СИЛАБУС ДИСЦИПЛІНИ «КОМПОНЕНТНА БАЗА ТА СХЕМОТЕХНІКА В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ (частина 1)»

Ступінь вищої освіти – Бакалавр
Спеціальність 125 – КІБЕРБЕЗПЕКА
Освітня програма «Кібербезпека»
Рік навчання 2, семестр 3
Форма навчання денна
Кількість кредитів ЄКТС 5
Мова викладання українська

Лектор дисципліни	 **Гусєв Борис Семенович, к.т.н., доцент (портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 5278724 e-mail gusevbs@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК** https://elearn.nubip.edu.ua/course/view.php?id=4023

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає забезпечення базової підготовки здобувачів вищої освіти в галузі теорії проектування апаратних складових комп'ютерів, ознайомлення студентів з логічними основами побудови апаратного забезпечення сучасних комп'ютерів; методами синтезу типових комп'ютерних пристроїв; засобами аналізу і синтезу функціональних операційних елементів та пристроїв сучасної цифрової апаратури; засобами проектування універсальних, функціонально-орієнтованих або спеціалізованих процесорів: методами організації функціонування керуючих пристроїв та операційних автоматів.

Передумови вивчення курсу. Вивчення курсу передбачає, що Ви знаєте основні розділи курсу «Комп'ютерна логіка»:

- логічні функції;
- запис логічних функцій у вигляді ДДНФ, ДКНФ;
- алгебри логіки: алгебри Буля, Шефера, Пірса;
- закони і аксіоматику зазначених вище алгебр;
- мінімізація логічних функцій від двох до шести змінних за допомогою карт Карно;
- мінімізація недовизначених логічних функцій;
- перетворення логічних виразів в базиси Шефера, Пірса;
- перетворення логічних виразів в базиси Шефера, Пірса з урахуванням обмежень на кількість входів логічних елементів.

Компетентності ОП:

Інтегральна компетентність (ІК): Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

СК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК 13. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

Програмні результати навчання (ПРН) ОП:

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення

ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН 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.

ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 56. Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для систем захисту інформації.

СТРУКТУРА КУРСУ

Тема	**Години** (лекції/ лабораторні,)	Результати навчання	Завдання	Оцінювання
Модуль 1. Асинхронні і синхронні однотактові тригерні схеми (ТС)				
Тема 1. Об'єкт, предмет, зміст, завдання та структура курсу. Асинхронні тригерні схеми	**6/6**	ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПРН 18. Використовувати програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 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. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**50**
Тема 2. RS-тригери з комбінованим керуванням	**4/4**			**30**
Тема 3. Синхронні однотактові тригерні схеми	**4/4**			**20**

		використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 56. Вміти застосовувати знання для розв'язування задач аналізу та синтезу цифрових пристроїв, характерних для систем захисту інформації.		
Модуль 2. Двотактні ТС і ТС з динамічним керуванням. Регістри.				
Тема 1. Двотактові ТС	**6/6**	ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення ПРН 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. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 56. Вміти застосовувати знання для розв'язування задач аналізу та синтезу цифрових пристроїв, характерних для систем захисту інформації.	1. Підготовка до лабораторної роботи. 2. Виконання лабораторної роботи. 3. Захист звітів з лабораторної роботи.	**40**
Тема 2. ТС з динамічним керуванням	**2/2**			**10**
Тема 3. Синтез ТС на базі ТС	**2/4**			**10**
Тема 4. Синтез регістрових схем на базі тригерів	**6/4**			**40**

Всього за семестр		**0,7*(100 +100)/2 = 70**
Залік	**Тест**	**30**
Всього за курс		**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. Роботи, які здаються з порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається з дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. з використанням мобільних пристроїв).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету)

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	відмінно	зараховано
74-89	добре	
60-73	задовільно	
0-59	незадовільно	не зараховано

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна

1. Методичні вказівки щодо організації самостійної роботи студентів при виконанні контрольних робіт та індивідуальних завдань з курсів «Комп'ютерна схемотехніка» і «Компонентна база та схемотехніка в системах захисту інформації» / Укл. Б.С.Гусєв. - Київ, НУБіП, 2021, 61с.
https://drive.google.com/file/d/1FrWdulXmgoYgb8w4yYxvqvXUYcsvLSLH/view?usp=sharing
2. Методичні вказівки до виконання лабораторних робіт з курсу « Комп'ютерна схемотехніка » і «Компонентна база та схемотехніка в системах захисту інформації» з використанням навчально-лабораторних стендів TRIGGER і LOGIC (частина 1) / Укладач Б.С.Гусєв. – Київ, НУБіП, 2022, 114с.
https://drive.google.com/file/d/18-FZZEo-IlIa8s9MoHUoXiYbHXXIPSHk/view?usp=sharing
3. Методичні вказівки до виконання лабораторних робіт з курсу «Комп'ютерна схемотехніка» з використанням навчально-лабораторних стендів TRIGGER і LOGIC (частина 2) / Укл. Б.С.Гусєв. – Київ, НУБіП, 2022, 115с.
https://drive.google.com/file/d/1b1XtcPJnbmCdqa0EwSUhI5k5Rw0vp-qM/view?usp=sharing
4. Методичні вказівки до виконання курсового проєкту з курсів «Комп'ютерна схемотехніка» і «Компонентна база та схемотехніка в системах захисту інформації». – Київ, НУБіП, 2022, 55с.
https://drive.google.com/file/d/1-1KQpowEX9k-TFZkP9fkM9VrgosMlygu/view?usp=sharing
5. Конспект лекцій з курсів «Комп'ютерна схемотехніка», «Компонентна база та схемотехніка в системах захисту інформації» / Укладач Б.С.Гусєв. – Київ, НУБіП, 2019, 88с.
https://drive.google.com/file/d/1dTxg_SO56O2YIwU9XozfoZP8VKNdwHe8/view?usp=sharing

Допоміжна

1. Комп’ютерна логіка та схемотехніка [навчальний посібник] / В.В.Лапко, Б.С.Гусєв, Д.Ю. Касаткін, В.В. Смолій, А.І. Блозва, Т.Ю. Осипова, Ю.В. Матус, Я.А. Савицька // - К.: НУБіП України, 2017.- 291с.
2. Бабич М.П., Жуков І.А. Комп'ютерна схемотехніка. Підручник для ВУЗів МК-Пресс 412с. 2004р.
3. Жабін В.І., Жуков І.А., Клименко І.А., Ткаченко В.В. Прикладна теорія цифрових автоматів. Навчальний посібник. Київ, Національний авіаційний університет, 2007р., 363с.
4. Комп’ютерна схемотехніка (частина 1) [навчальний посібник] / Б.С.Гусєв, Д.Ю. Касаткін, Т.Ю. Осипова // - К.: НУБіП України, 2022.- 264с.
5. https://www.ti.com
6. https://datasheetspdf.com