ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
Підпис Олег САВЕНКО
Ім'я, ПРІЗВИЩЕ
«31» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека безпроводових технологій та інтернету речей

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.11
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	3	5	5	150	68	34	34			82				+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека»

Робоча програма складена д-р філософії Микола СТЕЦЮК

Підпис(и) автора(ів) канд. техн. наук, доц Вікторія ОРЛЕНКО
Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри Підпис Юрій КЛЬОЦ
Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету Підпис Олег САВЕНКО
Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

БЕЗПЕКА БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ТА ІНТЕРНЕТ РЕЧЕЙ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	П'ятий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Денна

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем, в тому числі безпроводових мереж та інтернет речей; *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та *давати* оцінку результативності якості прийнятих рішень; *використовувати* сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних систем, зокрема безпроводових та інтернет речеф; *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах; *аналізувати* проекти безпроводових та інтернет речей, базуючись на стандартизованих технологіях та протоколах передачі даних, *виявляти* та *оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам безпроводових та мобільних систем згідно з встановленою політикою інформаційної та/або кібербезпеки.

Зміст навчальної дисципліни: Безпека інтернет-речей. Загрози конфіденційності в безпроводових мережах. Аналіз існуючих загроз і атак на безпроводові мережі. Моделі та критерії загроз у безпроводових мережах. Методи оцінки загроз у безпроводових мережах. Шляхи захисту безпроводових мереж. Безпека та конфіденційність у підтримці хмарних технологій. Управління даними в межах хмари. Управління ідентифікацією в хмарних технологіях. Керування масштабом для хмарних технологій. Зловмисні пристрої Cloud-supported IoT. Загрози і вразливості мобільних пристроїв. Управління мобільними пристроями. Життєвий цикл рішень з безпеки мобільних пристроїв. Загрози і вразливості мобільних телекомунікаційних систем. Загрози і вразливості Wi-Fi–мереж. Загрози і вразливості мобільних додатків.

Пререквізити: електроніка і схемотехніка систем захисту

Кореквізити: комплексні системи захисту інформації: проектування, в провадження, супровід

Запланована навчальна діяльність: лекцій 34 год., лабораторних занять 34 год., самостійної роботи 82 год., разом 150 год.

Форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, контекстні, моделювання, застосування інформаційно-комп'ютерних технологій (автоматизована система проектування Cisco Packet Tracer, інструменти та утиліти ОС Kali Linux).

Форми оцінювання результатів навчання: усне опитування, захист лабораторних робіт, письмова контрольна робота, підсумковий контрольний захід (семестровий контроль).

Вид семестрового контролю: іспит. **Навчальні**

ресурси:

1. Основи кібербезпеки: Безпека бездротових та мобільних технологій / Іваненко О.П., Коваленко М.С. – Київ: Національний технічний університет України, 2022. – 240 с.
2. Мобільні мережі та бездротові комунікації: Теорія та практика захисту / Петров В.Л., Гончаренко Т.М. – Харків: Харківський національний університет радіоелектроніки, 2023. – 210 с.
3. Безпека інтернету: Виклики і рішення / Лісовенко О.Г., Шевченко І.М. – Львів: Львівська політехніка, 2023. – 180 с.
4. Кібербезпека мобільних пристроїв та додатків / Дмитрук Н.С., Павленко Р.В. – Одеса: Одеський національний університет імені І.І. Мечникова, 2022. - 230 с.
5. Основи захисту даних у бездротових мережах / Козлов А.П., Ткаченко О.В. – Дніпро: Дніпровський національний університет імені Олеся Гончара, 2022. – 200 с.
6. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua.
7. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php

Викладач: доктор філософії Стецюк М.В.

ВСТУП

Дисципліна «Безпека безпроводових технологій та IoT» - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека», є однією з профілюючих дисциплін.

Метою викладання навчальної дисципліни «Безпека безпроводових і мобільних технологій» є формування у майбутніх спеціалістів умінь та компетенцій для оцінювання та забезпечення необхідного рівня захищеності інформації в безпроводових та мобільних мережах; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань безпеки та захисту сучасних безпроводових та мобільних технологій; сучасного програмноапаратного забезпечення безпроводових та мобільних технологій тощо.

