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

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Карина НЕМАШКАЛО

Інженерія безпеки інформаційно-комунікаційних систем
робоча програма навчальної дисципліни

Галузь знань	***усі галузі***
Спеціальність	***усі спеціальності***
Освітній рівень	***другий (магістерський)***
Освітня програма	***усі освітні програми***

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

Завідувач кафедри
кібербезпеки
та інформаційних технологій *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробник:
Алексієв В. О., д.т.н., проф. кафедри кібербезпеки та інформаційних технологій.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

Анотація навчальної дисципліни

Розвиток інформаційно-комунікаційних систем має вагомий вплив на всі галузі суспільства. Надання доступу до інформації та спілкування у цифровому просторі є основними складовими для господарчої діяльності будь-якої організації чи підприємства. Поруч з цим забезпечення безпеки інформаційного простору є первинним завданням для збереження конфіденційності, цілісності та доступності даних. Треба розуміти, що інформація та дані забезпечують підґрунтя для функціонування майже всіх бізнес процесів, а вдала їх обробка надає конкурентних переваг.

Існуючі інформаційні технології набули сталого розвитку завдяки стрімкому вдосконаленню обчислювальних систем та засобів передачі даних. Зараз набуває все більшого поширення технологія Інтернету речей та впроваджуються технологічні рішення для розвитку кіберфізичних систем. Тому, завданням дисципліни «Інженерія безпеки інформаційно-комунікаційних систем» є формування у студентів цілісного уявлення щодо застосування певних засобів безпеки у комплексі інженерних рішень із забезпечення працездатності та гнучкого застосування засобів та технологій інформаційно-комунікаційних систем.

Мета навчальної дисципліни – формування та розвиток здатності до застосування сучасних методів та підходів забезпечення кібербезпеки. Предметом дисципліни є інструментальні засоби забезпечення безпеки та основи їх застосування у галузі впровадження сучасних інформаційно-комунікаційних систем. Об’єктом – стандартизація та процеси забезпечення безпеки інформаційно-комунікаційних систем.

Характеристика навчальної дисципліни

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

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Введення в мережі	**Дипломне проектування**
Інформаційні системи та Інтернет технології	

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
Здатність застосовувати знання у практичних ситуаціях. Здатність до абстрактного мислення, аналізу та синтезу. Здатність оцінювати та забезпечувати якість виконуваних робіт. Здатність досліджувати, проектувати та супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівнях, зокрема на основі розуміння впровадження нових технологій та засобів інформаційно-комунікаційних систем. Аналізувати та оцінювати рівень захищеності інформаційно-комунікаційних систем.

інформаційної діяльності. Здатність аналізувати і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою на рівні застосування інформаційно-комунікаційних систем.	

Програма навчальної дисципліни

Змістовий модуль 1. Інформаційно-комунікаційні системи та корпоративні мережі.

Тема 1. *Розвиток інформаційно-комунікаційних систем..*
Тема 2. *Побудова корпоративних мереж.*
Тема 3. *Безпека корпоративної мережі на базі Windows Server.*
Тема 4. *Безпека рівня Linux-сервера..*
Тема 5. *Особливості побудови та захисту бездротових мереж зв'язку.*

Змістовий модуль 2. Хмарні обчислення та забезпечення захисту від кіберзагроз.

Тема 6. *Введення до технологій хмарних обчислень.*
Тема 7. *Особливості застосування засобів безпеки хмарних обчислень.*
Тема 8. *Правові аспекти захисту даних.*
Тема 9. *Засоби моніторингу стану мереж.*
Тема 10. *Системи виявлення та запобігання вторгненням.*

Перелік лабораторних занять 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 (Тема 1), презентації (Тема 4), бесіди (Тема 2, Тема 6).

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 практичних занять проводиться за такими критеріями:

- обробляти дані журналів серверу щодо роботи комп’ютерних мереж;
- вміння аналізувати архітектуру комп’ютерних мереж та розуміти засоби безпеки;
- вміння адмініструвати окремий сервер (або сервіс) відповідно до налагодження засобів безпеки;

- знання основ організації забезпечення безпеки корпоративної мережі;
- знання методології та технік побудови захисту інформаційно-комунікаційних систем;
- знати основи систем хмарних обчислень;
- використовувати технології забезпечення безпеки мережевих протоколів передачі даних;
- знання щодо структур даних, файлових структур та структур баз даних, які застосовуються у рішеннях забезпечення безпеки від кіберзагроз;
- розуміти концепцію побудови кіберфізичних систем та відповідних засобів безпеки;
- вміння застосовувати системи моніторингу та виявлення кіберзагроз.

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

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

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.

