|  |
| --- |
| **УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ**  |
|  | **СИЛАБУС** «Проектування засобів захисту інформації на ПЛІС» |

|  |  |
| --- | --- |
| **Статус дисципліни** | Вибіркова |
| **Код та назва спеціальності**  | 125 «Кібербезпека» |
| **Назва освітньої програми** | « Кібербезпека » |
| **Освітній ступінь** | Бакалавр |
| **Обсяг дисципліни** (кредитів ЄКТС) | 4 кредитів ЄКТС |
| **Терміни вивчення дисципліни** | 7-ий семестр |
| **Назва кафедри, яка викладає дисципліну,** **абревіатурне позначення** | Електронні обчислювальні машини, ЕОМ |
| **Мова викладання** | Українська |

|  |  |
| --- | --- |
| **Лектор (викладач)** | **К. т. н., доцент****Шаповалов Володимир Олександрович** |
| **Корпоративний Е-mail****v.o.shapovalov@ust.edu.ua** |
| **Лінк на персональну сторінку на сайті кафедри****http://ust.edu.ua/faculty/tk/kafedra/evm/sostav/personal\_page/350** |
| **ДІІТ, кімн. 3202, тел. 373-15-52** |
| **Передумови вивчення дисципліни** | Попереднє вивчення таких дисциплін: «Арифметичні та логічні основи ЕОМ»;«Комп’ютерна схемотехніка». Дисципліна «Проектування засобів захисту інформації на ПЛІС» використовуються здобувачами освіти при вивченні таких дисциплін: «Комп’ютерні мережі», «Локальні мережі», «Системи технічного захисту інформації». |
| **Мета навчальної дисципліни** | Сформувати у здобувача вищої освіти здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.У рамках лабораторних робіт здобувачі вищої освіти проходять, по суті, повний цикл проектування цифрових пристроїв, у тому числі і пристроїв захисту інформації: постановка задачі (завдання на проектування); розробка схеми та діаграми станів (при необхідності); VHDL-опис; синтез схеми; складання «дослідницького стенду» Test Bench; моделювання; прив'язка портів об'єкта до виводів ПЛІС та його реалізація в ПЛІС; дослідження апаратно реалізованого в ПЛІС пристрою. |
| **Очікувані результати навчання** | Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем з використанням сучасних САПР з можливістю моделювання компонентів системи і всієї системи. Основний очікуваний результат навчання – набуття навичок і вмінь розробляти апаратуру на основі її опису мовою VHDL з використанням ПЛІС.  |
| **Зміст дисципліни** | - Сучасний підхід до проектування апаратури. Порівняння і можливості САПР, ПЛІС і мов опису апаратури HDL. Характеристика систем на кристалі.- Паралельні та послідовні оператори мови VHDL. Обчислювач мовою VHDL з точок зору програміста, моделювання і апаратної реалізації. Стилі програмування мовою VHDL: поведінковий, потоковий і структурний; Основні етапи реалізації проекту в ПЛІС.- Особливості VHDL-опису комбінаційних і послідовністних функціональних вузлів ЕОМ;- Розробка спрощеного обчислювача (кінцевий автомат, пам'ять команд і результатів, арифметико-логичний пристрій) з використанням мови VHDL (контрольне завдання).- Особливості опису мовою VHDL і апаратної реалізації в ПЛІС криптографічних алгоритмів: поточного RC4 і блочного DES. |
| **Контрольні** **заходи та критерії** **оцінювання** | Методи контролю: усне опитування, поточний контроль (захист звітів з лабораторних робіт), захист контрольного завдання, залік. Підсумкове оцінювання академічної успішності здобувача вищої освіти в семестрі визначається за 100-бальною шкалою.Контрольні заходи: Поточний контроль 1 – 50 балів; Поточний контроль 2 – 50 балів.Оцінювання результатів навчання здійснюється по шкалі ЄКТС і за національною шкалою: A «Відмінно» - Відмінно; B «Дуже добре» - Добре; C «Добре» - Добре; D «Задовільно» - Задовільно; E «Достатньо» - Задовільно; FX «Незадовільно з можливістю повторного складання»; F «Незадовільно з повторним вивченням дисципліни». |
| **Політика викладання** | Умовою допуску до підсумкового контролю є виконання і захист лабораторних робіт, контрольного завдання. При оцінюванні за основу беруться повнота і правильність виконання завдань та відповідей під час захисту. Всі виконані види робіт (звіти з лабораторних робіт, контрольне завдання) повинні відповідати вимогам академічної доброчесності - не повинні містити академічного плагіату, фабрикації та фальсифікації. |
| **Засоби навчання** | При виконанні лабораторних робіт використовуються комп’ютери з інстальованою САПР Xilinx WebPACK і дослідні стенди Spartan-3 starter kit, поставлені на кафедру фірмою Xilinx.  |
| **Навчально-методичне забезпечення** | Основна література: - Бондарнко І.М., Бородін О.В., Карнаушенко В..П. Проектування напівпровідникових приладів та інтегральних схем: Навч. посібник для студентів ЗВО. − Харків: ХНУРЕ. − 2018. – 177 с.- Сергієнко А.М., Корнейчук В.І. Мікропроцесорні пристрої на програмованих логічних ІС (рос). - –К.: «Корнійчук», 2005. -108 с.- Корченко О. Г. К34 Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.:ілДопоміжна література:- Аврунін О.Г. Основи мови VHDL для проектування цифрових пристроїв на ПЛІС: навч. посібник / О.Г. Аврунін, Т.В. Носова, В.В. Семенець. − Харків: ХНУРЕ, 2018. − 196 с.Інформаційні ресурси в Інтернеті:- Сайт FPGA фірми AMD - AMD Acquires Xilinx: Creating the Industry’s High Performance and Adaptive Computing Leader [Електроний ресурс]. - Режим доступу до ресурсу: <https://www.amd.com/en/corporate/xilinx-acquisition> , <https://www.xilinx.com/products/silicon-devices/fpga.html> .- Сайт FPGA фірми Intel (Altera) - Intel FPGAs and Programmabie Solutions [Електроний ресурс]. - Режим доступу до ресурсу: <https://www.intel.com/content/www/us/en/products/programmable.html>/ |