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

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ В. В. Павліков
(підпис) (ініціали та прізвище)
«_31_» _____ 2020 р.
Відділ аспірантури і докторантури

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і технології критичного комп'ютингу
(назва навчальної дисципліни)

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

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

Освітня програма: "Кібербезпека"
(найменування освітньої програми)

Рівень вищої освіти: третій (освітньо-науковий)

Форма навчання: денна

Харків 2020 рік

РОБОЧА ПРОГРАМА
ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і технології критичного комп'ютингу
(назва дисципліни)

для здобувачів за спеціальністю 125 "Кібербезпека"

освітньо-наукової програми "Кібербезпека"

«26» 08 2020 р., – 13 с.

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

Гарант ОНП доцент, к.т.н. _____ Колісник М.О.
(посада, науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

Протокол №1 від «27» серпня 2020 р. засідання кафедри № 503

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

ПОГОДЖЕНО:

Завідувач відділу
аспірантури і докторантури В. Б. Селевко

Голова наукового товариства
студентів, аспірантів,
докторантів і молодих вчених Т. П. Старовойт

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	Характеристика навчальної дисципліни
		Денна форма навчання
Кількість кредитів – 5	**Галузь знань** 12 "Інформаційні технології" (шифр та найменування)	Обов'язкова
Кількість модулів – 2		**Навчальний рік**
Кількість змістовних модулів – 4	**Спеціальність** 125 "Кібербезпека" (код та найменування)	2020/ 2021
Індивідуальне завдання: 1		**Семестр**
Загальна кількість годин: денна – 68/150	**Освітньо-наукова програма** "Кібербезпека" (найменування)	3-й
		Лекції [1)]
		34 годин
Кількість тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 4,8	**Рівень вищої освіти:** третій (освітньо-науковий)	**Практичні, семінарські**[1)]
		0 годин
		Лабораторні [1)]
		34 годин
		Самостійна робота
		82 годин
		Вид контролю
		Модульний контроль, іспит

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – *68/82.*

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

2. Мета та завдання навчальної дисципліни

Мета: оволодіння теоретичними і технологічними основами критичного комп'ютингу, методами дослідження, оцінювання і забезпечення гарантоздатності (надійності та безпеки) комп'ютерних систем та інфраструктур (КСІС).

Завдання:

– систематизувати і проаналізувати таксономію понять критичного комп'ютингу і основні показники надійності і гарантоздатності КСІС;
– вивчити методи і засоби дослідження та оцінювання надійності і гарантоздатності КСІС, їх програмних, апаратних і системних компонентів;
– вивчити методи і засоби забезпечення надійності і гарантоздатності програмно-апаратних засобів КСІС на різних етапах створення і використання;
– оволодіти навичками дослідження і розрахунку показників і розроблення засобів забезпечення виконання вимог до надійності і гарантоздатності КСІС.

Програмні компетентності. Дисципліна має допомогти сформувати у аспірантів такі компетентності:
- здатність до абстрактного мислення, аналізу та синтезу;

- здатність до пошуку, оброблення та аналізу інформації з різних джерел;

- здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у кібербезпеці та дотичних до неї (нього, них) міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та суміжних галузей;

- здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок українською та англійською мовами, глибоке розуміння англомовних наукових текстів за напрямом досліджень;

- здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки.

Програмні результати навчання. В результаті вивчення дисципліни аспіранти мають досягти такі програмні результати навчання:

- мати передові концептуальні та методологічні знання з кібербезпеки і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій;

- розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеці та дотичних міждисциплінарних напрямах;

- знати сучасні підходи та засоби моделювання досліджуваних об'єктів та процесів управління, в тому числі в аерокосмічній галузі, вміти створювати нові, вдосконалювати та розвивати методи математичного і комп'ютерного моделювання складних систем, оптимізації та прийняття рішень.

Міждисциплінарні зв'язки. Дисципліна є обов'язковим компонентом освітній програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності та дисципліни «Наукові англомовні комунікації».

