Мониторинг информационной безопасности. Структурный подход

136 стр. PDF 2019 г.

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.