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

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

БЕЗПЕКА ІНТЕРНЕТ-РЕЧЕЙ

робоча програма навчальної дисципліни

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

Статус дисципліни	***базова***
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

Вибухове зростання кількості підключених пристроїв застосунків привело до повсюдної цифровізації всіх галузей, але це також збільшило кількість загроз безпеки IoT. Вивчивши курс, студенти зможуть оцінити ступінь уразливості і ризиків систем IoT, а також знаходити і рекомендувати стратегії захисту від поширених загроз безпеки IoT-систем.

Студенти, які розглядають кар'єру в швидко зростаючих областях IoT і безпеки, отримують практичні інструменти для оцінки вразливостей безпеки IoT-рішень, навчаться використовувати моделі оцінки ризиків, щоб рекомендувати заходи щодо зниження загроз. Ці навички затребувані як в IoT, так і в інших мережевих архітектурах. Освітня компонента основана на курсі мережевої академії Cisco "IoTF Security v1.1".

Після закінчення курсу студент зможе:

- пояснювати унікальні проблеми безпеки в різних секторах IoT;
- виконувати дії з моделювання загроз для оцінки вразливостей фізичної безпеки;
- виконувати дії з моделювання загроз для оцінки вразливостей безпеки локального доступу;
- виконувати дії з моделювання загроз для оцінки вразливостей безпеки віддаленого доступу;
- використовувати інструменти тестування на проникнення для виявлення вразливостей в системах IoT;
- використовувати моделювання загроз та оцінки ризиків, щоб рекомендувати заходи щодо пом'якшення загроз;
- пояснювати вплив нових технологій на безпеку Інтернету речей.

Предметом навчальної дисципліни є вивчення основних концепцій та підходів до розробки та впровадження надійних, безпечних систем IoT, дослідження моделей та методів забезпечення надійності та забезпечення безпеки та оцінки систем на основі IoT, ознайомлення з процесом тестування та пошуку вразливостей в пристроях IoT. В дисципліні основний акцент робиться на розумінні фундаментальних концепцій і механізмів які лежать в основі функціонування інтернет-речей.

Мета – сформувати систему знань студентів в області Інтернет речей та цифрових технологій, та більш широкої категорії, яка називається цифровим перетворенням на базі яких дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких системи на виробництві та в науковій сфері.

Результатами навчання за дисципліною є розуміння основних бізнес-процесів, притаманних для функціонування IoT-систем та набуття практичних навичок у розгортанні та застосуванні IoT-пристроїв.

Характеристика навчальної дисципліни

Курс	**1 М**
Семестр	**1**
Кількість кредитів ECTS	**3**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Організаційне забезпечення захисту інформації	Веб-безпека
Основи технічного захисту інформації	Цифрова криміналістика
Основи стеганографічного захисту інформації	Тестування на проникнення та етнічний хакінг

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).	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, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; 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-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-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 в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства).
КФ 8. Здатність розробляти, планувати, аналізувати та впроваджувати систему 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.	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-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-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-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

Програма навчальної дисципліни

Змістовий модуль 1. Загальна характеристика Інтернету-речей

Тема 1. *Основні поняття, стандарти IoT*

Тема 2. *Основні загрози IoT*

Тема 3. *Архітектура IoT. Загрози на прилади IoT*

Тема 4. *Загрози комунікаційного рівня моделі TCP/IPв мережі IoT*

Змістовий модуль 2. Особливості впровадження концепції безпеки інтернету речей

Тема 5. *Загрози рівня застосунків моделі TCP/IP в мережі IoT.*
Тема 6. *Оцінка вразливості та ризиків у системі IoT*
Тема 7. Формування системи безпеки в мережі IoT
Тема 8. Криптографічні застосунки системи безпеки мережі IoT

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:

- вміння виконувати розгортання та з'єднання інтернет-речей;
- вміння створювати просту мережу;
- вміння підключати та моніторити пристрої IoT;
- вміння створювати розумну кімнату;
- вміння створювати конвергентну мережу і встановлювати взаємозв'язок речей, забезпечувати питання безпеки та основних стовпів Cisco IoT, застосовувати до цього технології автоматизації;
- вміння будувати проект створення рішення інтернет речей, починаючи від планування і закінчуючи прототіпірованими рішеннями.

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 22 (робота на лекціях – 8, експрес-опитування – 14).

Лабораторні заняття: максимальна кількість балів становить 78 (виконання лабораторних робіт – 6, захист лабораторних робіт – 42, контрольні роботи – 30), а мінімальна – 50.