Предметом дисципліни є міжнародні практики щодо здійснення щодо здійснення професійної діяльності з питань захисту та безпеки мобільних технологій та безпроводових мереж; методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека»:

***компетентності*:**

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах; КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційнотелекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

результати навчання:

РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційнокомунікаційних технологій.

РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем, в тому числі безпроводових та мобільних систем; *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та *давати* оцінку результативності якості прийнятих рішень; *використовувати* сучасне програмноапаратне забезпечення інформаційно-телекомунікаційних систем, зокрема безпроводових та мобільних систем; *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та

інформаційно-телекомунікаційних (автоматизованих) системах; *аналізувати* проекти безпроводових та мобільних систем, базуючись на стандартизованих технологіях та протоколах передачі даних, *виявляти* та *оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам безпроводових та мобільних систем згідно з встановленою політикою інформаційної та/або кібербезпеки.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Основні проблеми, вимоги та принципи захисту безпроводових технологій	4	24	40
Тема 2. Проблеми безпеки мобільних пристроїв, систем і додатків	10	-	10
Тема 3. Безпека Інтернету речей.	14	4	20
Тема 4. Управління та підтримка даних в хмарних технологіях для ефективного їх захисту	6	6	12
Разом:	**34**	**68**	**82**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

№ п/п	Перелік тем лекцій, їх анотація	Години
Тема 1. Основні проблеми, вимоги та принципи захисту безпроводових технологій		
1	**Загрози та атаки на безпроводові мережі** 1. Класифікація атак на безпроводові мережі та їх характеристики 2. Моделі та критерії загроз у безпроводових мережах 3. Методи оцінки загроз у безпроводових мережах Літ.: [1] с. 20-30; [14] с. 120-135	2
2	**Захист безпроводових мереж** 1. Технології побудови безпроводових мереж 2. Шляхи захисту безпроводових мереж Літ.: [1] с. 35-60; [14] с. 140-160	2
Тема 2. Проблеми безпеки мобільних пристроїв, систем і додатків		
3	**Загрози та вразливості мобільних пристроїв** 1. Загальні положення 2. Класифікація загроз та вразливостей мобільних пристроїв Літ.: [Літ.: [4] с. 15-30; [14] с. 170-190	2
4	**Управління мобільними пристроями** 1. Управління з метою забезпечення захисту 2. Життєвий цикл рішень з безпеки мобільних пристроїв Літ.: [4] с. 35-50; [17] с. 50-70	2
5	**Загрози та вразливості мобільних телекомунікаційних систем** 1. Загрози та вразливості стандартів 3G 2. Загрози та вразливості стандартів 4G 3. Загрози та вразливості стандартів 5G Літ.: [2] с. 45-60; [16] с. 80-100	2
6	**Загрози та вразливості Wi-Fi-мереж** 1. Класифікація загроз та вразливостей Wi-Fi-мереж 2. Методи захисту Wi-Fi-мереж Літ.: [6] с. 20-40; [16] с. 120-135	2
7	**Загрози та вразливості мобільних додатків** 1. Класифікація загроз та вразливостей мобільних додатків 2. Аналіз захищеності мобільних додатків Літ.: [4] с. 75-90; [17] с. 150-170	2
Тема 3. Безпека Інтернету речей.		
8	**Вступ до Інтернету речей** 1. Загальні принципи побудови та архітектура IoT 2. Класифікація систем IoT Літ.: [3] с. 10-30; [18] с. 40-70	2
9	**Засоби ідентифікації** 1. Класифікація засобів автоматичної ідентифікації 2. MAC-адреса 3. Радіочастотна ідентифікація (RFID) 4. Система позиціонування в режимі реального часу RTLS 5. Оптичні ідентифікатори Літ.: [3] с. 35-50; [18] с. 80-100	2

