Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
“Харківський авіаційний інститут”

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

ЗАТВЕРДЖУЮ
Голова НМК
_____ М.С. Зряхов
(підпис) (ініціали та прізвище)
«30» 08 2019 р.

РОБОЧА ПРОГРАМА ОБОВ’ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Апаратні та програмні засоби захисту інформації
(назва навчальної дисципліни)

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

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

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

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2019 рік

Робоча програма «Апаратні та програмні засоби захисту інформації»
(назва навчальної дисципліни)

для студентів за спеціальністю 125 "Кібербезпека"
освітньою програмою Безпека інформаційних і комунікаційних систем
освітньою програмою Кібербезпека індустріальних систем

«26» 08 2019 р., – 9 с.

Розробник: Перепелицин А. Є., доцент кафедри 503, к.т.н. _____
(автор, посада, науковий ступень та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри _____
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)
Протокол №1 від «30» 08 2019 р.

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

)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="8">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем, Кібербезпека індустріальних систем
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Цикл загальної підготовки:
нормативна</td></tr>
<tr><td>Кількість модулів – 1</td><td rowspan="2">Навчальний рік
2019/2020</td></tr>
<tr><td>Кількість змістових модулів – 2</td></tr>
<tr><td>Індивідуальне завдання:
розрахунково-графічна робота «Реалізація алгоритму шифрування AES в FPGA».</td><td rowspan="2">Семестр:
5-й</td></tr>
<tr><td>Загальна кількість годин – 48/120</td></tr>
<tr><td rowspan="5">Кількість тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 4</td><td>Лекції [1)]
32 год.</td></tr>
<tr><td>Практичні, семінарські
0 год.</td></tr>
<tr><td>Лабораторні[1)]
16 год.</td></tr>
<tr><td>Самостійна робота
63 год.
Індивідуальні завдання: 9 год</td></tr>
<tr><td>Вид контролю:
іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 57/72.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: ознайомлення з особливостями апаратної реалізації генераторів випадкових чисел, фізично неклонованих функцій, деяких криптопримітівов, а також засобами підвищення стійкості до атак по сторонніх каналах і навичками й засобами проектування цифрових систем. Придбати навички й уміння розробляти системи (проекти) на ПЛІС, проводити пошук проектних помилок та вміти діагностувати розроблені апаратні рішення. Засвоїти мову опису апаратури VHDL. Ознайомитися з існуючими засобами автоматизованого проектування цифрових систем.

Завдання:

– розгляд апаратної реалізації генераторів випадкових чисел;
– розгляд фізично неклонованих функцій;
– розгляд атак по сторонніх каналах;
– розгляд процесу, методів та засобів проектування цифрових систем;
– засвоєння мови опису цифрових проектів VHDL;
– отримання навичок розробки цифрових проектів на мікросхемах програмованої логіки.

3. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1. Засоби та технології реалізації генератора псевдовипадкових чисел в FPGA.

Тема 1. Технології реалізації генератора псевдовипадкових чисел в FPGA.

Предмет, ціль вивчення й завдання дисципліни. Структура, зміст дисципліни й методичні рекомендації з її вивчення. Місце дисципліни в навчальному процесі. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Технології реалізації генератора псевдовипадкових чисел в FPGA.

Тема 2. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.

Регістри зсуву з лінійної зворотним зв'язком. Конфігурації ГПСЧ на основі РСЛОС. Порівняння структури конфігурацій Фібоначі і Галуа. Переваги та недоліки конфігурацій Фібоначі і Галуа.

Тема 3. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.

Регистры сдвига с нелинейной обратной связью. Порядок нелинейности полиномов. РСНОС второго порядка. Образующие полиномы для генерации последовательности макс. длины.

Тема 4. Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.

Клітинні автомати. Класифікація клітинних автоматів. ГПСЧ на основі одновимірних клітинних автоматів. Розгляд різних правил для одновимірних клітинних автоматів.

Тема 5. Реалізація криптостійкого генератора псевдовипадкових чисел в FPGA.

Оцінка якості формованих псевдовипадкових послідовностей. Реалізація криптостійких генераторів з використанням кріптопрімітівов.

Модуль 2

Змістовний модуль 2. Засоби та технології реалізації фізичної криптографії.

Тема 6. Генератори дійсно випадкових чисел.

Джерела ентропії. Апаратні реалізації генераторів істинно випадкових чисел. Генератор дійсно випадкових числових послідовностей в FPGA.

Тема 7. Реалізація фізично 5е клонованих функцій в FPGA.

Архітектури ФНФ. Поняття неклонованості. Властивості. Область застосування ФНФ. Протокол взаємодії. Оцінка якості реалізації ФНФ. Проблеми реалізації. Адаптація ФНФ для реалізації в FPGA.

Тема 8. Атаки по сторонніх каналах.