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 *"Основні поняття, стандарти IoT"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №1.* Моделювання бездротових локальних мереж в Packet Tracer	виконання лабораторної роботи	1
	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 *"Основні загрози IoT"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №2.* Моделювання пристроїв інтернету речей засобами Cisco Packet Tracer	виконання лабораторної роботи	1
			Захист лабораторної роботи № 1	7

	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 *"Архітектура IoT. Загрози на прилади IoT"*	Робота на лекції	1
	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 *"Загрози комунікаційного рівня моделі TCP/IPв мережі IoT"*	Робота на лекції	1
			Експрес-опитування	7
	Лабораторне заняття	Лабораторна робота №3. Моделювання загроз на рівні пристрою	виконання лабораторної роботи	1
			Захист лабораторної роботи № 2	7
			Контрольна робота 1	15
	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 *"Загрози рівня застосунків моделі TCP/IP в мережі IoT"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №4. Моделювання загроз на рівні зв'язку IoT	виконання лабораторної роботи	1
			Захист лабораторної роботи № 3	7
	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 *"Оцінка вразливості та ризиків у системі IoT"*	Робота на лекції	1
			виконання лабораторної роботи	1
	Лабораторне заняття	Лабораторна робота №5. Моделювання загроз на рівні пристрою IoT	Захист лабораторної роботи № 4	7
	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 *"Формування системи безпеки в мережі IoT"*	Робота на лекції	1
			Експрес-опитування	7
	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 *"Криптографічні застосунки системи безпеки мережі IoT"*	Робота на лекції	1
			виконання лабораторної роботи	1
	Лабораторне заняття	Лабораторна робота №6. Моделювання загроз для оцінки ризику в системі IoT	Захист лабораторних робіт № 5,6	14
			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. Дэвид Роуз, Дэвид Роуз (David Rose). Будущее вещей. Как сказка и фантастика становятся реальностью: монографія / Дэвид Роуз. – Москва: Альпина Паблишер, 2015. – 352с. ISBN: 978-5-91671-394-7

2. Сэмюэл Грингард, Характеристики Интернет вещей. Будущее уже здесь, : монографія / Сэмюэл Грингард. – Москва: Альпина Паблишер, 2016, - 188с. ISBN: 978-5-91671-394-7

3. В. А. Петин, Arduino и Raspberry Pi в проектах Internet of Things: учебное пособие/ В. А. Петин. Скт.Петербург: БХВ-Петербург, 2016, - 320с. , ISBN: 978- 5-9775-3646-2

4. Дэвид Роуз, Дивовижні технології. Дизайн та інтернет речей : навч. посібник/ Дэвид Роуз. Харків: «Книжный Клуб «Клуб Семейного Досуга», 2018- 336 с. ISBN978-617-12-5388-9

5. Алексей Гладкий, Основы безопасности и анонимности во Всемирной сети: монография/ Алексей Гладкий. Київ: Фенікс , 2012 - 256с. ISBN 978-5-222-19846-9

Додаткова

6. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.

7. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P.

8. Professor Dr.-Ing. Klaus Schwab, The Fourth Industrial Revolution, ASIN: B01JEMROIU, 2017, 189 P.

9. Cuno Pfister, Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud (Make: Projects) 1st Edition, ASIN: B00COVJUGI, 2011, 194 P.

10. Erik Brynjolfsson and Andrew McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies 1st Edition, ASIN: B00D97HPQI, 2014, 320 P.

11. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P.

12. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.

13. Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.

Інформаційні ресурси.

14. Лукацкий А.С. Криптография в "Интернете вещей" // www.slideshare.net : — 2016. – 23 марта. Эталонная архитектура безопасности интернета вещей (IoT). Часть 1 [Електронний ресурс]. – Режим доступу: URL https://www.anti-malware.ru/practice/solutions/iot-the-reference-securityarchitecture-part-1

15. Владислав Васильович Вишньовський, Олеся Петрівна Войтович Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс] – Режим доступу: https://conferences.vntu.edu.ua/index.php/all–fitki/all–fitki–2017/paper/view/2738

16. Катерина Володимирівна Савченко, Олеся Петрівна Войтович Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс] – Режим доступу: https://conferences.vntu.edu.ua/index.php/all–fitki/all–fitki–2017/paper/view/2736

17. Kateryna Savchenko, Vladislav Vyshnovskiy. System bezpieczeństwa inteligentnego domu //Materiały konferencyjne. Konferencja studenckich kół naukowych Pionu Hutniczego [Електронний ресурс] – Режим доступу: http://www.kolanaukowe.agh.edu.pl/ph/dzialalnosc//54.%20Konferencja%20SKNPH%20 – %20zeszyt.pdf

18. Lisa Goeke, Security Challenges of the Internet of Things [Електронний ресурс]. – Режим доступу: URL https://www.theseus.fi/bitstream/handle/10024/128420/Goeke_Lisa.pdf?sequence=1.

19. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Безпека інтернет речей" https://pns.hneu.edu.ua/enrol/index.php?id=7204.