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

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

« 31 » серпня 2021 р.

РОБОЧА ПРОГРАМА ВИБІРКОВА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

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

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

Спеціальність: 123 "Комп’ютерна інженерія"
(код та найменування спеціальності)

Освітня програма: Системне програмування

Форма навчання: денна

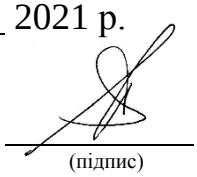
Рівень вищої освіти: другий (магістерський)

Харків 2021 рік

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 2021 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 – 6</td><td rowspan="8">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
123 "Комп’ютерна інженерія
(код та найменування)

Освітня програма
Системне програмування,
(найменування)

Рівень вищої освіти:

другий (магістерський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td rowspan="2">Навчальний рік
2021/2022</td></tr>
<tr><td>Кількість змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне завдання: немае</td><td rowspan="2">Семестр:
11-й</td></tr>
<tr><td>Загальна кількість годин – 64/180</td></tr>
<tr><td rowspan="4">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 6</td><td>Лекції [1)]
32 год.</td></tr>
<tr><td>Практичні, семінарські
0 год.</td></tr>
<tr><td>Лабораторні[1)]
32 год.</td></tr>
<tr><td>Самостійна робота
116 год.</td></tr>
<tr><td></td><td>Вид контролю:
іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: 64/116.

[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:

- 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:

- 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. Програма 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 випромінюванню (electromagnetic Analysis Attack). Акустичні атаки (Acoustic Attack). Атаки по видимому випромінюванню (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.

Модульний контроль

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					

1	2	3	4	5	6
Змістовний модуль 1. *Теоретичні аспекти технології забезпечення кібербезпеки апаратних та програмовних засобів*					
1. Вступ до дисципліни.	2	1		-	1
2. Особливості забезпечення кібербезпеки апаратних комплексів. Історія розвитку та еволюція.	13	3		-	10
3. Апаратні та програмовні засоби як об'єкт та інструмент проведення кібератак.	20	3		6	11
4. Сучасні вимоги та стандарти для забезпечення кібербезпеки апаратних комплексів.	15	3			12
5. Аналіз ризиків та загроз в галузі забезпечення кібербезпеки апаратних та програмовних засобів.	21	3		6	12
6. Види та характеристика атак на електроні та програмовні компоненти. Модульний контроль	15	3			12
Разом за змістовним модулем 1	**86**	**16**		**12**	**58**
Змістовний модуль 2. *Практичні аспекти забезпечення кібербезпеки апаратних та програмовних засобів*					
7. Інвазивні, напівінвазивні та неінвазивні атаки на електронні компоненти.	14	3		-	11
8. Атака сторонніми каналами.	14	3		-	11
9. Апаратні закладки (Trojans).	21	3		6	12
10. Захист апаратних та програмовних компонентів від несанкціонованого доступу та копіювання.	22	3		7	12
11. Захист сирцевого коду від несанкціонованого копіювання. Обфускатори. Модульний контроль	23	4		7	12
Разом за модулем 2	**94**	**16**		**20**	**58**
Усього годин	**180**	**32**		**32**	**116**

5. Теми семінарських занять

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

6. Теми практичних занять

№	Назва теми	Кількість

з/п		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).	6
2	Аналіз потенційних загроз та дослідження уразливості апаратних та програмовних компонентів системи на прикладі одноплатного комп'ютеру Raspberry Pi.	6
3	Розробка апаратного комплексу пошуку апаратних закладок (Backdoors) з використанням програмовної логіки класу FPGA.	6
4	Розробка апаратного комплексу аналізу проектних рішень комбінаційних та секвенційних схем з використанням програмовної логіки класу FPGA.	7
5	Розробка обфускатору сирцевого коду для захисту його від несанкціонованого копіювання та зміни.	7
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	1. Вступ до дисципліни.	1
2	2. Особливості забезпечення кібербезпеки апаратних комплексів. Історія розвитку та еволюція.	10
3	3. Апаратні та програмовні засоби як об'єкт та інструмент проведення кібератак.	11
4	4. Сучасні вимоги та стандарти для забезпечення кібербезпеки апаратних комплексів.	12
5	5. Аналіз ризиків та загроз в галузі забезпечення кібербезпеки апаратних та програмовних засобів.	12
6	6. Види та характеристика атак на електроні та програмовні компоненти.	12
7	7. Інвазивні, напівінвазивні та неінвазивні атаки на електронні компоненти.	11
8	8. Атака сторонніми каналами.	11
9	9. Апаратні закладки (Trojans).	12
10	10. Захист апаратних та програмовних компонентів від несанкціонованого доступу та копіювання.	12
11	11. Захист сирцевого коду від несанкціонованого копіювання. Обфускатори.	12

	Разом	**116**

9. Індивідуальні завдання

Не передбачено навчальним планом

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
Модульний контроль	0…18	1	0…18
Усього за семестр			**60…100**

Контроль знань при проведенні занять оцінюється за такими шкалами:

активність на лекції під час відповідей на питання:

- повна відповідь на питання - 2 бали;
- неповна відповідь - 1 бал;
- відсутність на лекції - 0 балів,

виконання і захист практичних робіт:

при виконанні всіх вимог завдань методик на роботи - 4 бали;

- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1балл;
- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль (всього 18 балів) виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 3 питання (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 6.

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.

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

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 систем.

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

3. Методичне забезпечення

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

4. Рекомендована література

1. D. 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. Nadia Nedjah. Embedded Cryptographic Hardware : Design and Security. – Nova Science Publishers Inc, 2006. 255 p.

5. Дж.Макнамара. Секреты компьютерного шпионажа, тактика и контрмеры. – М:Бином, 2006.

6. Бабак В.П., Теоритичні основи захисту інформації: Підручник. – К.: НАУ, 2008. 752 с.

7. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. Підручник. – К.: ДУІКТ, 2010. 316 с

8. Малюк О.О. Інформаційна безпека: концептуальні й методологічні основи захисту інформації. Учеб. Посібник для вузів. - М.: Гаряча лінія - Телеком, 2004.

9. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ: BHV, 2009.

10. Ленков С.В. Методы и средства защиты информации. В 2-х томах. Том1. Несанкционированное получение информации/ Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко. – К.: Арий, 2008. 464 с.

15. Інформаційні ресурси

1. Википедия – свободная энциклопедия [Електронний ресурс]. – Режим доступа: http://www. ru.wikipedia.org/.

2. ci.csn.khai.edu – CI-інфраструктура кафедри для виконання лабораторних робіт [Електронний ресурс]. – Режим доступа: http://ci.csn.khai.edu/.