

**ОБЕСПЕЧЕНИЕ ЗАЩИТЫ
ИНФОРМАЦИИ В ХОДЕ
ЭКСПЛУАТАЦИИ
АТТЕСТОВАННОЙ
ИНФОРМАЦИОННОЙ
СИСТЕМЫ**

МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ СИСТЕМЫ ЗАЩИТЫ

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется **оператором** в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации

МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ СИСТЕМЫ ЗАЩИТЫ

- управление (администрирование) системой защиты информации информационной системы;**
- выявление инцидентов и реагирование на них;**
- управление конфигурацией аттестованной информационной системы и ее системы защиты информации;**
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.**

УПРАВЛЕНИЕ (АДМИНИСТРИРОВАНИЕ) СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

- 1. заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;**
- 2. управление средствами защиты информации в ИС, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;**
- 3. установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации;**
- 4. централизованное управление системой защиты информации ИС (при необходимости);**

УПРАВЛЕНИЕ (АДМИНИСТРИРОВАНИЕ) СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

- 5. регистрация и анализ событий в информационной системе, связанных с защитой информации;**
- 6. информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;**
- 7. сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.**

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И РЕАГИРОВАНИЕ НА НИХ

- 1. определение лиц, ответственных за выявление инцидентов и реагирование на них;**
- 2. обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;**
- 3. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами.**

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И РЕАГИРОВАНИЕ НА НИХ

- 4. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;**
- 5. планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;**
- 6. планирование и принятие мер по предотвращению повторного возникновения инцидентов.**

УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ЕЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

- 1. поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации ИС, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИС и ее системы защиты информации);**
- 2. определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;**
- 3. управление изменениями базовой конфигурации ИС и ее системы защиты информации (определение типов возможных изменений, санкционирование внесения изменений, документирование действий по внесению изменений, сохранение данных об изменениях, контроль действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации);**

КОНТРОЛЬ (МОНИТОРИНГ) ЗА ОБЕСПЕЧЕНИЕМ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

- 1. контроль за событиями безопасности и действиями пользователей в ИС;**
- 2. контроль (анализ) защищенности информации, содержащейся в ИС;**
- 3. анализ и оценка функционирования системы защиты информации ИС, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИС;**
- 4. периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;**
- 5. документирование процедур и результатов контроля (мониторинга);**
- 6. принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИС и **повторной аттестации** ИС (в случае изменения класса защищенности ИС, состава актуальных угроз или проектных решений по системе ЗИ).**

НАИБОЛЕЕ ВАЖНЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ СИСТЕМЫ ЗАЩИТЫ

- контроль состояния защиты информации, включая контроль за событиями и действиями пользователей;**
- обнаружение и регистрация инцидентов, выявление их причин, принятие мер по предупреждению и устранению инцидентов;**
- анализ и оценка функционирования системы защиты с целью выявления и устранения недостатков и совершенствования;**
- периодический анализ уязвимостей;**
- анализ изменения угроз и выявление новых угроз;**
- анализ влияния на систему защиты планируемых изменений в информационной системе.**

МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ СИСТЕМЫ ЗАЩИТЫ

Обеспечение неизменности состава технических и программных средств, а также средств защиты и их настроек, соблюдение утвержденного технологического процесса обработки информации и принятие мер по нейтрализации актуальных угроз – основные задачи, решение которых обеспечивает высокую степень защищенности информации в информационной системе.

