



НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

МЕРЕЖЕВІ ТЕХНОЛОГІЇ ТА ПРОТОКОЛИ

Навчальний посібник



КИЇВ • НОВА ДУМКА • 2025

УДК 004.076

М52

Рецензенти:

В. Г. Сайко, доктор технічних наук, професор;

В. С. Шматко, кандидат технічних наук

Укладачі:

В. І. Шестаков – доктор технічних наук, доцент;

В. І. Гладких – кандидат технічних наук;

Н. М. Сивкова – доктор філософії зі спеціальності 172
телекомунікації та радіотехніка;

О. Ф. Шатирко

Рекомендовано до друку редакційно-видавничою радою

Національної академії СБ України

(протокол № 2 від 4 квітня 2025 р.)

Мережеві технології та протоколи : навч. посіб. / укладачі

В. І. Шестаков, В. М. Гладких, Н. М. Сивкова, О. Ф. Шатирко.

М52

Київ : ТОВ «Наукове видавництво “Нова Думка”», 2025. 312 с.

DOI:10.64696/9786178816407

ISBN 978-617-8816-40-7

У навчальному посібнику розглядаються принципи побудови сучасних комп'ютерних мереж, характеристики найпопулярніших сучасних мережевих технологій, розкриваються питання топології мереж, маршрутизації та фрагментації користувальницьких пакетів даних, захисту інформації на рівні мережі. Велику увагу приділено особливостям найпопулярнішого стека протоколів – TCP/IP, а також інших стеків, що лежать в основі internet / intranet мереж, зокрема глобальної мережі Інтернет. Акцентується увага на протоколах безпеки мережевого, транспортного, сеансового, прикладного рівнів еталонної моделі OSI. Пояснюється технологія віртуальних приватних мереж. Зазначаються типові сценарії та приклади кібератак на кожному з рівнів моделі OSI. Детально розкривається питання сегментації комп'ютерної мережі та наведено приклад побудови структурованої моделі кібербезпеки.

Навчальний посібник розроблено відповідно до робочої програми навчальної дисципліни «Мережеві технології та протоколи», яка буде викладатися з 2025–2026 навчального року для здобувачів вищої освіти за спеціальністю КЗ «Національна безпека» першого (бакалаврського) рівня вищої освіти.

УДК 004.076

Передрукування заборонено

© Національна академія

Служби безпеки України, 2025

© Шестаков В. І., Гладких В. М.,
Сивкова Н. М., Шатирко О. Ф., 2025

© ТОВ «Наукове видавництво
“Нова думка”», видання, 2025

ISBN 978-617-8816-40-7

ЗМІСТ

ВСТУП	7
Розділ 1 АРХІТЕКТУРА КОМП'ЮТЕРНИХ МЕРЕЖ	8
1.1 Основні терміни	8
1.2 Архітектура мереж.....	10
1.2.1 Однорангова архітектура.....	11
1.2.2 Архітектура клієнт-сервер.....	12
1.3 Мережеве обладнання	14
1.4 Вибір архітектури локальної мережі	18
1.5 Перелік контрольних і тестових питань розділу 1	19
Розділ 2 МЕРЕЖЕВІ СТАНДАРТИ.....	21
2.1 Пропрієтарні, відкриті та фактичні стандарти.....	21
2.2 Мережеві стандарти.....	24
2.3 Міжнародні організації зі стандартизації мереж	24
2.4 Мережеві галузеві групи	27
2.5 Організації зі стандартизації Інтернету	28
2.6 Центральний реєстраційний орган в Інтернеті	32
2.7 Сучасна ієрархія реєстраторів параметрів Internet	33
2.8 Інтернет-стандарти та запит коментарів (RFC)	34
2.9 Процес стандартизації Інтернету	36
2.10 Перелік контрольних і тестових питань розділу 2	38
Розділ 3 БАГАТОРІВНЕВА ОРГАНІЗАЦІЯ МЕРЕЖ	40
3.1 Принципи багаторівневої організації мережі.....	41
3.2 Модель взаємодії відкритих систем	42
3.3 Стек TCP/IP.....	47
3.4 Перелік контрольних і тестових питань розділу 3	50
Розділ 4 ФІЗИЧНИЙ РІВЕНЬ.....	52
4.1 Фізичні компоненти.....	52
4.1.1 Мідні кабелі.....	53
4.1.2 Волоконно-оптичні кабелі.....	56
4.1.3 Радіосередовище.....	57
4.2 Перелік контрольних і тестових питань розділу 4	58
Розділ 5 КАНАЛЬНИЙ РІВЕНЬ	59
5.1 Загальний огляд каналного рівня.....	59
5.2 Кадри каналного рівня.....	60
5.3 Протоколи безпеки на каналному рівні	62
5.4 Протокол визначення адрес (ARP).....	65
5.4.1 Необхідність визначення адрес	66
5.4.2 Адресація на рівнях 2 і 3.....	66