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін: «Теорія і методи сучасної криптології», «Методи пентестінгу та кіберзахисту розподілених систем», «Теорія і методи безпеки індустріальних систем», «Формальні методи аналізу безпеки», «Патерни проектування ПЗ систем критичного призначення».

3. Програма навчальної дисципліни

Модуль 1. Дослідження та оцінювання надійності КСІС

Змістовний модуль 1. Систематизація понять критичного комп'ютингу.

Тема 1. Загальна характеристика дисципліни. Базові поняття теорії надійності і гарантоздатності КСІС.

Предмет, мета вивчення і задачі дисципліни. Структура і зміст дисципліни, а також методичні рекомендації по її вивченню. Вимоги до знань і умінь. Характеристика рекомендованих джерел інформації. Стани і події КСІС внаслідок несправностей, вразливостей, відмова; їх класифікація; графи станів і подій. Системний аналіз властивостей; надійність та її складові, гарантоздатність та її складові; відмовостійкість і готовність; живучість, інформаційна та функціональна безпека. Поняття про резил'єнтність. Класифікація систем і елементів в теорії надійності і гарантоздатності КСІС. Таксономія критичного комп'ютингу.

Тема 2. Система показників надійності і гарантоздатності КСІС.

Класифікація показників надійності і гарантоздатності складних систем. Одиничні та комплексні показники. Закони розподілу випадкових величин в надійності і гарантоздатності. Класифікація і спеціальні показники відмовостійкості. Характеристика показників живучості та безпеки. Особливості застосування показників надійності і гарантоздатності для КСІС.

Змістовний модуль 2. Методи дослідження і оцінювання надійності КСІС.

Тема 3. Дослідження та оцінювання надійності невідновлюваних КСІС.

Класифікація методів забезпечення надійності при розробці, виробництві і експлуатації КСІС. Моделі для дослідження і оцінювання надійності нерезервованих і резервованих невідновлювальних систем. Класифікація і аналіз методів резервування. Надійність мажоритарних систем з одно- і

багатоярусної структурою. Дослідження і оцінювання адаптивних систем з одно- і багатоверсійною адаптацією.

Тема 4. Дослідження та оцінювання надійності відновлюваних КСІС.

Аналітичні моделі для оцінювання надійності відновлюваних нерезервованих систем. Дослідження і оцінювання надійності відновлюваних резервованих систем. Особливості використання марковських випадкових процесів для систем зі змінними параметрами програмно-апаратних компонентів та інструментальних засобів для оцінювання. Імітаційне моделювання в задачах дослідження та оцінювання надійності.

Модуль 2. Забезпечення надійності та гарантоздатності КСІС

Змістовний модуль 1. Методи діагностування і відновлення КСІС.

Тема 1. Методи діагностування апаратних і програмних компонентів КСІС.

Систематизація понять технічної діагностики. Структурна організація систем контролю і діагностування. Показники ефективності систем контролю і діагностування: моделі помилок, достовірність, оперативність, повнота і глибина контролю і діагностування. Класифікація методів контролю і діагностування. Методи робочого контролю і діагностування (контроль дублюванням, мажоритарний контроль, контроль за модулем, програмно-логічні методи контролю). Методи тестового контролю і діагностування апаратних і програмних компонентів. Методи відновлення працездатності КСІС при збоях і відмовах різного типу.

Тема 2. Методи забезпечення надійності і гарантоздатності програмних засобів КСІС.

Особливості оцінювання надійності та функціональної безпеки програмних засобів ІУС. Класифікація та аналіз дефектів, показники надійності і безпеки програмних засобів. Моделі якості. Огляд та вимоги стандартів IEC25010, IEC25010 та інш. Класифікація та аналіз моделей надійності програмних засобів – моделей SRGM. Методи комплексування, вибору і верифікації моделей надійності. Бази даних вразливостей та їх використання для оцінювання безпеки. Застосування методик і інструментальних засобів. Огляд і аналіз методів забезпечення надійності і гарантоздатності програмних компонентів.

Змістовний модуль 2. Методи та технології дослідження і забезпечення безпеки і гарантоздатності КСІС.

Тема 3. Методи та технології дослідження безпеки КСІС.

