



ИНФОРМАЦИОННОЕ ПРИМЕЧАНИЕ К ОБРАЗЦУ ДОКУМЕНТА

Настоящий документ является демонстрационным образцом локального организационного акта по использованию средств криптографической защиты информации (СКЗИ). Наличие отдельного положения с таким наименованием не установлено Федеральным законом № 152-ФЗ как универсальная обязанность для каждого оператора персональных данных. Документ применяется, если организация фактически использует СКЗИ и закрепляет внутренний порядок их эксплуатации.

При обработке персональных данных в ИСПДн применение СКЗИ определяется с учетом актуальных угроз, установленного уровня защищенности, архитектуры системы и применимых требований к защите. Если СКЗИ используются для обеспечения безопасности персональных данных в ИСПДн, учитываются Федеральный закон от 27.07.2006 № 152-ФЗ, постановление Правительства РФ от 01.11.2012 № 1119 и приказ ФСБ России от 10.07.2014 № 378.

Полная рабочая редакция должна учитывать конкретные типы СКЗИ, эксплуатационную документацию изготовителей, схему ключевого обеспечения, места установки, ответственных работников и фактические процессы организации.

[НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]

УТВЕРЖДАЮ

[должность

руководителя]

[Ф.И.О.]

«__» _____ 20__ г.

ПОЛОЖЕНИЕ ПО ИСПОЛЬЗОВАНИЮ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

1. Общие положения

1.1. Настоящее Положение устанавливает организационные правила учета, размещения, эксплуатации, хранения, передачи, обслуживания и вывода из эксплуатации СКЗИ, используемых [наименование организации] для защиты информации, в том числе персональных данных, если такие средства включены в систему защиты персональных данных.

1.2. Для целей настоящего Положения под СКЗИ понимаются применяемые организацией программные, программно-аппаратные и аппаратные средства криптографической защиты информации, а также относящиеся к ним ключевые документы и иные элементы ключевого обеспечения.

1.3. Решение о применении СКЗИ принимается с учетом назначения информационной системы, актуальных угроз безопасности информации, установленных требований к защите и эксплуатационной документации на соответствующие средства.

1.4. Использование СКЗИ не освобождает организацию от применения иных необходимых организационных и технических мер защиты информации.

2. Нормативная основа

2.1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе статья 19, предусматривающая принятие необходимых правовых, организационных и технических мер для защиты персональных данных.



2.2. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В соответствии с пунктом 4 указанных Требований выбор средств защиты информации осуществляется оператором в соответствии с нормативными правовыми актами ФСБ России и ФСТЭК России, принятыми во исполнение части 4 статьи 19 Федерального закона № 152-ФЗ.

2.3. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Составы 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» (зарегистрирован в Минюсте России 18.08.2014 № 33620) применяется в случаях использования СКЗИ для обеспечения безопасности персональных данных в ИСПДн.

2.4. Эксплуатация каждого конкретного СКЗИ осуществляется также с учетом его эксплуатационной документации и условий правомерного использования.

3. Организация работ с СКЗИ

3.1. Руководитель организации определяет работников, ответственных за организацию эксплуатации СКЗИ, а также лиц, которым разрешена работа с конкретными средствами и ключевыми документами.

3.2. Допуск к СКЗИ предоставляется в объеме, необходимом для исполнения трудовых обязанностей. Передача средств, ключевых документов и полномочий неуполномоченным лицам не допускается.

3.3. Для каждого применяемого СКЗИ должны быть определены назначение, информационная система или процесс, в котором оно используется, место установки либо хранения, ответственное лицо и основание для эксплуатации.

3.4. Установка, настройка, изменение конфигурации и удаление СКЗИ выполняются только уполномоченными лицами в порядке, установленном организацией и эксплуатационной документацией.

4. Учет СКЗИ и ключевого обеспечения

4.1. Организация ведет учет используемых СКЗИ и, при необходимости, относящихся к ним ключевых документов и носителей. Учет должен позволять определить вид средства, его назначение, место использования, ответственное лицо и текущее состояние.

4.2. Получение, выдача, возврат, замена и вывод из эксплуатации учитываемых экземпляров СКЗИ и ключевых носителей документируются в установленном организацией порядке.

4.3. Ключевая информация и носители ключевой информации не должны копироваться, передаваться или использоваться вне установленного порядка.



4.4. Сроки действия ключевой информации и порядок ее плановой замены определяются применительно к используемому СКЗИ и его эксплуатационной документации.

5. Размещение, хранение и физическая защита

5.1. СКЗИ и ключевые носители размещаются и хранятся в условиях, исключающих неконтролируемый доступ лиц, не имеющих соответствующих полномочий.

5.2. Для помещений, в которых размещаются СКЗИ, организация определяет правила доступа с учетом назначения средств, состава защищаемой информации и применимых требований безопасности.

5.3. Неиспользуемые ключевые носители хранятся в местах, обеспечивающих их сохранность и возможность контроля выдачи.

5.4. Вынос СКЗИ либо ключевых носителей за пределы установленного места эксплуатации допускается только в предусмотренных организацией случаях и по установленной процедуре.

6. Правила эксплуатации

- 6.1. использовать СКЗИ только по назначению и в пределах предоставленных полномочий;
- 6.2. соблюдать эксплуатационную документацию и утвержденную конфигурацию средств;
- 6.3. не отключать и не обходить функции защиты без разрешения уполномоченного лица;
- 6.4. не передавать третьим лицам пароли, PIN-коды, ключевые носители и иные средства доступа;
- 6.5. не устанавливать неразрешенное программное обеспечение, способное повлиять на работу СКЗИ;
- 6.6. при выявлении неисправности, признаков компрометации, утраты ключевого носителя либо несанкционированного доступа незамедлительно прекратить использование затронутого средства в необходимом объеме и сообщить ответственному лицу.