5.4.3 Загальні характеристики протоколу визначення адрес (ARP)	68
5.4.4 Принципи роботи ARP	68
5.4.5 Типи повідомлень ARP та визначення адрес	69
5.4.6 Загальна операція ARP	69
5.4.7 Формат повідомлень ARP	71
5.4.8 Проксі-сервери ARP	73
5.4.9 Визначення адрес в IP версії 6	74
5.4.10 Загрози безпеки при використанні ARP. Атака ARP-spoofing	75
5.4.11 Захист від підміни ARP-пакетів	77
5.5 Протоколи формування захищених каналів	77
5.5.1 Протокол PPTP	79
5.5.2 Протокол L2TP	81
5.6 Перелік контрольних і тестових питань розділу 5	84
Розділ 6 МЕРЕЖЕВИЙ РІВЕНЬ	86
6.1 Протокол IPv4	87
6.2 Протокол IPv6	97
6.3 Захист інформації на мережевому рівні	105
6.3.1 Протокол IPsec	105
6.3.2 Архітектура засобів безпеки IPsec	105
6.4 Захист даних, що передаються за допомогою протоколів AH і ESP	110
6.4.1 Протокол автентифікуючого заголовка AH	110
6.4.2 Протокол інкапсулюючого захисту ESP	113
6.5 Алгоритми автентифікації та шифрування в IPsec	117
6.6 Протокол управління криптографічними ключами IKE	119
6.7 Встановлення безпечної асоціації SA	120
6.8 Бази даних SAD та SPD	121
6.9 Особливості реалізації протоколу IPsec	122
6.10 Основні схеми застосування IPsec	123
6.11 Переваги IPsec	125
6.12 Перелік контрольних і тестових питань розділу 6	126
Розділ 7 ТРАНСПОРТНИЙ РІВЕНЬ	128
7.1 Призначення транспортного рівня	128
7.2 Протокол UDP	130
7.3 Протокол TCP	132
7.4 Безпека транспортного рівня	137
7.4.1 Протокол SSL	137
7.4.2 Протокол TLS	140
7.5 Перелік контрольних і тестових питань розділу 7	142

Розділ 8 СЕАНСОВИЙ РІВЕНЬ, РІВЕНЬ ПРЕДСТАВЛЕННЯ, ПРИКЛАДНИЙ РІВЕНЬ	144
8.1 Сеансовий рівень.....	144
8.2 Рівень представлення	149
8.3 Прикладний рівень.....	151
8.3.1 Гіпертекст	151
8.3.2 Протокол передавання гіпертексту (HTTP).....	156
8.3.3 Забезпечення безпеки HTTP	169
8.3.4 Протокол HTTPs.....	177
8.4 Перелік контрольних і тестових питань розділу 8	179
Розділ 9 МАРШРУТИЗАЦІЯ У КОМП'ЮТЕРНИХ МЕРЕЖАХ.....	182
9.1 Принципи маршрутизації в об'єднаних мережах. Класифікація протоколів маршрутизації	182
9.2 Протокол внутрішньої маршрутизації RIP.....	191
9.3 Протокол OSPF	197
9.4 Протоколи зовнішньої маршрутизації. Протокол BGP	202
9.5 Перелік контрольних і тестових питань розділу 9	206
Розділ 10 ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ (VPN).....	208
10.1 Концепція віртуальних захищених мереж VPN	208
10.2 Основні поняття та функції мережі VPN.....	209
10.3 Побудова віртуальних захищених каналів	214
10.4 Забезпечення безпеки віртуальної мережі.....	216
10.5 Побудова захищених мереж за допомогою VPN-рішень.....	218
10.6 Перелік контрольних і тестових питань розділу 10	222
Розділ 11 ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ.....	224
11.1 Технології Ethernet.....	224
11.1.1 Fast Ethernet.....	225
11.1.2 Три види Fast Ethernet	225
11.1.3 Gigabit Ethernet.....	225
11.2 Пасивні оптичні мережі	227
11.2.1 Розвиток технологій PON	227
11.2.2 Основні компоненти пасивних оптичних мереж	230
11.2.3 Забезпечення безпеки в PON.....	231
11.3 Протокол IEEE 802.11 (Wi-Fi).....	233
11.3.1 Структура IEEE 802.11 у рамках моделі ISO/OSI	234
11.3.2 Архітектура мереж IEEE 802.11	235
11.3.3 Послуги мереж IEEE 802.11	237
11.3.4 Безпека протоколів IEEE 802.11	238
11.3.5 Протокол WEP	238
11.3.6 Динамічне шифрування WEP	239
11.3.7 Протокол TKIP	240

