МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

БЕЗДРОТОВІ ТА ОПТИЧНОВОЛОКОННІ МЕРЕЖІ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***вибіркова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Євсеєв С. П., д.т.н., проф. кафедри КІТ.
Король О. Г., к.т.н., доц. кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів. У цей час розвиток телекомунікаційних мереж відбувається в напрямку росту ринку мультисервісних послуг, впровадження нових телекомунікаційних і інформаційних технологій, їх конвергенції. Інформація є одним з найцінніших предметів сучасного життя.

Одне з найважливіших напрямків діджиталізації є модернізація мереж зв'язку загального користування на основі концепції NGN (Next Generation Network) – мереж зв'язку наступного покоління з використанням стандартів оптоволоконних та бездротових каналів. Перспективна архітектура мереж нового покоління (NGN) припускає створення мультисервісної мережі з винесенням функціональності послуг в граничні вузли мережі, створення спеціальної підсистеми керування послугами у вигляді окремої мережевої підсистеми, а також розширення номенклатури інтерфейсів для підключення устаткування постачальників послуг. Мультисервісні мережі можуть бути створені як новий клас мереж зі забезпеченням можливості взаємодії з існуючими мережами.

Мета навчальної дисципліни "Бездротові та оптичноволоконні мережі" є вивчення принципів побудови мереж наступного покоління NGN на основі новітніх технологій та забезпечення інформаційної безпеки при наданні послуг зв'язку наступного покоління.

Характеристика навчальної дисципліни

Курс	**1М**
Семестр	**2**
Кількість кредитів	**5**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Інженерія безпеки інформаційно-комунікаційних систем	Дипломний проєкт
Безпека Інтернет-речей	

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації	– планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); – розробляти, планувати, аналізувати та

	впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;
Здатність планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів установи, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації	– планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки

Програма навчальної дисципліни

Тема 1. ***Загальна архітектура й завдання інформаційно- комунікаційних систем на основі технологій мобільного зв'язку. Формування безпеки в технологіях X-"G"***
Тема 2. ***Мережі на основі оптоволоконних каналів. Стандарти оптоволоконних каналів.***
Тема 3. ***Класифікація бездротових мереж. Принципи формування безпеки.***
Тема 4. ***Принципи формування мереж наступного покоління (NGN).***
Тема 5. ***Системи розподілу в мережах наступного покоління.***
Тема 6. ***Методи й засобу забезпечення якості обслуговування в NGN.***
Тема 7. ***Принципи керування мережами наступного покоління.***
Тема 8. ***IP Multimedia Subsystem.***
Тема 9. ***Безпека бездротових мереж Інтернет-речей.***
Тема 10.*Захист у мережах NGN.*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються лекції, презентації, бесіди, індивідуальні та групові міні-проєкти.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту поставити залік, – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- моделювати потокі трафіку в мережах;
- розробляти Cisco VoIP лабораторії на базі емулятора GNS3;
- застосовувати протокол MPLS;
- виконувати конфігурування IP-телефонії з використанням IP-телефонів та Cisco IP communicators.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: максимальна кількість балів становить 35 (робота на лекціях – 10, експрес-опитування – 25), а мінімальна – 18.

Лабораторні заняття: максимальна кількість балів становить 65 (захист лабораторних робіт – 35, контрольні роботи – 30), а мінімальна – 42.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями та контрольних робіт за лабораторними роботами дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням отриманих балів у продовж семестру.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Лекція *"Загальна архітектура й завдання інформаційно-комунікаційних систем на основі технологій мобільного зв'язку. Формування безпеки в технологіях X-"G""*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №1.* Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та систем	виконання лабораторної роботи	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Тема 2	***Аудиторна робота***			
	Лекція	Лекція *"Мережі на основі оптоволоконних каналів. Стандарти оптоволоконних каналів"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №1.* Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та систем	Захист лабораторної роботи № 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Класифікація бездротових мереж. Принципи формування безпеки"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №2.* Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі	виконання лабораторної роботи	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *"Принципи формування мереж наступного покоління (NGN)"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №2.* Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі	Захист лабораторної роботи № 2	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція *"Системи розподілу в мережах наступного покоління"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота 3.* Дослідження вразливостей системи або мережі за допомогою	виконання лабораторної роботи	

		спеціалізованого сканера вразливостей – Nessus		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Методи й засобу забезпечення якості обслуговування в NGN"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота 3.* Дослідження вразливостей системи або мережі за допомогою спеціалізованого сканера вразливостей – Nessus	Захист лабораторної роботи № 3	5
			Контрольна робота 1	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Лекція	*Лекція "Принципи керування мережами наступного покоління"*	Робота на лекції	1
			експрес-опитування	12
	Лабораторне заняття	*Лабораторна робота 4.* Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega	Захист лабораторної роботи № 4	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"IP Multimedia Subsystem"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота № 5.* Пошук вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego	Захист лабораторної роботи № 5	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Ма	***Аудиторна робота***			

	Лекція	Лекція *"Безпека бездротових мереж Інтернет речей"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота № 6.* Сніфери	Захист лабораторної роботи № 6	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Захист у мережах NGN"*	Робота на лекції	1
			експрес-опитування	13
	Лабораторне заняття	*Лабораторна робота № 7.* Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng	Захист лабораторної роботи № 7	5
			Контрольна робота № 2	15
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Рекомендована література

Основна

1. Чернышов Ю.Н. NGN: принципы построения и организации / Ю.Н.Чернышов. – М. : Эко–Трендз, 2008. – 400 с.

2. Захватов. Построение виртуальных частных сетей (VPN) на базе технологии MPLS / Захватов. – М. : Cisco Systems, 2005. – 52 с.

3. Олвейн В. Структура и реализация современной технологии MPLS / В. Олвейн. – М. : Вильямс, 2004. – 480 с.

4. Филимонов А. Ю. Построение мультисервисных сетей Ethernet / А.Ю. Филимонов. – СПБ. : БХВ-Петербург, 2007. – 592 с.

5. Гольдштейн А.Б. SOFTSWITCH / А.Б. Гольдштейн, Б.С. Гольдштейн. – СПБ. : БХВ, 2006. – 368 с.

6. Reagan, J. Cisco CCIP MPLS Study Guide / James Reagan. – Sybex, 2002. – 486 с.

Додаткова

7. Бакланов И.Г. NGN: принципы построения и организации. – М. : эко-трендз, 2008. – 400 с.

8. Глотиков К. IMS (IP multimedia Subsystem). М. : Эко-трендз. 2009. – 100 с.

9. Гольдштейн Б.С. Сети связи. Учебник для вузов / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. – СПБ. : БХВ, 2009. – 400 с.

10. Методичні вказівки до лабораторних робіт з дисципліни "Новітнє покоління мереж на основі багатопротокольних технологій NGN IP/MPLS" для студентів

спеціальності 123 "Комп'ютерна інженерія" всіх форм навчання / Укл. С.Ю. Скрупський. – Запоріжжя: ЗНТУ, 2018. – 46 с.

11. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд / В.Г.Олифер. – Питер.: СПБ, 2010. – 944с.

12. Сети связи пост С. Гольдштейн, А. Е. Кучерявый. — СПб.: БХВ Петербург, 20 — 160 с.: ил.

Інформаційні ресурси.

13. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Безпека програм та даних" https://pns.hneu.edu.ua/enrol/index.php?id=4941.