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

Рейтинг-план навчальної дисципліни

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Розвиток інформаційно-комунікаційних систем."*		
	Лабораторна робота	Лабораторна робота №1 *Основи криптографії. Шифрування даних за допомогою openssl.*		
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних завдань.		
Тема 2	***Аудиторна робота***			
	Лекція	Лекція *"Побудова корпоративних мереж."*		
	Лабораторна робота	Лабораторна робота №1 (продовження)	Захист лабораторної роботи № 1	20
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Безпека корпоративної мережі на базі Windows Server"*		
	Лабораторна робота	Лабораторна робота №2. *Основи криптографії. Протокол Діффі – Геллмана..*		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *"Безпека рівня Linux-сервера"*		
	Лабораторна робота	Лабораторна робота №2 (продовження).	Захист лабораторної роботи № 2	20
Т	***Аудиторна робота***			

Тема 5	Лекція	Лекція*" Особливості побудови та захисту бездротових мереж зв'язку"*	Експрес-опитування	
	Лабораторна робота	Лабораторна робота №3. *Побудова системи обміну повідомленнями на основі брокеру. Протокол MQTT та забезпечення його безпеки.*	Контрольна робота 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Введення до технологій хмарних обчислень"*		
	Лабораторна робота	Лабораторна робота №3.	Захист лабораторної роботи № 3	20
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Особливості застосування засобів безпеки хмарних обчислень"*		
			Експрес-опитування	5
	Лабораторна робота	Лабораторна робота № 4. *Дослідження систем моніторингу стану комп'ютерних мереж та засобів протидії кіберзагрозам.*		
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Правові аспекти захисту даних"*		
	Лабораторна робота	Лабораторна робота №4. (продовження)		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		
Тема 9	***Аудиторна робота***			
	Лекція	Лекція *"Засоби моніторингу стану мереж"*		
	Лабораторна робота	Лабораторна робота № 4. (продовження)	Контрольна робота № 2	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Системи виявлення та запобігання вторгненням"*		
	Лабораторна робота	Лабораторна робота №4 (продовження).	Захист лабораторної роботи № 4	20
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання практичних робіт. Виконання лабораторних завдань.		

Залік	100

Рекомендована література

Основна

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

2. Конспект лекцій з дисципліни «Інформаційно-комунікаційні системи», частина 1, для студентів усіх форм навчання спеціальності 125 «Кібербезпека» за освітньою програмою «Безпека інформаційних комунікаційних систем». Електрон. вид. / упоряд. : Г. З. Халімов ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 207 с. [Electronic resource]. – Access mode: http://openarchive.nure.ua/handle/document/9702

3. Конспект лекцій з дисципліни «Інформаційно-комунікаційні системи», частина 2, для студентів усіх форм навчання спеціальності 125 «Кібербезпека» за освітньою програмою «Безпека інформаційних комунікаційних систем». Електрон. вид. / упоряд. : Г. З. Халімов ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 207 с. [Electronic resource]. – Access mode: http://openarchive.nure.ua/handle/document/9701

5. Richard Klima, Richard E. Klima, Neil Sigmon, Neil P. Sigmon. Cryptology: Classical and Modern / CRC Press, 2018. - 496 p.

Додаткова

1. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с.

2. Кравченко П. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с.

3. Kravchenko, P. Blockchain and decentralized systems : in three volumes. V.3 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina. – Kharkiv : 2020. 298 p.

4. 1. Tim Pulver. Hands-On Internet of Things with MQTT: Build connected IoT devices with Arduino and MQ Telemetry Transport (MQTT) / Packt Publishing Ltd, 2019. — 350 p.

5. Initial Server Setup with Ubuntu 20.04 [Электронный ресурс] / Brian Boucheron. DigitalOcean, 2021. – Режим доступа : https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-20-04.

6. Жураковський, Б. Ю. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс]: навч. посіб. / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с. Режим доступа : https://ela.kpi.ua/handle/123456789/36615

7. Жураковський, Б. Ю. Комп'ютерні мережі. Частина 2. Навчальний посібник [Електронний ресурс] : навчальний посібник / Б. Ю. Жураковський, І. О. Зенів ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 4,73 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 372 с. – Режим доступа : https://ela.kpi.ua/handle/123456789/36641

8. Jamon Camisso. Sysadmin eBook: Making Servers Work – DigitalOcean, 2020. – 281 p.

9. Maarten van SteenAndrew S. Tanenbaum. Distributed Systems. Third edition., Maarten van Steen, 2018. – p. [Electronic resource]. – Access mode: https://www.distributed-systems.net/index.php/contact/

Інформаційні ресурси.

1. How To Install Linux, Apache, MySQL, PHP (LAMP) stack on Ubuntu 20.04 [Электронный ресурс] / Erika Heidi. DigitalOcean, 2021. – Режим доступа : https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu-20-04.

2. OWASP Web Security Testing Guide. [Electronic resource]. –Access mode : https://owasp.org/www-project-web-security-testing-guide/

3. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Інженерія безпеки інформаційно-комунікаційних систем" https://pns.hneu.edu.ua/ course/view.php?id=9293.