

УДК 004.7:004.056(075.8)

ББК 32.973.202-018.2я73

С33

Рецензенты:

канд. техн. наук *Т. Ю. Зырянова* (зав. каф. «Системы и технологии защиты информации» Уральского государственного университета путей сообщения);

д-р физ.-мат. наук проф. *В. А. Баранский* (дир. Регионального учебно-научного центра «Интеллектуальные системы и информационная безопасность»)

Андрончик, А. Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс [Электронный ресурс]: учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков ; под общ. ред. Н. И. Синадского. — 2-е изд., стер. — М. : ФЛИНТА : Изд-во Урал. ун-та, 2018. — 178 с.

ISBN 978-5-9765-3523-7 (ФЛИНТА)

ISBN 978-5-7996-1201-6 (Изд-во Урал. ун-та)

Учебное пособие раскрывает вопросы практического применения методов и средств защиты информации в компьютерных сетях. В качестве платформы для построения защищенных сетей рассмотрены технологии и программно-аппаратные комплексы фирмы Cisco Systems. В пособии рассмотрены основные команды операционной системы Cisco IOS, вопросы администрирования маршрутизаторов и межсетевых экранов, способы обнаружения сетевых компьютерных атак на базе комплексов Cisco IDS Sensor и Cisco MARS. Основной акцент в пособии делается на практическое изучение материала, что реализуется благодаря применению технологии виртуальных машин и использованию в образовательном процессе программных эмуляторов аппаратуры фирмы Cisco Systems.

Пособие будет полезно преподавателям, слушателям потоков повышения квалификации по направлению информационной безопасности, а также специалистам-практикам в области защиты компьютерной информации.

Библиогр.: 12 назв. Рис. 106.

УДК 004.7:004.056(075.8)

ББК 32.973.202-018.2я73

ISBN 978-5-9765-3523-7 (ФЛИНТА)

ISBN 978-5-7996-1201-6 (Изд-во Урал. ун-та)

© Уральский федеральный университет, 2014

ОГЛАВЛЕНИЕ

Введение.....	6
1. Основы конфигурирования в командной строке IOS.....	12
1.1. Основы моделирования компьютерной сети в Cisco Packet Tracer.....	12
1.2. Эмулятор оборудования Cisco GNS3.....	19
1.3. Операционная система Cisco IOS.....	28
2. Конфигурирование сетевых устройств фирмы Cisco.....	41
2.1. Конфигурирование коммутаторов.....	41
2.2. Конфигурирование маршрутизаторов.....	57
2.3. Конфигурирование протоколов управления оборудованием....	70
3. Межсетевое экранирование с использованием технологий фирмы Cisco.....	81
3.1. Списки управления доступом.....	81
3.2. Настройка Zone-Based Policy Firewall.....	90
3.3. Межсетевые экраны Cisco PIX.....	95
3.4. Организация защищенного канала на основе IPSec.....	108
4. Обнаружение сетевых компьютерных атак.....	117
4.1. Настройка комплекса Cisco IDS Sensor.....	117
4.2. Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco IDS Sensor.....	133
5. Обнаружение комплексных компьютерных атак.....	144
5.1. Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco MARS.....	144
5.2. Обнаружение компьютерных атак на узлы сети с использованием COA Cisco Security Agent и Cisco MARS....	163
Библиографический список.....	174
Приложение. Применение технологии виртуальных машин для имитации сетевых соединений.....	175