10	**Технології передачі даних в IoT (частина 1)** 1. Стандарт IEEE 802.15.4 2. Bluetooth (IEEE 802.15.1)	2
	3. ZigBee 4. Wi-Fi та IEEE 802.11 Літ.: [5] с. 15-35; [18] с. 110-140	
11	**Технології передачі даних в IoT (частина 2)** 1. Технологія LPWAN 2. Технологія PLC Літ.: [5] с. 40-55; [15] с. 150-170	2
12	**Огляд основних протоколів IoT** 1. Протоколи обміну даними Літ.: Літ.: [3] с. 60-75; [18] с. 160-180	2
13	**Забезпечення безпеки в IoT (частина 1)** 1. Проблема безпеки IoT 2. Проблеми конфіденційності в IoT Літ.: [3] с. 80-95; [15] с. 190-210	2
14	**Забезпечення безпеки в IoT (частина 2)** 1. Анатомія кібератак на IoT-пристрої 2. Фізична і апаратна безпека 3. Криптографія, як складова безпеки в IoT 4. Блокчейн і криптовалюта в Інтернеті речей Літ.: [3] с. 100-120; [15] с. 220-240	2
Тема 4. Управління та підтримка даних в хмарних технологіях для ефективного їх захисту		
15	**Топологія хмарних обчислень** 1. Модель хмарних сервісів 2. Види хмар та хмарна архітектура 3. Хмарна архітектура OpenStack 4. Обмеження хмарних архітектур Літ.: [9] с. 25-45; [16] с. 70-90	2
16	**Топологія туманних обчислень** 1. Туманні обчислення 2. Архітектура OpenFog RA 3. Amazon Greengrass і лямбда-функції 4. Туманні топології Літ.: [9] с. 50-70; [16] с. 100-120	2
17	**Технології Big Data** 1. Поняття Big Data, їх характеристики та сфери застосування 2. Категорії даних (грані даних) та процес data science 3. Технології та тенденції роботи з Big Data Літ.: Літ.: [9] с. 75-90; [16] с. 130-150	2
	Разом за семестр:	**34**

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кіль кість годин
1	Розгортання робочого середовища для проведення аудиту безпеки безпроводових мереж Літ.: [1] с. 15-30; [2] с. 40-55; [6] с. 10-20	**4**
2	Сканування мережевих протоколів Літ.: [1] с. 31-45; [2] с. 56-70;	**4**
3	Збирання технічної та чуттєвої інформації в безпроводових мережах Літ.: Літ.: [3] с. 15-30; [6] с. 36-50	**4**
4	Дослідження вразливостей безпроводових мереж Літ.: [2] с. 71-85; [3] с. 31-45;	**4**
5	Дослідження технологій злому безпроводових мереж Літ.: Літ.: [4] с. 20-35; [7] с. 56-70	**4**
6	Дослідження способів здійснення атак на відмову Літ.: [2] с. 101-115; [7] с. 71-85	**4**
7	Програмування пристроїв Інтернету речей засобами Cisco Packet Tracer Літ.: [3] с. 10-25; [5] с. 30-45; [8] с. 15-30	**4**
8	Захист хмарних сервісів Інтернету речей Літ.: Літ.: [5] с. 46-60; [8] с. 31-40	**4**
9	Підсумкове заняття. Контрольна робота	**2**
	Разом за семестр:	**34**

Зміст самостійної (у т.ч. індивідуальної) роботи

Об'єм самостійної роботи з дисципліни "Безпека безпроводових і мобільних технологій" становить 82 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до тестування, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

Номер тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №1.	5
2	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №1.	5
3	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №2.	5
4	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №2.	5
5	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №3.	5
6	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №3.	5
7	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №4.	5
8	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №4.	5
9	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №5.	5
10	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №5.	5
11	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №6.	5
12	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №6.	5
13	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №7.	5
14	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №7.	5
15	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №8.	5
16	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №8.	5
17	Опрацювання теоретичного матеріалу. Підготовка до контрольної роботи за пройденим матеріалом.	2
	Разом за семестр:	**82**

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням пояснювально-ілюстративними методами з супроводом презентаційних матеріалів, лабораторні роботи проводяться з використанням практичних, продуктивних, контекстних методів та методів моделювання, з застосуванням інформаційно-комп'ютерних технологій (автоматизована система проектування Cisco Packet Tracer, інструменти та утиліти ОС Kali Linux).

