СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Комплексні системи захисту інформації»

Ступінь освіти	бакалавр
Освітня програма	Кібербезпека
Тривалість викладання	1, 2 чверть
Заняття:	Осінній семестр
лекції:	3 години
практичні заняття:	2 година
Мова викладання	українська

Кафедра, що викладає Кафедра безпеки інформації та телекомунікацій
https://do.nmu.org.ua/enrol/index.php?id=1525

Кручінін Олександр Володимирович	Старший викладач
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/Kruchinin.php
E-пошта:	Kruchinin.o.v@nmu.one

1. Анотація до курсу

Розглянуто базові принципи функціонування мікропроцесорів та мікроконтролерів. Основну увагу зосереджено на вивченні архітектури 8-розрядних RISC-мікроконтролерів сім'ї PIC MICROCHIP. Детально розглянуті технічні характеристики та систему команд PIC мікроконтролерів, набір периферійних модулів, особливості їх функціонування і програмування. Викладено питання розроблення і налагодження програм мовою асемблера з використанням інтегрованого середовища проектування Proteus. Наведено архітектуру та характеристики захищених мікроконтролерів, призначених для побудови надійних систем захисту інформації.

2. Мета та завдання курсу

Мета дисципліни – ознайомлення з архітектурними характеристиками мікроконтролерів, орієнтованих на виконання функцій керування різними об'єктами, основними поняттями і визначеннями мікропроцесорної техніки, принципами побудови мікроконтролерів, організацією пам'яті, та стеку;

перериваннями складом процесорного ядра, набором і призначенням типових периферійних модулів та вивчення системи команд PIC мікроконтролерів.

Завдання курсу: вивчення дисципліни "Мікропроцесорні системи" є систематизація інформації щодо структури та принципів побудови мікропроцесорів та мікропроцесорних систем, інтерфейси для взаємодії мікропроцесорних систем, методів програмування мікропроцесорів, апаратно-програмного забезпечення систем захисту інформації.

3. Результати навчання

Знати:

- склад та основні характеристики мікроконтролерів сімейства PIC;
- склад, призначення окремих вузлів та роботу типового мікроконтролера сімейства PIC за структурною схемою;
- програмну модель, формати команд та даних, способи адресації операндів та характеристику окремих команд типового мікроконтролера сімейства PIC;
- особливості архітектури окремих функціональних модулів мікроконтролера: пам’яті; паралельних та послідовних інтерфейсів; таймерів/лічильників зовнішніх подій; переривань;
- організацію взаємодії мікроконтролера із типовими об’єктами управління.

Уміти:

- програмувати окремі модулі мікропроцесорних систем на базі мікроконтролера PIC;
- моделювати окремі частини мікропроцесорних систем на персональному комп’ютері;
- проектувати мікропроцесорні пристрої та системи на базі мікроконтролера PIC.

4. Структура курсу

ЛЕКЦІЇ

1. Забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.

1.1 Мікропроцесорні системи з фон-неймановською (прінстонською) і гарвардською архітектурами.

1.2 Архітектурні характеристики PIC мікроконтролерів та їх система команд.

1.3 Програмна реалізація часових затримок. Складання простих програм.

1.4 Порти вводу/виводу.

2. Забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем.

2.1 Організація переривань в МК PIC 16F84. Переривання по входу RB0/INT та зміні рівня сигналів на одному із контактів RB7…RB4.

2.2 Організація таймерного переривання за допомогою модуля таймера TMR0.

2.3 Пам 'ять данних EEPROM.

2.4 Організація скиду. Робота в режимі SLEEP. Використання сторожового таймеру (WDT).

ПРАКТИЧНІ ЗАНЯТТЯ

1. Забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту.

1.1 Вивчення арифметичних основ МП систем.

1.2 Ознайомлення з роботою МП. Робота з пам'ятю і машинними кодами.

1.3 Вивчення системи команд МК PIC.

2. Забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем.

2.1 Програмне формування часових затримок. Створення проекту в системі PROTEUS.

2.2 Ознайомлення з роботою портів вводу/виводу. Формування сигналів заданої тривалості та періоду на контактах МК.

2.3 Схема управління керованим випрямлячем з динамічною індикацією кута регулювання на МК PIC 16F628 та її дослідження за допомогою ітеративного стимулятора PROTEUS.

2.4 Формування переривання та сигналів заданої тривалості за допомогою модуля таймера.

5. Система оцінювання та вимоги

5.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
75-89	добре
60-74	задовільно
0-59	незадовільно

5.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
66	30	20	4	**100**

Теоретична частина оцінюється за результатами здачі контрольної тестової роботи, яка містить 20 запитань, з яких 17 – прості тести (1 правильна відповідь), 3 задачі.

