Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра обчислювальної техніки

Вбудовані системи: застосунки і безпека
Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*F Інформаційні технології*
Спеціальність	*F7 Комп'ютерна інженерія, F2 Інженерія програмного забезпечення,*
Освітня програма	*Комп'ютерні системи та мережі* *Інженерія програмного забезпечення комп'ютерних систем* *Інтегровані інформаційні системи* *Інформаційні управляючі системи та технології* *Інформаційне забезпечення робототехнічних систем* *Інженерія програмного забезпечення інформаційних систем* *Інженерія програмного забезпечення комп'ютерних систем*
Статус дисципліни	*Вибіркова компонента ОП, циклу професійної/наукової підготовки*
Форма навчання	*очна (денна) / заочна*
Рік підготовки, семестр	*1 курс (2 семестр)*
Обсяг дисципліни	*4 кредитів, 120 год.* *Денна форма: лекцій 18 (36 годин), лабораторних 9 (18 годин), СРС (66 годин)*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	*Згідно розкладу на весняний семестр поточного навчального року за адресою http://rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: Лабораторні: ас. кафедри ОТ, Гордієнко Нікіта Юрійович, nikita.gordiienko@comsys.kpi.ua
Розміщення курсу	Навчальний курс розміщений на платформі дистанційного навчання: https://classroom.google.com/c/ODEzOTA4ODgyMTA0?cjc=apsh5zr5

Програма навчальної дисципліни

1.Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Дисципліна "Вбудовані системи: застосунки і безпека" призначена для ознайомлення студентів з основними концепціями, методами та підходами, що використовуються в розробці вбудованих систем і забезпеченні їх безпеки. Завдяки швидкому розвитку технологій, вбудовані системи стають все більш поширеними та складними, що підвищує ризик їх вразливості перед потенційними атаками. Тому особлива увага приділяється аспектам забезпечення безпеки та захисту вбудованих систем від атак різних типів.

Вивчення даної дисципліни майбутніми науковцями дозволить їм набути важливих знань розвитку існуючих і використанню нових підходів проектування, розробки та використання вбудованих за стосунків з забезпечення їх безпеки та захисту від можливих атак та втручань.

Метою вивчення дисципліни "Вбудовані системи: застосунки і безпека" є надання студентам необхідних знань та навичок у галузі вбудованих систем та їх застосувань, ознайомлення з потенційними видами атак та методами захисту вбудованих систем від потенційних загроз.

Вивчення дисципліни підсилює наступні загальні та фахові компетенції:

Для спеціальності 121 Інженерія програмного забезпечення

- Здатність до абстрактного мислення, аналізу та синтезу
- Здатність застосовувати знання у практичних ситуаціях
- Здатність вчитися і оволодівати сучасними знаннями
- Здатність працювати в команді
- Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення
- Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами
- Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу
- Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя
- Здатність до алгоритмічного та логічного мислення
- Здатність розробляти та використовувати мережні технології
- Здатність розробляти та використовувати програмне забезпечення для високопродуктивних комп’ютерних систем
- Здатність використовувати принципи побудови, функціонування та узагальнену структуру мікропроцесорних систем та особливості програмного забезпечення мікропроцесорних систем та мікроконтролерів

Для спеціальності 123 «Комп’ютерна інженерія»

- Здатність вчитися і оволодівати сучасними знаннями
- Здатність працювати в команді

- Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.
- Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.
- Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.
- Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.
- Здатність розробляти, адаптувати, використовувати програмно-технічні засоби для збирання, оброблення та інтелектуального аналізу даних в комп'ютерних системах: паралельних, розподілених, хмарних, безпечних, інтелектуальних, розумних, Інтернет речей, зокрема, з використанням штучного інтелекту.

Згідно з вимогами ОНП здобувачі після засвоєння дисципліни "Вбудовані системи: застосунки і безпека" мають продемонструвати такі програмні результати навчання:

- Проектувати та розробляти вбудовані системи з врахуванням вимог до їх застосування в різних областях.
- Аналізувати та оцінювати вимоги до безпеки вбудованих систем і розробляти відповідні заходи забезпечення безпеки.
- Ідентифікувати потенційні загрози та ризики для вбудованих систем і розробляти стратегії захисту від них.
- Використовувати сучасні методи та технології для забезпечення безпеки вбудованих систем, включаючи криптографію, контроль доступу, механізми аутентифікації тощо.
- Проектувати захищені механізми комунікації та обміну даними в межах вбудованих систем.
- Проводити аналіз вразливостей вбудованих систем та вживати відповідні заходи щодо їх виправлення та підвищення рівня безпеки.
- Використовувати інструменти тестування та валідації для перевірки ефективності та безпеки вбудованих систем.