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт, контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторної роботи;
- письмова контрольна робота.

Семестровий контроль проводиться у формі іспиту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1,3,4	2	1-4
Ваговий коефіцієнт	0,45	0,15	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з теоретичного питання за відповідною темою. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичне питання, але у відповіді присутні дві-три несуттєві помилки.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичне питання.

Оцінку «незадовільно» отримує студент, який не дав відповіді на теоретичне питання.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двоматрьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Мережі Wi-Fi. Стандарти IEEE 802.11.
2. Фізичний рівень: методи модуляції.
3. Специфікації і топологія мереж IEEE 802.11.
4. Канальний рівень: формат і типи кадрів. Структура заголовків і призначення.
5. Доступ: централізований і децентралізований режими.
6. Загрози інформаційної безпеки мереж стандарту IEEE 802.11.
7. Класифікація загроз інформаційній безпеці бездротових мереж стандарту IEEE 802.11.
8. Класифікація бездротових мереж стандарту IEEE 802.11 по набору застосовуваних засобів захисту.
9. Порушники як джерела загроз інформаційній безпеці бездротових мереж стандарту IEEE 802.11.
10. Атаки на бездротові мережі стандарту IEEE 802.11
11. Відкрита аутентифікація і аутентифікація з загальним ключем. Шифрування. та аутентифікація в безпровідних мережах.
12. Механізм шифрування WEP. Специфікація WPA.
13. Стандарт IEEE 802.11i. Технології цілісності і конфіденційності переданих даних.
14. Архітектура мережі GSM. Основні принципи організації мережі GSM. Протоколи GSM. Сигнальні протоколи третього рівня Частотний план в стандарті GSM. Структура кадрів в стандарті GSM
15. Безпека в мережах GSM. Загальна схема криптографічного захисту GSM мереж. Можливі атаки. Безпека в GPRS
16. Безпека мобільної станції
17. Мережі на основі CDMA. архітектура мережі. Канали трафіку та управління.
18. Кодування в прямому каналі. Кодування в зворотному каналі. М'яка передача виклику і управління потужністю в CDMA.
19. Реалізація безпеки передачі інформації в стандарті стільникового зв'язку CDMA 2000 1xRTT. Безпека в CDMA мережах
20. Аутентіфікація. Безпека передачі голосових даних, інформації та службових повідомлень. Анонімность. 6.5 3G CDMA 2000
21. Технічні характеристики мереж стандарту 802.15. Фізичний і канальний уровени стандарту 802.15.1.
22. Топологія, стек протоколів і профілі Bluetooth.
23. Типи пристроїв, види з'єднань і взаємодія піко мереж Bluetooth.
24. Структура пакетів. Режими і обмін даними. Пошук і стикування пристроїв Bluetooth.
25. Безпека Bluetooth. Функції безпеки Bluetooth. Методи спарювання пристроїв. режими безпеки (Security Mode).
26. Стандарт Bluetooth Low Energy (BLE) з малими енергозатрарами.
27. Структура стека протоколів BLE. Види атак на Bluetooth. Bluetooth Piconet Security Checklist.
28. Комунікаційна архітектура сенсорних мереж. Сенсори і сенсорні мережі. Типи і архітектура. протоколи кластерно архітектури та і маршрутизації.
29. Показники QoS якості сенсорних мереж: тривалість життєвого циклу, верхове покриття, залишкова енергія, швидкість передачі, затримка і втрати пакетів.
30. Технологія ZigBee. Стандарт IEEE 802.15.4. Стек протоколів, мережі та профілі ZigBee.
31. Специфікації фізичного рівня і сервісів субрівнями MAC.
32. Формат кадрів. Алгоритм доступу до середовища передачі і взаємодії мережевих елементів.
33. Безпека в мережах ZigBee. Уразливості ZigBee Можливі атаки.

