Силабус освітнього компонента
Програма навчальної дисципліни

Безпека смарт-технологій

Шифр та назва спеціальності
К3 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Національна безпека у сфері кіберзахисту

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
5

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-наукової 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

Навчальна дисципліна "Безпека смарт-технологій" 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 заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК6. Здатність до адаптації та дії в новій ситуації.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.
СК10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
РН6. Вміти адаптовуватись до нових викликів та дій у певних ситуаціях.
РН7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог.
РН8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеки.
РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
РН10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
РН12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.
РН16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки.
РН17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

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)

Технології програмування, Математичні основи криптології, Менеджмент інформаційної безпеки.

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 розвиток Інтернету речей (IoT). Розглядаються етапи становлення Інтернету речей, основні тенденції розвитку, сфери застосування (промисловість, медицина, транспорт, енергетика, розумне місто). Аналізуються сучасні та майбутні напрямки розвитку IoT.	4
Тема 2. Основи смарт-технологій та компоненти IoT-систем. Вивчаються принципи побудови смарт-технологій, поняття "дані – інформація – знання". Розглядаються основні компоненти систем IoT: сенсори, контролери, виконавчі пристрої, системи живлення.	4
Тема 3. Комунікаційні технології та протоколи IoT. Аналізуються основи теорії комунікації, радіочастотний спектр, типи бездротових мереж (WPAN, WLAN), протоколи ZigBee, Bluetooth, 6LoWPAN, Thread, Wi-Fi. Розглядається взаємодія пристроїв у гетерогенних мережах.	4
Тема 4. Телекомунікаційні системи IoT: 4G, 5G, LoRa, Sigfox. Розглядаються стандарти мобільного зв'язку для IoT, архітектура мереж LTE, NB-IoT, LoRaWAN, Sigfox. Вивчаються їх топології, енергоспоживання, пропускна здатність та особливості застосування.	4
Тема 5. Архітектура IoT-систем: маршрутизація, шлюзи та хмарні технології. Описуються функції маршрутизаторів, шлюзів, VLAN, VPN. Розглядаються хмарні та туманні (fog) обчислення, взаємодія з хмарними платформами IoT (AWS IoT, Azure IoT, OpenStack).	4
Тема 6. Обробка та аналіз даних у смарт-системах. Вивчаються методи збору, зберігання й обробки даних із сенсорів IoT. Аналізуються моделі машинного навчання для розпізнавання шаблонів, прогнозування та оптимізації процесів у смарт-технологіях.	4
Тема 7. Безпека смарт-технологій та Інтернету речей. Розглядаються загрози, типи атак на IoT-пристрої, методи захисту даних і комунікацій. Вивчаються основи криптографії, захист апаратного рівня, архітектура програмно-обумовленого периметру (SDP), рекомендації з безпеки IoT.	4
Тема 8. Міжнародні консорціуми та стандарти у сфері IoT. Висвітлюються ключові організації, що формують стандарти IoT (Bluetooth SIG, Thread Group, ZigBee Alliance, LoRa Alliance, IEEE IoT). Розглядається роль спільнот у розвитку безпечних і сумісних рішень.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Packet Tracer – Розгортання та з'єднання пристроїв. Ознайомлення з інтерфейсом Cisco Packet Tracer. Створення робочого середовища для IoT-пристроїв. Розгортання маршрутизаторів, комутаторів та кінцевих пристроїв. Налаштування базового з'єднання між пристроями. Виявлення можливих уразливостей при неправильній конфігурації.	6	0,1
Тема 2. Створення простої мережі з використанням Packet Tracer. Проєктування локальної мережі з IoT-пристроями. Присвоєння IP-адрес та базова конфігурація TCP/IP. Перевірка зв'язності мережі (ping, traceroute). Використання протоколів DHCP та DNS. Аналіз мережевих ризиків у простих топологіях.	6	0,1
Тема 3. Підключення та моніторинг пристроїв IoT. Підключення датчиків та «розумних» пристроїв до мережі. Використання IoT Monitor у Packet Tracer. Взаємодія між IoT-пристроями (керування через додаток). Моніторинг роботи пристроїв та журнал подій. Виявлення та попередження несанкціонованого доступу.	5	0,1
Тема 4. Розумна кімната на базі Raspberry Pi і PL-App. В Ознайомлення з можливостями Raspberry Pi у IoT. Підключення сенсорів та керованих пристроїв. Програмування логіки роботи розумної кімнати (Python). Використання PL-App для автоматизації процесів. Виявлення ризиків безпеки у смарт-просторах.	5	0,1
Тема 5. Конвергентна мережа і взаємозв'язок речей, питання безпеки та основні стовпи Cisco IoT, технології автоматизації. Архітектура конвергентної мережі IoT. Протоколи обміну даними в IoT (MQTT, CoAP). Основні стовпи Cisco IoT (безпека, масштабованість, аналітика). Приклади атак на конвергентні мережі. Технології автоматизації для управління IoT-пристроями.	5	0,1
Тема 6. Побудова проєкту створення рішення інтернету речей, від планування до прототипування. Аналіз задачі та вимог до IoT-рішення. Вибір архітектури та технологій. Планування структури мережі IoT. Реалізація прототипу в Packet Tracer або на реальних пристроях. Тестування, виявлення ризиків і пропозиції з удосконалення безпеки.	5	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b

Тема 1. Основи побудови та захисту IoT-мереж. Архітектура інтернету речей: рівні, компоненти, приклади застосування. Типи IoT-пристроїв та їх роль у мережі. Протоколи комунікації в IoT (MQTT, CoAP, HTTP, AMQP). Загрози безпеці в IoT-середовищі: класифікація та приклади. Методи автентифікації та авторизації в IoT. Шифрування і захист передавання даних у IoT-мережах.	0,1
Тема 2. Атаки та захист в системах інтернету речей. Основні кіберзагрози для IoT (DDoS, підміна даних, перехоплення трафіку). Вразливості протоколів IoT та приклади їх використання зловмисниками. Методи моніторингу та виявлення атак на IoT-пристрої. Захист інфраструктури інтернету речей: принципи та інструменти. Рекомендації Cisco IoT Security Framework. Приклади реальних атак на IoT-системи та способи їхнього запобігання.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Протоколи зв'язку в IoT. Характеристика MQTT, CoAP, AMQP, Zigbee, Z-Wave. Порівняння їх ефективності та безпеки.	12
Тема 2. Моделі загроз для IoT-систем. STRIDE та інші моделі аналізу загроз. Приклади застосування для IoT-рішень.	10
Тема 3. Шифрування та криптографічні методи в IoT. Легкі криптографічні алгоритми для обмежених пристроїв. Використання симетричних і асиметричних методів.	10
Тема 4. Захист IoT-пристроїв на рівні апаратного забезпечення. Безпечне завантаження (Secure Boot). Трастові модулі (TPM) та їх застосування.	10
Тема 5. Аналіз вразливостей IoT-пристроїв. Використання сканерів безпеки (Nmap, Nessus). Методи пентесту IoT.	10
Тема 6. Хмарні сервіси для IoT та їх безпека. AWS IoT, Azure IoT Hub, Google IoT Core. Ризики та засоби захисту даних у хмарних платформах.	10
Тема 7. Стандарти та нормативне регулювання безпеки IoT. ISO/IEC 30141, ETSI EN 303 645. Рекомендації NIST щодо IoT Security.	10
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 «PaloAlto»
https://paloaltonetworksacademy.net/course/index.php.

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
0,2	0,2		0,4

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	F

(потрібне повторне вивчення)

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** Андрій ТКАЧОВ