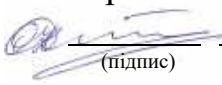
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

(підпис) Олег Ілляшенко (ініціали та прізвище)

« 29 » серпня 2025 р.

СИЛАБУС *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Програмовні засоби безпеки
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека та захист інфомарції"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Рівень вищої освіти: ***перший (бакалаврський)***

Силабус введено в дію з 01.09.2025 року

Харків 2025 рік

Розробник: Куланов В.О., доцент, к.т.н., доцент
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри «Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)

Протокол № 1 від « 29 » серпня 2025 року

Завідувач кафедри д.т.н., професор _____ В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

Погоджено з представником здобувачів освіти:

_____ Ілля МІЦИК
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: *Куланов Віталій Олександрович*

Посада: *доцент кафедри комп'ютерних систем, мереж і кібербезпеки*

Науковий ступінь: *кандидат технічних наук*

Вчене звання: *доцент*

E-mail: v.kulanov@csn.khai.edu

Перелік дисциплін, які викладає: *Програмовні засоби безпеки, Шаблони проєктування та моделювання, Програмування систем на кристалі, Технології захисту медичної інформації.*

Напрями наукових досліджень: *архітектури обчислювальних систем, системи збереження даних, інтернет речей (IoT), хмарні технології, AI/ML*

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна, заочна*
Семестр	*3*
Мова викладання	*Українська*
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС / кількість годин	*Денна: 3,5 кредиту / 105 годин (64 аудиторних, з яких: лекції – 32, лабораторні – 32, СРЗ – 41)* *Заочна: 3,5 кредиту / 105 годин (8 аудиторних, з яких: лекції – 4, лабораторні – 4, СРЗ – 97)*
Види навчальної діяльності	*Лекції, лабораторні заняття, самостійна робота здобувача, розрахунково-графічна робота*
Види контролю	*Поточний контроль, модульний контроль, семестровий контроль – залік*
Пререквізити	*"Комп'ютерна електроніка і схемотехніка", "Дискретна математика", "Основи функціонування комп'ютерів", "Фізика"*

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета: формування фундаментальних знань про цифрову схемотехніку та мікросхеми програмованої логіки як апаратну основу сучасних систем кібербезпеки; набуття практичних навичок синтезу та верифікації цифрових пристроїв, що застосовуються у складі апаратних засобів захисту інформації.

Завдання: оволодіння принципами побудови та синтезу основних цифрових вузлів – комбінаційної та секвенційної логіки, напівпровідникової пам'яті й ПЛІС – як базових компонентів апаратно-орієнтованих рішень у сфері захисту інформації; отримання практичних навичок проектування та верифікації цифрових схем із використанням сучасних САПР як інструментального середовища розробника апаратних засобів безпеки.

Компетентності, які набуваються:

Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК):

– ЗК1. Здатність застосовувати знання у практичних ситуаціях.

– ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

– ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

– ЗК4. Здатність спілкуватися іноземною мовою.

– ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні компетентності (СК):

– СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

– СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

– СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

– СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

– СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози

інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання (РН):

– РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

– РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

– РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

– РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

– РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

– РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

– РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

– РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

– РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

– РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

– РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

– РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Базові поняття та логічні елементи. Комбінаційна логіка.

Тема 1. Предмет, ціль вивчення й завдання дисципліни. Структура, зміст дисципліни й методичні рекомендації з її вивчення. Місце дисципліни в навчальному процесі.

Анотація: Місце дисципліни в підготовці фахівця з кібербезпеки. Роль цифрової схемотехніки як апаратного фундаменту систем захисту інформації. Огляд еволюції цифрової елементної бази – від дискретних схем до програмованої логіки – у контексті розвитку апаратних засобів безпеки. Характеристика рекомендованих джерел.

Тема лекції 1: Предмет, ціль вивчення й завдання дисципліни. Структура, зміст дисципліни й методичні рекомендації з її вивчення. Місце дисципліни в навчальному процесі.

Самостійна робота здобувача: Аналіз структури та перевірка доступу до ресурсів курсу в системі он-лайн навчання.