Атаки по сторонніх каналах. Фізичні характеристики, що лежать в основі атак по сторонніх каналах. Способи аналізу, що застосовуються в атаках по сторонніх каналах. Види атак по сторонніх каналах. Атаки по енергоспоживанню. Атаки за часом. Атаки за помилками обчислення. Атаки по електромагнітному випромінюванню. Атаки на основі акустичного аналізу. Атаки на кеш-пам’ять.

Тема 9. Апаратні трояни.

Класифікації апаратних закладок. Методи виявлення апаратних закладок. Заходи запобігання встановлення.

Тема 10. Обфускація і деобфускація FPGA.

Обфускація схем. Методи обфускації. Деобфускація схем. Фактори, що визначають застосовність обфускації. Оцінка ефективності обфускації схем.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	С.р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. *Засоби та технології реалізації генератора псевдовипадкових чисел в FPGA*					
Тема 1. Технології реалізації генератора псевдовипадкових чисел в FPGA.	9	3			6
Тема 2. Реалізація генератора	12	4		2	6

1	2	3	4	5	6
псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.					
Тема 3. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.	14	4		2	8
Тема 4. Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.	13	3		2	8
Тема 5. Реалізація криптостійкого генератора псевдовипадкових чисел в FPGA.	10	2			8
Разом за змістовим модулем 1	**58**	**16**		**6**	**36**
Змістовий модуль 2. *Засоби та технології реалізації фізичної криптографії*					
Тема 6. Генератори дійсно випадкових чисел.	7	2			5
Тема 7. Реалізація фізично неклонованих функцій в FPGA.	13	5		2	6
Тема 8. Атаки по сторонніх каналах.	11	4		1	6
Тема 9. Апаратні трояни.	15	3		4	8
Тема 10. Обфускація і деобфускація FPGA.	7	2		3	2
РГР	9				9
Разом за модулем 2	**62**	**16**		**10**	**36**
Усього годин	**120**	**32**		**16**	**72**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.	2
2	Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.	2
3	Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.	2
4	Експериментальне дослідження реалізації фізично неклонованих функцій в FPGA.	2
5	Реалізація блоку перемішування стовпців алгоритму шифрування AES в FPGA.	3
6	Реалізація операцій одного раунду алгоритму шифрування AES в FPGA.	2
7	Реалізація дешифратора алгоритму шифрування AES в FPGA.	2
8	Підвищення стійкості FPGA систем до атак по сторонніх каналах.	1
	Разом	**16**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Технології реалізації генератора псевдовипадкових чисел в FPGA.	4
2	Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.	8
3	Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.	4
4	Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.	4
5	Реалізація криптостійкого генератора псевдовипадкових чисел в FPGA.	4
6	Генератори дійсно випадкових чисел.	4
7	Реалізація фізично неклонованих функцій в FPGA.	4
8	Атаки по сторонніх каналах.	8
9	Апаратні трояни.	4

10	Обфускація і деобфускація FPGA.	4
11	Реалізація алгоритму шифрування AES в FPGA	24
	Разом	**72**

9. Індивідуальні завдання

Розрахунково-графічна робота «Реалізація алгоритму шифрування AES в FPGA».

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді екзамену.

12. Розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Робота на лекціях	0…2	8	0…16
Виконання і захист лабораторних (практичних) робіт	0...2	8	0...16
Модульний контроль	0…18	1	0…18
Змістовий модуль 2			
Робота на лекціях	0…2	8	0…16
Виконання і захист лабораторних (практичних) робіт	0...2	8	0... 16
Модульний контроль	0…18	1	0…18
Усього за семестр			**60…100**

*Підсумковий тест (іспит) у разі відмови від балів поточного тестування та допуску до іспиту.

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

13. Методичне забезпечення

Перепелицин А.Є. Лабораторні роботи (в електронному вигляді).

14. Рекомендована література

1. В. А. Куланов, А. Е. Перепелицын, А. А. Галькевич, А. В. Желтухин. Разработка специализированных вычислительных систем с использованием языка VHDL. Х.: Нац. аэрокосм. ун-т им. Н. Е. Жуковского «Харьк. авиац. ин-т», 2014. – 92 с.

2. Проектування комп'ютерних систем на основі мікросхем програмованої логіки : монографія / С. А. Іванець, Ю. О. Зубань, В. В. Казимир, В. В. Литвинов. – Суми : Сумський державний університет, 2013. – 313 с.

3. Digital Logic and Microprocessor Design with VHDL (soon with Verilog), Enoch O.Hwang, La Sierra University, Riverside, CA, Thomson – 2006, 2018.

4. Advanced FPGA Design: Architecture, Implementation, and Optimization - Steve Kilts. IEEE, 353 p.

15. Інформаційні ресурси

1. https://www.intel.com/content/www/us/en/products/programmable.html
2. https://www.xilinx.com/products/silicon-devices.html
3. http://www.csn.khai.edu