. Носители дистрибутивов СКЗИ, эксплуатационная и техническая документация к ним, формуляры подлежат поэкземплярному учету в журнале учета эксплуатационной и технической документации. Форма журнала учета эксплуатационной и технической документации приведена в Приложении №5.

24. Лицензии на СКЗИ подлежат поэкземплярному учету в журнале учета средств криптографической защиты информации. Форма журнала учета средств криптографической защиты информации приведена в Приложении №6.

25. Криптоключи подлежат поэкземплярному учету в журнале учета ключевых документов. Форма журнала учета ключевых документов приведена в Приложении №7.

Журналы ведутся ответственным пользователем СКЗИ до полного использования, после чего закрываются. Все числящиеся на момент закрытия журнала лицензии на СКЗИ, эксплуатационная и техническая документация к ним, формуляры, ключевые документы берутся на учет во вновь заведенном журнале.

При ведении журналов не допускается применение корректирующих средств. С учетом особенности эксплуатации отдельных СКЗИ допускается добавление в журналы полей или их перестановка.

26. Единицей поэкземплярного учета криптоключей является ключевой носитель. Если один и тот же ключевой носитель многократно используется для записи криптоключей, то каждый раз такой носитель подлежит отдельной регистрации.

27. Если эксплуатационной и технической документацией к СКЗИ криптоключи вводятся и хранятся (на весь срок их действия) в СКЗИ программно-аппаратной реализации, то электронная запись соответствующего криптоключа регистрируется в техническом (аппаратном) журнале. Форма технического (аппаратного) журнала приведена в Приложении №8.

Глава 5.Выдача СКЗИ, ключевых документов, эксплуатационной и технической документации к ним

28. Выдача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов осуществляется ответственным пользователем СКЗИ под подпись в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ допускается между пользователями СКЗИ и (или) ответственным пользователем СКЗИ под подпись в соответствующем журнале поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована ответственным пользователем СКЗИ.

29. Изготовление (заказ) ключевой информации для пользователей СКЗИ (далее - сотрудники), осуществляется на основании решения руководителя Управления социальной политики №21, поручения ответственного пользователя СКЗИ или служебной записки руководителя структурного подразделения сотрудника.

30. По истечению срока действия, криптоключ подлежит смене, в порядке, предусмотренном эксплуатационной и технической документацией к СКЗИ или регламентом удостоверяющего центра, от которого получен ключевой документ.

31. Ключи записываются только на учтенные машинные носители информации.

32. Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем СКЗИ только после поступления от всех заинтересованных пользователей СКЗИ подтверждения о получении ими очередных ключевых документов.

33. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю СКЗИ или по его указанию должны быть уничтожены на месте.

Глава 6.Инсталляция СКЗИ

34. Инсталляция СКЗИ на рабочие места пользователей СКЗИ осуществляется на основании поручения руководителя, ответственного пользователя СКЗИ или по заявке на инсталляцию СКЗИ от руководителя структурного подразделения.

Форма заявки на инсталляцию СКЗИ приведена в Приложении № 9.

35. Перед инсталляцией СКЗИ проводится обследование помещения на соответствие требованиям, предъявляемым к помещениям технической и эксплуатационной документацией к СКЗИ.

36. Допуск пользователей СКЗИ к работе с СКЗИ осуществляется после прохождения ими обучения работе с СКЗИ. Обучение проводит ответственный пользователь СКЗИ. Обучение включает ознакомление с требованиями нормативных правовых актов и локальных актов Управления социальной политики №21, регламентирующих организацию криптографической защиты информации и предусматривающих порядок обращения с СКЗИ, эксплуатационной и технической документацией к СКЗИ. О факте проведения обучения делается отметка в журнале учета пользователей СКЗИ. Форма журнала учета пользователей СКЗИ приведена в Приложении №10.

37. Инсталляция завершается составлением акта установки и ввода в эксплуатацию СКЗИ. В рабочую группу включается ответственный пользователь СКЗИ и непосредственный руководитель пользователя СКЗИ. Акт установки и ввода в эксплуатацию СКЗИ подлежит хранению у ответственного пользователя СКЗИ.

Форма акта установки и ввода в эксплуатацию СКЗИ приведена в Приложении №11.

