

КІБЕРБЕЗПЕКА В ІНТЕРНЕТІ РЕЧЕЙ
Кафедра менеджменту та інформаційних технологій
Економічний факультет

<i>Освітній ступінь</i>	Бакалавр
<i>Кількість кредитів ЄКТС</i>	3
<i>Форма контролю</i>	Залік

Загальний опис дисципліни

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, ритейлу та будівництва. Поступово пристрої IoT стають невід'ємною частиною багатьох бізнес-процесів, і зростання їх кількості спричиняє виникнення нових проблем безпеки. Дисципліна присвячена також вивченню основ криптографії та криптографічного аналізу, що застосовуються до захисту інформації в Інтернеті речей, знайомиться з поняттям шифрів, симетричною і асиметричною криптографії, електронним підписом, хешуванням і іншими математичними об'єктами криптографії.

Мета і завдання

Метою навчальної дисципліни сформувати систему знань студентів в області Інтернет речей та цифрових технологій, ознайомити з основами математичної теорії криптографії, придбати навички в практичному використанні, постановці і розв'язанні задач шифрування інформації, розуміти суть інформаційних процесів в криптографічних системах, застосувати комп'ютери для розв'язання завдань шифрування і дешифрування. В дисципліні основний акцент робиться на розумінні фундаментальних концепцій і механізмів які лежать в основі функціонування Інтернет-речей.

Завданням навчальної дисципліни є вивчення основних концепцій та підходів до розробки та впровадження надійних, безпечних систем IoT, вивчення основ теорії чисел, традиційних та сучасних алгоритмів шифрування, а також функцій та алгоритмів хешування для дослідження моделей та методів забезпечення надійності та забезпечення безпеки та оцінки систем на основі IoT.

Компетентності: здатність застосовувати відповідний математичний апарат для вирішення професійних завдань; здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою; здатність здійснювати управління інцидентами інформаційної та кібербезпеки.

Програмні результати навчання: Застосовувати математичні методи опису і дослідження криптографічних систем. Володіти навичками математичного моделювання в криптографії. Використовувати основні методи, моделі та алгоритми захисту даних в програмно-апаратних системах Інтернет-речей. Застосовувати різні методи та інструменти для пошуку програмно-апаратних вразливостей в Інтернет речах.

Зміст за темами:

1. Кібербезпека: основні поняття і визначення.
2. Історія Інтернету речей.
3. Функціональна безпека: основні поняття і визначення.
4. Вступ до криптографічних методів захисту.
5. Традиційне шифрування: класичні методи.
6. Традиційне шифрування: сучасні методи.
7. Кібербезпека в «Інтернет-речей».
8. Кібербезпека для систем «Разумного міста».
9. Кібербезпека в «Інтернет-речей» в промисловості.