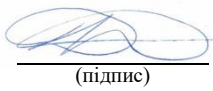
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Голова НМК



(підпис) Д.М. Крицький (ініціали та прізвище)

« 31 » серпня 2022 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології забезпечення кібербезпеки апаратних та програмовних засобів
(назва навчальної дисципліни)

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

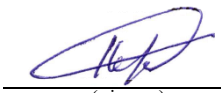
Спеціальність: 123 «Комп'ютерна інженерія»
(код та найменування спеціальності)

Освітні програми: «Системне програмування»
(найменування освітньої програми)

Форма навчання: денна

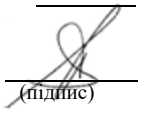
Рівень вищої освіти: другий (магістерський)

Харків 2022 рік

Розробник: Перепелицин Артем Євгенович, 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 » серпня 2022 року

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 rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань:
12 «Інформаційні технології»</td><td>Обов’язкова</td></tr>
<tr><td>Модулів – 2</td><td rowspan="4">Спеціальність:
123 «Комп’ютерна інженерія»
Освітні програми:
«Системне програмування»</td><td rowspan="2">Навчальний рік
2022/2023</td></tr>
<tr><td>Змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: немає</td><td rowspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – денна – 481)/120</td><td>3-й</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи здобувача – 4.5</td><td rowspan="10">Рівень вищої освіти:
другий (магістерський)</td><td>Лекції1)</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Практичні1)</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні1)</td></tr>
<tr><td>16 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72 година</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить *48/72*.

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: Дисципліна має допомогти сформувати у здобувачів такі загальні та спеціальні компетентності:

– здатність застосовувати знання у практичних ситуаціях;

– знання та розуміння предметної області та розуміння професії;

– здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;

– зміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

– здатність до пошуку, оброблення та аналізу інформації;

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

– здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

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

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

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

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

– 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. В результаті вивчення дисципліни здобувачі мають досягти такі результати навчання:

– виявляти небезпечні сигнали технічних засобів;

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

Пререквізити: 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 будуть отримані при вивченні дисципліни "Апаратні та програмні засоби захисту інформації" базуються дисципліни: "Захист інформації в інформаційно-комунікаційних системах", "Системи технічного захисту інформації", "Дипломний робота (проект) бакалавра".

3. Зміст навчальної дисципліни

Модуль 1
Змістовний модуль 1. Теоретичні аспекти технології забезпечення кібербезпеки апаратних та програмовних засобів.

Тема 1. Вступ до дисципліни
Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь. Характеристика рекомендованих під час вивчення дисципліни джерел інформації.

Тема 2. Особливості забезпечення кібербезпеки апаратних комплексів. Історія розвитку та еволюція
Історія розвитку сучасних апаратних засобів для забезпечення кібербезпеки. Програмні та апаратні засоби захисту від кібератак. Загальна характеристика. Відмінності. Особливості застосування.

Тема 3. Апаратні та програмовні засоби як об'єкт та інструмент проведення кібератак
Класифікація апаратних засобів з точку зору забезпечення кібербезпеки. Апаратні комплекси як об'єкт кібератак. Програмовні та апаратні платформи для здійснення кібератак.

Тема 4. Сучасні вимоги та стандарти для забезпечення кібербезпеки апаратних комплексів
Сучасні стандарти забезпечення кібербезпеки. Кібербезпека промислових систем управління. Стандарти ISA/IEC 62443. NERC-CIP. UL 2900-2-2.

Тема 5. Аналіз ризиків та загроз в галузі забезпечення кібербезпеки апаратних та програмовних засобів
Характеристика системи та ідентифікація загроз. Аналіз ризиків та загроз. Розрахунок ризиків та можливих впливів. Управління ризиками. Сучасні стандарти. ISO/IEC 27001.

Тема 6. Види та характеристика атак на електроні та програмовні компоненти
Таксономія та класифікація видів атак на електроні компоненти. Рівні атак, їх виявлення та аналіз післядії. Інвазивні, напівінвазивні та неінвазивні атаки. Особливості застосування. Класифікація програмовних компонентів та види атак. Атаки на електроні компоненти, в яких алгоритми виконуються програмно (мікроконтролери, мікропроцесори тощо). Атаки на апаратні компоненти з програмовною логікою (ПЛІС).

Модуль 2
Змістовний модуль 2. Практичні аспекти забезпечення кібербезпеки апаратних та програмовних засобів

Тема 7. Інвазивні, напівінвазивні та неінвазивні атаки на електронні компоненти
Загальна характеристика та особливості застосування. Відмінності, методи виявлення та протидії. Неінвазивні атаки - атаки сторонніми каналами (Side-channel attacks). Напівінвазивні атаки - атаки на основі помилок обчислень (Fault Attacks). Інвазивні атаки - атаки засновані на фізичному втручанні (Physical tampering).

Тема 8. Атака сторонніми каналами
Класифікація видів атак. Пасивні та активні атаки. Атаки за рівнем доступу. Методи впливу та протидії. Атаки зондуванням (Probing Attack). Атаки по енергоспоживанню (Power Analysis Attack). Атаки по електромагнітному випроміненню (electromagnetic Analysis Attack). Акустичні атаки (Acoustic Attack). Атаки по видимому випроміненню (Visible Light Attack).

Тема 9. Апаратні закладки (Trojans)
Загальна характеристика. Класифікація видів та рівнів внесення апаратних закладок. Класифікація по фізичному принципу роботи. Класифікація по методу активації. Класифікація по дії на систему. Оцінка потенційної загрози. Методи виявлення.