Глава 7. Порядок эксплуатации СКЗИ

38. Эксплуатация СКЗИ осуществляется в соответствии с технической и эксплуатационной документацией к нему.

39. Эксплуатационная и техническая документация к СКЗИ, ключевые документы должны храниться в хранилищах в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Отдельно от ключей подлежат хранению резервные ключевые документы, предназначенные для применения в случае компрометации действующих.

Неиспользуемые или выведенные из действия ключевые носители подлежат возращению ответственному пользователю СКЗИ либо криптоключи, записанные на них, подлежат уничтожению на месте.

40. Ежедневно перед началом работы с объектом информатизации (далее — ОИ) контролируется наличие и целостность номерной наклейки (пломбы), которой опечатан системный блок. После входа в операционную систему контролируется запуск антивирусного программного обеспечения и актуальность антивирусных баз.

41. Во время эксплуатации СКЗИ осуществляется контроль целостности установленного СКЗИ с помощью механизма самого СКЗИ или с помощью программного обеспечения контроля целостности.

42. Во время эксплуатации СКЗИ пользователям СКЗИ запрещается:

1) изменять настройки СКЗИ;

2) осуществлять вскрытие системного блока ОИ с установленными СКЗИ, подключать к ним дополнительные устройства без разрешения ответственного пользователя СКЗИ;

3) оставлять без контроля ключевые носители, а также ОИ с установленными СКЗИ при включенном питании;

4) вносить какие-либо несанкционированные изменения в СКЗИ;

5) выводить на монитор защищаемую информацию (в т.ч. информацию ключевых документов), обрабатываемых с использованием СКЗИ в присутствии лиц, не имеющих к такой информации права доступа;

6) применять скомпрометированные ключи и пароли;

7) осуществлять несанкционированное копирование ключевой информации;

8) вставлять ключевой носитель в устройства, штатный порядок работы которых не предусматривает использование ключевого носителя.

Глава 8. Контроль за соблюдением эксплуатации средств криптографической защиты информации

43. Ежегодно комиссией, в которую входят сотрудники Управления социальной политики №21, проводятся плановая проверка:

1) наличия, правильности учета и соблюдения правил обращения и хранения СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

2) выявление установочных носителей СКЗИ, ключевых документов, экземпляров технической и эксплуатационной документации подлежащей уничтожению;

3) соблюдения правил обращения с СКЗИ, предусмотренных настоящим Положением пользователями СКЗИ.

44. Внеплановые проверки проводятся комиссией, в которую входят сотрудники Управления социальной политики №21, в случаях нарушения установленного в Управлении социальной политики №21 порядка криптографической защиты информации.

Состав комиссии определяет руководитель Управления социальной политики №21.

45. По завершении проверки комиссией составляется акт проверки, в котором указывается состав комиссии, основание проверки, проверочные мероприятия, недостатки, выявленные в ходе проверки, и рекомендации по их устранению, рекомендации по совершенствованию криптографической системы защиты информации.

Глава 9. Проведение проверок по инцидентам, связанным с эксплуатацией СКЗИ

46. Инцидентом, связанным с эксплуатацией СКЗИ, является событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, результатом которой являются:

1) нарушение или возможное нарушение работы СКЗИ;

2) нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов Управления социальной политики №21 в области криптографической защиты информации;

3) нарушение или возможное нарушение в выполнении технологических процессов обработки информации с использованием СКЗИ.

В случае возникновения конфликтной ситуации и по фактам (подозрению) нарушения конфиденциальности информации, защищаемой с помощью СКЗИ, проводится проверка.

Проверка проводится ответственным пользователем СКЗИ.

Проверки проводятся на основании обращений сотрудников, информационных писем (претензий) сторонних организаций, при непосредственном обнаружении факта (подозрения) нарушения конфиденциальности защищаемой информации, безопасность которых обеспечивается с применением СКЗИ, с отметкой в журнале учета инцидентов в информационных системах.

О результатах проверки ответственный пользователь СКЗИ докладывает руководителю Управления социальной политики №21.

47. Решение об инициализации служебной проверки принимает ответственный за организацию обработки персональных данных.

48. Решение о назначении проведения служебной проверки принимает руководитель Управления социальной политики №21.

