МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ МІКРОПРОЦЕСОРНИХ СИСТЕМ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки
та інформаційних технологій *Ольга СТАРКОВА*

Харків
2022

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та інформаційних технологій
Протокол № 8 від 24.12.2022 р.

Розробники:
Лимаренко В.В., к.т.н., доц. кафедри кібербезпеки та інформаційних технологій

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Предметом вивчення дисципліни є принципи функціонування мікропроцесорних систем та методи проектування мікропроцесорних систем на основі мікроконтролерів.

Мікропроцесорна техніка – область електроніки, яка на даному етапі найшвидше розвивається. Для успішного оволодіння нею необхідно із самого початку засвоїти сучасні принципи організації мікропроцесорних систем. Засвоєння ключових понять мікропроцесорної техніки – це основне завдання курсу. Успіх при цьому може принести тільки комплексний підхід до проектування апаратних та програмних засобів. Розглядаються особливості систем різних рівнів складності та різноманітного призначення, принципи архітектурних рішень, способи та засоби організації обміну інформацією. Особливу увагу приділено принципам організації сучасних розподілених мікропроцесорних систем, та забезпечення безпеки даних систем при різноманітних спробах атаки на них.

Об'єктами вивчення виступають знання про проектування мікропроцесорних систем, підключення пристроїв мікропроцесорних систем для збору даних та контролю фізичного світу, методи візуалізації даних, управління наборами даних, як одним з типів інтелектуальних інформаційних систем та інструментальні засоби для розробки мікропроцесорних систем.

Мета навчальної дисципліни «Основи побудови та захисту мікропроцесорних систем» – сформувати системне базове уявлення, первинні знання, вміння і технічні та програмні навички студентів, що необхідні для генерації ідей, проектування, прототипування та представлення бізнес-рішень в галузі мікропроцесорної техніки, надати навички проектування систем на основі мікроконтролерів, як найрозповсюдженішого типу мікропроцесорних систем.

Завданнями навчальної дисципліни є надбання вміння і навичок з проектування, прототипування, налаштування та тестування мікропроцесорних систем, створення програмного забезпечення для мікропроцесорних систем, обробки масивів даних в мікропроцесорних системах.

Для її реалізації наводяться описи мікроконтролерів сімейства AVR, а також спеціальних програмних засобів проектування, розглядаються приклади рішення задач проектування практичних пристроїв. Передбачається, що більшість понять, які введені в даному курсі, стануть предметом детальнішого розгляду в інших, спеціальних курсах.

Результатами вивчення даної дисципліни є придбання навичок з використання функціональних елементів мікропроцесорних систем та мікроконтролерів в електронних системах та принципів захисту мікропроцесорних систем різноманітного призначення від сучасних загроз та інцидентів.

Характеристика навчальної дисципліни

Курс	**2**
Семестр	**4**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Фізичні основи технічних засобів розвідки	Виробнича практика

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з	РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних

встановленою політикою інформаційної та/або кібербезпеки	
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
КЗ 2. Знання та розуміння предметної області та розуміння професії. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних	РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент

комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
КЗ 1. Здатність застосовувати знання у практичних ситуаціях.	РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) система
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 6. Здатність відновлювати штатне функціонування інформаційних,	РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах

інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою	РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації

реалізації встановленої політики інформаційної та/або кібербезпеки КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 8. Здатність здійснювати процедури управління інцидентами,	РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз

проводити розслідування, надавати їм оцінку. КФ 11. Здатність виконувати моніторингпроцесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	

Програма навчальної дисципліни

Змістовий модуль 1. Принципи проектування мікропроцесорних систем

Тема 1. Введення в дисципліну. Відомі сімейства сучасних мікроконтролерів, їх архітектура і особливості. Основи конструювання МК пристроїв.

Тема 2. Мікроконтролери сімейства AVR. Загальна структура AVR мікроконтролерів. Система команд мікроконтролерів AVR. Налагоджувальні плати.

Тема 3. Налагоджувальна плата на базі МК AVR ATmega328. Порти I/O. Робота з цифровими і аналоговими сигналами, ШІМ.

Тема 4. Змінні та константи, їх особливості. Математичні оператори. Передача та прийом даних між комп'ютером та Arduino через COM порт.

Тема 5. Умовні оператори, оператори вибору. Робота з часовими інтервалами на МК.