Предметом дисципліни є:

- огляд архітектурних особливостей вбудованих систем;
- методи проектування та розробки вбудованих систем;
- аналіз та виявлення потенційних вразливостей вбудованих систем;
- методи атак на вбудовані системи;
- методи захисту та безпеки вбудованих систем;
- вивчення стандартів безпеки вбудованих систем.

Дисципліна "Вбудовані системи: застосунки і безпека" забезпечує наступні програмні компетентності і програмні результати освітньо-наукової програми (ОНП): ФК2, ФК3, ФК5, ФК6, ПРН4, ПРН6, ПРН7, ПРН17, ПРН20.

За результатами вивчення навчальної дисципліни "Вбудовані системи: застосунки і безпека" мають бути отримані такі знання.

1. Знання про основні принципи та концепції вбудованих систем, включаючи їх архітектуру, специфіку функціонування та обмеження.
2. Знання про вимоги до безпеки вбудованих систем у різних областях та усвідомлення необхідності вживання відповідних заходів захисту.
3. Розуміння методів і технологій забезпечення безпеки вбудованих систем, включаючи криптографічні методи, механізми аутентифікації та авторизації, контроль доступу тощо.
4. Знання про потенційні загрози та ризики, які можуть виникнути для вбудованих систем, і способи їх виявлення та усунення.
5. Розуміння методів аналізу вразливостей та використання відповідних інструментів для їх виявлення та виправлення.

Уміння, які мають бути отримані у рамках вивчення навчальної дисципліни "Вбудовані системи: застосунки і безпека".

1. Вміти аналізувати вимоги до безпеки вбудованих систем у різних областях застосування, враховуючи специфіку їх функціонування та потенційні загрози.
2. Вміти вивчати документацію та технічні характеристики апаратного забезпечення та аналізувати наявні захисні функції та потенційні вразливості.
3. Вміти виявляти потенційні вразливості вбудованих систем та розробляти стратегії для їх виправлення та підвищення рівня захищеності.
4. Вміти використовувати захисні механізми, такі як вбудовані захисні функції, шифрування, аутентифікація, контроль доступу тощо, для забезпечення конфіденційності, цілісності та доступності даних.
5. Вміти ефективно реагувати на інциденти безпеки, виявляти їх причини та розробляти плани відновлення та запобігання їх повторенню.

Здобувачі наукового ступеня також мають бути здатні.

1. Застосовувати вже існуючі методи захисту вбудованих систем для розробки цілісного захищеного застосунку на основі комплексного апаратного забезпечення.
2. Самостійно розробляти нові підходи та методи в області вбудованих систем і їх безпеки, враховуючи актуальні проблеми та потреби галузі.

Таке поєднання загальних та спеціальних компетентностей, теоретичних та практичних знань, умінь та здатностей сприяє підвищенню науково-практичного рівня здобувачів наукового ступеня магістра задля здійснення ними ефективних наукових досліджень.

2.Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного оволодіння дисципліною необхідні знання:

- Основи операційних систем,
- Комп’ютерна логіка,
- Архітектура комп’ютера,
- Паралельне програмування,
- Програмування мовою C/C++,
- Алгоритми і структури даних

Відповідно до освітньої програми необхідно попередньо оволодіти знаннями з дисциплін: «Вступ до операційної системи Linux», «Комп'ютерна логіка», «Архітектура комп'ютерів. Частина 1. Управляючі та арифметичні пристрої», «Архітектура комп'ютерів. Частина 2. Процесори», «Програмування», «Алгоритми і структури даних».

Компетентності, знання та вміння, отримані в рамках вивчення даної дисципліни, можуть бути застосовані для отримання обґрунтованих результатів досліджень та підвищення наукового рівня дисертаційних робіт.

