

УДК 004.4 : 378.245 (076.5)
 ББК 32.973-018.2я7+74.58я7
 Т 60

Рецензент – кандидат технических наук, доцент С.А. Щелоков

Т 60 **Тишина, Н.А.**
 Прикладные задачи безопасности информационно-телекоммуникационных систем: учебное пособие / Н.А.Тишина, Е.Н.Чернопрудова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2017. – 121 с.

ISBN 978-5-7410-1892-7

В учебном пособии содержатся материалы, необходимые студентам для изучения теории и формирования умений и навыков выполнения практических задач по дисциплине «Безопасность информационно-телекоммуникационных систем». В разделах учебного пособия содержатся теоретические вопросы, связанные с реализацией прикладных задач в области безопасности информации, примеры, методические материалы для выполнения лабораторных работ: цель, задачи, порядок выполнения работы, представлены варианты заданий.

Учебное пособие предназначено для преподавателей и магистров, обучающихся по направлению подготовки 09.04.04 Программная инженерия для изучения дисциплины «Безопасность информационно-телекоммуникационных систем».

Т 1602120000

УДК 004.4 : 378.245 (076.5)
 ББК 32.973-018.2Я7+74.5Я7

ISBN 978-5-7410-1892-7

© Тишина Н.А., 2017
 © Чернопрудова Е.Н., 2017
 © ОГУ, 2017

Содержание

Введение	5
1 Регистрация и анализ характеристик сетевого трафика.....	7
1.1 Анализатор сетевых пакетов	7
1.2 Постановка задания к лабораторной работе №1	15
1.3 Порядок выполнения.....	15
2 Имитация сетевых атак.....	18
2.1 Понятие сетевых атак.....	18
2.2 Настройка сети в VirtualBox.....	27
2.3 Постановка задания к лабораторной работе №2.....	30
2.4 Порядок выполнения.....	30
3 Применение межсетевого экрана.....	33
3.1 Межсетевые экраны	33
3.2 Межсетевой экран IPTables	39
3.3 Постановка задания к лабораторной работе №3	46
3.4 Порядок выполнения.....	46
4 Организация виртуальных частных сетей	51
4.1 Виртуальная частная сеть.....	51
4.2 Реализация технологии виртуальной частной сети OpenVPN	55
4.3 Постановка задания к лабораторной работе № 4.....	58
4.4 Порядок выполнения.....	59
5 Работа с системой обнаружения вторжений	67
5.1 Системы обнаружения вторжений	67
5.2 Система обнаружения вторжений Snort	76
5.3 Система обнаружения аномалий на основе прогнозирования поведения сетевого трафика	80
5.4 Постановка задания к лабораторной работе №5.....	87
5.5 Порядок выполнения работы	87

6	Оценка рисков информационной безопасности информационно-телекоммуникационных систем.....	91
6.1	Понятие и этапы оценки рисков	91
6.2	Идентификация угроз	95
6.3	Методы оценивания угроз.....	96
6.3.1	Определение оценки вероятности реализации угрозы.....	98
6.3.2	База данных и алгоритм оценки угроз	100
6.4	Постановка задания к лабораторной работе №6.....	101
6.5	Порядок выполнения работы	102
7	Проведение аудита информационной безопасности информационно-телекоммуникационных систем.....	105
7.1	Понятие аудита безопасности информации	105
7.2	Инструменты анализа защищенности.....	108
7.3	Постановка задания к лабораторной работе №7.....	113
7.4	Порядок выполнения.....	113
	Заключение.....	115
	Список использованных источников	116
	Приложение А (обязательное) Варианты адресов сетей и OpenVPN-туннеля.....	120