Тема 6. Масиви, одно- та багатовимірні масиви даних. Цикли.

Змістовий модуль 2. Принципи передачі та захисту даних в мікропроцесорних системах

Тема 7. Інтерфейси передачі даних. UART, SPI, I2C.

Тема 8. Бездротова передача даних. IrDA, Bluetooth.

Тема 9. Бездротова передача даних. RFID, NFC.

Тема 10. Бездротова передача даних. Радіомодулі 433 МГц, 2,44 ГГц.

Тема 11. Бездротова передача даних. WiFi.

Тема 12. Безпека даних в мікроконтролерних системах.

Перелік лабораторних занять, а також питань та завдань для самостійної роботи наведено у таблиці «Рейтинг-план навчальної дисципліни».

Методи навчання та викладання

Викладання дисципліни передбачає залучення пояснювально-ілюстративного, репродуктивного, дослідницького методів, а також методів проблемного навчання. Так під час проведення лекційних занять викладач надає здобувачам певний обсяг теоретичного матеріалу (теми 1-12), приклади побудови та методів захисту сучасних мікропроцесорних систем (теми 1-12), з наданням пояснень у графічному вигляді (схеми, таблиці, презентації) та за допомогою прикладів конкретної реалізації мікропроцесорних систем (теми 1-12). На лабораторних заняттях здобувачі мають змогу отримати практичні навички пошуку вирішення проблем на підставі вихідних даних, сформульованих за тематикою заняття (роботи 1-12). Вдосконалення практичних навичок відбувається під час виконання самостійної роботи (теми 1-12).

Наведені методи навчання спрямовані на формування у здобувачів здатності розв’язання складних комплексних задач з розробки сучасних мікропроцесорних систем.

Порядок оцінювання результатів навчання

ХНЕУ ім. С. Кузнеця використовує накопичувальну (100-бальну) систему оцінювання. Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні заняття, а також виконання самостійної роботи.

Контрольні заходи включають: поточний контроль, що здійснюється протягом семестру під час проведення лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що надає студенту можливість отримати залік, – 60 балів);

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лабораторних занять проводиться за такими критеріями:

– вміння розуміти та пояснювати поняття, можливості та проблеми сучасних мікропроцесорних систем;

– вміння розробляти та моделювати структуру мікропроцесорних систем з використанням інструментів моделювання;

– вміння проектувати та створювати прототипи мікропроцесорних систем з використанням електроніки, мікроконтролерів, сучасних сімейств мікропроцесорів та одноплатних комп'ютерів;

– вміння аналізувати структуру та технічний склад мікропроцесорних систем різного призначення;

– вміння використовувати засоби проектування, для створення структури мікропроцесорних систем різного призначення;

– вміння працювати в команді і застосовувати підхід до проектування, орієнтований на користувача («дизайнерське мислення»), щоб швидко розробити прототип, ітеративно вдосконалити та викласти бізнес-ідею для рішення завдань створення мікропроцесорних систем різного призначення.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: в технологічній карті бали на цей вид робіт не виділені.

Лабораторні заняття: максимальна кількість балів становить 100 (виконання та захист лабораторних робіт), а мінімальна – 60.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями, в технологічній карті бали на цей вид робіт не виділені.

Підсумковий контроль: проводиться у вигляді заліку. Максимальна кількість балів становить 100. Мінімальна умова допуску до заліку – отримання мінімального балу за лабораторні роботи (60). В разі невиконання плану лабораторних робіт студент вважається не атестованим.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі сумування оцінок за всі види контролю, які мали місце протягом семестру. Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у

балах за семестр складає: «60 і більше балів – зараховано», «59 і менше балів – не зараховано» та заноситься у залікову «Відомість обліку успішності» навчальної дисципліни.

Форми оцінювання та розподіл балів наведено у таблиці «Рейтинг-план навчальної дисципліни».