3.Зміст навчальної дисципліни

1. Огляд вбудованих систем та їх застосування
2. Особливості проектування вбудованих систем
3. Базові відомості схемотехніки і її застосування при проектуванні вбудованих систем
4. Особливості та функціонал CortexM архітектури.
5. Фреймворки для вбудованих систем та їх особливості (FreeRTOS, QP, ThreadX)
6. Основні компоненти програмного та апартаного забезпечення та їх особливості
7. Типи та основні принципи кібератак на вбудовані систем.
8. Безпека програмного забезпечення і апаратного забезпечення.
9. Вразливості вбудованих систем
10. Вектори кібератак на вбудовані системи
11. Криптографія та захист даних
12. Зворотня інженерія

4.Навчальні матеріали та ресурси

4.1. Базова література

1. Архітектура комп'ютерів 2. Процесори. Теорія та практикум [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за спеціальністю 123 «Комп'ютерна інженерія» / КПІ ім. Ігоря Сікорського ; уклад.: І. А. Клименко, А. В. Каплунов, В. А. Таранюк, В. В. Ткаченко. – Електронні текстові дані (1 файл: 3.73 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 92 с. – Назва з екрана. URI https://ela.kpi.ua/handle/123456789/52163
2. Архітектура комп'ютерів 3. Мікропроцесорні системи. Частина 2. Програмування для мікроконтролерів STM32. Теорія та практикум [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за спеціальністю 123 «Комп'ютерна інженерія» / КПІ ім. Ігоря Сікорського ; уклад.: І. А. Клименко, А. В. Каплунов, В. А. Таранюк, В. В. Ткаченко. – Електронні текстові данні (1 файл: 9.95 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 197 с. – Назва з екрана. URI https://ela.kpi.ua/handle/123456789/52015
3. Новацький, А. О. Комп'ютерна електроніка та мікропроцесорні системи [Електронний ресурс] : підручник для студентів, які навчаються за освітньою програмою «Інформаційне забезпечення робототехнічних систем» за спеціальністю 126 «Інформаційні системи та технології» / А. О. Новацький ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 34,1 Мбайта). – Київ : КПІ ім. Ігоря Сікорського, 2024. – 447 с. – Назва з екрана. URI https://ela.kpi.ua/handle/123456789/68194

4.2. Додаткова література

1. Barr, M., & Massa, A. (2006). Programming Embedded Systems: With C and GNU Development Tools. Publisher: O'Reilly Media.

2. Tanenbaum, A. S. (2014). Modern Operating Systems. Publisher: Pearson Education.
3. Tanenbaum, A. S. (2013). Structured Computer Organization. 6th Edition. Publisher: Pearson.
4. Ünsalan, C., Gürhan, H. D., & Yücel, M. E. (2022). Embedded System Design with ARM Cortex-M Microcontrollers: Applications with C, C++, and MicroPython.
5. Wolf, W. (2017). Computers as Components: Principles of Embedded Computing System Design. Fourth Edition. Morgan Kaufmann Series in Computer Architecture and Design.
6. Modern Embedded Systems Programming Course (https://github.com/QuantumLeaps/modern-embedded-programming-course)
7. STM32 32-bit Arm Cortex MCUs (https://www.st.com/en/microcontrollers-microprocessors/stm32-32-bit-arm-cortex-mcus.html)
8. FreeRTOS™ Real-time operating system for microcontrollers (https://www.freertos.org/index.html)

4.3. Інформаційні ресурси

1. Курс відеолекцій – на платформі дистанційного навчання «Сікорський» в середовищі Google Workspace for Education: https://classroom.google.com/c/ODEzOTA4ODgyMTA0?cjc=apsh5zr5

Обладнання, що необхідне для проведення занять

Лекційні заняття проводяться в аудиторії, яку обладнано проектором, практичні заняття – в комп'ютерному класі. Для проведення лабораторних робіт потрібне наступне обладнання:

- NUCLEO STM32
- Логічний аналізатор
- UART конвертер
- Макетна плата
- Mini USB x2

Навчальний контент

5.Методика опанування навчальної дисципліни (освітнього компонента)

Назви розділів, тем	Кількість годин			
	Всього	У тому числі		
		Лекції	Лабораторні роботи	СРС
Огляд вбудованих систем та їх застосування		2		5
Особливості проектування вбудованих систем		4	2	5
Базові відомості схемотехніки і її застосування при проектуванні вбудованих систем		4		5
Особливості та функціонал CortexM архітектури		2		5
Фреймворки для вбудованих систем та їх особливості (FreeRTOS, QP, ThreadX)		4	2	6
Основні компоненти програмного та апартаного забезпечення та їх особливості		2	2	6
Типи та основні принципи кібератак на вбудовані систем.		4	4	5
Безпека програмного забезпечення і апаратного забезпечення.		4	2	5
Вразливості вбудованих систем		2	2	6
Вектори кібератак на вбудовані системи		4	2	6
Криптографія та захист даних		2	2	6
Зворотня інженерія		2		6
Всього в семестрі:	**120**	**36**	**18**	**66**

Лабораторні заняття:

Метою проведення лабораторних занять є набуття студентами необхідних практичних навичок для побудови хмарних комп’ютерних систем.

