**ПРИКАЗ**

|  |  |  |
| --- | --- | --- |
| «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ г. |  | №\_\_\_\_\_\_\_ |

Об создании органа криптографической защиты

В целях исполнения требований "[Инструкции](https://normativ.kontur.ru/document?moduleid=1&documentid=45974#l11) об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденной приказом ФАПСИ от 13 июня 2001 г. N 152, приказываю:

1. Создать орган криптографической защиты и назначить ответственными за организацию работ по криптографической защите информации:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| (должность) |  | (ФИО) |
|  |  |  |
| (должность) |  | (ФИО) |
|  |  |  |
| (должность) |  | (ФИО) |
|  |  |  |
| (должность) |  | (ФИО) |

2. Утвердить Инструкцию по обращению со средствами криптографической защиты информации (СКЗИ) (приложение N 1).

3. Утвердить Инструкцию ответственного за организацию работ по криптографической защите информации (приложение N 2).

4. Утвердить Инструкцию пользователей средств криптографической защиты информации (приложение N 3).

5. Ответственному за организацию работ по криптографической защите информации ознакомиться под роспись и руководствоваться в своей деятельности Инструкцией по обращению со средствами криптографической защиты информации и Инструкцией ответственного за организацию работ по криптографической защите информации.

6. Ответственному за организацию работ по криптографической защите информации ознакомить под роспись пользователей СКЗИ с Инструкцией по обращению с СКЗИ и Инструкцией пользователей средств криптографической защиты информации.

7. Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти обучение и проверку знаний по правилам работы с СКЗИ.

8. Утвердить форму Перечня пользователей СКЗИ (приложение N 5).

9. Утвердить форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (приложение N 4).

10. Утвердить форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов (приложение N 6).

11. Контроль за исполнением настоящего приказа возложить на \_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| Руководитель | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

*Приложение N 1*

*к приказу от \_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_\_\_\_\_*

**ИНСТРУКЦИЯ ПО ОБРАЩЕНИЮ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

**1. Общие положения**

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ), которые осуществляют работы с применением СКЗИ.

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов другие действия согласно технической документации на СКЗИ.

Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Данная инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях "Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденной приказом ФАПСИ [от 13 июня. 2001 г. N 152](https://normativ.kontur.ru/document?moduleid=1&documentid=45974#l0) (далее - Инструкция ФАПСИ от 13 июня 2001 г. N 152), "[Положения](https://normativ.kontur.ru/document?moduleid=1&documentid=156612#l4) о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)", утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66, а также "[Состава](https://normativ.kontur.ru/document?moduleid=1&documentid=240493#l2) 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", утвержденных приказом ФСБ от 10.07.2014 N 378.

**2. Термины и определения**

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами;

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

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

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).

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.

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

Орган криптографической защиты (ОКЗ) - структурное подразделение Организации, работник Организации или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Ответственный за организацию работ по криптографической защите информации (Ответственный) - сотрудник Организации, отвечающий за реализацию мероприятий связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ - работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

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.

**3. Порядок получения допуска пользователей к работе с СКЗИ**

Для получения допуска к работе с СКЗИ, работнику необходимо пройти обучение правилам работы с СКЗИ и проверку знаний.

Основанием для допуска пользователя к работе с СКЗИ является внесение его в перечень пользователей СКЗИ, утверждаемый руководителем Организации.

Контроль над реализацией данных мероприятий возлагается на Ответственного.

**4. Работа с СКЗИ**

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей в присутствии посторонних лиц запрещено. В организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть промаркированы и должны использоваться, учитываться и храниться в общем порядке. Все копии учитываются за отдельным номером.

Каждый ключевой документ должен быть зарегистрировать в Журнале поэкземплярного учета СКЗИ.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только с разрешения руководителя организации с соответствующей пометкой в журнале поэкземплярного учета.

При обнаружении на рабочей станции с установленным СКЗИ программного обеспечения, не соответствующего объему и сложности решаемых задач на данном рабочем месте, а также вирусных программ, незамедлительно должны быть организованы работы по расследованию инцидента информационной безопасности.

**5. Действия в случае компрометации ключей**

О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за организацию работ по криптографической защите информации.