Тема 10. Захист апаратних та програмовних компонентів від несанкціонованого доступу та копіювання
Рівні та проблеми несанкціонованого доступу. Засоби обмеження фізичного доступу до апаратних компонентів на різних рівнях. Захист від читання (Readout Protection). Захист процесу завантаження (Boot Flow Protection) та ініціалізації. Шифрування даних, що зберігаються.

Тема 11. Захист сирцевого коду від несанкціонованого копіювання, обфускатори
Реверс інжиніринг. Обфускатори сирцевого коду. Техніки обфускації. Особливості використання сторонніх бібліотек з точки зору безпеки. Цифрова підпис (GPG). Ізоляція процесів розробки як частина процесів Continuous Integration/Continuous Delivery.

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					
1. Вступ до дисципліни.	1	1			
2. Особливості забезпечення кібербезпеки апаратних комплексів. Історія розвитку та еволюція.	15	3		2	10
3. Апаратні та програмовні засоби як об'єкт та інструмент проведення кібератак.	13	4		2	7
4. Сучасні вимоги та стандарти для забезпечення кібербезпеки апаратних комплексів.	8	2			6
5. Аналіз ризиків та загроз в галузі забезпечення кібербезпеки апаратних та програмовних засобів.	16	4		5	7
6. Види та характеристика атак на електроні та програмовні компоненти.	13	3			10
Модульний контроль	1	1			
Разом за змістовним модулем 1	67	18		9	40

Модуль 2					
Змістовний модуль 2					
7. Інвазивні, напівінвазивні та неінвазивні атаки на електронні компоненти.	10	2			8
8. Атака сторонніми каналами.	9	2			7
9. Апаратні закладки (Trojans).	9	2			7
10. Захист апаратних та програмовних компонентів від несанкціонованого доступу та копіювання.	14	4		5	5
11. Захист сирцевого коду від несанкціонованого копіювання. Обфускатори.	10	3		2	5
Модульний контроль	1	1			
Разом за змістовним модулем 2	53	14		7	32
Усього годин за дисципліною	**120**	**32**		**16**	**72**

5. Теми семінарських занять

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

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	Дослідження та розрахунок складності алгоритму зламу потенційної системи з застосування методів «грубої сили» (Brute Force Attack).	2
2	Аналіз потенційних загроз та дослідження уразливості апаратних та програмовних компонентів системи на прикладі одноплатного комп'ютеру Raspberry Pi.	2
3	Розробка апаратного комплексу пошуку апаратних закладок (Backdoors) з використанням програмовної логіки класу FPGA.	5
4	Розробка апаратного комплексу аналізу проектних рішень комбінаційних та секвенційних схем з використанням програмовної логіки класу FPGA.	5
5	Розробка обфускатору сирцевого коду для захисту його від несанкціонованого копіювання та зміни.	2
	Разом	**16**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	2. Особливості забезпечення кібербезпеки апаратних комплексів. Історія розвитку та еволюція.	10
2	3. Апаратні та програмовні засоби як об'єкт та інструмент проведення кібератак.	7
3	4. Сучасні вимоги та стандарти для забезпечення кібербезпеки апаратних комплексів.	6
4	5. Аналіз ризиків та загроз в галузі забезпечення кібербезпеки апаратних та програмовних засобів.	7
5	6. Види та характеристика атак на електроні та програмовні компоненти.	10
6	7. Інвазивні, напівінвазивні та неінвазивні атаки на електронні компоненти.	8
7	8. Атака сторонніми каналами.	7
8	9. Апаратні закладки (Trojans).	7
9	10. Захист апаратних та програмовних компонентів від несанкціонованого доступу та копіювання.	5
10	11. Захист сирцевого коду від несанкціонованого копіювання. Обфускатори.	5
	Разом	**72**

9. Індивідуальні завдання

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

10. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.14, 15).

11. Методи контролю

Проведення поточного контролю, електронного тестування, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Лабораторні заняття	0...10	3	0…30
Тести	0...5	1	0...5
Модульний контроль	0..10	1	0..10
Змістовний модуль 2			
Лабораторні заняття	0…10	4	0…40
Тести	0…5	1	0…5
Модульний контроль	0..10	1	0..10
Усього за семестр			**0…100**

Білет для іспиту складається з двох теоретичних питань (25 балів за кожне питання), практичного завдання (25 балів) та тесту (25 балів).

Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення робіт щодо розвитку та підтримки функціонування систем.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% 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

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки та у системі дистанційного навчання «Ментор».

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://elearn.csn.khai.edu
2. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/user/index.php?id=1613

14. Рекомендована література

Базова

1. Forte, S. Bhunia, M M. Tehranipoor. Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment. – Springer, 2017. 349 p.
2. R. Paul. Secure Hardware Design: Services and Security. – VDM Verlag Dr. Mülle, 2010. 152 p.
3. D. Mukhopadhyay, R.S. Chakraborty. Hardware Security: Design, Threats, and Safeguards. – Chapman & Hall/CRC, 2014 – 542 p.
4. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник. – К.: Дуікт, 2010. 316 с.
5. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ: BHV, 2009.

Допоміжна

1. Малюк О.О. Інформаційна безпека: концептуальні й методологічні основи захисту інформації. Учеб. Посібник для вузів. - М.: Гаряча лінія - Телеком, 2004.
2. Nadia Nedjah. Embedded Cryptographic Hardware : Design and Security. – Nova Science Publishers Inc, 2006. 255 p.
3. Бабак В.П., Теоритичні основи захисту інформації: Підручник. – К.: НАУ, 2008. 752 с.

15. Інформаційні ресурси

1. CI-інфраструктура кафедри для виконання лабораторних робіт [Ел. ресурс]. URL: http://ci.csn.khai.edu/