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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 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»
(шифр і назва галузі знань)

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

Освітня програма «Кібербезпека»
(найменування освітньої програми)

Форма навчання: денна

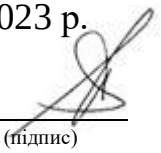
Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Розробник: Перепелицин А. Є., доцент, к.т.н., доцент 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри «Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)

Протокол № 1 від « 30 » 08 2023 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 – 4,5</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
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td rowspan="2">Навчальний рік
2023/ 2024</td></tr>
<tr><td>Кількість змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне завдання: немає</td><td rowspan="2">Семестр:
4-й</td></tr>
<tr><td>Загальна кількість годин – 48/135</td></tr>
<tr><td rowspan="4">Кількість тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 5.5</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
87 год.</td></tr>
<tr><td>Вид контролю:
іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 48/87.

[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.

Компетентності, які набуваються:

– КЗ1. Здатність застосовувати знання у практичних ситуаціях;

– КЗ2. Знання та розуміння предметної області та розуміння професії;

– КЗ3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;

– КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

– КЗ5. Здатність до пошуку, оброблення та аналізу інформації;

– КФ3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;

– КФ4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

– КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

– КФ7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);

– КФ10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;

– КФ11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;

– КФ12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

– ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

– ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

– ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

– ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.10

– ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

– ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

– ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

– ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

– ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.20

– ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

– ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.**Пререквізити –** дисципліна базується на знаннях, отриманих при вивченні дисциплін: "Архітектура комп'ютерів", "Операційні системи", "Технології проектування комп'ютерних систем", "Комп'ютерна електроніка і схемотехніка".

Кореквізити – на знаннях, що отримані при вивченні дисципліни "Апаратні та програмні засоби захисту інформації" базуються дисципліни: "Курс на вибір 1 Захист інформації в інформаційно-комунікаційних системах", "Системи технічного захисту інформації", "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 РЗЛЗЗ. 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.

Регістри зсуву з нелінійним зворотним зв'язком. порядок нелінійності поліномів. РЗНЗЗ другого порядка нелінійності. Поліноми, що утворюють структуру, для генерації послідовності макс. довжини.

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.	13	3	-	-	10
Тема 2. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.	15	3	-	2	10
Тема 3. Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.	12	3	-	2	7
Тема 4. Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.	14	3	-	2	9
Тема 5. Реалізація криптостійкого генератора псевдовипадкових чисел в FPGA. Модульний контроль	14	4	-	-	10
Разом за змістовним модулем 1	**68**	**16**	**-**	**6**	**46**
Змістовий модуль 2. *Засоби та технології реалізації фізичної криптографії*					
Тема 6. Генератори дійсно випадкових чисел.	13	2	-	2	9
Тема 7. Реалізація фізично неклонованих функцій в FPGA.	16	5	-	2	9
Тема 8. Атаки по сторонніх каналах.	15	4	-	2	9
Тема 9. Апаратні трояни.	12	3	-	2	7
Тема 10. Обфускація і деобфускація FPGA. Модульний контроль	11	2	-	2	7

1	2	3	4	5	6
Разом за змістовним модулем 2	**67**	**16**	**-**	**10**	**41**
Усього годин	**135**	**32**	**-**	**16**	**87**

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.	10
2	Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з лінійним зворотним зв'язком.	10
3	Реалізація генератора псевдовипадкових чисел в FPGA на основі регістру зсуву з нелінійними зворотними зв'язками.	7
4	Реалізація генератора псевдовипадкових чисел в FPGA на основі клітинних автоматів.	9
5	Реалізація криптостійкого генератора псевдовипадкових чисел в FPGA.	8
6	Генератори дійсно випадкових чисел.	10
7	Реалізація фізично неклонованих функцій в FPGA.	9
8	Атаки по сторонніх каналах.	10
9	Апаратні трояни.	7
10	Обфускація і деобфускація FPGA.	7
	Разом	**87**

9. Індивідуальні завдання

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

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…18
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…8
Модульний контроль	0…12	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.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Захистити не менше 85% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення робіт щодо розвитку та підтримки функціонування СТЗІ.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 95% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення робіт щодо розвитку та підтримки функціонування інформаційних систем, уміти виконувати інформаційне забезпечення та виявляти небезпечні сигнали технічних засобів. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Мати навички забезпечення и функціонування програмних та програмно-апаратних комплексів, виявлення вторгнень різних рівнів та класів.

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

1. Перепелицин А.Є. Лабораторні роботи (в електронному вигляді).
2. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https:// elearn.csn.khai.edu/xsl-portal/site/24650914-259c-4c0f-8198-5ac8f37d67db.
3. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=1633.

14. Рекомендована література

1. В. О. Куланов, А. Є. Перепелицин, О. О. Галькевич, О. В. Желтухин. Розробка спеціалізованих обчислювальних систем із використанням мови VHDL. Х.: Нац. аерокосм. ун-т ім. М. Є. Жуковського «ХАІ», 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.
5. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – Київ: BHV, 2009

15. Інформаційні ресурси

1. Intel Programmable Solutions Group Altera®, an Intel Company, URL: https://www.intel.com/content/www/us/en/products/programmable.html
2. AMD Solutions, URL: https://www.xilinx.com/products/silicon-devices.html
3. Department of computer systems, networks and cybersecurity, URL: http://www.csn.khai.edu