Тема 2. Поняття сигналу. Рівні сигналів. Поняття шини. Часові характеристики. Сигнали синхронізації.

Анотація: Цифровий сигнал як основа апаратної обробки даних у системах захисту. Логічні рівні, шини та часові характеристики як параметри надійності та захищеності цифрових інтерфейсів. Сигнали тактування та стробу в контексті синхронізації апаратних криптографічних та захисних модулів.

Тема лекції 2: Поняття сигналу. Рівні сигналів. Поняття шини. Часові характеристики. Сигнали синхронізації.

Самостійна робота здобувача: Ознайомлення з поняттями логічних та електричних сигналів, рівнями сигналів і призначенням шин у цифрових пристроях.

Тема 3. Логічний елемент. Часові діаграми. Особливості побудови та синтезу схем з використанням мікросхем програмовної логіки.

Анотація: Базові логічні елементи як будівельні блоки апаратних модулів безпеки. Синтез комбінаційних схем та мінімізація логічних функцій як основа проектування ефективних апаратних рішень захисту. Таблиці станів та часові діаграми як інструменти верифікації коректності роботи цифрових вузлів. Перший погляд на ПЛІС як платформу реалізації програмованих апаратних засобів безпеки.

Тема лекції 3: Логічний елемент. Часові діаграми. Особливості побудови та синтезу схем з використанням мікросхем програмовної логіки.

Тема лабораторної роботи 1: Знайомство з середовищем пакету Quartus II. Розробка простих проєктних рішень.

Самостійна робота здобувача: Ознайомлення з видами логічних елементів, їх умовно-графічними позначеннями та принципами роботи. Вивчення типів інтегральних мікросхем, аналіз часових діаграм і складання таблиць станів для різних логічних схем.

Тема 4. Комбінаційна та секвенційна логіка. Комбінаційні пристрої. Дешифратори. Шифратори.

Анотація: Шифратори та дешифратори як апаратні компоненти систем розмежування доступу, адресації захищених областей пам'яті та кодування інформації. Шифратор пріоритетів у контексті апаратної обробки переривань та сигналів тривоги в системах безпеки. Синтез та верифікація на платформі ПЛІС.

Тема лекції 4: Комбінаційна та секвенційна логіка. Дешифратори. Шифратори. Класифікація дешифраторів/шифраторів. Приклади застосування.

Тема лабораторної роботи 2: Шифратори. Дешифратори. Знайомство з мегафункціями та бібліотечними елементами пакету Quartus II.

Самостійна робота здобувача: Ознайомлення з видами дешифраторів і шифраторів, їх умовно-графічними позначеннями та принципами роботи. Вивчення таблиці станів і часові діаграми для різних типів дешифраторів/шифраторів, а також дослідження області їх застосування у цифрових пристроях.

Тема 5. Комбінаційні пристрої. Мультиплексори. Демультиплексори.

Анотація: Мультиплексори та демультиплексори як апаратні засоби комутації та маршрутизації захищених інформаційних потоків. Застосування в апаратних схемах вибору каналів передачі даних, реалізації функцій керування доступом та побудові захищених комунікаційних вузлів на ПЛІС.

Тема лекції 5: Мультиплексори. Демультиплексори. Умовно графічні позначення. Схема функціонування. Таблиця станів. Часові діаграми. Логічна формула. Область застосування.

Тема лабораторної роботи 3: Мультиплексори. Демультиплексори.

Самостійна робота здобувача: Ознайомлення з видами мультиплексорів і демультиплексорів. Вивчення таблиці станів, часових діаграм і аналіз області застосування мультиплексорів та демультиплексорів у цифрових пристроях.

Тема 6. Цифрові компаратори. Схеми контролю парності. Мажоритарні елементи.

Анотація: Цифрові компаратори як апаратна основа систем верифікації та автентифікації. Схеми контролю парності як засіб виявлення помилок і апаратного захисту цілісності даних при передачі та зберіганні. Мажоритарні елементи як основа відмовостійких та захищених від збоїв апаратних систем.