11.3.8 MAC-фільтр	241
11.3.9 Маскування SSID	242
11.3.10 Протокол 802.11i.....	243
11.3.11 Протокол WPA3	243
11.3.12 Принцип роботи WPA3.....	245
11.3.13 Огляд існуючих вразливостей у стандарті WPA3.....	246
11.3.14 Автентифікація PSK.....	247
11.3.15 Безпека Wi-Fi 7 (безпека в діапазоні частот 6 ГГц)	248
11.4 Технологія Bluetooth	248
11.4.1 Призначення та особливості Bluetooth.....	248
11.4.2 Архітектура та версії Bluetooth.....	250
11.5 Перелік контрольних і тестових питань розділу 11.....	251
Розділ 12 ОСНОВИ МЕРЕЖЕВОЇ БЕЗПЕКИ	253
12.1 Завдання керування системою мережевої безпеки.....	254
12.2 Глобальна та локальна політики безпеки.....	255
12.3 Типові інформаційно-технічні впливи на комп'ютерні мережі та системи	257
12.3.1 Класифікація атакуючих інформаційно-технічних впливів з боку злоумисників	257
12.3.2 Віддалені мережеві атаки. Визначення та класифікація віддалених мережевих атак.....	259
12.3.3 Приклади інформаційно-технічних впливів на основі віддалених мережевих атак.....	264
12.3.4 Аналіз мережевого трафіку	266
12.3.5 Підміна довіреного об'єкта або суб'єкта інформаційної системи ..	267
12.3.6 Впровадження хибного об'єкта в систему	268
12.3.7 Використання хибного об'єкта для організації віддаленої атаки на систему	270
12.3.8 Атаки типу «відмова в обслуговуванні».....	272
12.3.9 Приклади засобів інформаційно-технічних впливів на основі комп'ютерних вірусів	275
12.3.10 Програмні закладки.....	279
12.3.11 Апаратні закладки.....	281
12.4 Сегментація комп'ютерної мережі.....	281
12.5 Концепція Сітчастої архітектури кібербезпеки.....	284
12.6 Перелік контрольних і тестових питань розділу 12.....	286
ВИСНОВКИ	288
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	290
ГЛОСАРІЙ	294
ЛІТЕРАТУРА.....	309

ВСТУП

Навчальний посібник «Мережеві технології та протоколи» надає інструменти та знання, необхідні для швидкої навігації у складному світі комп'ютерних мереж, що швидко розвиваються.

У цій книжці ви вивчите основи мережевих технологій і протоколів, зрозумієте складнощі мережевої безпеки, а також дізнаєтеся про нові тенденції та технології, які визначатимуть майбутнє індустрії.

Сфера комп'ютерних мереж лежить в основі цифрових технологій, комунікації в локальних і глобальних мережах. Оскільки мережеві технології продовжують розвиватися як ніколи раніше, для теперішніх і майбутніх мережевих професіоналів стає все більш важливим залишатися в курсі подій і адаптуватися до цих змін.

Одним із найважливіших уроків, що можна винести з зазначеного вище, є необхідність безперервного навчання та професійного розвитку.

Будучи динамічною галуззю, що постійно змінюється, комп'ютерні мережі пропонують багато можливостей для зростання та інновацій, але вони також вимагають узгоджених зусиль для того, щоб бути в курсі останніх розробок і передових практик.

Постійно навчаючись і слідкуючи за новими тенденціями та технологіями, ви будете краще підготовлені до нових можливостей і викликів у світі мережевих технологій.

Від периферійних обчислень і квантових мереж до бездротових технологій наступного покоління, таких як 6G, світ комп'ютерних мереж побачить багато цікавих розробок у найближчі роки. Знання, отримані сьогодні, забезпечать міцний фундамент для прийняття цих змін і сприятимуть подальшому розвитку галузі.

«Мережеві технології та протоколи» було задумано як навчальний посібник, що пропонує огляд галузі, практичні ідеї в побудові систем мережевої безпеки, а також посібник для подолання численних складнощів при побудові таких систем.

У міру просування вперед у своїй кар'єрі або особистих заняттях пам'ятайте, що майбутні комп'ютерні мережі обмежені тільки нашою колективною уявою та нашою готовністю розсунути межі можливого.