34. Загальна схема криптографічного захисту ZigBee мереж.
35. Ключі шифрування в ZigBee.
36. Аналіз існуючих загроз і атак на безпроводові технології.
37. Дерево атак на безпроводові мережі та їх характеристики.
38. Моделі та критерії загроз у безпроводових технологіях. 39. Методи оцінки загроз у безпроводових мережах
40. Шляхи захисту безпроводових мереж.
41. Загрози і вразливості мобільних пристроїв.
42. Управління мобільними пристроями.
43. Життєвий цикл рішень з безпеки мобільних пристроїв.
44. Загрози і вразливості мобільних телекомунікаційних систем
45. Загрози і вразливості Wi-Fi – мереж 46. Загрози і вразливості мобільних додатків
47. Проблема безпеки IoT.
48. Проблеми конфіденційності в IoT.
49. Анатомія кібератак на IoT-пристрої.
50. Фізична і апаратна безпека IoT. Криптографія.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Безпека безпроводових технологій та інтернет речей» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Основи кібербезпеки: Безпека бездротових та мобільних технологій / Іваненко О.П., Коваленко М.С. – Київ: Національний технічний університет України, 2022. – 240 с.
2. Мобільні мережі та бездротові комунікації: Теорія та практика захисту / Петров В.Л., Гончаренко Т.М. – Харків: Харківський національний університет радіоелектроніки, 2023. – 210 с.
3. Безпека інтернету промов: Лісовенко О.Г., Шевченко І.М. – Львів: Львівська політехніка, 2023. – 180 с.
4. Кібербезпека мобільних пристроїв та додатків / Дмитрук Н.С., Павленко Р.В. – Одеса: Одеський національний університет імені І.І. Мечникова, 2022. - 230 с.
5. Основи захисту даних у бездротових мережах / Козлов А.П., Ткаченко О.В. – Дніпро: Дніпровський національний університет імені Олеся Гончара, 2022. – 200 с.
6. Захист інформації в мережах Wi-Fi: сучасні методи та засоби / Михайленко В.С., Зубарєв І.В. – Київ: Київський політехнічний інститут, 2022. – 220 с.

Додаткова

7. Мережеві технології та безпека: Навчальний посібник / Сидоренко П.О., Чебан О.В. – Харків: ХНУ ім. В.М. Каразіна, 2023. - 190 с.
8. Сучасні технології шифрування для мобільних пристроїв / Ковальчук Д.М., Пономаренко С.О. – Одеса: ОНУ ім. І.І. Мечнікова, 2023. - 180 с.
9. Безпека інформації у хмарних технологіях / Гриценко О.О., Марченко Ю.П. – Київ: Київський національний університет імені Тараса Шевченка, 2022. – 250 с.
10. Методи аналізу загроз у мобільних мережах / Романенко В.В., Ткаченко Л.М. – Харків: Харківський національний університет радіоелектроніки, 2023. – 200 с.
11. Технології блокчейн у мобільних мережах / Василенко Т.О., Кучеренко М.О. – Київ: Національний технічний університет України, 2022. – 210 с.
12. Захист даних в інтернеті промов / Бондаренко І.В., Орлов А.С. – Львів: Львівський національний університет, 2022. – 210 с.
13. Protection of data on the Internet of speeches / Bondarenko I.V., Orlov A.S. – Lviv: Lviv National University, 2022. – 210 p.
14. "Cybersecurity for Mobile and Wireless Networks: Threats and Countermeasures" / Edited by A. Hassan, M. S. Khan – CRC Press, 2023. – 520 p.
15. "Advanced IoT Security: Privacy and Challenges" / Edited by H. Kumar, J. Nayak - Springer, 2022. - 330 p.
16. "Emerging Security Technologies in Wireless Communications" / Edited by L. Wang, Y. Zhang – CRC Press, 2022. – 300 p.
17. "Cybersecurity in Mobile Applications and Services" / Edited by K. Chatterjee, N. Kumar – Elsevier, 2023. – 290 p.
18. "Internet of Things (IoT): Architectures, Protocols, and Applications" / Edited by J. Lee, W. Lee, Y. Kim – Springer, 2023. – 450 p.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.

2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.