К компрометации ключей относятся следующие события:

1) утрата носителей ключа;

2) утрата иных носителей ключа с последующим обнаружением;

3) возникновение подозрений на утечку ключевой информации или ее искажение;

4) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура, опечатывания сейфов;

5) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

7) доступ посторонних лиц к ключевой информации;

8) другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ.

В случае компрометации ключа пользователя незамедлительно должны быть приняты меры по отзыву ключа (отзыв ключа электронной подписи в удостоверяющем центре, обновление списков отозванных сертификатов, замена криптоключа пользователя и т.п.), а также проведено расследование по факту компрометации.

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

Расследование инцидентов информационной безопасности, связанных с компрометацией ключевых носителей и ключевой документацией, осуществляет (обладатель скомпрометированной информации ограниченного доступа). При необходимости, привлекается орган криптографической защиты.

**6. Ответственность лиц, допущенных к работе с СКЗИ**

За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

**Лист ознакомления с Инструкцией по обращению со средствами криптографической защиты информации**

**(утверждена приказом от "\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. N \_\_\_\_\_)**

|  |  |  |  |
| --- | --- | --- | --- |
| N п/п | ФИО | Должность | Подпись, дата |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Приложение N 2*

*к приказу от \_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_\_\_\_\_*

**ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ РАБОТ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ**

**1. Общие положения**

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за организацию работ по криптографической защите информации (далее - Ответственный), которые осуществляют работы с применением средств криптографической защиты информации (далее - СКЗИ).

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия согласно технической документации на СКЗИ.

Ответственный назначается приказом руководителя Организации.

Данная инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях "[Инструкции](https://normativ.kontur.ru/document?moduleid=1&documentid=45974#l11) об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденной приказом ФАПСИ от 13 июня 2001 г. N 152 (далее - Инструкция ФАПСИ от 13 июня 2001 г. N 152), "[Положения](https://normativ.kontur.ru/document?moduleid=1&documentid=156612#l4) о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)", утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66, а также "[Состава](https://normativ.kontur.ru/document?moduleid=1&documentid=240493#l2) 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", утвержденных приказом ФСБ от 10.07.2014 N 378.

**2. Термины и определения**

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

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).

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.

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

Орган криптографической защиты (ОКЗ) - структурное подразделение Организации, работник Организации или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ - работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

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.

**3. Обязанности Ответственного**

При реализации мероприятий, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться действующим законодательством Российской Федерации, Инструкцией по обращению с СКЗИ, а также настоящей инструкцией.

На Ответственного возлагается проведение следующих мероприятий:

1) Ведение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

2) Хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним;

3) Принятие ключевых документов к СКЗИ от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

4) Своевременная актуализация перечня пользователей СКЗИ;

5) Ежегодная проверка наличия СКЗИ, эксплуатационной и технической документации к ним, согласно Журналу поэкземплярного учета СКЗИ.

Ответственный обязан:

1) Не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;

2) Обеспечивать сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;

3) Обеспечить соблюдение требований к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

4) Контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

5) Немедленно уведомлять непосредственного руководителя о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

6) Не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

**4. Права Ответственного**

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

1) Требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ и Инструкции пользователя СКЗИ;

2) Обращаться к непосредственному руководителю с предложением прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

3) Инициировать проведение служебных расследований по фактам нарушения в Организации порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

**5. Порядок передачи обязанностей при смене Ответственного**

При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

**6. Ответственность за невыполнение настоящей инструкции**

За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

**Лист ознакомления с Инструкцией ответственного за организацию работ по криптографической защите информации**

**(утверждена приказом от "\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. N \_\_\_\_)**

|  |  |  |  |
| --- | --- | --- | --- |
| N п/п | Фамилия, Имя, Отчество | Должность | Подпись, дата |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Приложение N 3*

*к приказу от \_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_\_\_\_\_*

**ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЕЙ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

**1. Общие положения**

Настоящая Инструкция разработана в целях регламентации действий работников, допущенных к работам с использованием средств криптографической защиты информации (далее - Пользователей).

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия согласно технической документации на СКЗИ.

Данная инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях "[Инструкции](https://normativ.kontur.ru/document?moduleid=1&documentid=45974#l11) об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденной приказом ФАПСИ от 13 июня 2001 г. N 152 (далее - Инструкция ФАПСИ от 13 июня 2001 г. N 152), "[Положения](https://normativ.kontur.ru/document?moduleid=1&documentid=156612#l4) о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)", утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66, а также "[Состава](https://normativ.kontur.ru/document?moduleid=1&documentid=240493#l2) 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", утвержденных приказом ФСБ от 10.07.2014 N 378.