Тема лекції 6: Цифрові компаратори. Схеми контролю парності. Мажоритарні елементи.

Самостійна робота здобувача: Ознайомлення з видами цифрових компараторів, схемами контролю парності та мажоритарними елементами, їх умовно-графічними позначеннями й основними принципами роботи.

Тема 7. Суматори. Пристрій віднімання двійкових кодів чисел. Суматори двійково-десяткових кодів. Помножувачі двійкових кодів чисел. Арифметико-логічний пристрій.

Анотація: Суматори, множники та АЛП як апаратна основа криптографічних обчислень – модульної арифметики, хешування та операцій у скінченних полях. Архітектурні рішення АЛП у контексті продуктивності та захищеності апаратних криптографічних прискорювачів, що реалізуються на ПЛІС.

Тема лекції 7: Суматори. Пристрій віднімання двійкових кодів чисел. Суматори двійково-десяткових кодів. Помножувачі двійкових кодів чисел.

Тема лекції 8: Арифметико-логічний пристрій. Архітектури АЛП в складі сучасних архітектур обчислювачів.

Тема лабораторної роботи 4: Арифметико-логічні пристрої. Синтез АЛП

Самостійна робота здобувача: Відпрацювання матеріалів лекції. Аналіз побудови сучасних архітектур обчислювальних пристроїв з використанням АЛП.

Модульний контроль 1.

МОДУЛЬ 2
Змістовний модуль 2. Секвенційна логіка та напівпровідникова пам'ять.

Тема 8. Тригери. Класифікація тригерів. Типи тригерів. Синтез тригерів. Скінченні автомати. Синтез автоматів Мілі та Мура

Анотація: Тригери як елементна база апаратних генераторів псевдовипадкових послідовностей, регістрів зсуву та схем синхронізації в системах безпеки. Скінченні автомати як формальна модель для проектування апаратних протоколів автентифікації, керування доступом та детекторів аномальних станів на ПЛІС.

Тема лекції 9: Тригери. Класифікація тригерів. Типи тригерів. Синтез тригерів.

Тема лекції 10: Скінченні автомати. Синтез автоматів Мілі та Мура.

Тема лабораторної роботи 5: Тригери. Скінченні автомати. Синтез.

Самостійна робота здобувача: Ознайомлення з класифікацією та видами тригерів, аналіз їх принципи функціонування, а також часових діаграм і таблиць станів. Аналіз застосування тригерів у сучасних цифрових пристроях, використовуючи знання, отримані під час лекції та лабораторної роботи.

Тема 9. Регістри. Класифікація та основні типи регістрів. Застосування. Лічильник Джонсона. Кільцевий лічильник.

Анотація: Регістри зсуву як апаратна основа потокових шифрів та генераторів псевдовипадкових послідовностей (LFSR). Паралельні та послідовні регістри в архітектурі апаратних криптографічних модулів. Регістри послідовного наближення в системах захищеного аналого-цифрового перетворення. Кільцеві структури як апаратні генератори часових міток та лічильники подій у системах моніторингу безпеки.

Тема лекції 11: Регістри. Класифікація та основні типи регістрів. Застосування. Лічильник Джонсона. Кільцевий лічильник

Тема лабораторної роботи 6: Регістри. Синтез регістрів.

Самостійна робота здобувача: Ознайомлення з класифікацією та видами регістрів, аналіз їх принципів функціонування, а також часових діаграм і умовно графічних позначень. Аналіз застосування регістрів у сучасних цифрових пристроях із використанням знань, отриманих під час лекції та лабораторної роботи.

Тема 10. Лічильники. Загальна класифікація та типи лічильників. Принципи функціонування. Умовно графічні позначення. Часові діаграми. Синтез лічильників.

Анотація: Лічильники як апаратні компоненти систем аудиту та моніторингу подій безпеки, схем антиреплей-захисту та генераторів одноразових кодів. Дільники частоти в задачах синхронізації та тактування захищених комунікаційних інтерфейсів. Синтез лічильників із керованим модулем рахунку на ПЛІС для задач апаратного контролю доступу.

