Силабус освітнього компонента
Програма навчальної дисципліни

Безпека смарт-технологій

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Науково-професійного спрямування, Вибіркова

Семестр
3

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 "Розширена мережева та хмарна безпека" є нормативною навчальною дисципліною. Вивчення дисципліни базується на засвоєнні основ розробки та програмування пристроїв, які працюють з використанням смарт-технологій та технологій Інтернету речей. При цьому пристрої IoT розглядаються як сукупність технічних, інформаційних та програмних засобів, призначених для вирішення широкого кола завдань у різних галузях економіки, освіти, промисловості тощо.

Мета та цілі дисципліни

Формування системи знань студентів в області смарт-технологій та Інтернет речей, та більш широкої категорії, що називається цифровим перетворенням. На базі цих знань дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких систем на виробництві та в науковій сфері. В дисципліні основний акцент направлений на розуміння фундаментальних концепцій і механізмів, які лежать в основі функціонування інтернет-речей.

Формат занять

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

Компетентності

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Результати навчання

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Веб безпека, Технології програмування, Математичні основи криптології та криптоаналіз, Менеджмент інформаційної безпеки, Моделювання систем критичної інфраструктури.

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. Основи смарт-технологій: визначення, принципи, приклади.

Визначення і принципи Смарт-технологій. Дані, інформація, знання. Приклади практичної реалізації Смарт-технологій у мережі.

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 інт ерференція. Теорія інформації. Межі бітрейта і теорема Шеннона-Хартлі. Частота бітових помилок. Узкополосная 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. 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 LoRa і LoRaWAN. Фізичний урове нь 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 внеполосное управління. VLAN.VPN. Управління швидкістю трафіку і QoS. Функції безпеки. Метрики і аналітика. Обробка на краю. Програмне мережеве взаємодія. Архітектура SDN. Традиційне межсетевое взаємодія. Переваги SDN.

Тема 9. Проблематика проектування і реалізації систем класу IoT – Internet of Things.

Основні поняття Інтернету речей. Компетенції розробника IoT. Історія виникнення й розвитку напрямку IoT. Основні області застосування. Ключові технологічні рішення. Ринок виробників і користувачів рішень IoT. Відкриті проблеми в дизайні, реалізації й експлуатації систем «Інтернету речей».

Тема 10. Структура інформаційної системи на основі технології «Інтернет речей».

Структура системи Інтернету речей та її основні складові частини. Хмари та платформи IoT. Комутація між електронними простоями та мережею.

Тема 11. IoT-протоколи передачі даних від граничного пристрою в хмару.

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

Тема 12. 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 13. 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 15. Безпека смарт-технологій та Інтернет речей.

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

Тема 16. 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 прототіпіруванії 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.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том I. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.
https://pravo-izdat.com.ua/image/data/Files/476/3_Internet_rechej_Tom_I_vnutri.pdf
2. Грінгард С. Інтернет речей. Київ: Книжковий клуб «Клуб сімейного дозвілля», 2018. 176 с. 2. Посібник з Node-Red. URL: https://github.com/pupenasan/ NodeREDGuidUKR.
3. Пархоменко А.В. та ін. Програмно-апаратна платформа для навчання технологіям Інтернету речей: навч. посіб. Запоріжжя: Дике Поле, 2017. 120 с.
https://eir.zp.edu.ua/items/920b4a42-219b-4f0d-beed-116ff69abba2
4. Lea P. IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security, 2nd Edition. Pact Publishing Ltd., 2020. 608 p.
https://www.perlego.com/book/1388466/iot-and-edge-computing-for-architects-implementing-edge-and-iot-systems-from-sensors-to-clouds-with-communication-systems-analytics-and-security-2nd-edition-pdf
5. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

6. 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
7. Amazon Web Services (AWS) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/amazon-aws-security/.
8. Microsoft Azure (Azure) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/microsoft-azure-security/.
9. Google Cloud Platform (GCP) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/google-cloud-platform-security/.
10. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/.

Додаткова література

11. Serpanos D., Wolf M.C.Internet-of-Things (IoT) Systems. Architectures, Algorithms, Methodologies. Springer, 2018. 95 p. (eBook) https://doi.org/10.1007/9783-319-69715-4.
12. Khan J.Y., Yuce M.R. Internet of Things (IoT): Systems and Applications 1st Edition. Jenny Stanford Publishing Pte, Ltd., 2019. 340 p.
https://www.academia.edu/100734810/internet_of_things_iot_systems_and_applications
13. Cloud Computing Security [Електронний ресурс]. – Режим доступу : https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm.
14. Computer Network Security [Електронний ресурс]. – Режим доступу : https://www.javatpoint.com/computer-network-security.
15. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
16. 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.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
17. 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. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
18. Security of Linux operating system: laboratory workshop / S. Yevseiev, S. Pogasiy, A. Goloskokova, O. Shmatko, M. Melnik (Кібербезпека: безпека операційної системи Linux: лабораторний практикум: навчальний посібник для студентів вищих навчальних закладів англійською мовою / Євсеєв С.П., Погасій С.С., Голоскокова А.О., Шматко О.В., Мельник М.О. – Львів: Видавництво «Новий Світ – 2000», 2021. – 256 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 30% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 20% 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 — Станіслав МІЛЕВСЬКИЙ