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 » серпня 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., – 10 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="9">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 змістовних 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 – 49/120</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
1 год.</td></tr>
<tr><td>Лабораторні[1)]
16 год.</td></tr>
<tr><td>Самостійна робота
71 год.</td></tr>
<tr><td>Індивідуальні завдання: 9 год</td></tr>
<tr><td></td><td>Вид контролю:
іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 49/71.

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

2. Мета та завдання навчальної дисципліни

Мета: діяльності на основі застосування системи теоретичних знань і практичних навичок, отриманих у процесі всього періоду навчання відповідно до вимог стандартів вищої освіти.

Завдання: вивчення основних закономірностей, методів та моделей засоби захисту інформації; можливість їх використання щодо захисту інформації; реалізація сучасних крипто алгоритмів.

Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

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

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

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

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

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

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання.

В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

ПРН 36 виявляти небезпечні сигнали технічних засобів;

ПРН 50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

Міждисциплінарні зв’язки. Дисципліна базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності.

Дисципліна базується на знаннях, отриманих при вивченні дисциплін: ОК17 "Архітектура комп'ютерів", ОК20 "Операційні системи", ОК32 "Технології проектування комп'ютерних систем", ВБ14 "Комп'ютерна електроніка і схемотехніка".

На знаннях, отримані при вивченні дисципліни "Апаратні та програмні засоби захисту інформації" базуються дисципліни: ОК15 "Курс на вибір 1 Захист інформації в інформаційно-комунікаційних системах", ОК25 "Системи технічного захисту інформації", ОК36 "Дипломний робота (проект) бакалавра".

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.

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 е 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 змістовних модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	С.р.
1	2	3	4	5	6
Модуль 1					
Змістовний 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 псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.	14	4	-	2	8
Тема 3. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.	12	4	-	2	6
Тема 4. Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.	11	3	-	2	6

1	2	3	4	5	6
Тема 5. Реалізація криптостійкого генератора псевдовипадкових чисел в FPGA. Модульний контроль	8	2	-	-	6
Разом за змістовним модулем 1	**54**	**16**	**-**	**6**	**32**
Змістовий модуль 2. *Засоби та технології реалізації фізичної криптографії*					
Тема 6. Генератори дійсно випадкових чисел.	10	2	-	2	6
Тема 7. Реалізація фізично неклонованих функцій в FPGA.	14	5	-	2	7
Тема 8. Атаки по сторонніх каналах.	13	4	-	2	7
Тема 9. Апаратні трояни.	9	3	-	2	4
Тема 10. Обфускація і деобфускація FPGA. Модульний контроль	10	2	-	2	6
РГР	10	-	1	-	9
Разом за змістовним модулем 2	**66**	**16**	**1**	**10**	**39**
Усього годин	**120**	**32**	**1**	**16**	**71**

5. Теми семінарських занять

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

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Розрахунково-графічна робота «Реалізація алгоритму шифрування AES в FPGA».	1
	Разом	1

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.	5
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.	3
7	Реалізація фізично неклонованих функцій в FPGA.	4
8	Атаки по сторонніх каналах.	8
9	Апаратні трояни.	4
10	Обфускація і деобфускація FPGA.	2
11	Реалізація алгоритму шифрування AES в FPGA	20
12	РГР	9
	Разом	**71**

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
Змістовний 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…12
Змістовний модуль 2			
Робота на лекціях	0…2	8	0…16
Виконання і захист лабораторних (практичних) робіт	0...2	8	0... 16
Виконання РГР			0…12
Модульний контроль	0…18	1	0…12
Усього за семестр			**60…100**

Семестровий контроль у вигляді заліку за наявності допуску до заліку. Під час складання семестрового заліку студент має можливість отримати максимум 100 балів.

Білет для заліку складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

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