МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
М.В. Афанасьєв

БЕЗПЕКА ІНТЕРНЕТ-РЕЧЕЙ

робоча програма навчальної дисципліни

Галузь знань	**12 “ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”**
Спеціальність	**125 “КІБЕРБЕЗПЕКА”**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**“КІБЕРБЕЗПЕКА”**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця

2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 6 від 10.12.2019 р.
Розробник(-и): Погасій Сергій Сергійович,
к.е.н., доцент кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

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

1. **Вступ**

Програма вивчення навчальної дисципліни "Безпека інтернет-речей" складена відповідно до освітньої програми підготовки бакалаврів зі спеціальності 125 "Кібербезпека".

Анотація навчальної дисципліни: Дисципліна “ Безпека інтернет-речей” є базовою навчально дисципліною за спеціальністю “Кібербезпека”.

Сьогодні пристрої Інтернету речей не лише масово використовуються у щоденному вжитку, але й у сучасному бізнес-середовищі. Зокрема Інтернет речей (Internet-of-Things або IoT) активно впроваджується в різних галузях — від промислової сфери до сільського господарства, рітейлу та будівництва. Поступово пристрої IoT стають невід’ємною частиною багатьох бізнес-процесів, і зростання їх кількості спричиняє виникнення нових проблем безпеки.

Студенти, спеціальності "Кібербезпека", досліджують основні етапи для посилення захисту:

- багатофакторна аутентифікація: використовуйте апаратні токени або спеціальне програмне забезпечення для управління даними облікових записів;

- мережевий інтелект (network intelligence): багато пристроїв IoT здебільшого підключаються до роутера, тому пошук загроз можна здійснювати за допомогою аналізу аномалій мережевого трафіку. Різні постачальники пропонують обладнання, яке підключається до роутера та надає можливість дізнатися про підозрілі події, а також забезпечує огляд мережевої поведінки пристроїв IoT.

- резервне копіювання. Забезпечення регулярних і надійних резервних копій систем і даних є необхідним кроком для запобігання втратам важливих даних.

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.

Метою навчальної дисципліни сформувати систему знань студентів в області Інтернет речей та цифрових технологій, та більш широкоїкатегорії, яка називається цифровим перетворенням на базі яких дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких системи на виробництві та в науковій сфері. В дисципліні основний акцент робиться на розумінні фундаментальних концепцій і механізмів які лежать в основі функціонування інтернет-речей.

Головне завдання курсу – знайомить студентів з базовими теоретичними аспектами надійності та безпеки систем на основі IoT.

Курс	**2**	
Семестр	**4**	
Кількість кредитів ECTS	**4**	
Аудиторні навчальні заняття	**лекції**	**30**
	лабораторні	**30**
Самостійна робота		**60**
Форма підсумкового контролю	**залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Комп'ютерні мережі такомунікації	Захист систем електронної комерції та мультисервісних систем
Безпека в інформаційно-комунікаційних системах	Системи виявлення та протидія атакам
Основи побудови та функціонування мікропроцесорних систем	

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою	Використовувати основні методи, моделі та алгоритми захисту даних в програмноапаратних системах Інтернет-речей.
Здатність здійснювати управління інцидентами інформаційної та кібербезпеки	Застосовувати різні методи та інструменти для пошуку програмно-апаратних вразливостей в Інтернет речах.
Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій	Надавати рекомендації щодо побудови та використання апаратних засобів та протоколів при проектуванні надійних та безпечних систем Інтернет-речей.

3. Програма навчальної дисципліни

Змістовий модуль 1. Загальна характеристика Інтернету-речей.

Тема.1 Історія інтернету речей

1.1. Історія розвитку інтернету речей.

1.2.Перспективи розвитку інтернету речей. Індустрія і виробництво Споживачі. Роздрібна торгівля, фінанси і маркетинг. Медицина. Транспорт і логістика. Сільське господарство та навколишнє середовище. Енергетика. Розумне місто. Уряд і армія

Тема 2. Архітектура і ключові модулі інтернету речей

2.1. Екосистема інтернету речей. Інтернет речей проти межмашинного взаємодії

Корисність мережі і закони Меткалфа і Бекстрома. Архітектура інтернету речей Роль архітектора

2.2. Загальна характеристика взаємодії складових архитектури (датчики і харчування;Передача даних; Інтернет-маршрутизація і протоколи; Туманні і граничні обчислення, аналітика і машинне навчання; Загроза і безпеку в інтернеті речей

Тема 3. Датчики, кінцеві точки і системи живлення

3.1.Сенсорні пристрої. Термопари і температурні датчики. Ефект Холла і датчик і струму. Фотоелектричні датчики. Датчики PIR .LiDAR і активні датчики. Датчики MEMS.

3.2. Інтелектуальні кінцеві точки IoT.Відеосистема

3.3. Злиття датчиків

3.4.Пристрої введення. Пристрої виведення.

