

УДК 004.056.53

ББК 16.84

Б27

*Печатается по решению кафедры безопасности информационных технологий  
Института компьютерных технологий и информационной безопасности  
Южного федерального университета (протокол № 15 от 15 мая 2023 г.)*

**Рецензенты:**

доцент кафедры информационной безопасности автоматизированных систем  
Института цифрового развития, заместитель директора по научной работе  
института цифрового развития Северо-Кавказского федерального университета,  
кандидат физико-математических наук, доцент *Лапина М. А.*

заведующий кафедрой безопасности информационных технологий  
Института компьютерных технологий и информационной безопасности  
Южного федерального университета, кандидат технических наук,  
доцент *Абрамов Е. С.*

**Басан, Е. С.**

Б27      Безопасность сетей ЭВМ : учебное пособие / Е. С. Басан, О. Ю. Пескова ;  
Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издатель-  
ство Южного федерального университета, 2024. – 181 с.

ISBN 978-5-9275-4634-3

Учебное пособие предназначено для студентов специалитета, обучающихся по специальностям 10.05.03 «Информационная безопасность автоматизированных систем» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» в рамках теоретической и практической подготовки по курсу «Безопасность сетей ЭВМ», но может быть также полезно студентам других специальностей и направлений, предусматривающих изучение курсов по организации и технологии защиты информации, и может быть применено для организации дополнительного профессионального обучения специалистов, чья сфера деятельности лежит в области киберфизических систем и сетевой безопасности.

Пособие содержит теоретический материал и практические примеры, касающиеся обеспечения сетевой безопасности на нижних уровнях сетевой модели OSI – физическом, канальном и сетевом. В приложении приведены рекомендации по подготовке к выполнению лабораторного практикума по курсу.

УДК 004.056.53

ББК 16.84

Б27

ISBN 978-5-9275-4634-3

© Южный федеральный университет, 2024

© Басан Е. С., Пескова О. Ю., 2024

© Оформление. Макет. Издательство

Южного федерального университета, 2024

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	6
1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ .....	7
2. СЕТЕВЫЕ АТАКИ И ЗАЩИТА ОТ НИХ .....	11
2.1. Структура и модели атак .....	11
2.2. Древовидная модель сценария многоэтапной атаки .....	13
3. УГРОЗЫ И АТАКИ НА ФИЗИЧЕСКОМ УРОВНЕ .....	20
3.1. Основные понятия .....	20
3.2. Атаки на проводные сети .....	21
3.3. Атаки на беспроводные сети .....	21
3.3.1. Атаки прослушивания .....	22
3.3.2. Атака Replay (повтор) .....	25
3.3.3. Перехват «рукопожатия» и брут-форс атака на Wi-Fi с шифрованием WPA/WPA2 (CAPEC-49) .....	25
3.3.4. Атака «человек посередине» (CAPEC-94) .....	29
3.3.5. Поддельная точка доступа Wi-Fi .....	30
3.3.6. Атака Blueprinting .....	32
3.3.7. Атака деаутентификации и подключения к удаленному устройству .....	33
3.4. Атаки на систему навигации .....	36
3.4.1. Современные навигационные системы .....	36
3.4.2. Подделка сигнала GPS (GPS spoofing) (CAPEC-627) .....	45
3.4.3. Глушение сигнала GPS (CAPEC-599) .....	53
3.5. Защита от атак на физическом уровне .....	56
4. УГРОЗЫ И АТАКИ КАНАЛЬНОГО УРОВНЯ .....	57
4.1. Особенности передачи и обработки данных на канальном уровне .....	57
4.2. Основные типы атак .....	58
4.3. Отравление ARP (ARP-poisoning) .....	59
4.3.1. Описание атаки .....	59
4.3.2. Пример практической реализации .....	61
4.3.3. Защита от атак типа ARP-poisoning .....	71

4.4. Переполнение таблицы MAC-адресов на коммутаторе (Overflow CAM table) .....	76
4.4.1. Описание атаки .....	76
4.4.2. Пример практической реализации .....	77
4.4.3. Защита от атак типа Overflow CAM table .....	79
4.5. Истощение и отравление DHCP-сервера (DHCP Starvation и DHCP Poisoning) .....	84
4.5.1. Описание атак .....	84
4.5.2. Пример практической реализации .....	85
4.5.3. Защита от атак типа DHCP Starvation и DHCP Poisoning ...	92
4.6. Переключение VLAN (VLAN Hopping) .....	100
4.6.1. Описание атаки .....	100
4.6.2. Пример практической реализации .....	100
4.6.3. Защита от атак типа VLAN Hopping .....	105
4.7. Атака на корневой коммутатор STP (STP Claiming Root) .....	105
4.7.1. Описание атаки .....	105
4.7.2. Пример практической реализации .....	109
4.7.3. Защита от атак типа STP Claiming Root .....	114
4.8. Общие приемы защиты от атак на канальном уровне .....	115
4.9. Технология MACSec .....	119
4.9.1. Основные понятия и определения .....	119
4.9.2. Механизм работы протокола MACSec .....	120
4.9.3. Особенности и ограничения протокола MACSec .....	123
4.9.4. Зеркальные порты .....	124
4.9.5. Пример настройки протокола MACSec .....	124
5. УГРОЗЫ И АТАКИ НА СЕТЕВОМ УРОВНЕ .....	130
5.1. Основные понятия .....	130
5.2. Проблемы с маршрутизацией источника .....	131
5.3. Проблемы, связанные с протоколом ICMP .....	131
5.3.1. Общая характеристика протокола ICMP .....	131
5.3.2. Проблемы с недостижимостью узла назначения .....	132
5.3.3. Проблемы с перенаправлением протокола ICMP .....	132
5.3.4. Реализация атаки на отказ в обслуживании с использо- ванием протокола ICMP .....	134

## Содержание

5.4. Перехват BGP и его использование .....	135
5.5. Атаки на OSPF .....	141
5.6. Защита каналов связи на сетевом уровне с использованием VPN .....	145
5.6.1. Протокол IPSec .....	145
5.6.2. Протокол L2TP .....	149
5.6.3. Атаки на протокол IPSec .....	151
5.7. Настройка и анализ протоколов динамической маршрутизации .....	151
5.7.1. Описание используемой топологии .....	151
5.7.2. Настройка протокола OSPF .....	153
5.7.3. Настройка протокола eBGP .....	157
5.8. Настройка туннеля L2TP/IPSEC .....	158
ЗАКЛЮЧЕНИЕ .....	167
СПИСОК ЛИТЕРАТУРЫ .....	168
ПРИЛОЖЕНИЯ .....	172
Приложение А. Подготовка к выполнению лабораторного практикума .....	172
ПА.1. Установка программного обеспечения Pnetlab .....	172
ПА.2. Запуск лабораторных работ .....	172
ПА.3. Запуск сетевых устройств .....	177
ПА.4. VPC .....	179