Силабус освітнього компонента
Програма навчальної дисципліни

Безпека інтернет-речей

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
7

Мова викладання
Українська

Викладачі, розробники

ПОГАСІЙ Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua
Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека інтернет-речей" є обов`язковою навчальною дисципліною. Дисципліна спрямована на 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.

Мета та цілі дисципліни

Формування системи 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.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання

РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН–12. Розробляти моделі загроз та порушника.
РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН–16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН–23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН–32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки
РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків

РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН–50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредитів ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Розробка веб-додатків, Основи побудови та захисту мікропроцесорних систем.

Особливості дисципліни, методи та технології навчання

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 презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Історія інтернету речей.
Історія розвитку інтернету речей. 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. Історія інтернету речей.

Архітектура та ресурси сучасних операційних систем.

Тема 3. Датчики, кінцеві точки і системи живлення.

Злиття датчиків. Пристрої введення. Пристрої виведення. Функціональні приклади (всі разом). Функціональний приклад - TI SensorTag CC2650. Між датчиком і контролером. Джерела енергії та управління живленням. Відтворення електроенергії. Сховище енергії.

Тема 4. Теорія комунікації та інформації.

Теорія комунікації. Радіочастотна енергія і теоретичний діапазон. Радіочастотна інтерференція. Теорія інформації. Межі бітрейта і теорема Шеннона-Хартлі. Частота бітових помилок. Вузькосмуговий і широкосмуговий зв'язок. Радіоспектр. Керуюча структура.

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

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

Тема 6. WPAN і WLAN на базі IP.

Протокол інтернету і протокол управління передачею. Роль протоколу IP в інтернеті речей. WPAN з IP - 6LoWPAN. WPAN з IP - Thread. Архітектура і топологія Thread. Стек протоколу Thread Маршрутизація Thread. Адресація Thread. Виявлення сусіда Протоколи IEEE 802.11.

Тема 7. Системи та протоколи телекомунікації (ГВС).

Функціональна сумісність пристроїв стільникового зв'язку. Стандарти та модель управління. Технології доступу стільникового зв'язку. Категорії абонентського обладнання 3GPP. Росподіл 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 LoRa і LoRaWAN. Фізичний рівень LoRa. Рівень MAC LoRaWAN. Топологія LoRaWAN. Короткий опис LoRaWAN. Sigfox. Фізичний рівень Sigfox. Рівень MAC Sigfox. Стек протоколу Sigfox. Топологія Sigfox.

Тема 8. Маршрутизатор і шлюзи.

Функції маршрутизації. Функції шлюзу. Маршрутизація відмов стійкість і позасмугове управління. VLAN.VPN. Управління швидкістю трафіку і QoS. Функції безпеки. Метрики і аналітика. Обробка на краю. Програмне мережеве взаємодія. Архітектура SDN. Традиційна міжмережева взаємодія. Переваги SDN.

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

Протоколи. MQTT. MQTT-SN. Архітектура і топологія MQTT-SN. Обмежений прикладної протокол. Деталі архітектури CoAP. Інші протоколи. STOMP. AMQP. Зведення і порівняння протоколів.

Тема 10. Топологія хмарних і туманних обчислень.

Модель хмарних сервісів. Публічне, приватна і гібридна хмара. Хмарна архітектура OpenStack. Keystone. Обмеження хмарних архітектур для IoT. Туманні обчислення.

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

Простій аналіз даних в інтернеті речей. Машинне навчання в інтернеті речей. Моделі машинного навчання.

Тема 12. Безпека інтернет речей.

Загальновживані поняття кібербезпеки пов'язані з атакою. Анатомія кібератак на IoT-пристрої. Фізична і апаратна безпека. Криптографія. Архітектура про програмно-обумовленого периметра. Рекомендації щодо захисту IoT-пристроїв.

Тема 13. Консорціуми і спільноти.

Консорціуми з персональним мереж. Bluetooth SIG. Thread Group. Альянс Zigbee Консорціуми за протоколами Open Connectivity Foundation і Allseen Alliance. Консорціуми з глобальних обчислювальних мереж. Weightless SIG . LoRa Alliance. Інженерний рада інтернету. Wi-Fi Alliance Консорціуми з туманним і граничним обчислень. OpenFog. EdgeX Foundry. Спеціалізовані організації Консорціум промислового інтернету. Інститут інженерів з електротехніки та електроніки IoT (IEEE IoT).

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Packet Tracer - Розгортання та з'єднання пристроїв.

Тема 2. Створення простої мережі з використанням Packet Tracer.

Тема 3. Підключення та моніторинг пристроїв IoT.
Тема 4. Розумна кімната на базі Raspberry Pi і PL-App.
Тема 5. Конвергентна мережа і взаємозв'язок речей, питання безпеки та основні стовпи Cisco IoT, технології автоматизації.
Тема 6. Побудова проекту створення рішення інтернет речей, починаючи від планування і закінчуючи прототіпіровані рішення.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
Introduction to IoT and Digital Transformation, Exploring Networking with Cisco Packet Tracer https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література:

1. David Rose, Enchanted Objects: Design, Human Desire, and the Internet of Things, 2015. https://responsiveobjects.wordpress.com/wp-content/uploads/2016/01/enchanted-objects_-design-human-desire-and-the-internet-of-things-rose-david.pdf
2. Баранов А.А., Інтернет речей: теоретико-методологічні засади правового регулювання. Том І. Сфери застосування, ризики та бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с. https://jurkniga.ua/nternet-rechey-teoretiko-metodologchn-osnovi-pravovogo-regulyuvannya-tom--sferi-zastosuvannya-riziki--barri-problemi-pravovogo-regulyuvannya/
3. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P. https://ru.scribd.com/document/441966460/the-internet-of-things-the-mit-press-essential-knowledge-series-by-samuel-greengard
4. 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. https://www.openhacks.com/uploadsproductos/getting_started_with_the_internet_of_things_pachube_client.pdf
5. 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. http://digamo.free.fr/brynmacafee2.pdf
6. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P. https://www.perlego.com/book/2433384/digital-transformation-survive-and-thrive-in-an-era-of-mass-extinction-pdf
7. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. http://kist.ntu.edu.ua/textPhD/tzi.pdf.
8. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.

https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover

Додаткова література :

9. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.
https://pdfcoffee.com/machine-learning-the-new-ai-alpaydin-2016pdf-pdf-free.html
10. Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.
https://s3.amazonaws.com/arena-attachments/911381/0ea8a9793158a95d9b91911e49240a43.pdf
11. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
12. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
13. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
14. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено

28.08.2024

Завідувач кафедри

Сергій ЄВСЕЄВ

28.08.2024

Гарант ОП

Сергій ЄВСЕЄВ