Глава 10. Порядок действий при компрометации ключа

49. Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

50. Различают явную и неявную компрометацию ключей. Явной называется компрометация, факт которой становится известным на отрезке установленного времени действия данного ключа. Неявной называется компрометация ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа.

События, квалифицируемые как явная компрометация:

1) утрата ключевого носителя;

2) утрата ключевого носителя с последующим обнаружением;

3) нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации.

К событиям, связанным с неявной компрометацией ключей и требующим их рассмотрения в каждом конкретном случае, относятся:

1) навязывание заведомо ложной информации в документах, защищенных имитовставками;

2) случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями, содержащими ключевую информацию, в том числе случаи, когда дискета (*eToken* и др.) вышла из строя и доказательно не опровергнуто, что данный факт произошел в результате несанкционированного доступа злоумышленника.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их чтения, копирования.

51. При наступлении компрометации ключа или подозрения в компрометации ключа пользователь СКЗИ обязан немедленно прекратить работу с СКЗИ и сообщить ответственному пользователю СКЗИ о факте компрометации (в том числе и предполагаемом).

По факту компрометации ключей (в том числе предполагаемому) проводится проверка в соответствии с главой 8 настоящего Положения.

52. Скомпрометированные ключи по завершению проверки подлежат уничтожению.

Взамен скомпрометированных ключей ответственный пользователь СКЗИ производит выдачу новых ключей в порядке, предусмотренном технической и эксплуатационной документацией к СКЗИ и/или регламентом удостоверяющего центра.

Глава 11. Деинсталляция средств криптографической защиты информации

53. Деинсталляция СКЗИ с рабочих мест пользователей СКЗИ осуществляется на основании поручения руководителя Управления социальной политики №21, ответственного пользователя СКЗИ, информации об увольнении или уходе в отпуск по уходу за ребенком от отдела кадров или по заявке на деинсталляцию СКЗИ от руководителя структурного подразделения.

Форма заявки на деинсталляцию СКЗИ приведена в Приложении №12.

54. Деинсталляция СКЗИ осуществляется рабочей группой в соответствии с процедурой, предусмотренной эксплуатационной и технической документацией к СКЗИ, с составлением акта деинсталляции СКЗИ. В рабочую группу включается ответственный пользователь СКЗИ и непосредственный руководитель

пользователя СКЗИ. Акт о деинсталляции СКЗИ подлежит хранению у ответственного пользователя СКЗИ.

Форма акта деинсталляции СКЗИ приведена в приложении № 13.

55. Одновременно с деинсталляцией СКЗИ уничтожаются криптоключи, если не планируется их дальнейшее использование. В противном случае они возвращаются ответственному пользователю СКЗИ с отметкой в журнале учета ключевых документов.

Факт уничтожения криптоключей с ключевого носителя совместно с деинсталляцией СКЗИ фиксируется в акте деинсталляции СКЗИ.

56. О факте деинсталляции СКЗИ делается отметка в журнале учета средств криптографической защиты информации.

Глава 12. Уничтожение СКЗИ

57. Уничтожение инсталляционных носителей СКЗИ, эксплуатационной и технической документации, лицензий, утративших свое практическое значение, производится по акту уничтожения инсталляционных носителей СКЗИ, лицензий, эксплуатационной и технической документации и внесением информации об уничтожении в журналы учета. В акте указывается, что уничтожается и в каком количестве, а также делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых инсталлирующих носителей СКЗИ, эксплуатационной и технической документации к ним, лицензий.

Образец оформления акта уничтожения инсталляционных носителей СКЗИ, лицензий, эксплуатационной и технической документации приведена в Приложении №14.

Акт уничтожения инсталляционных носителей СКЗИ, лицензий, эксплуатационной и технической документации подлежит хранению у ответственного пользователя СКЗИ.

Бумажные и прочие сгораемые носители эксплуатационной и технической документации к СКЗИ, инсталляционные носители СКЗИ, лицензий уничтожают путем сжигания или с помощью любых бумагорезательных машин.

Уничтожение производится комиссией в составе не менее трех человек.

58. Уничтожение криптоключей производится истечение срока их действия, вывод из эксплуатации СКЗИ, увольнение сотрудника, снятие с сотрудника обязанностей, связанных с использованием СКЗИ, компрометация ключей.

