

# ЗМІСТ

<b>Вступ</b> .....	7
<b>Розділ 1. Огляд типових атак на локальну мережу</b> .....	9
1.1. Убезпечення локальної мережі та її кінцевого користувача від типових атак засобами технологій компанії “Cisco”.....	9
1.2. Огляд загроз мережевій безпеці комутатора на каналному рівні моделі відкритих систем OSI.....	13
1.3. Огляд атак на таблиці MAC-адрес та запобігання цим атакам.....	16
1.4. Огляд типових атак на локальні мережі.....	18
1.4.1. Огляд атак на VLAN та запобігання цим атакам.....	18
1.4.2. Дослідження атак на сервер DHCP.....	22
1.4.3. Типові атаки на основі роботи протоколу ARP та типові атаки підміни адрес.....	27
1.4.4. Дослідження атак на STP.....	31
1.4.5. Типові атаки, пов’язані із роботою протоколу CDP.....	32
1.5. Режим роботи портів комутатора та перевірка конфігурації його портів.....	33
1.6. Огляд базових команд ОС Cisco IOS для перевірки роботи комутатора та початкової конфігурації його портів.....	34
1.7. Помилки передавання даних, що виникають на каналному рівні моделі OSI.....	36
<b>Розділ 2. Особливості реалізації бездротових мереж та основи їх захисту від типових атак</b> .....	40
2.1. Огляд базових понять бездротового зв’язку.....	40
2.1.1. Бездротові технології та типи бездротових мереж.....	40
2.1.2. Бездротові технології та стандарти і частоти.....	43
2.2. Компоненти бездротових мереж.....	47
2.2.1. Бездротові мережі.....	47
2.2.2. Бездротовий домашній маршрутизатор.....	47
2.2.3. Бездротові точки доступу.....	48
2.2.4. Категорії точок доступу.....	48
2.2.5. Бездротові антени.....	50
2.3. Функціонування бездротових мереж.....	51
2.3.1. Режими бездротової топології за стандартом 802.11.....	51
2.3.2. Сервіси BSS та ESS.....	53
2.3.3. Структура кадру 802.11.....	54
2.3.4. Метод доступу CSMA/CA.....	56
2.3.5. Підключення клієнта до бездротової точки доступу.....	56

2.3.6. Режими пошуку бездротової точки доступу.....	58
2.4. Робота протоколу CAPWAP.....	59
2.4.1. Розподілення функцій на рівні архітектури MAC .....	60
2.4.2. Шифрування DTLS.....	61
2.4.3. Технологія FlexConnect.....	62
2.5. Управління каналами.....	63
2.5.1. Частотний канал.....	63
2.5.2. Вибір каналу.....	65
2.5.3. Планування розгортання бездротової мережі.....	67
2.6. Типові загрози бездротових мереж.....	68
2.6.1. Огляд безпеки бездротового зв'язку.....	68
2.6.2. DoS атаки.....	69
2.6.3. Розгортання фейкових точок доступу.....	69
2.6.4. Атака “людина – посередині”.....	71
2.7. Методи та засоби захисту бездротової мережі.....	72
2.7.1. Маскування SSID та фільтрація MAC-адрес.....	72
2.7.2. Оригінальні методи автентифікації 802.11.....	74
2.7.3. Методи автентифікації спільних ключів.....	74
2.7.4. Автентифікація домашнього користувача.....	75
2.7.5. Методи шифрування.....	76
2.7.6. Автентифікація на підприємстві.....	77
2.7.7. WPA3.....	78
<b>Розділ 3. Сучасні технології захисту локальних мереж.....</b>	<b>80</b>
3.1. Запобігання атакам на таблиці MAC-адрес.....	80
3.1.1. Реалізація Port Security та захист невикористаних портів.....	80
3.1.2. Режими порушення Port Security.....	86
3.1.3. Перевірка роботи Port Security.....	89
3.2. Запобігання атакам на VLAN.....	91
3.2.1. Дослідження атак на VLAN.....	91
3.2.2. Запобігання атакам Hopping VLAN.....	91
3.3. Запобігання атакам на сервер DHCP.....	93
3.3.1. Структура атаки DHCP.....	93
3.3.2. Упровадження DHCP Snooping.....	93
3.4. Запобігання атакам на ARP.....	96
3.4.1. Застосування динамічної інспекції ARP.....	96
3.4.2. Упровадження DAI.....	97
3.5. Запобігання атакам на STP.....	100
3.5.1. Застосування PortFast та BPDU Guard.....	100
3.5.2. Налаштування PortFast.....	101
3.5.3. Налаштування BPDU Guard.....	101

<b>Розділ 4. Практичні аспекти налаштування безпеки локальних мереж на обладнанні CISCO</b> .....	103
4.1. Організація безпечного віддаленого доступу .....	103
4.1.1. Операція Telnet .....	103
4.1.2. Операція SSH .....	104
4.1.3. Налаштування SSH .....	105
4.2. Базова конфігурація маршрутизатора .....	108
4.2.1. Налаштування основних параметрів маршрутизатора .....	108
4.2.2. Перевірка безпосередньо підключених мереж .....	111
4.3. Базова конфігурація комутатора .....	115
4.3.1. Керування комутатором .....	115
4.3.2. Конфігурація віртуального інтерфейсу керування свічем SVI .....	116
4.3.3. Налаштування портів комутатора .....	118
4.4. Управління доступом до ресурсів локальної мережі .....	120
4.4.1. Автентифікація за допомогою локального пароля .....	120
4.4.2. Компоненти сервісу AAA .....	122
4.4.3. Стандарт 802.1X .....	125
4.5. Налаштування бездротової мережі .....	126
4.5.1. Бездротовий маршрутизатор та підключення до нього .....	126
4.5.2. Базові налаштування мережі .....	128
4.5.3. Базові бездротові налаштування .....	129
4.5.4. Налаштування бездротової мережі .....	130
4.6. Налаштування основної бездротової локальної мережі на основі контролера WLC .....	132
4.6.1. Суть роботи та топологія WLC .....	132
4.6.2. Перегляд інформації про базові налаштування бездротової точки доступу .....	135
4.6.3. Розширені налаштування бездротової точки доступу .....	136
4.6.4. Налаштування бездротової локальної мережі .....	137
4.7. Налаштування серверів SNMP та RADIUS на WLC .....	140
4.7.1. Налаштування інформації про сервери SNMP та RADIUS .....	140
4.7.2. Налаштування VLAN для нової бездротової локальної мережі .....	143
4.7.3. Налаштування пулу DHCP .....	147
4.7.4. Налаштування WPA2 Enterprise у бездротовій локальній мережі .....	149
4.8. Усунення проблем із бездротовою мережею .....	152
4.8.1. Підходи до усунення несправностей підключення .....	152
4.8.2. Підходи до подолання втрати продуктивності бездротової мережі .....	156
<b>Список літератури</b> .....	160

<b>Додаток 1. Блок тестування теоретичних знань</b> .....	161
<b>Завдання для поточного контролю</b> .....	161
Тест 1. Безпека хоста у локальній мережі та управління доступом.....	161
Тест 2. Огляд загроз мережеві безпеці на каналному рівні моделі OSI.....	162
Тест 3. Атаки на таблиці MAC-адрес.....	163
Тест 4. Атаки на локальні мережі.....	164
Тест 5. Основи бездротового зв'язку.....	165
Тест 6. Компоненти бездротових мереж.....	166
Тест 7. Функціонування бездротових мереж.....	167
Тест 8. Робота протоколу CAPWAP.....	168
Тест 9. Управління каналами бездротової мережі.....	169
Тест 10. Загрози у бездротовій мережі.....	170
Тест 11. Захист бездротової мережі.....	171
Тест 12. Перевірка роботи безпосередньо підключених мереж.....	172
<b>Завдання для комплексного рубіжного контролю</b> .....	172
Фінальний тест 1. Мережева безпека локальної мережі.....	172
Фінальний тест 2. Конфігурація безпеки комутатора локальної мережі.....	175
Фінальний тест 3. Базова конфігурація мережевого пристрою.....	178
Фінальний тест 4. Концепції бездротових мереж.....	180
Фінальний тест 5. Конфігурація бездротової мережі.....	183
<b>Додаток 2. Блок формування практичних вмінь</b> .....	187
Практичне завдання 1. Налаштування Port Security.....	187
Практичне завдання 2. Комплексна конфігурація безпеки комутатора локальної мережі.....	190
Практичне завдання 3. Налаштування безпечного віддаленого доступу.....	193
Практичне завдання 4. Налаштування інтерфейсів маршрутизатора.....	195
Практичне завдання 5. Перевірка безпосередньо підключених мереж.....	197
Практичне завдання 6. Конфігурування локальної мережі.....	200
Практичне завдання 7. Налаштування бездротової мережі.....	203
Практичне завдання 8. Налаштування основної WLAN на WLC.....	209
Практичне завдання 9. Налаштування WPA2 Enterprise WLAN на WLC.....	214
Практичне завдання 10. Усунення несправностей WLAN.....	222
Практичне завдання 11. Конфігурація бездротової мережі.....	225

## ВСТУП

Відомо, що підготовка висококваліфікованих фахівців технічного напрямку, зокрема професіоналів у галузі забезпечення захисту локальних комп'ютерних мереж (провідних, безпроводних, гібридних), потребує і змістовного теоретичного підґрунтя, і досконалих практичних навичок з метою успішного працевлаштування на сучасному ринку праці.

Локальні комп'ютерні мережі, зокрема безпроводні, є чільним аспектом організації праці в сучасних умовах, тому для проектування, організації, підтримки й досягнення безпеки обладнання та інфраструктури таких мереж галузь потребує висококваліфікованих фахівців.

Мережі – важлива складова усіх сфер життя, і нині дедалі швидше розвиваються саме безпроводні мережі як елемент не лише локальної мережі, а й мереж значно більших масштабів.

Інтерес до бездротових мереж зумовлений зручністю роботи у мережі, гнучкістю доступу до публічної та/або корпоративної мережі. Із часом це привело до обвального падіння цін на бездротове обладнання. Нині бездротові адаптери використовують ноутбуки, стаціонарні комп'ютери, планшети, телефони, елементи і складові “smart home” та багато інших пристроїв.

Компанія “Cisco” є не лише світовим лідером у галузі виробництва та впровадження мережевих технологій, а й має потужну навчальну базу для роботи зі своїм обладнанням у вигляді регіональних академій “Cisco”; тому можна впевнено стверджувати, що стосовно апаратних та програмних рішень компанія “Cisco” є флагманом світових трендів у галузі сучасних комп'ютерних мереж.

Компанія “Cisco” була і є ініціатором важливих історичних змін у галузі інформаційних технологій і нині вона продовжує цей тренд. І сьогодні, коли галузь високих технологій вкотре переживає періоди істотних змін, “Cisco” зберігає лідерство в таких мережевих напрямках, як маршрутизація, комутація, бездротовий зв'язок і безпека.

Навчальний посібник розрахований на студентів закладів вищої освіти спеціальностей 123 “Комп'ютерна інженерія” та 125 “Кібербезпека” і допоможе ґрунтовно готувати фахівців із мережевої безпеки локальних мереж для роботи на обладнанні компанії “Cisco”.