3.5 Функціональні приклади (всі разом). Функціональний приклад - TI SensorTag CC2650. Між датчиком і контролером

3.6 Джерела енергії та управління живленням Управління харчуванням. Відтворення електроенергії Сховище енергії

Тема 4. Теорія комунікації та інформації

4.1.Теорія комунікації. Радіочастотна енергія і теоретичний діапазон. Радіочастотна інт ерференція.

4.2.Теорія інформації. Межі бітрейта і теорема Шеннона-Хартлі. Частота бітових помилок. Узкополосная і широкосмуговий зв'язок .

4.3.Радіоспектр.Керуюча структура

Змістовий модуль 2. Специфіка передачі даних інтернету речей у мережах

Тема 5. Бездротова персональна мережа (WPAN) не на основі IP

5.1. Стандарти бездротової персональної локальної мережі. Стандарти 802.15. Bluetooth.IEEE 802.15.4. Zigbee.Z-Wave.

Тема 6. WPAN і WLAN на базі IP

6.1. Протокол інтернету і протокол управління передачею. Роль протоколу IP в інтернеті речей.

6.2. WPAN з IP - 6LoWPAN. Топологія 6LoWPAN. Стек протоколу 6LoWPAN. Адресація і маршрутизація в mesh-мережі. Стиснення і фрагментація заголовка Виявлення сусідів. Безпека 6LoWPAN.

6.3. WPAN з IP - Thread. Архітектура і топологія Thread. Стек протоколу Thread Маршрутизація Thread. Адресація Thread. Виявлення сусіда

6.3. Протоколи IEEE 802.11 і WLAN. Огляд і порівняння протоколів IEEE 802.11 Архітектура IEEE 802.11. Розподіл спектра IEEE 802.11. Методи модуляції і

кодування IEEE 802.11. IEEE 802.11 MIMO. Структура пакета IEEE 802.11.Робота IEEE 802.11. Безпека IEEE 802.11. Протокол IEEE 802.11ac Транспорт-к-т ранспорта IEEE 802.11p. Протокол IEEE 802.11ah.

Тема 7. Системи та протоколи телекомунікації (ГВС)

7.1. Функціональна сумісність пристроїв стільникового зв'язку. Стандарти та модель управління. Технології доступу стільникового зв'язку. Категорії абонентського обладнання 3GPP. Р аспределеніе спектра і смуг частот в 4G LTE Топологія та архітектура мережі 4G LTE. Стек протоколів мережі E-UTRAN 4G LTE Географічні області 4G LTE, потоки даних і процедури передачі обслуговування Структура пакета 4G LTE. Категорії 0, 1, M1 і NB-IoT. 5G

7.2. LoRa і LoRaWAN. Фізичний урове нь LoRa. Рівень MAC LoRaWAN. Топологія LoRaWAN. Короткий опис LoRaWAN.

7.3. Sigfox. Фізичний рівень Sigfox. Рівень MAC Sigfox. Стек протоколу Sigfox. Топологія Sigfox.

Тема 8. Маршрутизатор і шлюзи

8.1. Функції маршрутизації. Функції шлюзу. Маршрутизація відмов стійкість і внеполосное управління. VLAN.VPN. Управління швидкістю трафіку і QoS. Функції безпеки. Метрики і аналітика. Обробка на краю.

8.2. Програмне мережеве взаємодія. Архітектура SDN. Традиційне межсетевое взаємодія. Переваги SDN.

Тема 9. IoT-протоколи передачі даних від граничного пристрою в хмару

9.1. Протоколи. MQTT. Видання-підписка MQTT. Деталі архітектури MQTT. Рекламування і виявлення шлюзу. Структура пакета MQTT. Формати з'єднань MQTT. Робочий приклад MQTT

9.2. MQTT-SN. Архітектура і т опологія MQTT-SN. Прозорі і збирають шлюзи Відмінності між MQTT і MQTT-SN

9.3. Обмежений прикладної протокол. Деталі архітектури CoAP. Формати повідомлень CoAP. Приклад використання CoAP

9.4. Інші протоколи. STOMP. AMQP. Зведення і порівняння протоколів

Тема 10. Топологія хмарних і туманних обчислень

10.1.Модель хмарних сервісів

NaaS. SaaS. PaaS. IaaS

10.2. Публічне, приватна і гібридна хмара.Приватна хмара. Публічна хмара Гібридна хмара

10.3. Хмарна архітектура OpenStack.

10.4. Keystone - управління ідентифікацією та обслуговуванням. Glance - сервіс зображень. Обчислення Nova. Swift - зберігання об'єкт ів. Neutron - мережеві сервіси. Cinder - блочне сховище. Horizon. Heat - оркестрації (опція). Ceilometer - телеметрія (опція)

10.5. Обмеження хмарних архітектур для IoT. Ефект затримки

10.6. Туманні обчислення. Філософія Hadoop для туманних обчислень. Порівняння туманних, граничних і хмарних обчислень. Архітектура OpenFog RA .Amazon Greengrass і лямбда-функції. Туманні топології.