Особливості оцінювання функціональної та інформаційної (кібер) безпеки ІУС. Огляд та вимоги стандартів IEC61508, IEC62443, IEC15408 та інш. Класифікація і огляд методів дослідження та оцінювання. Аналіз сутності та приклади застосування методів XMECA, XTA, XIT, XBD, HAZOP. Особливості дослідження та оцінювання функціональної та інформаційної (кібер) безпеки ІУС з використанням марковських випадкових процесів.

Тема 4. Методи та технології забезпечення гарантоздатності КСІС.

Загальна послідовність та зміст етапів забезпечення надійності і гарантоздатності при створенні та використанні КСІС. Методи оптимального резервування при проектуванні надійних і безпечних КСІС. Принципи одиничної відмови, незалежності та диверсності та їх впровадження. Методи і технології багатоверсійного проектування. Перспективні технології забезпечення надійності, безпеки і гарантоздатності КСІС. Резил'єнтні обчислення та технології. Підведення підсумків дисципліни.

Модульний контроль

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Систематизація понять критичного комп'ютингу					
Тема 1. Загальна характеристика дисципліни. Базові поняття теорії надійності і гарантоздатності КСІС.	5	2			3
Тема 2. Система показників надійності і гарантоздатності КСІС. Модульний контроль	20	4		4	12
Разом за змістовним модулем 1	**25**	**6**		**4**	**15**
Змістовний модуль 2. Методи дослідження і оцінювання надійності КСІС					
Тема 3. Дослідження та оцінювання надійності невідновлюваних КСІС	27	8		4	15
Тема 4. Дослідження і оцінювання надійності відновлюваних КСІС. Модульний контроль	23	2		6	15
Разом за змістовним модулем 2	**50**	**10**		**10**	**30**
Усього годин	**75**	**16**		**14**	**45**
Модуль 2					
Змістовний модуль 1. Методи діагностування і відновлення КСІС					
Тема 1. Методи діагностування апаратних і програмних компонентів КСІС	18	4		4	10

Тема 2. Методи забезпечення надійності і гарантоздатності програмних засобів КСІС. Модульний контроль	23	2		8	13
Разом за змістовним модулем 1	**41**	**6**		**12**	**23**
Змістовний модуль 2. Методи та технології дослідження і забезпечення безпеки і гарантоздатності КСІС					
Тема 3. Методи та технології дослідження безпеки КСІС	14	6		4	8
Тема 4. Методи та технології забезпечення гарантоздатності КСІС. Модульний контроль	20	6		4	6
Разом за змістовним модулем 2	**34**	**12**		**8**	**14**
Усього годин	**75**	**18**		**20**	**37**
Усього годин	**150**	**34**		**34**	**82**

5. Теми семінарських занять

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

6. Теми практичних занять

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

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Таксономія критичного комп'ютингу і показників надійності і гарантоздатності КСІС. Дослідження залежності показників від вхідних параметрів систем.	4
2	Систематизація та аналіз методів і програмно-апаратних засобів резервування невідновлюваних КСІС. Дослідження залежності показників надійності для різних методів	4

	резервування від вхідних параметрів систем.	
3	Класифікація методів і засобів діагностування сучасних КСІС при використанні. Дослідження методів робочого і тестового діагностування.	6
4	Аналіз методів і засобів підвищення гарантоздатності програмного забезпечення КСІС.	4
5	Сучасні методи, засоби та технології забезпечення гарантоздатності КСІС. Дослідження багатоверсійних гарантоздатних систем.	8
6	Дослідження гарантоздатності програмно-апаратних комплексів з використанням апарату марковських випадкових процесів.	4
7	Дослідження моделей надійності програмних засобів SRGM з використанням з використанням інструментальних пакетів.	4
	Разом	34

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Показники надійності і гарантоздатності КСІС. Ризики критичних відмов та методи його визначення.	15
2	Принципи програмно-апаратної реалізації методів резервування КСІС.	15
3	Програмні засоби оцінювання надійності і гарантоздатності КСІС.	15
4	Методи он-лайн і оф-лайн контролю вбудованих і розподілених КСІС.	10
5	Моделі зростання надійності (SRGM) програмних засобів, їх вибір, комплексування і використання для оцінювання.	13
6	Оцінка надійності і безпеки з використанням різних типів дерев відмов і атак.	4
7	Оптимальне резервування компонентів	4

	КСІС для забезпечення гарантоздатності.	
8	Типові архітектури та технології проектування гарантоздатних і резіл'єнтних КСІС.	6
	Разом	82

9. Індивідуальні завдання

Підготовка наукової статті за темою гарантоздатності ІТ в контексті дисертаційних досліджень (розділ 8 – п.п. 2, 3, 8).

