**ПРИКАЗ**

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

|  |
| --- |
| Об утверждении перечня мер, направленныхна выполнение требований законодательстваРоссийской Федерации в области защитыинформации с использованием средствкриптографической защиты |

В целях выполнения требований законодательства Российской Федерации в области защиты информации при ее передаче по открытым каналам в связи с использованием средств криптографической защиты, приказываю:

1. Назначить ответственным пользователем криптосредств в *<наименование организации> <должность> <ФИО>*.
2. Утвердить инструкцию ответственного пользователя криптосредств в *<наименование организации>* (Приложение 1).
3. Утвердить инструкцию пользователя криптосредств в *<наименование организации>* (Приложение 2).
4. Утвердить перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных (пользователи криптосредств) в *<наименование организации>*(Приложение 3).
5. Утвердить Форму Журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (Приложение 4).
6. Утвердить Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств (Приложение 5).

Контроль за исполнением настоящего приказа оставляю за собой.

|  |  |
| --- | --- |
| Руководитель | *<ФИО руководителя>* |

Приложение №1 к приказу №\_\_\_\_\_\_

от « » \_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

**ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ В *<наименование учреждения>***

г. Белгород

20\_\_ г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция ответственного пользователя криптосредств в <*наименование учреждения* > (далее - Инструкция) определяет основные обязанности и права ответственного пользователя криптосредств.

1.2. Ответственный пользователь криптосредств назначается распоряжением <*наименование учреждения* > (далее - Учреждение) и отвечает за организацию, обеспечение функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн).

1.3. Ответственный пользователь криптосредств должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки персональных данных.

1.4. В своей деятельности, связанной с обработкой персональных данных, ответственный пользователь криптосредств руководствуется настоящей Инструкцией.

1. ОБЯЗАННОСТИ ответственного пользователя криптосредств

Ответственный пользователь криптосредств обязан:

2.1. Соблюдать требования нормативных актов Учреждения, устанавливающих порядок работы с персональными данными.

2.2. Осуществлять контроль за организацией, обеспечением функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных:

- контролировать соблюдение условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

- обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

- вносить предложения по режиму охраны помещений, в которых установлены криптосредства или хранятся ключевые документы к ним;

- вести Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (далее - Журнал);

- выдавать пользователям криптосредств экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов под расписку в соответствующем Журнале;

- вести на каждого пользователя криптосредств Лицевой счет, в котором регистрировать числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы;

- контролировать передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующем Журнале;

- пломбировать (опечатывать) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование криптосредств, а также аппаратных и аппаратно-программных криптосредствах;

- контролировать получение и доставку криптосредств, эксплуатационной и технической документации к ним;

- заблаговременно делать заказы на изготовление очередных ключевых документов и рассылку на места использования для своевременной замены действующих ключевых документов;

- контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку в соответствующем Журнале;

- выводить из действия носители ключевой информации (далее - НКИ), в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие НКИ;

- принимать решение в чрезвычайных случаях, когда отсутствуют НКИ для замены скомпрометированных, об использовании скомпрометированных НКИ;

- проводить инструктаж пользователей криптосредств по правилам работы с криптосредствами и ключевыми документами.

2.3. Требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ с криптосредствами или нарушения функционирования криптосредств.

2.4. Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.5. Контролировать исполнение пользователями криптосредств требований нормативных актов Учреждения в части обеспечения защиты персональных данных с помощью криптосредств.

2.6. Принимать все необходимые меры для обеспечения безопасности персональных данных, в случае получения от пользователей криптосредств информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

- в каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводится служебное расследование; результатом расследования является квалификация или не квалификация данного события как компрометация;

- о факте компрометации ключевой информации пользователями криптосредств совместно с ответственным пользователем криптосредств производится информирование всех заинтересованных участников информационного обмена;

- выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в Журнале;

- для своевременного восстановления связи пользователю криптосредств выдается новый НКИ; для этого создается резервный запас НКИ, использование которых осуществляется в случаях крайней необходимости по решению ответственного пользователя криптосредств.

2.7. Подготавливать копии НКИ, которые подлежат основному учету и хранятся в сейфе ответственного пользователя криптосредств. Данные копии применяются с разрешения руководителя Учреждения, если по результатам расследования не было установлено факта компрометации.

2.8. Хранить резервные НКИ отдельно от рабочих (актуальных) НКИ, с целью обеспечения невозможности их одновременной компрометации.

2.9. Своевременно информировать руководителя Учреждения о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

1. ПРАВА ответственного пользователя криптосредств

Ответственный пользователь криптосредств имеет право:

3.1. Знакомиться с нормативными актами Учрежления, регламентирующими процессы обработки персональных данных.

3.2. Требовать от пользователей криптосредств соблюдения требований нормативных актов Учреждения в части обеспечения защиты информации с помощью криптосредств.

3.3. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных пользователей криптосредств, в случае выявления нарушений требований по работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных, или в связи с нарушением функционирования криптосредств.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *ФИО Руководителя* «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

Приложение №2 к приказу №\_\_\_\_\_\_

от « » \_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

**ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ**

***<наименование учреждения>***

г. Белгород

20\_\_ г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция пользователя криптосредств <*наименование учреждения*> (далее - Инструкция) определяет права и обязанности пользователей криптосредств, порядок обращения с криптосредствами, а также определяет порядок восстановления связи в случае компрометации действующих ключей к криптосредствам.

1.2. Пользователем криптосредств является сотрудник <*наименование учреждения* > (далее - Учреждение), включенный в перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных, утвержденный нормативным актом Учреждения.