5.3. Критерії оцінювання підсумкової роботи

25 тестових завдань з чотирма варіантами відповідей, **1** правильна відповідь оцінюється у **3 бали (разом 51 бал)**. Опитування за тестом проводиться з використанням технології Microsoft Forms Office 365.

Задачі наводяться також у системі Microsoft Forms Office 365. Вирішена на папері задача сканується (фотографується) та відсилається на електронну пошту викладача впродовж часу, відведеного на здачу теоретичної частини. Несвоєчасно вислана відповідь враховується такою, що не здана.

Правильно вирішена **задача** оцінюється в 5 балів, причому:

– **5 балів** – відповідність еталону, з одиницями виміру;

– **4 бали** – відповідність еталону, без одиниць виміру або помилками в розрахунках;
– **3 бали** – незначні помилки у формулах, без одиниць виміру;
– **2 бали** – присутні суттєві помилки у рішенні;
– **1 бал** – наведені формули повністю не відповідають еталону;
– **0 балів –** рішення не наведене.

5.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує 5 запитань з переліку контрольних запитань. Кількість вірних відповідей визначають кількість отриманих балів.

6. Політика курсу

6.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

6.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

6.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

6.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

6.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

6.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освітим буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни «**Мікропроцесорні системи**». За участь у анкетуванні здобувач вищої освіти отримує **4 бали**.

7 Рекомендовані джерела інформації

7.1. Основні

1. Хорошко В. О. та ін Проектування комплексних систем захисту інформації - Л.: Львівська політехніка, 2020. - 320с
2. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин, 2019. – 144 с.
3. Комплексні системи захисту інформації : навчальний посібник /[Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] –Вінниця : ВНТУ, 2018. – 118 с.
4. Комплексні системи захисту інформації: конспект лекцій/ Ю.І. Хлапонін. -Київ: КНУБА, 2022. – 84 с.

7.2. Нормативна

1. Закон України „Про Державну службу спеціального зв’язку та захисту інформації України”.
2. Закон України „Про інформацію”.
3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”.
4. Закон України „Про основні засади державного нагляду (контролю) у сфері господарської діяльності”.
5. Закон України „Про наукову і науково-технічну експертизу”.
6. Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.
7. Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України. Указ Президента України від 30.06.2011 № 717/2011.
8. Концепція технічного захисту інформації в Україні. Постанова КМ України від 08.10.1997 № 1126.
9. Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.
10. Положення про державний контроль за станом технічного захисту інформації. Наказ Адміністрації Держспецзв’язку від 16.05.2007 № 87, зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052.
11. Перелік обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних. Постанова КМ України від 04.02.1998 № 121.
12. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Постанова КМ України від 16.02.1998 № 180.
13. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Постанова КМ України від 16.11.2002 № 1772.
14. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМ України від 29.03.2006 № 373.
15. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
16. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

17. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
18. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
19. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
20. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
21. ДСТУ 1.5:2003 Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.
22. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
23. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
24. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
25. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53.
26. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215
27. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
28. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
29. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
30. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 20.12.2000 № 60.
31. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
32. НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБ України від 13.12.2002 № 84.
33. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.
34. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95), затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25.

35. НД ТЗІ 2.7-011-2012 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.
36. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95), затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.1995 № 25.
37. Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв’язку від 26.03.2007 № 45, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587.
38. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ Адміністрації Держспецзв’язку від 02.12.2014 № 660 зареєстрований в Міністерстві юстиції Українит28 січня 2015 р. за № 90/26535.
39. Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв’язку від16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087 із змінами, затвердженими наказом Адміністрації Держспецзв’язку від 10.10.2012 № 567, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175.
40. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджене наказом ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрованим в Міністерстві юстиції України 13.03.2002 за № 245/6533.
41. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України. Постанова КМ України від 16 листопада 2016 р. № 821
42. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Наказ ДСТСЗІ СБ України від 23.02.2002 № 9, зареєстрований в Міністерстві юстиції України 13.03.2002 за №245/6533.
43. Ліцензійні умови провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України Затверджена Постановою КМ України від 16 листопада 2016 р. № 821
44. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.
45. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
46. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
47. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію. Постанова КМ України від 19 жовтня 2016 р. № 736.

7.3. Допоміжні

1. ."Безпека інформаційно-комунікаційних систем" в галузі знань "Інформаційна безпека". Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко, 2015. – 449 с.
2. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. К. ДУТ. 2020 – 126 с.
3. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2018. – 476 с.
4. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.

7.4. Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації України. – Спосіб доступу: URL: https://cip.gov.ua. – Нормативні документи
2. Верховна Рада України. – Спосіб доступу: URL: rada.gov.ua. – Нормативні документи