10. Методи навчання

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

11. Методи контролю

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

12. Розподіл балів, які отримують аспіранти

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

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Змістовний модуль 1			
Робота на лекціях	0…1	3	0…3
Виконання і захист лабораторних робіт	0...3	2	0…6
Змістовний модуль 2			
Робота на лекціях	0…1	5	0…5
Виконання і захист лабораторних робіт	0...3	5	0...15
Модульний контроль	0…15	1	0…15
Модуль 2			
Змістовний модуль 1			
Робота на лекціях	0…1	3	0…3
Виконання і захист лабораторних робіт	0...3	6	0...18
Змістовний модуль 2			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних робіт	0...3	4	0...12
Модульний контроль	0…17	1	0…17
Усього за семестр			**0 …100**

Семестровий контроль (іспит) проводиться у разі відмови аспіранта від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту аспірант має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних і одного практичного запитання. За перше та друге запитання аспірант отримує по 30 балів, за практичне – 40 балів.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки. Аспірант має знати:

– основні поняття критичного комп'ютингу і показники надійності і КСІС та їх взаємозв'язки;

– методики оцінювання і дослідження гарантоздатності з використанням ССН, дерев відмов і марковського моделювання;

– методи резервування і відновлення працездатності програмно-апаратних засобів КСІС на різних етапах створення і використання.

Необхідний обсяг вмінь для одержання позитивної оцінки. Аспірант має вміти:

– здійснювати аналіз і підготовку статей у галузі гарантоздатності ІТ-систем в контексті тематики дисертаційних досліджень;

– користуватись сучасними програмними засобами для проведення наукових досліджень;

– використовувати сучасні методи розрахунку показників і забезпечення виконання вимог до надійності і гарантоздатності КСІС.

12.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Показати необхідний обсяг знань та вмінь для одержання позитивної оцінки відповідно до п.12.2. Захистити не менше 80% від усіх завдань практичних робіт. Виконати пошук і анотування літератури для підготовки проєкту наукової статті за темою дисертації з оглядом проблем у галузі надійності та гарантоздатності для обраної предметної галузі.

Добре (75-89). Показати достатньо глибоке знання програмного матеріалу, володіти понятійним апаратом, вміти аргументувати свої відповіді. У відповідях допускаються неточності, які впливають тільки на чіткість. Виконати не менше 90% завдань практичних робіт. Підготувати план розділу наукової статті за темою дисертації з оглядом проблем у галузі надійності та гарантоздатності для обраної предметної галузі.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконало знати всі теми та уміти їх застосовувати. Підготувати проєкт наукової статті за темою дисертації з оглядом проблем у галузі надійності та гарантоздатності для обраної предметної галузі.

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. Харченко В. С. Конспект лекцій (Харченко В. С. (ред). Надійність цифрових систем. Підручник. МОН України, 2006, 342 с.)
2. Лисенко І. В., Тарасюк О. М., Харченко В. С., Надійність і відмовостійкість комп'ютерних систем. Методичний посібник до лабораторних робіт, ХАІ, 2016, 98 с.
3. Харченко В. С. Методичні вказівки до підготовки до семінару.
4. Харченко В. С. Методичні вказівки до виконання розрахунково-графічної роботи.

