Силабус освітнього компонента
Програма навчальної дисципліни

Аналогові та цифрові електронні пристрої

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
1

Мова викладання
Українська

Викладачі, розробники

Погасій Сергій Сергійович

Serhii.Pohasii@khpi.edu.ua
Кандидат економічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Аналогові та цифрові електронні пристрої" є вибірковою навчальною дисципліною. Дисципліна дає загальні відомості про цифрові пристрої та принципи їх роботи, знайомить з основними властивостями їх використання, критеріями вибору елементів при розробки цифрових пристроїв.

Мета та цілі дисципліни

Формування у здобувача компетенцій, що грунтуються на засвоєнні знань про основні електронні компоненти і типові електронні схеми і пристрої, а також засвоєнні умінь і навичок по розробці,

розрахунку і аналізу схем електронних пристроїв. Вивчення матеріалу даної дисципліни орієнтовано на широке застосування обчислювальної техніки.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Організаційне забезпечення засобів інформації.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Безперервне вдосконалення електронних пристроїв та їх сучасна класифікація.
Етапи розвитку електроніки. Класифікація електронних пристроїв.
Тема 2. Принципи функціонування та характеристики напівпровідникових приладів.
Напівпровідникові діоди. Транзистори. Тиристори. Інтегральні схеми. Напівпровідникові датчики та індикаторні прилади.
Тема 3. Розрахунок нелінійних електричних кіл.
Основні поняття та визначення. Методи розрахунку нелінійних ланцюгів. Розрахунок нелінійних ланцюгів постійного, змінного струму, при одночасному впливі джерела постійної і змінної напруги.
Тема 4. Основні властивості аналогових підсилювальних пристроїв.

Загальні відомості класифікація та основні характеристики підсилювача. Математичне опис підсилювальних пристроїв. Частотні властивості. Зворотній зв'язок у підсилювачах. Поняття про стійкість підсилювача.

Тема 5. Схемотехніка підсилювальних пристроїв на біполярних та польових транзисторах.

Підсилювальний каскад за схемою із загальним емітером. Принцип роботи та основні параметри. Підсилювальний каскад за схемою із загальним джерелом. Емітерний і стоковий повторювачі. Джерела постійного струму та напруги. Вихідні підсилювачі потужності. Операційні підсилювачі.

Тема 6. Перетворювачі аналогових сигналів на операційних підсилювачах.

Повторювач напруги. Підсилювач, що інвертує, суматор. Інтегратор, диференціатор. Нелінійні перетворювачі. Джерела струму. Активні фільтри Підсилювачі змінного струму.

Тема 7. Пристрої порівняння аналогових сигналів.

Робота операційного підсилювача при високих амплітудах вхідного сигналу. Однопорогове пристрій порівняння. Регенеративна схема порівняння. Інтегральні компаратори.

Тема 8. Джерела вторинного електроживлення.

Класифікація складу та основні параметри. Перетворювачі змінної напруги в пульсуючу напругу (випрямлячі). Пристрої стабілізації напруги живлення. Керований випрямляч. Пристрої перетворення напруги.

Тема 9. Математичний опис цифрових пристроїв.

Системи числення. Логічні константи та змінні Операції булевої алгебри. Методи запису функцій алгебри логіки. Логічні елементи та схеми Принцип двоїстості. Теореми булевої алгебри. Класифікація логічних пристроїв.

Тема 10. Мінімізація логічних пристроїв.

Цілі мінімізації логічних пристроїв. Загальні засади мінімізації. Комбінаційні логічні устрою.

Тема 11. Послідовні логічні пристрої.

Призначення та класифікація тригерних пристроїв. Одноступінчасті тригери. Двоступінчасті тригери. Тригери з динамічним керуванням. Особливості побудови мікроелектронних тригерів. Реєстри. Лічильники.

Тема 12. Арифметико-логічні пристрої.

Призначення та основні параметри. Суматори. Підвищення швидкодії суматорів. Алгоритм віднімання двійкових чисел. Реалізація операцій арифметичного складання та віднімання. Двійково десяткові суматори. Виконання логічних операцій. Інтегральні схеми АЛП. Виконує операції арифметичного множення.

Тема 13. Базові логічні елементи.

Способи подання логічних змінних електричними сигналами.

Тема 14. Напівпровідникові пристрої, що запам'ятовують.