**МЕРЫ ПО ЗАЩИТЕ
ИНФОРМАЦИИ В ХОДЕ ВЫВОДА
ИНФОРМАЦИОННОЙ СИСТЕМЫ
ИЗ ЭКСПЛУАТАЦИИ ИЛИ ПОСЛЕ
ОКОНЧАНИЯ ОБРАБОТКИ
ИНФОРМАЦИИ**

МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ХОДЕ ВЫВОДА ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЗ ЭКСПЛУАТАЦИИ ИЛИ ПОСЛЕ ОКОНЧАНИЯ ОБРАБОТКИ ИНФОРМАЦИИ

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется **оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации**

МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ХОДЕ ВЫВОДА ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЗ ЭКСПЛУАТАЦИИ ИЛИ ПОСЛЕ ОКОНЧАНИЯ ОБРАБОТКИ ИНФОРМАЦИИ

- при необходимости дальнейшего использования накопленной информации, осуществляется ее архивирование;
- при выводе из эксплуатации машинных носителей осуществляется их уничтожение;

МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ХОДЕ ВЫВОДА ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЗ ЭКСПЛУАТАЦИИ ИЛИ ПОСЛЕ ОКОНЧАНИЯ ОБРАБОТКИ ИНФОРМАЦИИ

- при необходимости передачи машинных носителей между пользователями информационной системы, в сторонние организации для ремонта, обслуживания или утилизации, осуществляется стирание данных и остаточной информации.

**РЕМОНТ И
ТЕХНИЧЕСКОЕ
ОБСЛУЖИВАНИЕ
АВТОМАТИЗИРОВАННЫХ
СИСТЕМ**

ПОРЯДОК ДЕЙСТВИЙ ПРИ ВЫХОДЕ ИЗ СТРОЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

**Определить мероприятия, которые необходимо
выполнить в организации**

**Провести выбор организации, которая имеет
право проводить ремонт автоматизированной
системы (техническое обслуживание)**

**Определить порядок ввода в строй
автоматизированной системы после проведения
ремонта (технического обслуживания)**

ПОРЯДОК ДЕЙСТВИЙ ПРИ ВЫХОДЕ ИЗ СТРОЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

**Приказом руководителя организации
приостановить обработку информации**

**Письменно уведомить организацию, проводившую
аттестацию объектов информатизации**

**После проведения, в случае необходимости, организацией
дополнительной проверки эффективности системы защиты
объекта информатизации, внести соответствующие
изменения в документы**

ИЗМЕНЕНИЕ УСЛОВИЙ И ТЕХНОЛОГИИ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

**6.6.5. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить организацию, проводившую аттестацию, которая принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты информации объекта информатизации
(ГОСТ РО 0043-003-2012)**

ИЗМЕНЕНИЕ УСЛОВИЙ ЭКСПЛУАТАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

При изменении условий эксплуатации, а также технических, программных и программно-технических средств объекта информатизации, приводящих к нарушению его штатной работы, включая штатную работу системы защиты информации, или к образованию угроз безопасности информации, проводят его **повторную аттестацию**

ПОРЯДОК ДЕЙСТВИЙ ПРИ ИЗМЕНЕНИИ УСЛОВИЙ ЭКСПЛУАТАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

**Приказом руководителя организации
приостановить обработку информации**

**Письменно уведомить организацию, проводившую
аттестацию объектов информатизации**

**Провести повторную аттестацию объектов
информатизации**

**КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ
ПОРЯДКА АТТЕСТАЦИИ
И ЭКСПЛУАТАЦИИ
АТТЕСТОВАННЫХ ОБЪЕКТОВ
ИНФОРМАТИЗАЦИИ**

КОНТРОЛЬ ЗА СОБЛЮЖДЕНИЕМ ПОРЯДКА АТТЕСТАЦИИ И ЭКСПЛУАТАЦИИ АТТЕСТОВАННЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Государственный контроль и надзор

В ходе государственного контроля и надзора проверяют соответствие аттестованного объекта информатизации требованиям безопасности информации

Заявители организуют ежегодный контроль соответствия системы защиты информации объекта информатизации требованиям безопасности информации

По результатам проведенного контроля оформляют соответствующие заключение и протоколы.

При добровольной аттестации необходимость и периодичность ежегодного контроля устанавливает заявитель.



**Управление ФСТЭК России
по Приволжскому
федеральному округу
организует и контролирует
проведение работ
по аттестации объектов
информатизации
по требованиям безопасности
информации.**

СПАСИБО ЗА ВНИМАНИЕ