



Пособие посвящено вопросам организации защиты информации в единых автоматизированных информационных системах (ЕАИС) министерств и ведомств России, представляет собой практическое руководство для специалистов служб безопасности и отделов информационных технологий. Описаны методы обеспечения непрерывности функционирования ЕАИС в условиях внешних воздействий и чрезвычайных ситуаций.

## Введение

### **Глава 1. Переход на безопасные и защищенные компьютерные технологии. Отечественные сетевые технологии**

- 1.1.** Создание единого информационного пространства России – МСР.Система.хх

### **Глава 2. Анализ лучшей практики разработки процедур непрерывности функционирования ЕАИС**

- 2.1.** Международное законодательство и требования международных стандартов по обеспечению непрерывности бизнеса и анализу рисков
- 2.2.** Требования законодательства и стандартов РФ по внедрению процедур обеспечения непрерывности работы информационных систем
- 2.3.** Оценка рисков и управление рисками
- 2.4.** Анализ воздействия на деятельность (BIA)
- 2.5.** Оценка рисков и управление рисками
- 2.6.** Разработка стратегии восстановления ИТ-сервисов
- 2.7.** Классификация факторов, влияющих на отказоустойчивость вычислительных систем и их деятельность в условиях аварий и катастроф
- 2.8.** Методики ведущих зарубежных производителей ИС по определению и оценке факторов влияющих на устойчивость
- 2.9.** Технологии обеспечения непрерывности функционирования информационных систем
- 2.10.** Требования и показатели качества функционирования информационных систем в РФ

### **Глава 3. Обоснование и выбор показателей устойчивости функционирования информационных систем**

- 3.1.** Идеология действий разработчика процедур обеспечения непрерывности деятельности компаний
- 3.2.** Оценка влияния на бизнес (BIA)
- 3.3.** Стратегия непрерывности функционирования ИТ-ресурсов
- 3.4.** Анализ вариантов стратегий непрерывности для ресурсов
- 3.5.** Описание частных технических решений
- 3.6.** Обзор выявленных проблемных областей
- 3.7.** Оценка наличия элементов стратегий восстановления
- 3.8.** Оценка влияния чрезвычайных ситуаций на ИТС
- 3.9.** Мероприятия обеспечения непрерывности работы информационных систем и снижения ущерба при сбоях и катастрофах
- 3.10.** Отечественные защищенные компьютерные технологии

### **Глава 4. План действий ИТС в условиях чрезвычайных ситуаций**

- 4.1.** План действий ИТС при крупных бедствиях (катастрофах)
- 4.2.** Обнаружение и реагирование
- 4.3.** Начало развертывания резервного плана
- 4.4.** Восстановление деятельности в резервном помещении
- 4.5.** Группы восстановления деятельности после бедствия
- 4.6.** Тестирование плана

## Заключение

## Список литературы