Уничтожение криптоключей производится путем стирания (разрушения) криптоключей без повреждения ключевого носителя, а в случае отсутствия возможности стирания путем физического уничтожения ключевого носителя.

Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков, SmartCard и т.п.). Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируется эксплуатационной и технической документацией к соответствующем СКЗИ, а также указаниями организаций, производивших запись криптоключей.

Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а

также восстановление 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.

Бумажные и прочие сгораемые ключевые носители уничтожают путем сжигания или с помощью любых бумагорезательных машин.

Криптоключи (ключевые носители) должны уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то криптоключи (ключевые носители) должны быть уничтожены не позднее десяти дней после вывода их из действия.

Информация, хранящиеся в криптографически защищенном виде, должна быть перешифрована на новых криптоключах.

Об уничтожении криптоключей делается отметка в журнале учета ключевых документов.

59. Уничтожение СКЗИ производится путем их изъятия из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к ним процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

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 должна быть надежно удалена.

Удаление программного обеспечения СКЗИ проводится в порядке, предусмотренном главой 11 настоящего Положения.

Приложение № 1

ЖУРНАЛ
учета хранилищ и ключей от них

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Номер ключа от хранилища,вид и регистра-ционный (инвентарный) номер хранилища	Местонахождения хранилища	Ключ в пенале(да/нет)	ПОЛУЧЕНО (Фамилия, инициалы, подпись получившего ключ, дата)	СДАНО (Фамилия, инициалы, подпись сдавшего ключ, дата)	УТЕРЯНО (Фамилия, инициалы, подпись утерявшего ключ, дата)	Примечание
1	2	3	4	5	6	7	8

Шаблон оформления журнала учета хранилищ и ключей от них

Приложение № 2

ЖУРНАЛ
проверок работы средств охранной сигнализации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Дата	Номер помещения	Вид работы	Ф.И.О., подпись ответственного лица
1	2	3	4	5

Шаблон оформления журнала проверок работы средств охранной сигнализации

Приложение № 3

ЖУРНАЛ

опечатывания (вскрытия) помещений (хранилищ)

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Номер печати, которой опечатано помещение (хранилище)	Дата и время опечатывания помещения (хранилища)	Ф.И.О. и подпись лица, опечатавшего помещение (хранилище)	Дата и время вскрытия помещения (хранилища)	Номер печати, которой было опечатано помещение (хранилище)	Ф.И.О.и подпись лица, вскрывшего помещение (хранилище)
1	2	3	4	5	6	7

Шаблон оформления журнала опечатывания (вскрытия) помещений (хранилищ)

Приложение № 4

ЖУРНАЛ

учета личных печатей, предназначенных для опечатывания помещений (хранилищ)

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п.	Наименование печати	Оттиск печати	Наименование подразделения, должность, фамилия, имя, отчество получателя	Подпись в получении, дата	Результат ежегодной проверки печатей(их оттиски и дата проверки)	Оттиск печатей, возвращенных для уничтожения, дата возврата	Отметка об уничтожении, номер акта и дата	Приме-чание
1	2	3	4	5	6	7	8	9

Шаблон оформления журнала учета личных печатей, предназначенных для опечатывания помещений (хранилищ)

Приложение № 5

ЖУРНАЛ

учета эксплуатационной и технической документации к СКЗИ

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Наименование эксплуатационной и технической документации, формуляров к СКЗИ	Тип носи-теля	Регистрационные номера	№ экз.	Отметка о получении			Отметка о выдаче
					от кого полу-чены	дата и номер сопрово-дительного письма, товарной накладной (иного документа о получении)	Ф.И.О. ответственного пользователя СКЗИ получившего документацию, дата получения, подпись	Ф.И.О./ наименование организации получателя
1	2	3	4	5	6	7	8	9

Шаблон оформления журнала учета эксплуатационной и технической документации к СКЗИ (левый разворот)

Отметка о выдаче	Отметка о выдаче		Отметка о возврате			
дата получения и номер доверенности/дата и номер сопроводительного письма	Ф.И.О. получившего, дата, расписка/дата и номер подтверждения получения	Ф.И.О. сотрудника, выдавшего СКЗИ,	Ф.И.О. ответственного пользователя СКЗИ принявшего	дата и расписка в получении	Дата и номер акта об уничтожении/перерегистрации	Примечание
10	11	12	13	14	15	16