- Лабораторна робота №1:
  Використання STMCube IDE, аналіз коду та виконання вбудованих систем
- Лабораторна робота №2:
  Застосування захисних механізмів на STM32 мікропроцесорах
- Лабораторна робота №3:
  Аналіз, пошук та виправлення основних вразливостей вбудованих систем
- Лабораторна робота №4:
  Застосування та захист від атак перехоплення контролю
- Лабораторна робота №5:
  Застосування та захист від атак викрадення даних та відмови від обслоговування
- Лабораторна робота №6:
  Застосування криптографії та інших механізмів для захисту чутливої інформації

6.Самостійна робота студента

- підготовка до лекцій
- підготовка до практичних занять
- підготовка до заліку

Політика та контроль

7.Політика навчальної дисципліни (освітнього компонента)

Під час занять з навчальної дисципліни «Вбудовані системи: застосунки і безпека» студенти повинні дотримуватись певних дисциплінарних правил:

- забороняється запізнюватись на заняття;
- не допускаються сторонні розмови або інший шум, що заважає проведенню занять;
- не допускається користування мобільними телефонами та іншими технічними засобами без дозволу викладача.

Перевірка результатів лабораторних робіт включає перевірку протоколу, який студент готує особисто.

Роботи, які здаються із порушенням зазначених термінів без поважних причин, оцінюються на нижчу оцінку.

8.Види контролю та рейтингова система оцінювання результатів навчання (РСО)

для спеціальності: 121 «Інженерія програмного забезпечення»

Розподіл навчального часу за видами занять і завдань з дисципліни згідно з робочим навчальним планом.

Учбовий	Кількість годин за учбовим планом							
Семестр	Усього	Лекції	Практ. заняття	Лаборат. заняття	ДКР	МКР	Самост. робота	залік
2	120	36		18			66	залік
Всього	120	36		18			66	залік

Критерії оцінювання лабораторних робіт наступні:

- своєчасність підготовки протоколу до лабораторного заняття, повнота виконання теоретичного або практичного завдання в протоколі, вчасне його завантаження: 0 – 6 бали;
- коректність функціонування розробленого програмного забезпечення, демонстрація власного репозиторію на GitHub з матеріалами готової лабораторної роботи: 0 – 2 бали;
- опитування за тематикою лабораторної роботи для зарахування практичної частини роботи, захист одержаних в роботі результатів, відповіді на додаткові теоретичні запитання викладача: 0 – 2 балів.

Поточний контроль: опитування за темою заняття

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

Семестровий контроль: залік

Умови допуску до семестрового контролю: зарахування усіх лабораторних робіт

Оцінювання окремих видів виконаної студентом навчальної роботи – лабораторних робіт здійснюється в балах за 100 бальною шкалою. Загальний рейтинг студента з кредитного модуля складається з середнього балу за всі виконані лабораторні роботи та оцінки за залік.

Табл.1 Відповідність рейтингових балів оцінкам за університетською шкалою

RD	Оцінка ECTS	Традиційна оцінка
95...100	Відмінно	Зараховано
85...94	Дуже добре	Зараховано
75...84	Добре	
65...74	Задовільно	Зараховано
60...64	Достатньо	
$R_C < 60$	Незадовільно	Не зараховано
$R_C \leq 50$ або не виконані інші умови допуску до заліку	Не допущено	Не допущений

9. Додаткова інформація з дисципліни (освітнього компонента)

теоретичні та практичні питання, що виносяться на семестровий контроль, відповідають переліку основних тем, що входять до програми вивчення дисципліни “Вбудовані системи: застосунки і безпека”.

Умова зарахування додаткових балів.

В рамках вивчення навчальної дисципліни допускається зарахування балів, одержаних в результаті

- виконання індивідуального науково-дослідного проєкту за темою дисципліни та умови попереднього погодження напряму дослідження з викладачем та подачі статті про результати дослідження на міжнародну наукову конференцію рівня не нижче IEEE/ACM.

Робочу програму навчальної дисципліни (силабус):

Складено: аспірантом кафедри обчислювальної техніки, Гордієнком Нікітою Юрійовичем

Ухвалено: кафедрою обчислювальної техніки (протокол No 12 від 23.06.2025)

Погоджено: методичною комісією факультету інформатики та обчислювальної техніки (протокол No 11 від 27.06.2025)