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
«_31_» ___01_____ 2019 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «БЕЗПЕКА БЕЗПРОВОДНИХ, МОБІЛЬНИХ ТА ХМАРНИХ ТЕХНОЛОГІЙ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма №
(підпис) (прізвище, ініціали)
«___» _____ 2019 р.

Київ – 2019

Розробник:

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 №1 від 16.01.2019 р.

Завідувач кафедри _____ (підпис) В.Л. Бурячок

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ (підпис) В.В. Семко

Робочу програму перевірено

___.___. 20___ р.

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

Пролонговано:

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

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

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

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

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	4 / 120	
Курс	1 (3)	
Семестр	2 (6)	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	42	
Модульний контроль	6	
Семестровий контроль	30	
Самостійна робота	42	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Безпека безпроводних, мобільних та хмарних технологій» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.01 «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 першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Безпека безпроводних, мобільних та хмарних технологій» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Безпека безпроводних, мобільних та хмарних технологій» складається з двох змістових модулів: «Загрози для безпроводових технологій і їх аналіз», «Атаки на комерційні безпроводові протоколи». Обсяг дисципліни – 120 год. (4 кредити).

Метою викладання навчальної дисципліни «Безпека безпроводних, мобільних та хмарних технологій» 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-11 — здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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;

уміти:

- розробляти безпроводові інфраструктури;
- вибирати безпроводову конфігурацію;
- створювати політики безпеки;
- встановлювати рейтинги дозволів;
- проводити аудит службової мережі;

та досягти наступних **програмних результатів навчання:**

ПРз-4 — вирішувати задачі супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискриційних, рольових); вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в ІТС.

ПРз-6 — вирішувати задачі управління процесами забезпечення неперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; вирішувати задачі корекції цілей, стратегій, планів забезпечення неперервності бізнесу після здійснення кібератак, збоїв та відмов різних класів; створювати і впроваджувати плани процесу забезпечення неперервності бізнесу; виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.

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	12	2		4			6
Тема 2. Безпроводовий збір даних та WiFi MAC-аналіз.	16	4		4			8
Тема 3. Безпроводові засоби інформаційного аналізу.	16	4		4			8
Модульний контроль	2						
Разом	46	10		12			22
Змістовий модуль 2. Атаки на комерційні безпроводові протоколи							
Тема 4. Атаки на Bluetooth, DECT і ZigBee.	20	4		6			10
Тема 5. Розширені методики атак WiFi.	20	4		6			10
Модульний контроль	4						
Разом	44	8		12			20
Підготовка та проходження контрольних заходів	30						
Усього	120	18		24			42

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.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної 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	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	5	5	4	4
Відвідування семінарських занять	1				
Відвідування практичних занять	1	6	6	6	6
Відвідування лабораторних занять	1				
Робота на семінарському занятті	10				
Робота на практичному занятті	10	6	60	6	60
Лабораторна робота (в тому числі допуск, виконання, захист)	10				
Виконання завдань для самостійної роботи	5	2	10	2	10
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
Разом		-	106	-	105
Максимальна кількість балів: 211					
Розрахунок коефіцієнта: 211/60=3,52					

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		22	10
1	Основи аналізу загроз у безпроводових мережах: • виконання завдань відповідно до теми; • опрацювання фахових видань.	22	10
Змістовий модуль 2. Атаки на комерційні безпроводові протоколи		20	10
2	Порядок реакції на атаки на комерційні безпроводові мережі: • виконання завдань відповідно до теми; • опрацювання фахових видань.	20	10

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 екзамену, умовою отримання якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 10 балів – комплексний комп'ютерний тест з дисципліни; 30 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями здійснювати інтерактивного контенту за спеціальністю.

Оцінювання практичного завдання відбувається в межах від 0 до 30 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Стандарти WiFi.
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.

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: 120 год., лекції – 18 год., практичні заняття – 24 год., модульний контроль – 6 год., семестровий контроль – 30 год., самостійна робота – 42 год.

Модулі (назви, бали)	**Змістовий модуль 1. Загрози для безпроводових технологій і їх аналіз (106 балів)**			**Змістовий модуль 2. Атаки на комерційні безпроводові протоколи (105 балів)**	
Лекції (теми, бали)	Безпроводові мережі загрози моделей (1 бали)	Безпроводовий збір даних та WiFi MAC-аналіз (2 бали)	Безпроводові засоби інформаційного аналізу (2 бали)	Атаки на Bluetooth, DECT і ZigBee (2 бал)	Розширені методики атак WiFi (2 бал)
Практичні, семінарські заняття (теми, бали)	Моделі загроз для безпроводових мереж (22 балів)	Організація та стандарти безпроводової мережі (22 балів)	Атаки на WEP (22 балів)	Експлуатація вразливостей ZigBee (33 бали)	Вплив DoS-атак на інфраструктуру WiFi (33 балів)
Самостійна робота	Самостійна робота (10 балів)			Самостійна робота (10 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)				

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. Wireless Geographic Logging Engine database https://wigle.net/graph-large.html.
3. “CC2500 Low-Cost Low-Power 2.4 GHz RF Transceiver,” Texas Instruments, 2016, 97 p.
4. “Pololu Wixel User’s Guide,” Pololu Corporation, 2015, 67 p.
5. “nRF24L01 Single Chip 2.4GHz Transceiver Product Specification,” Nordic Semiconductor ASA, Version 2.0, July 2007, 74 p.
6. Graham, E., Steinbart, P.J. Wireless Security. 2006.
7. Cisco. Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, 19 July 2004.
8. CSI. CSI/FBI Computer Crime and Security Survey. 2004.
9. Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.
10. IEEE 802.11-2007, New York, NY, USA. 2007.
11. IEEE 802.11i-2004, New York, NY, USA. 2004.

Додаткова

1. IEEE: IEEE 802.11e-2005, New York, NY, USA. 2005.
2. 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.