

Специалисты структурного подразделения по безопасности обязаны непрерывно осуществлять мониторинг уровня защищенности информации, содержащейся в корпоративной информационной системе, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации, анализ новых угроз безопасности информации, принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов. По результатам мониторинга принимаются решения о доработке (модернизации) СЗИ, повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

Пособие посвящено вопросам разработки процедур для проведения мониторинга использования средств обработки информации и средств защиты информации для обнаружения неавторизованных действий, связанных с обработкой информации. Пособие предназначено для специалистов ИБ-подразделений, подразделений, обеспечивающих функционирование объектов ИТ-инфраструктуры организаций. В нем использованы положения национальных стандартов в ИТ-области. Описаны типовые процедуры мониторинга безопасности для организаций различного вида деятельности. Приведен обзор технических средств поддержки процедур мониторинга и регистрации событий ИБ.

Учебное пособие может быть использовано при обучении по специальностям 10.05.03 «Информационная безопасность автоматизированных систем», 10.04.01, 10.03.01 «Информационная безопасность».

Пособие написано к. т. н. Р. И. Кисловым. Приложение № 2 подготовлено М. И. Мининой.

Введение

Обозначения и сокращения

Термины и определения

Глава 1. **Задачи мониторинга безопасности информации**

- 1.1. **Понятие мониторинга безопасности информации**
- 1.2. **Мониторинг в системе управления информационной безопасностью организации**
 - 1.2.1. Система управления информационной безопасностью организации
 - 1.2.2. Проведение мониторинга и анализа системы менеджмента информационной безопасности
 - 1.2.3. Внедрение средств контроля и управления информационной безопасностью
 - 1.2.4. Менеджмент инцидентов информационной безопасности
 - 1.2.5. Менеджмент непрерывности бизнеса
 - 1.2.6. Управление документами и записями системы менеджмента информационной безопасности
 - 1.2.7. Анализ системы менеджмента информационной безопасности со стороны руководства
- 1.3. **Мониторинг в системе управления информационной инфраструктурой организации**
 - 1.3.1. Система управления информационной инфраструктурой организации
 - 1.3.2. Реализация системы ИТ-мониторинга
 - 1.3.3. Суть и значение ИТ-мониторинга, его роль в управлении информационной инфраструктурой организации
- 1.4. **Мониторинг рисков информационной безопасности**
 - 1.4.1. Общие вопросы менеджмента рисков информационной безопасности
 - 1.4.2. Мониторинг рисков информационной безопасности
- 1.5. **Измерение, анализ и улучшение деятельности организации**
 - 1.5.1. Общие положения
 - 1.5.2. Измерение информационной безопасности
 - 1.5.3. Анализ результатов измерения информационной безопасности
 - 1.5.4. Мониторинг, проверка и оценивание программы измерений
- 1.6. **Услуги по мониторингу информационной безопасности средств и систем информатизации**
 - 1.6.1. Лицензирование отдельных видов деятельности
 - 1.6.2. Услуги по мониторингу информационной безопасности средств и систем информатизации

- Глава 2. Структурный подход к мониторингу информационной безопасности**
 - 2.1. Общие положения
 - 2.2. Планирование и подготовка мониторинга информационной безопасности
 - 2.3. Эксплуатация системы мониторинга информационной безопасности
 - 2.4. Контроль системы мониторинга информационной безопасности
 - 2.5. Усовершенствование системы мониторинга информационной безопасности

- Глава 3. Мониторинг информационной безопасности в системе управления организацией**
 - 3.1. Мониторинг информационной безопасности в информационных системах персональных данных
 - 3.2. Мониторинг информационной безопасности государственных информационных систем
 - 3.3. Мониторинг информационной безопасности объектов критической информационной инфраструктуры Российской Федерации
 - 3.4. Мониторинг информационной безопасности в автоматизированных системах управления производственными и технологическими процессами
 - 3.5. Мониторинг информационной безопасности банковских (финансовых) операций
 - 3.6. Мониторинг информационной безопасности для телекоммуникационных организаций

- Глава 4. Планирование и подготовка мониторинга информационной безопасности**
 - 4.1. Программа мониторинга информационной безопасности
 - 4.2. Политика мониторинга информационной безопасности
 - 4.3. Технические средства мониторинга информационной безопасности
 - 4.3.1. Система защиты информации от несанкционированного доступа Dallas Lock 8.0
 - 4.3.2. Безопасная среда Dallas Lock SandBox
 - 4.4. Внутренние и внешние взаимодействия системы мониторинга информационной безопасности

Заключение

Литература

Приложения

- Приложение 1.* Мониторинг радиообстановки в помещениях
- Приложение 2.* Средства анализа защищенности