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Проблемна лекція	Введення в дисципліну. Відомі сімейства сучасних мікроконтролерів, їх архітектура і особливості. Основи конструювання МК пристроїв	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №1. Ознайомлення з інструментами розробника для МК AVR	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Проблемна лекція	Мікроконтролери сімейства AVR. Загальна структура AVR мікроконтролерів. Система команд мікроконтролерів AVR. Налагоджувальні плати.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №2. Порти I/O МК AVR ATmega328. Робота портів I/O в цифровому і аналоговому режимах. ШІМ.	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Проблемна лекція	Налагоджувальна плата на базі МК AVR ATmega328. Порти I/O. Робота з цифровими і аналоговими сигналами, ШІМ	Робота на лекції	

	Лабораторне заняття	Лабораторна робота №3. Функції роботи з часом, використання тактових кнопок	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Проблемна лекція	Змінні та константи, їх особливості. Математичні оператори. Передача та прийом даних між комп'ютером та Arduino через COM порт.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №4. Робота з датчиками. Передача даних через послідовний порт. Виведення даних на монітор комп’ютера	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Проблемна лекція	Умовні оператори, оператори вибору. Робота з часовими інтервалами на МК.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №5. Робота з рідкокристалічними індикаторами LCD 1602 по паралельному інтерфейсу і інтерфейсу I2C	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 6	***Аудиторна робота***			
	Проблемна лекція	Масиви, одно- та багатовимірні масиви даних. Цикли.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №6. Робота з 7-сегментним індикатором. Дисплеї на базі драйвера TM1637	Виконання та захист лабораторної роботи	8
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Проблемна лекція	Інтерфейси передачі даних. UART, SPI, I2C.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №7. Протоколи передачі даних. Передача даних з використанням різних протоколів між мікроконтролерами	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Проблемна лекція	Бездротова передача даних. IrDA, Bluetooth.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №8. Бездротові протоколи передачі даних. IrDA, Bluetooth	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 9	***Аудиторна робота***			
	Проблемна лекція	Бездротова передача даних. RFID, NFC.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №9. Бездротові протоколи передачі даних. RFID та NFC	Виконання та захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тем	***Аудиторна робота***			
	Проблемна лекція	Бездротова передача даних. Радіомодулі 433 МГц, 2,44 ГГц.	Робота на лекції	

Тема 10	Лабораторне заняття	Лабораторна робота №10. Бездротові протоколи передачі даних. Радіомодулі 433 МГц	Виконання та захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 11	***Аудиторна робота***			
	Проблемна лекція	Бездротова передача даних. WiFi.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №11. Матрична мембранна клавіатура	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 12	***Аудиторна робота***			
	Проблемна лекція	Безпека даних в мікроконтролерних системах.	Робота на лекції	
	Лабораторне заняття	Лабораторна робота №12. Крокові двигуни. Драйвери двигунів	Виконання та захист лабораторної роботи	8
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Загалом				100

Рекомендована література

Основна

1. Белов А.В. Мікроконтролери AVR: від азів програмування до створення практичних пристроїв / А.В. Белов. – К. : Наука і Техніка, 2019. – 544 с.

2. Белов А.В. Програмування мікроконтролерів для початківців і не тільки / А.В. Белов. – К. : Наука і Техніка, 2018. – 352 с.

3. Williams Elliot. AVR Programming: Learning to Write Software for Hardware (Make: Technology on Your Time) / Williams Elliot. – Make Community, LLC, 2019. – 472 p.p.

4. Sepehr Naimi. The AVR Microcontroller and Embedded Systems Using Assembly and C: Using Arduino Uno and Atmel Studio / Sepehr Naimi. – MicroDigitalEd, 2020. – 537 p.p.

5. Hughes J. M. Arduino: A Technical Reference: A Handbook for Technicians, Engineers, and Makers / J. M. Hughes. – O'Reilly Media, 2021. – 1125 p.p.

6. Jeremy Blum. Exploring Arduino: Tools and Techniques for Engineering Wizardry / Jeremy Blum. – Wiley, 2019. – 478 p.p.

Додаткова

1. Vibhav Kumar Sachan. Digital Electronics & Microprocessor: Principle, Design and Programing / Vibhav Kumar Sachan. – O'Reilly Media, 2019. – 473 pp.

2. Uwe Meyer-Baese. Embedded Microprocessor System Design using FPGAs / Uwe Meyer-Baese. – Springer, 2021. – 525 pp.

3. David A. Patterson.Computer Organization and Design RISC-V Edition: The Hardware Software Interface (The Morgan Kaufmann Series in Computer Architecture and Design) / David A. Patterson, John L. Hennessy. – O'Reilly Media, 2020. – 736 pp.

Інформаційні ресурси

1. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною «Основи побудови та захисту мікропроцесорних систем» https://pns.hneu.edu.ua/course/view.php?id=8481