Силабус освітнього компонента
Програма навчальної дисципліни

Безпека смарт-технологій

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Науково-професійного спрямування, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

Викладачі, розробники

ПОГАСІЙ Сергій Сергійович
Serhii.Pohasii@khpi.edu.ua
Доктор технічних наук, доцент, професор 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. Гарант освітньо-науової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, 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

У процесі вивчення курсу здобувачі знайомляться з архітектурою смарт-систем, принципами їх функціонування та основними загрозами інформаційній безпеці. Розглядаються сучасні методи і засоби захисту даних, комунікацій та пристроїв у смарт-інфраструктурах. Особлива увага приділяється виявленню вразливостей, моделюванню атак на IoT-пристрої, захисту персональних даних користувачів і застосуванню криптографічних протоколів у смарт-середовищах..

Мета та цілі дисципліни

Формування у здобувачів знань, умінь та навичок із забезпечення кібербезпеки в середовищах, що використовують інтелектуальні (смарт) технології — зокрема системи «розумного» дому, «розумного» міста, промислового Інтернету речей (IIoT), транспортних та енергетичних мереж. Після завершення курсу студенти набувають практичних навичок у розгортанні безпечних смарт-інфраструктур, тестуванні безпеки пристроїв та впровадженні заходів захисту для забезпечення конфіденційності, цілісності й доступності даних у системах нового покоління.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований 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.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
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.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

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 – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи кібербезпеки, Комп'ютерні мережі, Основи програмування, Безпека інтернет-речей, Архітектура та захист сучасних операційних 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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Історія та еволюція Інтернету речей і смарт-технологій. Розглядається історія розвитку Інтернету речей (IoT), основні етапи становлення та сучасні тенденції. Аналізується вплив IoT на промисловість, медицину, транспорт, сільське господарство, енергетику та розумні міста.	2
Тема 2. Основи смарт-технологій та їх архітектура. Визначаються поняття «смарт-технології» та «Інтернет речей», принципи їх функціонування, компоненти систем: сенсори, контролери, актуатори, пристрої введення-виведення, джерела живлення. Розглядаються функціональні приклади сучасних IoT-рішень.	2
Тема 3. Комунікаційні основи IoT: теорія та стандарти. Описуються основи теорії комунікації та інформації, передавання сигналів, радіочастотні діапазони, інтерференція. Розглядаються стандарти бездротового зв'язку WPAN, WLAN і Bluetooth, IEEE 802.15.4, Zigbee, Z-Wave, 6LoWPAN, Thread та інші IP-базовані рішення.	2
Тема 4. Телекомунікаційні системи IoT: 4G, 5G, LoRa, Sigfox. Вивчаються стільникові технології зв'язку (3GPP, LTE, 5G), їх архітектура, протоколи, частотні діапазони та моделі доступу. Аналізуються технології для IoT — LoRaWAN, Sigfox, NB-IoT, їх топології, особливості передачі даних і енергоефективність.	2
Тема 5. Інфраструктура IoT: маршрутизатори, шлюзи та протоколи передачі даних.	2

Розглядаються функції маршрутизаторів і шлюзів, протоколи маршрутизації, VLAN, VPN, QoS, SDN-архітектури. Аналізуються протоколи зв'язку IoT: MQTT, MQTT-SN, CoAP, AMQP, STOMP — їх структура, принципи роботи та сфери застосування.	
Тема 6. Хмарні та туманні обчислення у смарт-технологіях. Досліджується архітектура хмарних систем (OpenStack, приватні та гібридні хмари), а також концепція туманних (fog) обчислень. Розглядається їхня роль у зберіганні, обробці та передачі даних IoT-пристроїв, а також моделі взаємодії з граничними вузлами.	2
Тема 7. Інтелектуальний аналіз даних та машинне навчання в IoT-системах. Розкриваються принципи обробки великих даних (Big Data) у середовищах IoT, алгоритми машинного навчання, методи кластеризації, прогнозування та прийняття рішень у смарт-системах.	2
Тема 8. Безпека та стандартизація смарт-технологій. Розглядаються основи кібербезпеки IoT: типові атаки, архітектура програмно-визначеного периметру, методи захисту пристроїв і даних. Аналізуються консорціуми, стандарти та спільноти (Zigbee Alliance, LoRa Alliance, IEEE IoT, Thread Group, Wi-Fi Alliance), що формують екосистему безпечних смарт-технологій.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Packet Tracer – Розгортання та з'єднання пристроїв. Ознайомлення з середовищем Cisco Packet Tracer. Відпрацювання навичок розгортання IoT-пристроїв, налаштування з'єднань між ними та моделювання базової топології мережі.	6	0,2
Тема 2. Створення простої мережі з використанням Packet Tracer. Практичне моделювання локальної IoT-мережі з використанням сенсорів, контролерів і маршрутизаторів. Налаштування IP-адресації, перевірка зв'язку та тестування обміну даними між пристроями.	6	0,2
Тема 3. Підключення та моніторинг пристроїв IoT. Дослідження процесів реєстрації, підключення та моніторингу IoT-пристроїв у мережі. Використання інструментів для збору телеметричних даних і візуалізації стану пристроїв у реальному часі.	6	0,1
Тема 4. Розумна кімната на базі Raspberry Pi і PL-App. Розробка та налаштування системи «розумної кімнати» з використанням Raspberry Pi. Підключення сенсорів, створення сценаріїв автоматизації та керування за допомогою платформи PL-App.	6	0,1
Тема 5. Конвергентна мережа і взаємозв'язок речей. Безпека та автоматизація Cisco IoT.	4	0,1

Вивчення архітектури конвергентних мереж IoT, принципів взаємодії між пристроями. Аналіз безпекових ризиків, засобів захисту Cisco IoT та основ технологій автоматизації у смарт-мережах.		
Тема 6. Побудова проєкту рішення Інтернету речей: від планування до прототипування. Розробка повноцінного IoT-рішення: постановка задачі, вибір архітектури, планування мережевої інфраструктури, реалізація прототипу та оцінка його ефективності. Врахування вимог безпеки на кожному етапі проєктування.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи Інтернету речей та архітектура смарт-технологій. Вивчення концепцій Інтернету речей (IoT), архітектури смарт-систем і принципів взаємодії пристроїв. Аналіз типів сенсорів, протоколів зв'язку та особливостей передачі даних у мережах IoT. Оцінка ключових напрямів використання IoT у промисловості, медицині, енергетиці та «розумних містах».	0,1
Тема 2. Безпека, протоколи та управління даними в смарт-технологіях. Дослідження механізмів забезпечення безпеки IoT-систем. Розгляд протоколів обміну даними (MQTT, CoAP, HTTP, LoRaWAN), методів шифрування та автентифікації пристроїв. Аналіз типових загроз і вразливостей IoT-інфраструктури та способів їх мінімізації.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Еволюція смарт-пристроїв та тренди розвитку IoT. Дослідження сучасних тенденцій розвитку «розумних» технологій, взаємодії пристроїв та концепції Industry 5.0.	8
Тема 2. Архітектура IoT-платформ: хмара, туман і крайові обчислення.. Порівняння різних моделей обробки даних. Роль Edge- і Fog-технологій у підвищенні безпеки систем.	8
Тема 3. Протоколи зв'язку в IoT: MQTT, CoAP, AMQP, XMPP. Поглиблене вивчення мережевих протоколів, форматів обміну повідомленнями та механізмів безпечної комунікації.	7
Тема 4. Загрози кібербезпеці смарт-пристроїв. Аналіз основних типів атак на IoT: DDoS, фішинг, перехоплення даних, маніпуляції через оновлення ПЗ.	7
Тема 5. Захист персональних даних у смарт-середовищах.	7

Методи забезпечення конфіденційності, шифрування даних користувача та політики GDPR у контексті IoT.	
Тема 6. IoT-інфраструктура в розумних містах. Структура систем Smart City, приклади впровадження та ризики інформаційної безпеки міських IoT-мереж.	7
Тема 7. Використання штучного інтелекту для моніторингу безпеки IoT. Застосування алгоритмів машинного навчання для виявлення аномалій та прогнозування кібератак.	7
Тема 8. Безпечне оновлення прошивок та управління пристроями IoT. Методи автентифікації оновлень, перевірка цілісності та захист від підробленого ПЗ.	7
Тема 9. IoT і блокчейн: нові можливості безпеки. Інтеграція технології блокчейн для захисту даних, управління ідентифікацією та підвищення довіри в IoT-середовищах.	7
Тема 10. Етичні аспекти використання смарт-технологій. Баланс між інноваціями, приватністю користувача та контролем даних у мережевому суспільстві.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «Introduction to IoT and Digital Transformation, Exploring IoT with Cisco Packet Tracer (5)»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. 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.
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

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4

0,8	0,2

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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

Здобувач вищої освіти 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	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Станіслав МІЛЕВСЬКИЙ