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

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

БЕЗДРОТОВА ТА МОБІЛЬНА БЕЗПЕКА

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:
Корольов Р.В., к.т.н., доцент 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

В світі існує багато технологій і способів передачі інформації між її користувачами. Останнім часом для цього все частіше застосовуються безпроводові мережі, які розгортаються в аеропортах, університетах, готелях, ресторанах, на підприємствах та служать для підключення користувачів до мережі; об'єднання просторово рознесених підмереж в одну загальну мережу там, де кабельне з'єднання підмереж неможливо або небажано; підключення до мереж провайдерів інтернет-послуг замість використання виділених проводових ліній або звичайного модемного з'єднання тощо.

Разом з цим, поява і активне поширення послуг безпроводового зв'язку вивели перший план питання забезпечення захисту безпроводових мереж та способи захисту даних в них від проявів стороннього кібернетичного впливу, оскільки комунікаційні сигнали при їх розповсюдженні через радіоефір легкодоступні для перехоплення.

Метою навчальної дисципліни «Бездротова та мобільна безпека» 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.

Результатами вивчення даної дисципліни є придбання навичок з проведення розрахункі дальності роботи бездротового каналу зв'язку, проектування та планування бездротової локальної мережі.

Характеристика навчальної дисципліни

Курс	**1М**
Семестр	**1**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**Екзамен**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Забезпечення ІБ	Дипломний проект
Основи технічного захисту інформації	

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (інформаційних, інформаційно-телекомунікаційних, автоматизованих).; КФ 7. Здатність аналізувати причини та наслідки збоїв або відмов функціонування інформаційних систем, що викликані реалізацією різного класу кіберінцидентів, а також розробляти й впроваджувати методи і заходи відновлення штатного функціонування інфраструктури організації в цілому; КФ 8. Здатність розробляти, планувати, аналізувати та впроваджувати систему	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – 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; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої,

Компетентності	Результати навчання
доступу до інформаційних ресурсів, а також систему аудиту і контролю функціонування інформаційно-комунікаційних систем та технологій (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.; КФ 9. Здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів.	нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-8 – 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); ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати,

Компетентності	Результати навчання
	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; ПРН-13 – 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; ПРН-14 – 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; ПРН-15 – 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; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень

Компетентності	Результати навчання
	в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства).

Програма навчальної дисципліни

Змістовний модуль 1. Безпровідні системи передачі даних

Тема 1. *Загальні поняття і класифікація безпровідних систем передачі даних.*

Тема 2. *Безпека бездротових мереж .*

Змістовний модуль 2. Захист інформації в мережах стільникового зв'язку

Тема 3. *Структурні компоненти мережі GSM / GPRS як об'єкти захисту від несанкціонованого доступу.*

Тема 4. *Аналіз методів і алгоритмів забезпечення інформаційної безпеки в мережах стандарту GSM / GPRS.*

Тема 5. *Характеристика та аналіз роботи мобільних мереж четвертого покоління.*

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 проблемні лекції, презентації, бесіди, індивідуальні та групові 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 – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

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

Порядок здійснення поточного оцінювання знань студентів.

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

- вміння організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності;

- вміння діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

- вміння вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою;

- вміння здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни

здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лекційні заняття: максимальна кількість балів становить 5 (робота на лекції.

Лабораторні заняття: максимальна кількість балів становить 55 (захист лабораторної роботи – 50, контрольна робота – 5), а мінімальна –26.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Зміст практичних завдань екзаменаційних білетів побудований таким чином, щоб перевірити ступінь відповідності підготовки студента вимогам положень освітньо-кваліфікаційної характеристики за напрямом підготовки.

Кожне з практичних завдань оцінюється за 10-бальною системою з наступною підсумковою оцінкою за виконання всього екзаменаційного завдання.

Кожне теоретичне питання оцінюється за 20-бальною системою з наступною підсумковою оцінкою за виконання всього екзаменаційного завдання. Загальна сума – 40 балів.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної “Відомості обліку успішності”.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та 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.

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 №1. Загальні поняття і класифікація безпровідних систем передачі даних	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 1. Розрахунок дальності роботи бездротового каналу зв'язку.	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 2.	***Аудиторна робота***			
	Лекція	Лекція №2. Безпека бездротових мереж	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 2. Попереднє планування бездротової локальної мережі 802.11	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 3.	***Аудиторна робота***			
	Лекція	Лекція №3. Структурні компоненти мережі GSM / GPRS як об'єкти захисту від несанкціонованого доступу	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 3. Розрахунок параметрів мережі 802.11e (мобільний WiMAX)	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 4.	***Аудиторна робота***			
	Лекція	Лекція №4. Аналіз методів і алгоритмів забезпечення інформаційної безпеки в мережах стандарту GSM / GPRS	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 4. Налаштування Wi-Fi 802.11 в ОС сімейства GNU / Linux	Захист лабораторної роботи	10
	Контрольна робота			5
	Самостійна робота			
	Питання та завдання	Пошук, підбір та огляд		

	до самостійного опрацювання	літературних джерел за заданою тематикою		
Тема 5.	***Аудиторна робота***			
	Лекція	Лекція №5. Характеристика та аналіз роботи мобільних мереж четвертого покоління	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота 5. Дослідження алгоритму потокового шифрування RC4.	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		

Рекомендована література

Основна

1. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум
2. В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с.
3. Wireless Geographic Logging Engine database https://wigle.net/graph-large.html. Graham, E., Steinbart, P.J. Wireless Security. 2006.
4. Cisco. Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, 19 July 2004.
5. CSI. CSI/FBI Computer Crime and Security Survey. 2004.
6. Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.
7. IEEE 802.11-2007, New York, NY, USA. 2007.
8. IEEE 802.11i-2004, New York, NY, USA. 2004.

Додаткова

9. Cisco Systems Inc.: Enterprise Mobility 4.1 Design Guide, San Jose, CA, USA. 2009.

Інформаційні ресурси в Інтернет

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

11. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Бездротова та мобільна безпека” https://pns.hneu.edu.ua/course/view.php?id=7124