КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою КНТЕУ
(пост. п. 9 від "23" 12 2021 р.)
Ректор
_____ А.А. Мазаракі

БЕЗПЕКА ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ / SECURITY OF THE INTERNET OF THINGS

ПРОГРАМА/
COURSE SUMMARY

Київ 2021

Автори: В.І. ЧУБАЄВСЬКИЙ, кандидат політичних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Д.О. ТИЩЕНКО, кандидат економічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Т.М. ФРАНЧУК, кандидат економічних наук, асистент кафедри інженерії програмного забезпечення та кібербезпеки
М.В. САШНЬОВА, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Ю.О. САМОЙЛЕНКО кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 1 листопада 2021 р., протокол № 10.

Рецензенти: Н.О. КОТЕНКО, канд. пед. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Б.Т. БЕБЕШКО, Senior Software Engineer Softorino Ltd.

БЕЗПЕКА ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ / SECURITY OF THE INTERNET OF THINGS

ПРОГРАМА / COURSE SUMMARY

ВСТУП

Дисципліна «Безпека технологій інтернету речей» є вибірковою дисципліною навчальних планів підготовки студентів денної форми навчання освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» освітньої програми «Безпека систем електронних комунікацій в економіці».

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.

Програму підготовлено відповідно до Стандарту вищої освіти України із зазначеної спеціальності та відповідної освітньо-професійної програми підготовки магістрів КНТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання навчальної дисципліни «Безпека технологій інтернету речей» є формування у майбутніх спеціалістів умінь та компетенцій в області Інтернет речей та цифрових технологій, та більш широкої категорії, 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.

Завданням дисципліни є: ознайомити студентів з базовими теоретичними аспектами надійності та безпеки систем на основі IoT.

Предметом вивчення 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.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ

ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- інформаційних технологій;
- безпека інформаційних систем та мереж;
- іноземної мови за професійним спрямуванням;
- організації комп'ютерних мереж.

вміння: вільно працювати:

- з офісними додатками Microsoft;
- з хмарними сервісами Office 365;
- з пошуковою системою Google.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Безпека технологій інтернету речей» як вибіркова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

Безпека систем електронних комунікацій в економіці
(ОС магістр, ОП 2022р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ-1.	Здатність застосовувати знання у практичних ситуаціях.	1-10
КЗ-3.	Здатність до абстрактного мислення, аналізу та синтезу.	1-10
КЗ-5.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	1-10

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Спеціальні (фахові, предметні) компетентності за освітньою програмою		
КФ2.	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	1-10
КФ5.	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес / операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	1-10
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.	1-10
Програмні результати навчання за освітньою програмою		
РН2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	1-10
РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	1-10

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	1-10
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.	1-10
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.	1-10
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.	1-10
РН18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	1-10

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Цифрова трансформація бізнесу

Еволюція цифрової трансформації. Вплив цифрової трансформації на бізнес. Чи можуть смарт-пристрої думати? Що таке IoT (Інтернет речей). Історія розвитку Інтернету речей. Зростання пристроїв IoT. Переваги та недоліки пристроїв IoT. Типи мереж. Як підключені пристрої IoT до мережі? Підключення та моніторинг «речей».

Список рекомендованих джерел:

Основний: 1-3

Додатковий: 6-15

Інтернет-ресурси: 23

Тема 2. Загальновизнані технології та стандарти для забезпечення безпеки IoT

Стандартизація для IoT. Промисловий Інтернет-консорціум, OpenFog Consortium та Фонд Відкритого зв'язку. Моделі TCP та OSI. Референтна модель світового форуму IoT. Спрощена структура IoT.

Зв'язок даних та мережеві з'єднання. Протоколи додатків, створені для підтримки пристроїв IoT. Вплив з'єднань на конфіденційність та безпеку. Модель End-to-End IoT-системи.

Список рекомендованих джерел:

Основний: 1-4

Додатковий: 5-9, 11

Інтернет-ресурси: 23

Тема 3. Апаратна частина «Інтернету Речей». Безпека обладнання IoT

Наявність IoT у сучасному світі. Складові блоки системи IoT: контролер, датчики, виконавчі механізми. Процеси в керованих системах: системи керування, зворотній зв'язок. Створення, налаштовування підключення пристроїв Інтернету речей.

Компоненти вразливості апаратного забезпечення OWASP. Основні типи процесорів, що використовуються в IoT – ARM, MIPS та x86. Вразливості та атаки на рівні обладнання. Вразливості прошивки. Заходи щодо зменшення загроз пристроям IoT. Безпека даних і паролів пристроїв IoT.

Список рекомендованих джерел:

Основний: 1-4

Додатковий: 5-9,11,15

Інтернет-ресурси: 23

Тема 4. Застосування автоматизації в IoT

Що таке автоматизація? Використання автоматизації: Інтелектуальна автоматизація будинку, Розумні будівлі, Промислові IoT та розумні заводи, Розумні міста, Розумні мережі електропостачання, Розумні машини, Магазини та послуги, Медична діагностика та хірургія, Літаки на авто-пілоті.

Датчики, кінцеві точки і системи живлення. Термопари і температурні датчики. Резистивні датчики температури. Ефект Холла і датчик і струму. Фотоелектричні датчики. Датчики PIR .LiDAR і активні датчики. Датчики MEMS. Датчики тиску та мікрофони MEMS. «Інтелектуальні» точки IoT, Пристрої введення. Пристрої виведення. Поєднання, «злиття» датчиків.

Модель системи IoT. Представлення моделі домашньої автоматизації. Компоненти Smart Home.

Список рекомендованих джерел:

Основний: 1-4

Додатковий: 5, 16, 17

Тема 5. Застосування Big Data для підтримки пристроїв IoT

Великі дані (Big Data) та Інтернет речей. Звідки беруться великі дані. Структуровані та неструктуровані дані. Управління великими даними. Основні технології управління даними. Використання великих даних. Приклади даних, зібраних датчиками. Де зберігаються Великі Дані? Хмари та Хмарні обчислення. Аналіз великих даних для ефективного використання в бізнесі. Програмні інструменти для візуалізації аналізу даних. Збір та підготовка даних. Етика великих даних.

Список рекомендованих джерел:

Основний: 1-4

Додатковий: 5-9, 20

Тема 6. Застосування AI та ML, базового програмування для підтримки пристроїв IoT

Штучний Інтелект (AI) та Машинне Навчання(ML). Мережі на основі намірів (IBN). Як пов’язані ML, AI, та IBN? Байєсовські моделі. Нейронні мережі. Рекурентні нейронні мережі Навчання та отримання логічних висновків в Інтернеті речей. Аналіз даних в IoT і порівняння / оцінка методів машинного навчання.

Застосування базового програмування для підтримки пристроїв IoT. Основні концепції програмування: системне програмне забезпечення, прикладне програмне забезпечення та комп'ютерні мови. Ресурси для прототипування. Електронні інструменти.

Проблеми безпеки в IoT: зберігання даних, передача даних.

Список рекомендованих джерел:
Основний: 1-4
Додатковий: 5-9, 20, 21

Тема 7. Застосування хмарних технологій в IoT

Основні сервісно-орієнтовані архітектури, принципи, моделі та класифікація хмарного обчислення, сфери застосування IoT. Застосування хмарних технологій в «Інтернеті Речей». Порівняльний аналіз апаратних і програмних засобів в різних сферах застосування «Інтернету Речей».

Хмарна архітектура Microsoft Azure IoT. Підключення пристроїв до хмари. Налаштувати центру Інтернету речей. Рішення IoT за допомогою Azure IoT Central.

Список рекомендованих джерел:
Основний: 1-4
Додатковий: 5-9, 11, 20, 21

Тема 8. Безпека в цифровому світі на основі IoT

Безпека в цифровому світі: Чому безпека важлива? Проблеми забезпечення безпекою пристроїв IoT. Безпечне користування Wi-Fi. Захист пристроїв.

Площина контролю, Площина даних, Площина управління. Захист площин котролю, даних та керування в IoT. Захист речей з використанням системи Cisco IoT.

Модель безпеки IoT. Рівні безпеки IoT. Моделювання загроз IoT. Система NICE Cybersecurity Workforce Framework.

Діаграма бізнес-моделі галузей і вертикалей в IoT. Використання IoT в медицині. IoT для Розумного міста: освітлення, операційні центри, паркування, безпека, безпека руху, рух транспорту та Wi-Fi. IoT в енергосистемі. IoT у виробництві.

Небезпека та вразливість систем «розумних» міст: відсутність безпеки та надійності IoT. Кіберзлочинність, кібертероризм і кібершпигунство.

Список рекомендованих джерел:
Основний: 1-4
Додатковий: 5-9, 11, 20, 21
Інтернет-ресурси: 23-27

Тема 9. Принципи безпечного підключення «Інтернету Речей» до мережі

Мережні протоколи. Протоколи IoT. Протокол інтернету і протокол управління передачею. Роль протоколу IP в інтернеті речей. WPAN і WLAN на базі IP.

Гарантування безпеки мережі. Бездротові технології: WiFi, ZibBee, Bluetooth, 4G/5G, LoRaWAN. Вразливості комунікаційного рівня OWASP.

Вразливості IP. Вразливості TCP і UDP. Безпека комунікаційних протоколів IoT.

Туманні та хмарні обчислення. Туманні та хмарні служби. Модель хмарних обчислень. Хмарні сервіси: Amazon AWS, IFTTT, Zapier, Built.io, Cisco Spark. Модель туманних обчислень.

Список рекомендованих джерел:

Основний: 1-4

Додатковий: 5-9, 11, 17, 20, 21

Тема 10. Приклади безпечного підключення пристроїв Інтернету речей

Розгортання рішення IoT за допомогою бази даних SQL Azure. Зберігання та обробка даних IoT в режимі реального часу за допомогоб бази даних SQL Azure. Забезпечення безпечної роботи з даними Інтернету речей в базі даних SQL Azure.

Відстеження та керування кавоваркою за допомогою Azure IoT Central.

Безпечне підключення пристроїв Інтернету речей до хмари. Реалізація інфраструктури рішень IoT. Створення та налаштування центру Інтернету речей. Налаштування фізичних пристров IoT, керування ними. Автоматизація керування пристроями IoT за допомогою Azure IoT Hub. Відстеження, усунення неполадок та оптимізація рішення IoT.

Список рекомендованих джерел:

Основний: 1-4

Додатковий: 5-9, 11, 17, 20, 21

Інтернет-ресурси: 23-27

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Соколов В. Ю. Безпека безпроводових і мобільних мереж: Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.
2. Девід Роуз, Дивовижні технології. Дизайн та інтернет речей : навч. посібник/ Девід Роуз. Харків: «Книжковий Клуб», 2018. – 336 с.
3. *Хорошко О.В. Захист систем електронних комунікацій: навч.посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.*
4. Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 1. Основи і технології: посібник / За ред. В.С. Харченка. – Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. – 547 с.

Додатковий

5. Гладкий А. Основи безпеки та анонімності у Всесвітній мережі: монографія / А. Гладкий. Київ: Фенікс , 2012 – 256 с.
6. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security of IoT: Practicum / Kharchenko V.S. and Sklyar V.V. (Eds.) – Ministry of Education and Science of Ukraine, National Aerospace University “KhAI”, Ternopil National Economic University, 2019. – 98 p.
7. Hanssen G., Stålhane T, Myklebust T. SafeScrum® – Agile Development of Safety-Critical Software. Springler, 2018.
8. 4. NISTIR 8200, Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT). –National Institute of Standards and Technologies, 2018.
9. NIST SP 1500-201, Framework for Cyber-Physical Systems. National Institute of Standards and Technologies, 2017.
10. Martins B., Laranjeiro N., Vieira M. INTENSE: INteroperability TEstiNg as a Service // Proceedings of 2017 IEEE International Conference on Web Services (ICWS 2017).
11. Nunes P., Medeiros I., Fonseca J. at all. Benchmarking Static Analysis Tools for Web Security. IEEE Transactions on Reliability (2018), 67(3): 1159-1175
12. Sklyar V., Kharchenko V. Green Assurance Case: Applications for Internet of Things. Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control, vol 171. Springer, Cham, 2019.

13. Haddon-Cave C. The Nimrod Review. An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. Crown Copyright, 2009.

14. Kelly T. Are Safety Cases Working? Safety Critical Systems Club Newsletter, Vol. 17, n. 2, 2008.

15. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P.

16. Professor Dr.-Ing. Klaus Schwab, The Fourth Industrial Revolution, ASIN: B01JEMROIU, 2017, 189 P.

17. 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.

18. 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.

19. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P.

20. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.

21. Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.

Інтернет-ресурси

23. Основи Інтернету речей. Школа автоматики. – URL: http://edu.asu.in.ua/mod/book/tool/print/index.php?id=112

24. В.В. Вишньовський, О.П. Войтович. Структурна схема системи захисту розумного будинку. – URL: https://conferences.vntu.edu.ua/index.php/all–fitki/all–fitki–2017/paper/view/2738

25. К.В. Савченко, О.П. Войтович. Структурна схема системи захисту розумного будинку – URL: https://conferences.vntu.edu.ua/index.php/all–fitki/all–fitki–2017/paper/view/2736

26. Войтович О.П., Вишняковський В.В., Савченко К.В. Дослідження безпеки системи розумного будинку. – Вінниця: ВНТУ. – URL: https://epsi.vntu.edu.ua/uploads/2017/67-3wbzu2z9ouo8vv4oeo00yr4n7ve8fqpq.pdf

27. Lisa Goeke, Security Challenges of the Internet of Things. URL: https://www.theseus.fi/bitstream/handle/10024/128420/Goeke_Lisa.pdf?sequence=1

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*