Тема лекції 12: Лічильники. Загальна класифікація та типи лічильників. Принципи функціонування. Умовно графічні позначення. Часові діаграми. Синтез лічильників

Тема лабораторної роботи 7: Лічильник. Синтез лічильників.

Самостійна робота здобувача: Аналіз різновидів та класифікації лічильників, принципів їх функціонування, часових діаграм і таблиць роботи. Ознайомлення із застосуванням лічильників у сучасних цифрових пристроях на основі матеріалу лекції та лабораторної роботи.

Тема 11. Пам'ять. Класифікація та структурна організація напівпровідникових запам’ятовуючих пристроїв. ПЗП, ОЗП, ППЗП. Динамічні та статичні напівпровідникові запам’ятовуючі пристрої.

Анотація: Напівпровідникова пам'ять як критичний компонент систем захисту інформації: порівняння типів з точки зору захищеності, енергозалежності та стійкості до несанкціонованого зчитування. Flash та EEPROM як носії ключового матеріалу та захищених завантажувачів. FIFO та LIFO в апаратних буферах захищеного обміну даними. Архітектура пам'яті ПЛІС як середовища зберігання конфігурацій та секретних параметрів.

Тема лекції 13: Пам'ять. Класифікація та структурна організація напівпровідникових запам’ятовуючих пристроїв. Статична та динамічна пам’ять.

Тема лекції 14: Архітектура сучасної напівпровідникової пам’яті. Архітектура 2D, 3D, 2DM. Нарощування розрядності. Архітектура модулів пам’яті.

Тема лекції 15: Багатопортова пам’ять. Пам'ять типу FIFO (черга) та LIFO (стек). Загальна структура, функціональне призначення.

Тема лабораторної роботи 8: Напівпровідникова пам’ять. Моделювання архітектури напівпровідникової пам’яті різних типів.

Самостійна робота здобувача: Ознайомлення з класифікацією та структурною організацією напівпровідникових запам’ятовуючих пристроїв, а

також аналіз їх типів і різновидів, часові характеристики та принципи функціонування.

Тема 12. Програмовні логічні інтегральні схеми. Історія розвитку мікросхем програмованої логіки. Класифікація ПЛІС. Загальна структура мікросхем програмованої логіки. Структура мікросхем FPGA, CPLD.

Анотація: ПЛІС як сучасна платформа реалізації апаратних засобів безпеки: від вбудованих криптографічних модулів до апаратних міжмережевих екранів та систем виявлення вторгнень. Порівняння архітектур FPGA та CPLD з позицій захищеності, гнучкості переконфігурування та стійкості до апаратних атак. Огляд провідних виробників та їх продуктових ліній, що застосовуються в сертифікованих засобах захисту інформації.

Тема лекції 16: Програмовні логічні інтегральні схеми. Історія розвитку мікросхем програмованої логіки. Класифікація ПЛІС. Загальна структура мікросхем програмованої логіки. Структура мікросхем FPGA, CPLD

Самостійна робота здобувача: Детальне опрацювання теоретичного матеріалу за темою, самостійний розгляд принципів побудови та функціонування ПЛІС класу FPGA.

Модульний контроль 2

5. Індивідуальні завдання

Виконання РГР за темою "Синтез скінченних автоматів Мілі та Мура відповідно до наданого графу переходів"

6. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів курсу (п.14, 15).

7. Методи контролю

Проведення поточного контролю, модульного контролю, електронного тестування, підсумкового контролю у вигляді іспиту.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Виконання і захист лабораторних робіт	0…9	4	0…36
Модульний контроль	0…10	1	0…10
Змістовний модуль 2			
Виконання і захист лабораторних робіт	0...9	4	0…36
Модульний контроль	0…10	1	0…10
Розрахунково-графічна робота	0...8	1	0…8
Усього за семестр			**0…100**

Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань складає 30 балів за відповідь за кожне теоретичне питання та 40 балів за практичне.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Виконати та захистити 75% лабораторних робіт та пройти 100% тестових завдань. Вміти аналізувати вимоги щодо проектування елементів/вузлів комп'ютерних обчислювальних систем. Вміти чітко визначати тип логіки що застосовується для розв'язання певного коло задач. Володіти знаннями в галузі існуючих методів, програмно-технічних засобів які використовуються в процесі проектування обчислювальних вузлів комп'ютерних систем.

Добре (75-89). Володіти необхідним мінімумом знань в галузі проектування комп'ютерних систем з використанням елементної бази ПЛІС. Об'єм знань має бути достатніми для самостійного розв'язання задач середньої складності. Виконати та захистити 85% лабораторних робіт та пройти 100% тестових завдань. Вільно володіти програмно-технічними та інструментальними засобами розроблення обчислювальних вузлів комп'ютерних систем, їх тестування та імплементація з використанням

елементної бази ПЛІС. Розв'язувати завдання на високому рівні з використанням сучасних підходів до проектування та загальних рекомендацій.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконало володіти темами та вміти застосовувати на практиці отриманні знання. Допомагати одногрупникам в процесі оволодінням знаннями в рамках дисципліни.

Таблиця 8.2 – Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

9. Політика навчального курсу

Відвідування занять. Інтерактивний характер курсу передбачає обов'язкове відвідування лабораторних занять. Здобувачі освіти, які за певних обставин не можуть відвідувати лабораторні заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувачі освіти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки та у системі дистанційного навчання «Ментор».

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://elearn.csn.khai.edu
2. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=3719

11. Рекомендована література

Базова

1. Матвієнко М. П., Розен В. П. Комп'ютерна схемотехніка. Навчальний посібник. – К.: Видавництво Ліра-К, 2020. – 192 с.
2. Азаров О. Д., Гарнага В. А., Клятченко Я. М., Тарасенко В. П. Комп'ютерна схемотехніка: підручник. – Вінниця: ВНТУ, 2018. – 230 с.
3. Схемотехніка: пристрої цифрової електроніки : електрон. підручник для вищих навчальних закладів Т. 1 / В. М. Рябенький, В. Я. Жуйков, Ю. С. Ямненко, А. В. Заграничний. – Київ : НТУУ КПІ, 2016. – 400 с.
4. Схемотехніка: пристрої цифрової електроніки : електрон. підручник для вищих навчальних закладів Т. 2 / В. М. Рябенький, В. Я. Жуйков, Ю. С. Ямненко, А. В. Заграничний. – Київ : НТУУ КПІ, 2016. – 358 с.

Допоміжна

1. Строкань О.В, Прийма С.М., Литвин Ю.О. Комп'ютерна схемотехніка та архітектура комп'ютерів: лабораторний практикум. – Мелітополь, 2019. – 186 с.
2. Основи прикладної теорії цифрових автоматів: підручник / І. А. Дичка, В. П. Тарасенко, М. В. Онай ; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 506 с.
3. Комп'ютерна схемотехніка: Навчальний посібник. – Луцьк: РРВ Луцького НТУ, 2016. – 236 с.
4. Paul Horowitz, Winfield Hill. The Art of Electronics 3rd Edition. 2015. – 1225 p. ISBN 978-0-521-80926-9
5. David M. Harris, Sarah L. Harris. Digital Design and Computer Architecture. Elsevier Inc. 2012. – 1684 p.
6. Introduction to Digital Systems Design. Donzellini Giuliano et all. 2018. Springer Publishing Company, Incorporated. ISBN: 978-3-319-92803-6.
7. A.P. Plakhtyeyev. E.V. Babeshko, V.A. Tkachenko, J.V. Zdorovets. Architectures and Embedded Platform Based development of Internet / Web of Things systems: Laboratory works / V.S. Kharchenko (edit.) - Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", 2019. – 147 p.

12. Інформаційні ресурси

1. Quartus II Web Edition Design Software – [Ел. ресурс]. – Режим доступу: https://www.intel.com/content/www/us/en/software-kit/711791/intel-quartus-ii-web-edition-design-software-version-13-0sp1-for-windows.html

2. ModelSim – Intel FPGA Edition Simulation Quick-Start – [Ел. ресурс]. – Режим доступу: https://cdrdv2-public.intel.com/666396/ug_gs_msa_qii-683248-666396.pdf