Шаблон оформления журнала учета эксплуатационной и технической документации к СКЗИ (правый разворот)

Приложение № 6

ЖУРНАЛ

учета средств криптографической защиты информации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Наименование СКЗИ, номер лицензий	Отметка о получении			Отметка об установке (выдаче)	
		от кого получены	дата и номер сопроводительного письма, товарной накладной (иного документа о получении)	Ф.И.О. ответственного пользователя СКЗИ получившего документацию, дата получения, подпись	Ф.И.О (наименование) пользователя СКЗИ	Наименование и регистрационный номер АРМ (дата, номер доверенности)
1	2	3	4	5	6	7

Шаблон оформления журнала учета средств криптографической защиты информации (левый разворот)

Отметка об установке (выдаче)		Отметка о деинсталляции		Номер и дата акта об уничтожении лицензии	Примечание
дата и номер акта установки (дата и расписка в получении)	Ф.И.О./наименование производившего установку (выдачу)	дата и номер акта деинсталляции СКЗИ	Ф.И.О. /наименование производившего деинсталляцию		
5	6	7	8	9	10

Шаблон оформления журнала учета средств криптографической защиты информации (правый разворот)

Приложение № 7

ЖУРНАЛ
учета ключевых документов

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Наименование и номер ключевого документа,	Номера серий ключевых документов	Номер экземпляра ключевого документа	Отметка о получении	
				Наименование юридического лица, от кого получен ключевойдокумент	Дата получения/изготовления ключевых документов
1	2	3	4	5	6

Шаблон оформления журнала учета ключевых документов (левый разворот)

Отметка о выдаче			Возврат	Уничтожение	Примечание
Ф.И.О. получателя, наименование организации получателя	Дата получения/дата и номер доверенности/дата и номер сопроводительного письма	Ф.И.О. получившего, расписка/дата и номер подтверждения получения	Ф.И.О. получившего, дата получения, подпись	Ф.И.О. уничтожившего, дата, подпись/дата и номер документа об уничтожении	
7	8	9	10	11	12

Шаблон оформления журнала учета ключевых документов (правый разворот)

Приложение № 8

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ) ЖУРНАЛ

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

Шаблон оформления технического (аппаратного) журнала

Приложение № 9

ЗАЯВКА

на инсталляцию средства криптографической защиты информации

Прошу инсталлировать средство криптографической защиты информации

_____

(наименование средства криптографической защиты информации)

на АРМ, расположенный в помещении № _____,

в связи с_____

(причина инсталляции средства криптографической защиты информации)

_____

(должность) *(подпись)* *(расшифровка подписи)*

Шаблон оформления заявки на инсталляцию средства криптографической защиты информации

Приложение № 10

ЖУРНАЛ

учета пользователей средств криптографической защиты информации

Начат с _____20___г.
Окончен _____20___г.

На _____листах
Срок хранения _____ лет

№ п/п	Дата	Ф.И.О. пользователя СКЗИ	Наименование СКЗИ	Номер помещения, где размещено СКЗИ	Подпись пользователя СКЗИ, прошедшего инструктаж	Ф.И.О. и подпись ответственного пользователя СКЗИ
1	2	3	4	5	6	7

Шаблон оформления журнала учета пользователей средств криптографической защиты информации

Приложение № 11

АКТ
установки и ввода в эксплуатацию средства криптографической защиты информации

№ _____ «___» _____ 20__ г.

Рабочая группа в составе:

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

_____ _____
(должность) *(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что на основании _____
(№, дата документа на инсталляцию СКЗИ)

на технические средства и системы, приведенные в таблице 1, и находящиеся в пользовании

_____ _____
(должность, фамилия, имя, отчество пользователя СКЗИ)

_____

(далее — пользователь СКЗИ)установлено средство криптографической защиты информации (далее — СКЗИ) _____
(наименование, версия, сборка СКЗИ)

_____в

соответствии с эксплуатационно-технической документацией и введено в эксплуатацию.