Призначення, основні параметри та класифікація. Статичні ОЗП на біполярних транзисторах. Статичні ОЗП на польових транзисторах. Динамічні ОЗП. Постійні ЗП (ПЗП).

Тема 15. Логічні пристрої з програмованими характеристиками.

Призначення та сфери застосування. Застосування мультиплексора як універсальний ЛЕ. Узагальнена структурна схема програмованої логічної інтегральної схеми (ПЛІС). Застосування ППЗУ як ПЛІС. Програмована матрична логіка. Програмовані логічні матриці. Базові матричні кристали.

Тема 16. Аналого-цифрові та цифро-аналогові перетворювачі.

Призначення, основні властивості та класифікація. ЦАП із підсумовуванням струмів. АЦП послідовного рахунку. АЦП порозрядного кодування. АЦП паралельного перетворення. АЦП із подвійним інтегруванням. Області застосування АЦП різних типів.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Створення віртуальних приладів у середовищі LabView.

Тема 2. Програмування віртуальних приладів у середовищі LabView.

Тема 3. Дослідження логічних функцій двох змінних.

Тема 4. Дослідження методів мінімізації і синтез комбінаційних пристроїв за заданою логічною функцією.

Тема 5. Дослідження характеристик напівпровідникових діодів і пристрій на їх основі.
Тема 6. Дослідження характеристик тиристора та випрямчувача, що керується.
Тема 7. Дослідження вольтамперної характеристики туннельного діоду.
Тема 8. Дослідження характеристик біполярного транзистора.
Тема 9. Дослідження цифрових комбінаційних пристроїв.
Тема 10. Програмування в середовищі LabViewцифрових портів введення-виведення пристрою збору даних NI myDAQ.
Тема 11. Комбінований віртуальний прилад VIMEL-AC.
Тема 12. Віртуальний прилад VIMEL-GRAF.
Тема 13. Дослідження цифрових мікросхем.
Тема 14. Вивчення пристрою збирання даних на прикладі DAQ плати PCI-6251.
Тема 15. Дослідження логічних пристроїв з запам'ятовуванням.
Тема 16. Аналого-цифрове перетворення сигналу.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт та заліку.

Література та навчальні матеріали

Основна література:

1. Цифрова схемотехніка та архітектура мікропроцесорів: навчальний посібник / Євсеєв С. П., Дженюк Н.В., Охрименко М.Ю. та ін. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 513 с.
2. Жуйков В.Я., Терещенко Т.О., Петергеря Ю.С. і ін «Мікропроцесори і мікроконтролери» - Електронний підручник [Електронний ресурс]. – Режим доступу : http://www.kaf-pe.ntu-kpi.kiev.ua/. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
3. Мікропроцесорна техніка. Друге видання. Доповнене./ Ю.І. Якименко, Т.О. Терещенко, Є.І. Сокол, В.Я. Жуйков, Ю.С. Петергеря. За ред. Т.О. Терещенко. – Київ, 2004. – 440 с.
4. Схемотехніка електронних систем. Том 3. Мікропроцесори та мікроконтролери / Бойко В.І., Гуржій А.М., Жуйков В.Я., Зорі А.А., Петергеря Ю.С., Співак В.М., Терещенко Т.О, Якименко Ю.І. - К.: Вища школа, 2004. – 399 с.:іл.
5. Євсеєв С.П., Смірнов О.А., Король О.Г., Коваленко О.В. Архітектура мікропроцесорів та компонентів ЕОМ. Кіровоград: Вид. Лисенко В.Ф., 2015. – 550 с.

Додаткова література :

1 Мортон Дж. Микроконтроллеры AVR. Вводный курс. -М.: Додэка-XXI, 2006. 4. Трамперт В. Измерение, управление и регулирование с помощью A VR-микроконтроллеров. -Киев: МК-Пресс, 2007.
2. 8-bit AVR Instruction Set Manual [Електронний ресурс]. – Режим доступу : (http://www.atmel.com/images/doc08S6.pdf).
3. Кнут Дональд Э. Искусство программирования. Т. 2. Получисленные алгоритмы. -Киев: Вильяме, 2005.
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- лабораторні роботи: 40% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 10% семестрової оцінки;
- залік: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено

28.08.2023 — Завідувач кафедри — Сергій ЄВСЕЄВ

28.08.2023 — Гарант ОП — Олександр МІЛОВ