1.3. Пользователь криптосредств должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки персональных данных.

1.4. В своей деятельности, связанной с обработкой персональных данных, пользователь криптосредств руководствуется настоящей Инструкцией.

1.5. Пользователи криптосредств несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту криптосредств от несанкционированного использования.

1. ОБЯЗАННОСТИ И ПРАВА пользователя криптосредств

2.1. Пользователь криптосредств обязан:

- соблюдать требования по обеспечению безопасности функционирования криптосредств;

- обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;

- сдать ответственному пользователю криптосредств Учреждения (далее - Ответственный) носители ключевой информации (далее - НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

- сдать Ответственному НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;

- немедленно уведомлять руководителя структурного подразделения или Ответственного о компрометации НКИ, о фактах утраты или недостачи криптосредств;

- в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования криптосредств.

2.2. Пользователю криптосредств запрещается:

- осуществлять несанкционированное и безучетное копирование ключевых данных;

- хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

- передавать НКИ каким бы то ни было лицам, кроме Ответственного;

- во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

- хранить на НКИ какую-либо информацию, кроме ключевой;

- использовать в помещениях, где применяются криптосредства, личные технические средства, позволяющие осуществлять копирование ключевой информации;

- использовать НКИ, выведенные из действия.

2.3. Пользователь имеет право:

- вносить предложения руководителю Учреждения по вопросам использования криптосредств;

- повышать свой уровень квалификации по использованию криптосредств.

1. ПОРЯДОК ОБРАЩЕНИЯ С криптосредствАМИ

3.1. Монтаж и установка криптосредства осуществляются органом криптографической защиты.

3.2. Служебные помещения, в которых размещаются криптосредства, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения НКИ помещения обеспечиваются сейфами (металлическими шкафами), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, опечатываются личными печатями ответственных лиц (либо закрываются кодовым замком) и сдаются под охрану.

3.3. Для хранения НКИ пользователь криптосредств должен быть обеспечен личным сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня пользователь криптосредств обязан сдавать НКИ Ответственному.

3.4. Дубликаты ключей от сейфов (а также значения кодов - при наличии кодовых замков) пользователей криптосредств должны храниться в сейфе руководителя структурного подразделения или Ответственного в упаковках, опечатанных личными печатями пользователей криптосредств. Несанкционированное изготовление дубликатов ключей запрещено. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменен.

3.5. К эксплуатации криптосредств допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным криптосредством.

3.6. Все программное обеспечение ПЭВМ, предназначенной для установки криптосредств, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую криптосредства, не допускается.

1. ВОССТАНОВЛЕНИЕ СВЯЗИ В СЛУЧАЕ КОМПРОМЕТАЦИИ действующих ключей к криптосредствам

4.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца НКИ и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- утрата (хищение) НКИ, в том числе - с последующим их обнаружением;

- увольнение (переназначение) сотрудников, имевших доступ к НКИ;

- передача секретных ключей по линии связи в открытом виде;

- нарушение правил хранения НКИ;

- вскрытие фактов утечки передаваемой информации или ее искажения (подмены, подделки);

- ошибки при совершении криптографических операций;

- несанкционированное или безучетное копирование ключевой информации;

- все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда НКИ вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

4.2. При наступлении любого из перечисленных выше событий пользователь криптосредств или владелец НКИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь криптосредств или владелец НКИ обязан убедиться, что его сообщение получено и прочтено.

4.3. При подтверждении факта компрометации действующих ключей пользователь криптосредств обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу Ответственному в течение 3 рабочих дней.

4.4. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь криптосредств получает у Ответственного новые ключи.

**Лист ознакомления**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | ФИО | Должность | Подпись, дата |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение №3 к приказу №\_\_\_\_\_\_

от « » \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

**Перечень сотрудников, допущенных к работе с криптосредствами,**

**предназначенными для обеспечения безопасности персональных данных**

**в информационных системах персональных данных**

**(пользователи криптосредств), <наименование Учреждения>**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | ФИО | Должность | Подпись, дата |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение №4 к приказу №\_\_\_\_\_\_

от « » \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

**Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | |
|  |  |  |  | От кого получено | Дата и номер сопроводительного письма | Ф.И.О. 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. 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 |  | |  |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение №5 к приказу №\_\_\_\_\_\_

от « » \_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Настоящий Порядок регламентирует условия и порядок осуществления доступа в помещения <*наименование учреждения* > (далее - Учреждение), где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств (далее – Помещения) в целях организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.
   2. Настоящий Порядок разработан в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
   3. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.
   4. Помещения должны оснащаться входными дверьми с замками, должно обеспечиваться постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода, а также опечатывание Помещений по окончании рабочего дня или оборудования Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений.
2. ПРАВИЛА ДОСТУПА В ПОМЕЩЕНИЯ В РАБОЧЕЕ, НЕРАБОЧЕЕ ВРЕМЯ, В НЕШТАТНЫХ СИТУАЦИЯХ
   1. Доступ в Помещения в рабочее (служебное) время имеют сотрудники, включенные в Перечень лиц, имеющих доступ в Помещения, утвержденный нормативным актом Учреждения.
   2. В нерабочее (неслужебное) время пребывание вышеуказанных сотрудников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем Учреждения.
   3. Нахождение в Помещениях посторонних лиц в рабочее (служебное) и нерабочее (неслужебное) время запрещается.
   4. Руководитель и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.
   5. О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать руководителю структурного подразделения Учреждения.
   6. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать руководителю структурного подразделения Учреждения.
   7. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Учреждения.

**Лист ознакомления**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | ФИО | Должность | Подпись, дата |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |