Чернівецький національний університет імені Юрія Федьковича

Навчально-науковий інститут фізико-технічних та комп'ютерних наук

Кафедра радіотехніки та інформаційної безпеки

СИЛАБУС
навчальної дисципліни
Основи кібербезпеки пристроїв та систем IoT

вибіркова

Освітньо-професійна програма _____

Спеціальність _____

Галузь знань _____

Рівень вищої освіти **перший (бакалаврський)**

Навчально-науковий інститут фізико-технічних та комп'ютерних наук

Мова навчання **українська**

Розробники (викладачі): Саміла Андрій Петрович, доктор технічних наук, професор
Рождественська Маргарита Григорівна, к. ф.-м. н., доцент кафедри радіотехніки та інформаційної безпеки,

Профайл викладача (-ів) http://radiotech.cv.ua/teachers/

Контактний тел. +38 (0372) 581271,
E-mail: a.samila@chnu.edu.ua, m.rozhdestvenska@chnu.edu.ua
Сторінка курсу в Moodle https://classroom.google.com
Консультації Онлайн-консультації: понеділок та четвер з 14.00 до 15.00.

1. Анотація дисципліни (призначення навчальної дисципліни)

Навчальна дисципліна «Основи кібербезпеки пристроїв та систем IoT» уможливлює вивчення основних засад забезпечення безпеки сегменту Internet of Things (IoT, Інтернет речей), що мають бути враховані в ході експлуатації пристроїв та систем IoT. Політики безпеки, процедур та стандартів слід дотримуватися при розробленні та налаштуванні всіх компонент пристроїв і систем IoT, які охоплюють: канали зв'язку; дані, що передаються; дані, що зберігаються; мережеві пристрої та кінцеві фізичні пристрої.

Предметом вивчення навчальної дисципліни «Основи кібербезпеки пристроїв та систем IoT» є принципи і методи виявлення та знешкодження прихованих та явних загроз в обчислювальних мережах фізичних предметів, оснащених вбудованими технологіями для взаємодії один з одним або із зовнішнім середовищем.

Місце навчальної дисципліни «Основи кібербезпеки пристроїв та систем IoT» в структурі професійної підготовки майбутніх фахівців. Освоєння матеріалу дисципліни передбачає, що студент володіє знаннями, отриманими при вивченні загальних розділів математики та основ комп'ютерних технологій.

2. Мета навчальної дисципліни

Метою викладання дисципліни «Основи кібербезпеки пристроїв та систем IoT» є формування системи знань та навиків, які дозволяють студенту вивчити методи ефективного захисту сегменту IoT від кібератак для забезпечення максимально можливого конфіденційного передавання інформації між фізичними пристроями та кіберпростором IoT.

Переваги, які надає вивчення даної вибіркової дисципліни:

- обізнаність в особливостях автоматизації та IoT, вивчення цінностей даних для цифрового бізнесу і суспільства;
- уміння програмувати інтелектуальні пристрої, підключені до Інтернету;
- навики конфігурування бездротових сенсорних мереж, налаштування їх конфіденційності та безпеки;
- обізнаність в особливостях безпечного проведення фінансових платежів із застосуванням банківських карт та смартфонів;
- знайомство з особливостями конфігурування захищених систем «розумний дім», налаштуванням віддаленого доступу для їх моніторингу та керування;
- знайомство з рішеннями від українських операторів мобільного зв'язку для розгортання проєктів «Розумне місто» в Україні на основі пристроїв та систем IoT.

3. Завдання навчальної дисципліни

В дисципліні основна увага приділяється задачам виявлення і захисту від можливих загроз в різноманітних комунікаційних сеансах інформаційного простору IoT. Вивчення навчальної дисципліни «Основи кібербезпеки пристроїв та систем IoT» передбачає формування та розвиток у студентів наступних компетентностей.

Загальних:

- застосовувати отримані знання у практичних ситуаціях;
- знати та розуміти предметну області та професію;
- вміти виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
- здійснювати пошукову діяльність, обробляти та аналізувати інформацію.

Фахових:

- забезпечувати захист інформації, що обробляється в системах сегменту IoT з метою реалізації встановленої політики інформаційної та кібербезпеки;

- досягати відновлення штатного функціонування інформаційних, інформаційно-телекомунікаційних систем IoT після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;
- застосовувати методи та засоби технічного захисту інформації на фізичних пристроях IoT;
- виконувати моніторинг процесів функціонування пристроїв та систем IoT згідно встановленої політики інформаційної та кібербезпеки;
- аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам IoT згідно з встановленою політикою інформаційної та кібербезпеки.

4. Пререквізити

Для підвищення ефективності засвоєння курсу здобувач вищої освіти має вивчити дисципліни: загальні розділи математики, основи комп'ютерних технологій. Як альтернативний варіант, дозволяється проходження сертифікованих курсів CISCO Networking Academy за напрямками IoT Fundamentals.

5. Результати навчання

Унаслідок вивчення навчальної дисципліни «Основи кібербезпеки пристроїв та систем IoT» студент повинен бути здатним продемонструвати наступні результати навчання (компетентності).

Знати:

- основні концепції, методологію побудови і методи реалізації та конфігурування пристроїв і систем IoT;
- базові принципи посилення безпеки в оцифрованому світі згідно з встановленою політикою інформаційної та кібербезпеки;
- основні принципи використання захищених мережних технологій та основи мережевої безпеки пристроїв і систем IoT;
- алгоритми роботи спеціалізованих хмарних сервісів та принципи застосування хмарних обчислень в IoT;
- навики роботи з системами забезпечення безпеки IoT;
- особливості безпечного проведення фінансових платежів із застосуванням пристроїв IoT;
- особливості конфігурування захищених систем «Розумний дім», налаштування віддаленого доступу для їх моніторингу та керування.

Вміти:

- використовувати спеціальні сервіси для реалізації захищених пристроїв та систем IoT;
- застосовувати базове програмування для конфігурування фізичних пристроїв IoT на основі вбудованих рішень;
- виявляти й усувати приховані загрози за допомогою рішень для IoT;
- використовувати новітні технології, щоб оцінювати вразливість і ризики індустріального IoT;
- вивчати і вибирати стратегію щодо зниження ризиків, пов'язаних із загрозами безпеці для IoT-систем;
- застосовувати отримані знання у практичній діяльності при конфігуруванні, налаштування, обслуговуванні захищених пристроїв та систем IoT.

Результати вивчення даної дисципліни деталізують такі **програмні результати навчання**:

- здатність застосовувати знання для конфігурування та налаштування захищених пристроїв та систем IoT;
- здатність до використання програмних та інструментальних засобів для вирішення практичних проблем в області кібербезпеки IoT;
- здатність до креативного мислення при вирішенні проблемних ситуацій, обумовлених загрозами та дестабілізуючими чинниками інформаційному простору та інформаційним ресурсам IoT;
- здатність використовувати професійні знання й практичні навички з фундаментальних дисциплін в процесах аналізу та створення комп'ютерних, комунікаційних, інформаційних та інших технічних систем IoT;
- здатність керувати роботою пристроїв та систем IoT, забезпечувати безпеку функціонування їх інформаційних підсистем;
- здатність організовувати та конфігурувати захищені Web-системи IoT, використовуючи принципи розподілених систем, гіпертекстових систем, відповідні технічні та програмні засоби.

3. Опис навчальної дисципліни

3.1. Загальна інформація

Назва навчальної дисципліни «Основи кібербезпеки пристроїв та систем IoT»												
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсумкового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	3-4	6-8	3.0	90	2	30	-	-	30	30	-	залік
Заочна	3-4	6-8	3.0	90	2	8	-	-	4	78	-	залік

3.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Теми лекційних занять	**Змістовий модуль 1**. Взаємодія між компонентами систем IoT											
Тема 1. Загальні положення IoT	6	2	-	2	-	2	6	1	-	-	-	5
Тема 2. Цифрова трансформація	6	2	-	2	-	2	6	-	-	-	-	6
Тема 3. Захищені мережі - основа IoT	8	4	-	2	-	2	8	2	-	2	-	4
Тема 4. Програмування захищених пристроїв IoT	9	4	-	2	-	3	9	-	-	-	-	9
Тема 5. Прототипування захищених пристроїв	7	2	-	2	-	3	7	-	-	-	-	7
Тема 6. Великі дані та хмарні сервіси	9	2	-	4	-	3	9	1	-	-	-	8
Разом за ЗМ1	45	16	-	14	-	15	45	4	-	2	-	39
Теми лекційних занять	**Змістовий модуль 2.** Безпека в цифровому світі пристроїв IoT											
Тема 1. Автоматизація IoT, розумні будинки та міста	6	2	-	2	-	2	6	1	-	2	-	4
Тема 2. Штучний інтелект і машинне навчання	9	4	-	2	-	3	9	-	-	-	-	9
Тема 3. Безпека в цифровому світі IoT	6	2	-	2	-	2	6	-	-	-	-	6
Тема 4. Захист корпоративного світу IoT	6	2	-	2	-	2	6	-	-	-	-	6
Тема 5. Захист персональних даних в IoT	9	2	-	4	-	3	9	1	-	-	-	8
Тема 6. Захист пристроїв IoT	9	2	-	4	-	3	9	2	-	-	-	7
Разом за ЗМ 2	45	14	-	16	-	15	45	4	-	2	-	39
Усього годин	90	30	-	30	-	30	90	8	-	4	-	78

3.2.1. Теми лабораторних занять

№	Назва теми
1	Розгортання та з'єднання пристроїв IoT
2	Створення простої мережі з використанням Packet Tracer
3	Додавання IoT пристроїв до розумного будинку
4	Підключення та моніторинг пристроїв IoT
5	Налаштування бездротової безпеки
6	Налаштування віртуалізованого серверного середовища
7	Основи програмування мовою Python
8	Введення до Arduino
9	Введення до Raspberry Pi
10	Автоматизація повсякденних подій
11	Інтернет-відбиток пальців
12	Дослідження ризиків своєї поведінки в Інтернеті

3.2.2. Тематика індивідуальних завдань

Згідно навчального плану для даної дисципліни індивідуальні заняття не передбачені.

3.2.3. Самостійна робота

№	Назва теми
1	Практики безпеки даних в IoT
2	Цифрова трансформація та її вплив на бізнес
3	Еволюція цифрової трансформації
4	Інтелектуальність розумних пристроїв
5	Референсні моделі Інтернету речей, IoT - CISCO
6	Web речей WoT
7	Когнітивний Інтернет речей CIoT
8	Інтернет нано речей
9	Фізична безпека апаратно-програмних рішень IoT
10	Packet Tracer - розгортання та з'єднання пристроїв
11	Захист персональних даних та пристроїв
12	Переваги та недоліки пристроїв IoT
13	Типи пристроїв IoT, які підключаються до мереж
14	Підключення пристроїв IoT до мережі
15	Основні поняття Штучного Інтелекту і Машинного Навчання
16	Захист корпоративного світу

4. Система контролю та оцінювання

Види та форми контролю

Формами поточного контролю є усна чи письмова (тестування, реферат, творча робота, лабораторна робота) відповідь студента.

Форма підсумкового контролю - залік.

Засоби оцінювання:

- контрольні роботи;
- стандартизовані тести;
- реферати;
- розрахункові, графічні, розрахунково-графічні роботи;
- презентації результатів виконаних завдань та досліджень;
- студентські презентації та виступи на наукових заходах;
- завдання на лабораторному обладнанні, реальних об'єктах тощо;
- інші види індивідуальних та групових завдань.

Критерії оцінювання результатів навчання з навчальної дисципліни

(Оцінка "*відмінно*" виставляється:
коли студентом дані правильні вичерпні відповіді на всі поставлені запитання, уміло застосовані теоретичні знання, висвітлені питання не за завченою схемою, а своїми словами, з глибоким розумінням всіх основних закономірностей навчального процесу у вищій школі; формування таких складових психолого- педагогічної компетенції, як психологічна, операційно-методична, конструктивно-проективна, оцінювання й контролю, експертно-аналітична, науково-дослідна, методично-виховну, системи психолого-педагогічних знань, які сприятимуть ефективності професійної діяльності, підвищенню психологічної культури викладачів і студентів ВНЗ.

Оцінка "*добре*" виставляється:
коли студентом дані правильні відповіді на всі поставлені запитання, але відповіді не зовсім повні, в окремих випадках допущені незначні неточності у формулюванні закономірностей навчального процесу у вищій школі, методів оцінювання й контролю, експертно-аналітичної, науково-дослідної, методично-виховної, системи психолого-педагогічних знань, а окремі моменти не дістали належного з'ясування.

Оцінка "*задовільно*" виставляється:
коли відповідь студента правильна і становить більше 50 % матеріалу програми, але містить істотні помилки у обґрунтування методологічних і теоретичних засад педагогічного процесу у вищій школі на сучасному етапі розвитку науки і людства, відповідь подається за завченою схемою з неповним розумінням сутності, особливостей і закономірностей педагогічного процесу та таких його складових, як складових навчання, виховання в процесі навчання відповідно до вимог Болонського процесу.

Оцінка "*незадовільно*" виставляється:
коли не дано правильні відповіді на поставлені запитання, або відповіді надто поверхові, непослідовні і неточні, виявляють незнання студентом програмного матеріалу, містять грубі помилки, що свідчить про нерозуміння основних понять і нерозуміння умов успішної реалізації вимог принципів навчання й виховання для діяльності в різних сферах, шляхів удосконалення й розвитку організаційних форм навчально-виховної роботи, підвищення ефективності різних способів контролю, оцінки навчально-виховного процесу, рівнів підготовленості студентів і груп, про які йдеться.

Згідно шкали ECTS загальна кількість балів, яку студент може отримати у процесі вивчення дисципліни становить 100 балів, з яких 70 балів студент набирає при поточних видах контролю і 30 балів – у процесі підсумкового виду контролю (залік).

Оцінка за навчальну дисципліну виводиться відповідно до шкали оцінювання, затвердженої Міністерством освіти і науки України:

ШКАЛА ОЦІНЮВАННЯ

Оцінка за національною шкалою	**Оцінка за шкалою ECTS**	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Відмінно	A (90-100)	відмінно
Добре	B (80-89)	дуже добре
	C (70-79)	добре
Задовільно	D (60-69)	задовільно
	E (50-59)	достатньо
Незадовільно	FX (35-49)	(незадовільно) з можливістю повторного складання
	F (1-34)	(незадовільно) з обов'язковим повторним курсом

Підсумкова оцінка за навчальну дисципліну виводиться з суми балів поточного контролю за модулями (70 балів) та модуля-контролю (залік) – (30 балів).

Максимальна кількість балів при поточному контролі обов’язкових видів роботи становить 70 балів.

Мінімальна кількість балів для отримання заліку – 50. Якщо студент набирає 50 балів при поточному контролі, він може отримати залік, який в системі ECTS відповідає рівню Е. Для отримання заліку вищого рівня студент здає його.

Таким чином згідно шкали ECTS загальна кількість балів, яку студент може отримати у процесі вивчення дисципліни:

Змістовий модуль 1 + Змістовий модуль 2 + Оцінювання лабораторних робіт =

= 25 + 25 + 20 = 70 балів

Підсумковий модуль (залік) – **30 балів.**

Всього за курс – **100 балів.**

Розподіл балів, які отримують студенти

Поточне оцінювання (*аудиторна та самостійна робота*)																							Кількість балів (залік)	Сума
Змістовий модуль 1						Змістовий модуль 2						Захист лабораторних робіт													
Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Лаб.р. 1	Лаб.р. 2	Лаб.р. 3	Лаб.р. 4	Лаб.р. 5	Лаб.р. 6	Лаб.р. 7	Лаб.р. 8	Лаб.р. 9	Лаб.р. 10	Лаб.р. 11	Лаб.р. 12		
Тематична письмова робота			Самостійна робота			Тематична письмова робота			Самостійна робота			**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**1**	**1**	**1**		
20			**5**			**20**			**5**			**20**												**30**	**100**

5. Рекомендована література

5.1. Базова (основна)

1. Дэвид Роуз, Дэвид Роуз (David Rose), Будущее вещей. Как сказка и фантастика становятся реальностью, ISBN: 978-5-91671-394-7, 2015
2. Сэмюэл Грингард, Характеристики Интернет вещей. Будущее уже здесь, 2016, 188с.
3. В. А. Петин, Arduino и Raspberry Pi в проектах Internet of Things, ISBN: 978-5-9775-3646-2, 2016, 320с.
4. Дэвид Роуз, Дивовижні технології. Дизайн та інтернет речей, 336 с.
5. Алексей Гладкий, Основы безопасности и анонимности во Всемирной сети, 2012, 256с.
6. Виктор Петин, Arduino и Raspberry Pi в проектах Internet of Things, 2016, 432с.
7. 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.

5.2. Допоміжна

1. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P.
2. Professor Dr.-Ing. Klaus Schwab, The Fourth Industrial Revolution, ASIN: B01JEMROIU, 2017, 189 P.
3. 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.
4. 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.
5. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P.
6. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.

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

6. Інформаційні ресурси

1. http://www.chnu.edu.ua/index.php?page=ua
2. http://ptcsi.chnu.edu.ua/departments/
3. http://radiotech.cv.ua/
4. https://www.coursera.org/
5. https://www.netacad.com/ru/courses/iot
6. https://www.udemy.com/topic/internet-of-things/?lang=en&sort=popularity
7. https://stepik.org/course/50513/promo