Комплектация СКЗИ соответствует составу, приведенному в таблице 2.

Таблица 1.

Технические средства и системы, размещенные в помещении № _____,
расположенном по адресу _____

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), на жесткий диск которого установлено СКЗИ*		
2	*Приводятся сведения о жестком диске, на который установлено СКЗИ*		

Таблица 2.

№ п/п	Наименование
1	2
1	*Сообщаются сведения о наименовании СКЗИ*
1.1	*Сообщаются сведения о специальном защитном знаке, размещенном на установочном компакт-диске с программным обеспечением и эксплуатационной документацией*

1.2	*Сообщаются сведения о формуляре на СКЗИ*
1.3	*Сообщаются сведения о сертификате соответствия на СКЗИ*

Проведена проверка работоспособности СКЗИ. Установленное программное обеспечение работает в штатном режиме, настройки СКЗИ соответствуют требованиям технической и эксплуатационной документации к ним и правам пользователя СКЗИ, а также параметрам, приведенным в приложении к настоящему акту*(при наличии таковых параметров).*

Проведено обучение пользователя СКЗИ работе с СКЗИ.

Проведено обследование помещения № _____ на соответствие требованиям эксплуатационной и технической документации. Размещение и оборудование помещения отвечают требованиям технической и эксплуатационной документации к СКЗИ, позволяют установить СКЗИ и обеспечить сохранностьСКЗИ,информации ограниченного доступа, и ключевых документов *(при наличии ключевых документов).*

Корпус технического средства с установленным СКЗИ опечатан пломбами (номерными наклейками) № _____ от «___» _____ 20__ года. Замечания отсутствуют.

Криптоключ(и) № _____ установлены на ключевой носитель № _____ и переданы пользователю СКЗИ*(при наличии ключевых документов).*

Лицо, проводившее установку:_____

(должность,подпись, расшифровка подписи)

Руководитель
пользователя СКЗИ: _____

(должность, подпись, расшифровка подписи)

Шаблон оформления акта установки и ввода в эксплуатацию средства криптографической защиты информации

Приложение № 12

ФОРМА ЗАЯВКИ
на деинсталляцию средств криптографической защиты информации

ЗАЯВКА
на деинсталляцию средства криптографической защиты информации

Прошу деинсталлировать средство криптографической защиты информации

_____

(наименование средства криптографической защиты информации)

с АРМ, расположенного в помещении № _____,

в связи с_____

(причина деинсталляции средства криптографической защиты информации)

_____

(должность) *(подпись)* *(расшифровка подписи)*

Шаблон оформления заявки на деинсталляцию средства криптографической защиты информации

Приложение № 13

АКТ

деинсталляциисредства криптографической защиты информации

№ _____ «___» _____ 20__ г.

Рабочая группа в составе:

_____ _____

(должность) *(Фамилия, Имя, Отчество)*

_____ _____

(должность) *(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что на основании заявки/служебной записки_____

_____

(№, дата документа на инсталляцию СКЗИ)

с технических средств и систем, приведенных в таблице 1, и находящихся в пользовании

_____

(должность, фамилия, имя, отчество пользователя СКЗИ)

произведена деинсталляция средства криптографической защиты информации (далее — СКЗИ)

_____

(наименование, версия, сборка СКЗИ)

следующим способом:[3]_____.

Таблица 1.

Технические средства и системы, размещенные в помещении № _____ ,
расположенном по адресу _____

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), с жесткого диска которого деинсталлировано СКЗИ*		
2	*Приводятся сведения о жестком диске, с которого деинсталлировано СКЗИ*		

Ключевые документы № _____, находящиеся на ключевом носителе № _____ уничтожены (возвращены ответственному пользователю СКЗИ)*(при наличии ключевых документов).*

Лицо, проводившее деинсталляцию: _____ ___

(должность,подпись, расшифровка подписи)

Руководитель
пользователя СКЗИ: _____

(должность,подпись, расшифровка подписи)

Шаблон оформления акта деинсталляции средства криптографической защиты информации

---

3 Способ уничтожения СКЗИ и ключевых документов регламентируется эксплуатационной и технической документацией к ним. В частности, к способам уничтожения относятся переформатирование, удаление программного обеспечения СКЗИ, физическое уничтожение носителей.