14. Рекомендована література

Базова

1. Основи діагностики цифрових систем. Підручник/ За ред. Харченка В.С., Ілюшка В.М. - Харків: Міністерство освіти та науки, 2007. – 360 с.
2. Основи надійності цифрових систем. Підручник/ За ред. Харченка В.С., Жихарева В.Я. - Харків: Міністерство освіти та науки, 2006. – 342 с.
3. Харченко В.С., Скляр В.В., Тарасюк О.М. Методи моделювання та оцінки якості і надійності програмного забезпечення. Навчальний посібник. - Харків: ХАІ, 2008. - 221 с.
4. Харченко В.С., Тарасенко В.В., Ушаков А.А. Відмовостійкі вбудовані цифрові системи на ПЛІС.- Навчальний посібник. – Харків: ХАІ, 2012. - 189 с.
5. Відмовостійкі інформаційно-керуючі системи на програмовній логіці/ За ред. Харченка В.С., Скляра В.В. НАКУ «ХАІ», НВП «Радій», 2013. - 291 с.
6. Харченко В.С., Лисенко І.В., Тарасюк О.М. Надійність та відмовостійкість комп'ютерних систем. Лабораторний практикум. – Харків: ХАІ, 2016. - 98 с.

Допоміжна

1. Харченко В.С., Скляр В.В., Конорев Б,М. та ін. Оцінка та забезпечення якості програмних засобів космічних систем. Національне космічне агенство України, НАКУ «ХАІ», Сертцентр АСУ, 2013. - 294 с.
2. Основи цифрових систем. Підручник/ За ред. Благодарного М.П., Харченка В.С. - Харків: Міністерство освіти та науки, 2004. – 351 с.
3. Федоров Ю.Н. Довідник інженера по АСУ ТП. – Інфра-інженерія, 2012.

4. Методи системного аналізу у комп'ютерній інженерії та радіоелектроніці: підручник / За ред. С.Ю. Даншиної, В.С. Харченка.– Х.: Нац. аерокосм. ун-т «Харьк. авіац. ін-т», 2013. – 312 с.

5. Behrooz Parhami. Textook on Dependable Computing. University of California, 2020 https://web.ece.ucsb.edu/~parhami/text_dep_comp.htm#slides https://web.ece.ucsb.edu/~parhami/ece_257a.htm

15. Інформаційні ресурси

1. Бабчук С.М. Надійність комп'ютерних систем і мереж, 2017 [Электрон. ресурс]. – http://194.44.112.13/chytalna/5417/index.html#p=1.

2. Вишнівський В.В. Основи надійності та діагностики телекомунікаційних систем, 2016 [Электрон. ресурс]. – Режим доступа: http://www.dut.edu.ua/uploads/l_1092_31009342.pdf

3. The First 50 Years of Software Reliability Engineering: A History of SRE withFirst Person AccountsJames J. Cusick, PMP, New York, 2017 [Электрон. ресурс]. – Режим доступа: https://arxiv.org/ftp/arxiv/papers/1902/1902.06140.pdf/

4. Operating System Reliability from the Quality of Experience Viewpoint: An Exploratory Study [Электрон. ресурс]. – Режим доступа: https://www.researchgate.net/publication/236332149_Operating_System_Reliability_from_the_Quality_of_Experience_Viewpoint_An_Exploratory_Study

5. Advances in System Reliability Engineering [Электрон. ресурс]. – Режим доступа: https://www.elsevier.com/books/advances-in-system-reliability-engineering/ram/978-0-12-815906-4

6. Safety Assessment for Facilities and Activities. IAEA Safety Standards, 2017. [Электрон. ресурс]. – Режим доступа: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1714web-7976998.pdf

7. Joint safety and security modeling for risk assessment in cyber physical systems, 2018. [Электрон. ресурс]. – Режим доступа: https://tel.archives-ouvertes.fr/tel-01318118/document

8. Systems-Theoretic Safety Assessment of Robotic Telesurgical Systems, 2016. [Электрон. ресурс]. – Режим доступа: https://www.researchgate.net/publication/275588035_Systems-Theoretic_Safety_Assessment_of_Robotic_Telesurgical_Systems/download

9 . Видання XAI по проектах MASTAC (2009-2010), SAFEGUARD (2011-2013), GREENCO (2014-2015), SEREIN (2015-2018), ALIOT (2016-2020).