7. Компрометация и инциденты

7.1. Основанием для реагирования являются, в частности, утрата ключевого носителя, подозрение на копирование ключевой информации, получение доступа неуполномоченным лицом, нарушение целостности средства, выявление вредоносного воздействия либо иные обстоятельства, способные поставить под сомнение защищенность информации.

7.2. Работник, выявивший такие обстоятельства, обязан незамедлительно уведомить ответственное лицо и выполнить указания по ограничению дальнейшего использования СКЗИ.

7.3. Ответственное лицо организует фиксацию обстоятельств, оценку необходимости блокирования или замены ключевой информации, восстановление безопасной конфигурации и документирование принятых мер.



7.4. Если инцидент связан с нарушением безопасности персональных данных, дополнительно применяются процедуры оператора по реагированию на инциденты и требования законодательства о персональных данных.

8. Техническое обслуживание и изменение конфигурации

8.1. Обновление, ремонт, техническое обслуживание и иные изменения СКЗИ выполняются уполномоченными лицами с учетом эксплуатационной документации.

8.2. После изменения конфигурации, замены компонентов или восстановления работоспособности проверяется возможность дальнейшего безопасного использования средства в составе соответствующей информационной системы.

8.3. Изменения, влияющие на систему защиты персональных данных, оцениваются на предмет необходимости актуализации модели угроз, состава мер защиты и эксплуатационной документации.

9. Вывод из эксплуатации

9.1. При прекращении использования СКЗИ организация обеспечивает прекращение действия относящихся к нему полномочий доступа и учетного статуса.

9.2. Ключевая информация и ключевые носители, дальнейшее использование которых не предусмотрено, подлежат возврату, уничтожению либо иному предусмотренному эксплуатационной документацией обращению.

9.3. Вывод из эксплуатации фиксируется в учетных документах. При передаче оборудования на ремонт, списание или утилизацию должны быть исключены условия для восстановления защищаемой информации и ключевых данных в случаях, когда это требуется.

ДЕМОНСТРАЦИОННАЯ ВЕРСИЯ

В публичный образец не включены конкретные наименования СКЗИ, серийные номера, версии, места установки, схемы ключевого обеспечения, номера ключевых носителей, сроки действия ключей, параметры криптографических протоколов, сведения о защищенных каналах и иные технические данные, раскрытие которых может снизить уровень безопасности.

В полной редакции целесообразно включать приложения с перечнем СКЗИ, формой журнала учета, перечнем допущенных лиц, формой выдачи и возврата ключевых носителей, порядком действий при компрометации и актом вывода из эксплуатации.

10. Контроль и ответственность

10.1. Контроль соблюдения настоящего Положения осуществляется ответственным лицом либо иным уполномоченным подразделением в пределах установленных полномочий.

10.2. Работники, допущенные к использованию СКЗИ, несут ответственность за соблюдение установленных правил в соответствии с законодательством Российской Федерации, трудовыми обязанностями и локальными актами организации.

10.3. Настоящее Положение пересматривается при изменении применимых нормативных требований, состава СКЗИ, архитектуры защищаемых систем либо порядка эксплуатации средств.



Справочная нормативная основа

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: статья 19.
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: пункты 2–4 и иные применимые положения.
- Приказ ФСБ России от 10.07.2014 № 378, зарегистрирован в Минюсте России 18.08.2014 № 33620, в части ИСПДн, в которых для защиты персональных данных используются СКЗИ.
- Эксплуатационная документация на фактически используемые СКЗИ.

Посетите **Telegram**-канал **Антагора** и подпишитесь, чтобы следить за новостями, изменениями законодательства и практическими обзорами по ПДн, ИБ, КИИ, АТЗ, БПЛА, комплаенсу и защите бизнеса.

Читайте нас в Telegram: [@antagora](https://t.me/antagora)

Нужна адаптация документа под вашу организацию?

Группа компаний **АНТАГОРА**

Телефон: **8 (800) 333-8-222**

Сайт: antagora.ru / antagora.pf

Электронная почта: info@antagora.ru

Telegram-канал: [@antagora](https://t.me/antagora)

Перед применением образец необходимо проверить и адаптировать под вашу деятельность, реальные процессы, используемые системы, состав информации, сайт, каналы связи, договоры, локальные документы, обязанности работников и требования законодательства.

Мы можем помочь:

- оценить, подходит ли образец именно вам;
- адаптировать текст под вашу организацию;
- подготовить полный или минимально необходимый комплект документов;
- проверить связку документов между собой;
- найти пробелы и противоречия;
- подготовить документы по персональным данным (ПДн), информационной безопасности (ИБ), критической информационной инфраструктуре (КИИ), по АТЗ и противодействию БПЛА, противодействию коррупции, комплаенсу и защите бизнеса.

Для заказа комплекта документов, консультации и прочим услугам звоните **8 (800) 333-8-222** или пишите info@antagora.ru ещё **больше информации и документов на сайте [антагора.рф](https://antagora.pf)**

Образец документа - Страница 5 из 6 - **требует проверки и адаптации под организацию.**



Если после скачивания шаблона стало понятно, что просто заменить название организации недостаточно, обратитесь к нам. Мы разберем вашу ситуацию и предложим нормальный состав работ.