Тема 11. Аналіз даних і машинне навчання в хмарних і туманних платформах

11.1. Простій аналіз даних в інтернеті речей. Верхній рівень хмарної архітектури. Система правил. Споживання інформації: потоки, обробка та озера даних.Обробка складних подій. Lambda-архітектура. Промислове застосування.

11.2. Машинне навчання в інтернеті речей. Моделі машинного навчання.

Класифікація Регресія. Випадковий ліс. Байєсовські моделі. Згорткові нейронні мережі. Рекурентні нейронні мережі Навчання та отримання логічних висновків в інтернеті речей. Аналіз даних в IoT і порівняння / оцінка методів машинного навчання.

Змістовий модуль 3 Особливості впровадження концепції безпеки інтернету речей

Тема 12. Безпека інтернету речей

12.1. Загальновживані поняття кібербезпеки пов'язані з атакою. Терміни, пов'язані із захистом

12.2. Анатомія кібератак на IoT-пристрої. Mirai. Stuxnet. Ланцюжкова реакція

12.3.Фізична і апарати атная безпеку. Корінь довіри. Управління ключами і модулі TPM. Адресний простір в процесорі і пам'яті. Безпека зберігання даних. Фізична безпека.

12.4. Криптографія. Симетрична криптографія. Асиметрична криптографія. Криптографічний хеш (аутентифікація і цифровий підпис). Інфраструктура відкритого ключа. Мережевий стек: протокол захисту транспортного рівня

12.5. Програмно-який визначається периметр. Архітектура про програмно-обумовленого периметра

12.6. Блокчейн і криптовалюта в інтернеті речей .Bitcoin (блокчейн) IOTA (спрямований ациклічний граф)

12.7.Реко мендації щодо захисту IoT-пристроїв

Тема 13. Консорціуми і спільноти

13.1. Консорціуми з персональним мереж. Bluetooth SIG. Thread Group. Альянс Zigbee

13.2. Консорціуми за протоколами Open Connectivity Foundation і Allseen Alliance.

OASIS. Object Management Group. IPSO Alliance.

13.3.Консорціуми з глобальних обчислювальних мереж. Weightless SIG . LoRa Alliance. Інженерний рада інтернету. Wi-Fi Alliance

13.4. Консорціуми з туманним і граничним обчислень. OpenFog. EdgeX Foundry

13.5. Спеціалізовані організації Консорціум промислового інтернету. Інститут інженерів з електротехніки та електроніки IoT (IEEE IoT)

Теми лабораторних робіт

Лабораторна робота №1. Packet Tracer - Розгортання та з'єднання пристроїв

Лабораторна робота №2. Створення простої мережі з використанням Packet Tracer

Лабораторна робота №3. Підключення та моніторинг пристроїв IoT

Лабораторна робота №4. Розумна кімната на базі Raspberry Pi і PL-App

Лабораторна робота №5 Конвергентна мережа і взаємозв'язок речей, питання безпеки та основні стовпи Cisco IoT, технології автоматизації.

Лабораторна робота №6 Побудова проекту створення рішення інтернет речей, починаючи від планування і закінчуючи прототіпіруванії рішення.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів максимальна сума – 100 балів;

модульний контроль, що проводиться у формі контрольних робіт, як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

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

Порядок проведення поточного оцінювання знань студентів.

Оцінювання знань студента під час лабораторних занять проводиться за наступними критеріями:

Застосовувати інструментальні засоби реалізації «розумних систем» в середовищі IoT.

Володіти методами посилення безпеки в оцифрованому світі.

Використоваваи основні методи інтеграції IoT в сучасний бізнес

Впроваджувати методи проектування та експлуатації інтелектуальних систем.

Розробляти та аналізувати автономні системи в середовищі IoT.

Самостійно здійснювати пошук новітніх тенденцій в сфері IoT безпеки.

Розробляти та впроваджувати самостійні стартапи IoT.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового заліку та за накопичуваними балами, що були отримані протягом навчального семестру,.

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами навчальної дисципліни розраховується з урахуванням балів, отриманих під 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.

Розподіл балів за тижнями

Теми змістового модуля				Лекційні заняття	Захист лабораторних робіт	Експрес-опитування	Поточні КР	Усього
	1	**Тема 1**	1 тиждень	1				1
		Тема 2	2 тиждень	1	5	3		9
		Тема 3	3 тиждень	1				1
		Тема 4	4 тиждень	1	5	3		9
	2	**Тема 5**	5 тиждень	1			12	13
		Тема 6	6 тиждень	1		3		4
		Тема 7	7 тиждень	1	5			6
		Тема 8	8 тиждень	1		3		4
		Тема 9	9 тиждень	1			11	13
		Тема 10	10 тиждень	1	5	3		9
		Тема 11	11 тиждень	1				1
	3	**Тема 12**	12 тиждень	1		3		4
		Тема 12	13 тиждень	1	5			6
		Тема 12	14 тиждень	1		3	11	16
		Тема 13	15 тиждень	1	5			6
Усього				15	30	21	34	100

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
1 – 34	F		

5. Рекомендована література

5.1 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

5.1 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.

5.3. Інформаційні ресурси в Інтернеті

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