**2. Термины и определении**

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами;

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

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

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).

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.

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

Орган криптографической защиты (ОКЗ) - структурное подразделение Организации, работник Организации или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Ответственный за организацию работ по криптографической защите информации (Ответственный) - сотрудник Организации, отвечающий за реализацию мероприятий, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ - работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

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.

**3. Обязанности пользователей СКЗИ**

Пользователи СКЗИ обязаны:

1) соблюдать конфиденциальность информации ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;

2) обеспечивать сохранность вверенных ключевых носителей и ключевой документации на них;

3) соблюдать требования безопасности информации ограниченного доступа при использовании СКЗИ;

4) незамедлительно сообщать Ответственному о ставших им известными попытках получения посторонними лицами доступа к сведениям об используемых СКЗИ, ключевым носителям и ключевой документации;

5) при увольнении или отстранении от исполнения обязанностей сдать Ответственному носители с ключевой документацией;

6) при подозрении на компрометацию ключевой документации, а также при обнаружении факта утраты или недостачи СКЗИ, ключевых носителей, ключевой документации, хранилищ, личных печатей незамедлительно уведомлять Ответственного.

Пользователям СКЗИ запрещается:

1) выводить ключевую информацию на средствах отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.);

2) оставлять ключевые носители с ключевой документацией без присмотра;

3) записывать на ключевой носитель информацию, не связанную с работой СКЗИ (текстовые и мультимедиа файлы, служебные файлы и т.п.);

4) вносить любые изменения в программное обеспечение СКЗИ;

**4. Ответственность пользователей СКЗИ**

За нарушение установленных требований по эксплуатации криптосредств пользователь СКЗИ несет ответственность в соответствии с действующим законодательством Российской Федерации.

**Лист ознакомления с Инструкцией пользователей средств криптографической защиты информации (утверждена приказом от "\_\_" \_\_\_\_\_\_\_\_ 20\_\_ г. N \_\_)**

|  |  |  |  |
| --- | --- | --- | --- |
| N п/п | ФИО | Должность | Подпись, дата |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Приложение N 4*

*к приказу от \_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_\_\_\_\_*

**ЖУРНАЛ ПОЭКЗЕМПЛЯРНОГО УЧЕТА СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ (ДЛЯ ОБЛАДАТЕЛЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ)**

*Начат: "\_\_" \_\_\_\_\_\_\_\_20\_\_ г.*

*Окончен: "\_\_" \_\_\_\_\_\_\_\_20\_\_ г.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N 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 | | Отметка о подключении (установке) СКЗИ | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | | Примечание |
| От кого получены | Дата и номер сопроводительного письма | Ф.И.О. пользователя СКЗИ | Дата и расписка в получении | Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, 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. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение) | Номер акта или расписка об уничтожении |  |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

*Приложение N 5*

*к приказу от \_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_\_\_\_\_*

**ПЕРЕЧЕНЬ ПОЛЬЗОВАТЕЛЕЙ, ДОПУЩЕННЫХ К РАБОТЕ С СКЗИ**

|  |  |  |
| --- | --- | --- |
| N | ФИО сотрудника | Должность |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Приложение N 6*

*к приказу от \_\_\_\_\_\_\_\_\_\_\_ N \_\_\_\_\_\_\_\_\_\_\_*

**ФОРМА АКТА N \_\_\_\_ ОТ "\_\_" \_\_\_\_\_\_\_\_ 20\_\_ Г. ОБ УНИЧТОЖЕНИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ, СОДЕРЖАЩИХСЯ НА КЛЮЧЕВЫХ НОСИТЕЛЯХ И КЛЮЧЕВЫХ ДОКУМЕНТОВ**

|  |  |  |
| --- | --- | --- |
| Комиссия |  | в составе: |
|  | (название организации) |  |
|  |  |  |
|  |  |  |
|  |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N п/п | Учетный номер ключевого носителя (документа) | Номер (идентификатор) криптографического ключа, наименование документа | Владелец ключа (документа) | Количество ключевых носителей (документов) | Номера экземпляров |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

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 СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов подтверждаю:

|  |  |
| --- | --- |
|  | Председатель комиссии |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Члены комиссии: |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |