Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б.Жильцов
«14» 09 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ БЕЗПЕКИ БЕЗПРОВОДОВИХ І МОБІЛЬНИХ МЕРЕЖ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

Київ – 2018

Розробники:

Соколов Володимир Юрійович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладачі:

Соколов Володимир Юрійович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 13.09.2018 р. № 6

Завідувач кафедри _____ В.Л. Бурячок
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ (В.Л. Бурячок)
(підпис)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ І.Ю. Мельник
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	7 / 210	
Курс	5	
Семестр	9	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	7	
Обсяг годин, в тому числі:	210	
Аудиторні	56	
Модульний контроль	14	
Семестровий контроль	-	
Самостійна робота	140	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Технології безпеки безпроводових і мобільних мереж» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.02 «Безпека інформаційних і комунікаційних систем».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Технології безпеки безпроводових і мобільних мереж» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Технології безпеки безпроводових і мобільних мереж» складається з трьох змістових модулів: «Загрози для безпроводових технологій і їх аналіз», «Атаки на комерційні безпроводові протоколи», «Забезпечення безпеки безпроводових систем і мереж». Обсяг дисципліни – 210 год. (7 кредитів).

Метою викладання навчальної дисципліни «Технології безпеки безпроводових і мобільних мереж» є формування у студентів уміння вирішувати задачі адміністрування безпроводових і мобільних мереж і систем, застосовувати нормативно-правові, організаційні та технічні процедури при роботі безпроводових і мобільних технологій.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері безпроводових і мобільних технологій, інформаційної та кібернетичної безпеки та набуття **наступних компетентностей**:

Фахові компетентності

КФ-3 — здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ-5 — здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації**.**

3. **Результати навчання за дисципліною**

У результаті вивчення навчальної дисципліни студент повинен

знати:

- Wi-Fi протоколи та їх слабкі сторони;
- методи та інструменти для аналізу протоколів Bluetooth, ZigBee та ін., а також компрометуючих методів;
- функції вбудованих і кібернетичних фізичних систем та аспекти безпеки;
- безпека мобільних мереж (GSM, протоколи CDMA).

уміти:

- розробляти безпроводові інфраструктури;
- вибирати безпроводову конфігурацію;
- створювати політики безпеки;
- встановлювати рейтинги дозволів;
- проводити аудит службової мережі;
- збігати поточну мережу з іншими провідними та безпроводовими мережами;
- забезпечувати доступності та масштабованості безпроводової мережі;
- захищати мобільні пристрої та канали зв’язку від кібератак.

та досягти наступних **програмних результатів навчання:**

ПРз-8 — вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки; забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.

ПРз-9 — володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Загрози для безпроводових технологій і їх аналіз							
Тема 1. Безпроводові мережі загрози моделей	28	4		2	2		20
Тема 2. Безпроводовий збір даних та WiFi MAC-аналіз.	28	4		2	2		20
Тема 3. Безпроводові засоби інформаційного аналізу.	28	4		2	2		20
Модульний контроль	6						
Разом	90	12		6	6		60
Змістовий модуль 2. Атаки на комерційні безпроводові протоколи							
Тема 4. Атаки на Bluetooth, DECT і ZigBee.	28	2		4	2		20
Тема 5. Розширені методики атак WiFi.	28	2		2	4		20
Модульний контроль	4						
Разом	60	4		6	6		40
Змістовий модуль 3. Забезпечення безпеки безпроводових систем і мереж							
Тема 6. Безпроводові стратегії забезпечення безпеки та їх реалізація.	28	2		4	2		20
Тема 7. Засоби захисту в мобільних технологіях.	28	2		2	4		20
Модульний контроль	4						
Разом	60	4		6	6		40
Усього	210	20		18	18		140

5. Програма навчальної дисципліни

Змістовий модуль 1. Загрози для безпроводових технологій і їх аналіз

Основні питання:

- Розуміння незалежних органів стандартів, роль WiFi Alliance для тестування сумісності, можливості та особливості WPA та WPA2, стандарти IETF, розуміння протоколів RADIUS та EAP.
- Визначення та розуміння впливу корпоративних стандартів безпеки, включаючи: 802.11z, 802.11ac, 802.11af.
- Отримання інформації про роботу органів стандартів та ресурсів робочої групи.
- Використання безпроводового сніфінгу як механізму аналізу, розуміння режиму роботи WLAN-картки, сніфінг у керованому режимі, сніфінг в режимі монітора, переваги RFMON-сніфінгу, реалізація RFMON.
- Аналіз безпроводового трафіку за допомогою tcpdump, Wireshark та Kismet.
- Вилучення безпроводового зв’язку за допомогою Wireshark, визначення безпроводовиї мереж за допомогою Kismet, відображення безпроводових мереж за допомогою gpsmap, Google Maps, Google Earth.
- Побудова GPS-карт для точок безпроводового доступу (airodump-ng).

● Загальні можливості IEEE 802.11 MAC, розуміння архітектури та експлуатації мереж ad hoc та інфраструктури, етапи автентифікації та асоціації станцій, розуміння операцій та поведінки автентифікації IEEE 802.1X.
● Визначення можливостей та особливостей типів EAP, включаючи PEAP, EAP/TLS, TTLS, EAP-FAST.
● Пакетне оформлення в безпроводових мережах, розуміння формату та полів заголовка 802.11.

Змістовий модуль 2. Атаки на комерційні безпроводові протоколи

Основні питання:

● Введення в ZigBee, випадках використання ZigBee та розгортання.
● Атаки на системи ZigBee та інші безпроводові промислові системи.
● Архітектура ZigBee і IEEE 802.15.4 фізичної та MAC-рівня.
● Механізми захисту ZigBee та IEEE 802.15.4; автентифікація та криптографічний контроль.
● Слабкі сторони у механізмах надання та керування ключовими інструментами ZigBee.
● Інструменти для підслуховування та керування мережами ZigBee.
● Використання резервування ключів ZigBee Over-the-Air (OTA).
● Пошук ZigBee-пристроїв за допомогою інструментів аналізу сигналу.
● Введення технології Bluetooth, оцінка стек протоколу Bluetooth.
● Аналіз пристрою Bluetooth Classic, процедура приєднання Bluetooth-піконета , компонентів фізичного рівня.
● Аналіз технології Bluetooth Low Energy (4.0), випадки використання, моделі та структура розгортання.
● Профілі Bluetooth та можливості програми, параметри безпеки Bluetooth, використання автентифікації посилань Bluetooth та шифрування.
● Методи аудиту та ідентифікації пристроїв Bluetooth, методи визначення місцезнаходження передавачів Bluetooth на платформах Windows і Android.
● Найкращі методи роботи з політикою безпеки Bluetooth та налаштування пристрою.

Змістовий модуль 3. Забезпечення безпеки безпроводових систем і мереж

Основні питання:

● Введення в концепції IDS, диференціювання справжніх позитивних фактів з помилкових спрацьовувань, оцінка подій, що становлять інтерес.
● Моделі розгортання WIDS, включаючи оверлейні, інтегровані та гібридні розгортання.
● Методи виявлення атак, включаючи аналіз сигнатур, аналіз тенденцій та аналіз аномалій.
● Оцінюючи атаки за допомогою аналізу трафіку.
● Оцінка WIDS-систем, агрегації подій, розгортання світлових ламп, захищених протоколів зв’язку, служб захисту від вторгнення, інтеграції з сторонніми системами IDS.
● Розгортання WIDS, включаючи охоплення об’єкта, час затримки, вірність реєстрації, зберігання подій, аналіз тенденцій.
● Управління політикою довіри клієнтів сертифіката.
● Способи розгортання нового кореневого сертифіката.
● Керування налаштуваннями клієнтської конфігурації безпроводової інфраструктури.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми-емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	6	6	2	2	2	2
Відвідування семінарських занять	1						
Відвідування практичних занять	1	3	3	3	3	3	3
Відвідування лабораторних занять	1	3	3	3	3	3	3
Робота на семінарському занятті	10						
Робота на практичному занятті	10	3	30	3	30	3	30
Лабораторна робота (в тому числі допуск, виконання, захист)	10	3	30	3	30	3	30
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
Виконання модульної роботи	25	1	25	1	25	1	25
Виконання ІНДЗ	30						
Разом		-	107	-	103	-	103
Максимальна кількість балів: 313							
Розрахунок коефіцієнта: 313/100=3,13							

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Загрози для безпроводових технологій і їх аналіз		60	10
1	Основи аналізу загроз у безпроводових мережах: • виконання завдань відповідно до теми; • опрацювання фахових видань.	60	10
Змістовий модуль 2. Атаки на комерційні безпроводові протоколи		40	10
2	Порядок реакції на атаки на комерційні безпроводові мережі: • виконання завдань відповідно до теми; • опрацювання фахових видань.	40	10
Змістовий модуль 3. Забезпечення безпеки безпроводових систем і мереж		40	10
3	Порядок забезпечення безпеки безпроводових мереж: • виконання завдань відповідно до теми; • опрацювання фахових видань.	40	10
	Разом	140	30

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. СтандартиWiFi Alliance.
2. Стандарти IETF.
3. Протоколи RADIUS та EAP.
4. Визначення та розуміння впливу корпоративних стандартів безпеки, включаючи: 802.11z, 802.11ac, 802.11af.
5. Отримання інформації про роботу органів стандартів та ресурсів робочої групи.
6. Використання безпроводового сніфінгу як механізму аналізу
7. Розуміння режиму роботи WLAN-картки.
8. Сніфінг у керованому режимі. Сніфінг в режимі монітора.
9. Переваги RFMON-сніфінгу, реалізація RFMON.
10. Аналіз безпроводового трафіку за допомогою tcpdump, Wireshark та Kismet.
11. Вилучення безпроводового зв'язку за допомогою Wireshark.
12. Визначення безпроводовиї мереж за допомогою Kismet.
13. Відображення безпроводових мереж за допомогою gpsmap, Google Maps, Google Earth.
14. Побудова GPS-карт для точок безпроводового доступу (airodump-ng).
15. Загальні можливості IEEE 802.11 MAC.
16. Архітектура та експлуатація мереж ad hoc та інфраструктури.
17. Етапи автентифікації та асоціації станцій.
18. Операції та автентифікація IEEE 802.1X.
19. Визначення можливостей та особливостей типів EAP, включаючи PEAP, EAP/TLS, TTLS, EAP-FAST.
20. Пакетне оформлення в безпроводових мережах, формат та поля заголовків 802.11.
21. Введення в ZigBee, випадках використання ZigBee та розгортання.
22. Атаки на системи ZigBee та інші безпроводові промислові системи.
23. Архітектура ZigBee і IEEE 802.15.4 фізичної та MAC-рівня.
24. Механізми захисту ZigBee та IEEE 802.15.4; автентифікація та криптографічний контроль.

25. Слабкі сторони у механізмах надання та керування ключовими інструментами ZigBee.
26. Інструменти для підслуховування та керування мережами ZigBee.
27. Використання резервування ключів ZigBee Over-the-Air (OTA).
28. Пошук ZigBee-пристроїв за допомогою інструментів аналізу сигналу.
29. Введення технології Bluetooth, оцінка стек протоколу Bluetooth.
30. Аналіз пристрою Bluetooth Classic, процедура приєднання Bluetooth-піконета , компонентів фізичного рівня.
31. Аналіз технології Bluetooth Low Energy (4.0), випадки використання, моделі та структура розгортання.
32. Профілі Bluetooth та можливості програми.
33. Параметри безпеки Bluetooth.
34. Використання автентифікації посилань Bluetooth та шифрування.
35. Методи аудиту та ідентифікації пристроїв Bluetooth.
36. Методи визначення місцезнаходження передавачів Bluetooth на платформах Windows і Android.
37. Найкращі методи роботи з політикою безпеки Bluetooth та налаштування пристрою.
38. Введення в концепції IDS, диференціювання справжніх позитивних фактів з помилкових спрацьовувань, оцінка подій.
39. Моделі розгортання WIDS, включаючи оверлейні, інтегровані та гібридні розгортання.
40. Методи виявлення атак, включаючи аналіз сигнатур, аналіз тенденцій та аналіз аномалій.
41. Оцінюючи атаки за допомогою аналізу трафіку.
42. Оцінка WIDS-систем, агрегації подій, розгортання світлових ламп, захищених протоколів зв’язку, служб захисту від вторгнення, інтеграції з сторонніми системами IDS.
43. Розгортання WIDS, включаючи охоплення об’єкта, час затримки, вірність реєстрації, зберігання подій, аналіз тенденцій.
44. Управління політикою довіри клієнтів сертифіката.
45. Способи розгортання нового кореневого сертифіката.
46. Керування налаштуваннями клієнтської конфігурації безпроводової інфраструктури.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре — достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре — в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно — посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо — мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання — незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу — досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 210 год., лекції – 20 год., практичні заняття – 18 год., лабораторні роботи – 18 год., модульний контроль – 14 год., самостійна робота – 140 год.

Модулі (назви, бали)	**Змістовий модуль 1. Загрози для безпроводових технологій і їх аналіз (107 балів)**			**Змістовий модуль 2. Атаки на комерційні безпроводові протоколи (103 бали)**		**Змістовий модуль 3. Забезпечення безпеки безпроводових систем і мереж (103 бали)**	
Лекції (теми, бали)	Безпроводові мережі загрози моделей (2 бали)	Безпроводовий збір даних та WiFi MAC-аналіз (2 бали)	Безпроводові засоби інформаційного аналізу (2 бали)	Атаки на Bluetooth, DECT і ZigBee (1 бал)	Розширені методики атак WiFi (1 бал)	Безпроводові стратегії забезпечення безпеки та їх реалізація (1 бал)	Засоби захисту в мобільних технологіях (1 бал)
Практичні, семінарські заняття (теми, бали)	Моделі загроз для безпроводових мереж (11 балів)	Організація та стандарти безпроводової мережі (11 балів)	Атаки на WEP (11 балів)	Експлуатація вразливостей ZigBee (22 бали)	Вплив DoS-атак на інфраструктуру WiFi (11 балів)	Розгортання безпечної безпроводової інфраструктури (22 бали)	Вразливість в GSM/GPRS, атаки та контрзаходи (11 балів)
Лабораторні заняття (теми, бали)	Безпроводове картографування (11 балів)	Моніторинг мережевого трафіку (11 балів)	Технології злому WEP та WPS (11 балів)	Радіочастотний ресурс Wi-Fi 2,4–2,5 ГГц (11 балів)	DoS-атаки на Wi-Fi мережі (22 бали)	Wi-Fi фазинг (11 балів)	Завантаження прошивки «по повітрю» (22 бали)
Самостійна робота	Самостійна робота (10 балів)			Самостійна робота (10 балів)		Самостійна робота (10 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)	
Підсумковий контроль (вид, бали)	залік						

8. Рекомендовані джерела

Основна (базова):

1. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с.
2. Sokolov, V. Wireless and Mobile Security : Laboratory Workshop / V. Sokolov, M. Taj Dini, V. Buryachok. — K. : SUT, 2017. — 124 p.
3. Wireless Geographic Logging Engine database https://wigle.net/graph-large.html.
4. Astapenya V. M., Sokolov V. Yu. "Modified accelerating lens as a means of increasing the throughput, range and noise immunity of IEEE 802.11 systems," ICATT'2015 Proceedings of the X Anniversary International Conference on Antenna Theory and Techniques, Kharkiv, Apr. 2015, pp. 267–269.
5. "CC2500 Low-Cost Low-Power 2.4 GHz RF Transceiver," Texas Instruments, 2016, 97 p.
6. "Pololu Wixel User's Guide," Pololu Corporation, 2015, 67 p.
7. V. Buryachok, G. Gulak, V. Sokolov. "Miniaturization of Wireless Monitoring Systems 2.4–2.5 GHz Band," Proceedings of the II International Scientific-Technical Conference on Actual Problems of Science and Technology, Kiev, Dec. 2015, p. 41.
8. "nRF24L01 Single Chip 2.4GHz Transceiver Product Specification," Nordic Semiconductor ASA, Version 2.0, July 2007, 74 p.
9. Graham, E., Steinbart, P.J. Wireless Security. 2006.
10. Cisco. Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, 19 July 2004.
11. CSI. CSI/FBI Computer Crime and Security Survey. 2004.
12. Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.
13. IEEE 802.11-2007, New York, NY, USA. 2007.
14. IEEE 802.11i-2004, New York, NY, USA. 2004.
15. Bellardo, J., Savage, S. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: Proceedings of the 12th USENIX Security Symposium, Berkeley, CA, USA, USENIX Association, 2003.
16. Aime, M.D., Calandriello, G., Lioy, A.: Dependability in wireless networks: Can we rely on WiFi IEEE Security and Privacy 5, p. 23–29, 2004.
17. Devine, C., d'Otreppe, T., Beck, M.: Aircrack-ng. 2009. http://www.aircrack-ng.org.
18. Smith, J.: Denial of service: Prevention, modelling and detection. 2007.
19. Glass, S., Muthukkumarasamy, V.: A study of the TKIP cryptographic DoS attack. In: ICON 2007: Proceedings of the 15th IEEE International Conference on Networks, New York, NY, USA, IEEE, p. 59–65. 2007.
20. Tews, E., Beck, M.: Practical attacks against WEP and WPA. In: WiSec '09: Proceedings of the second ACM conference on Wireless network security, New York, NY, USA, ACM, p. 79–86. 2009.

Додаткова

1. IEEE: IEEE 802.11e-2005, New York, NY, USA. 2005.
2. Halvorsen, F.M., Haugen, O., Eian, M., Mjølsnes, S.F.: An improved attack on TKIP. In: NordSec '09: Proceedings of the 14th Nordic Conference on Secure IT Systems, Berlin, Heidelberg, Springer-Verlag, p. 120–132. 2009.
3. IEEE: IEEE 802.11h-2003, New York, NY, USA. 2003.
4. Harkins, D.: Attacks against Michael and Their Countermeasures. IEEE 802.11 Working Group Document 03/211r0, New York, NY, USA. 2003.
5. The OpenWrt Project: OpenWrt. 2009. http://www.openwrt.org.
6. Malinen, J.: hostapd: IEEE 802.11 AP, IEEE 802.1X / WPA / WPA2 / EAP / RADIUS Authenticator. 2009. http://hostap.epitest.fi/hostapd.
7. Zarate, J.: Tomato Firmware (2009) http://www.polarcloud.com/tomato.
8. Cisco Systems Inc.: Enterprise Mobility 4.1 Design Guide, San Jose, CA, USA. 2009.

9. Додаткові ресурси

1. M. Beck. Enhanced TKIP michael attacks. Retrieved 4 Februari, 2013, from http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf.

2. J. Bellardo and S. Savage. 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In Proceedigns of the USENIX Security Symposium, 2003.

3. K. Bicakci and B. Tavli. Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks, 2009.

4. A. Stubblefield, J. Ioannidis, A. D. Rubin. A key recovery attack on the 802.11b wired equivalent privacy protocol (wep). ACM Trans. Inf. Syst. Secur., 7(2), 2004.

5. E. Tews, M. Beck. Practical attacks against WEP and WPA. In Proceedings of the second ACM conference on Wireless network security, WiSec ’09, 2009.

6. Y. Todo, Y. Ozawa, T. Ohigashi, M. Morii. Falsification attacks against WPA-TKIP in a realistic environment. IEICE Transactions, 95-D(2), 2012.

7. F. M. Halvorsen, O. Haugen, M. Eian, and S. F. Mjølsnes. An improved attack on TKIP. In 14th Nordic Conference on Secure IT Systems, NordSec ’09, 2009.

8. B. Harris, R. Hunt. Review: TCP/IP security threats and attack methods. Computer Communications, 22(10):885–897, 1999.

9. J. Huang, J. Seberry, W. Susilo, M. W. Bunder. Security analysis of michael: The IEEE 802.11i message integrity code. In EUC Workshops, pp. 423–432, 2005.