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)
«__24__» ____08____ 2020 р.
Відділ аспірантури і докторантури

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і методи захисту критичних інфраструктур
(назва навчальної дисципліни)

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

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

Освітньо-наукова програма "Комп'ютерна інженерія"
(найменування)

Рівень вищої освіти: третій (освітньо-науковий)

Форма навчання: денна

Харків 2020 рік

РОБОЧА ПРОГРАМА
ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і методи захисту критичних інфраструктур
(назва дисципліни)

для здобувачів за спеціальністю 123 "Комп'ютерна інженерія"

освітньо-наукової програми Комп'ютерна інженерія

«26» серпня 2020 р., – 10 с.

Розробник: доцент, к.т.н., доцент _____ _____ Фесенко Г.В.
(посада, науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

Гарант ОНП доцент, к.т.н. _____ Бабешко Є.В.
(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)	Вибіркова
Кількість модулів – **1**		**Навчальний рік**
Кількість змістовних модулів – **2**		2020/ 2021
Індивідуальне завдання - немає (назва)	**Спеціальність** 123 "Комп'ютерна інженерія" (код та найменування)	**Семестр**
Загальна кількість годин: **68/150**		4-й
	Освітньо-наукова програма "Комп'ютерна інженерія" (найменування)	**Лекції** *
Кількість тижневих годин для денної форми навчання: аудиторних – **4** самостійної роботи аспіранта – **4,8**		**34** годин
		Практичні, семінарські*
		0 годин
		Лабораторні*
	Рівень вищої освіти: третій (освітньо-науковий)	**34** години
		Самостійна робота
		82 годин
		Вид контролю
		Іспит

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: **68/82**.

*Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

1. Мета вивчення: ознайомлення аспірантів з базовими поняттями, методами та засобами забезпечення безпеки, що використовуються у сучасних критичних інфраструктурах, а також – в придбанні навичок з реалізації технічних та організаційних заходів щодо оцінювання та забезпечення безпеки індустріальних систем.

2. Завдання: вивчити базові поняття з безпеки; вивчити основи управління безпекою та життєвим циклом критичних інфраструктур; вивчити основи кількісного оцінювання функціональної безпеки та розрахунку показників їх функціональної безпеки; вивчити основи технічних та організаційних заходів забезпечення їх безпеки.

3. Програмні компетентності. Дисципліна має допомогти сформувати у аспірантів такі компетентності:

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

– здатність працювати в міжнародному контексті;

– здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності;

– здатність здійснювати науково-педагогічну діяльність у вищій освіті;

– здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері комп'ютерної інженерії;

– здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в комп'ютерній інженерії та дотичні до неї міждисциплінарні проекти, лідерство під час їх реалізації.

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

– планувати і виконувати експериментальні та/або теоретичні дослідження з комп'ютерної інженерії та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми;

– застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи;

– здійснювати пошук та критичний аналіз інформації, концептуалізацію та реалізацію наукових проектів з комп'ютерної інженерії;

– знати, розуміти та вміти застосовувати методи та засоби створення інформаційних технологій та програмного забезпечення розподілених систем, інтернету речей, хмарних обчислень, систем штучного інтелекту, віртуальної

реальності у предметних областях різних галузей, в тому числі в аерокосмічній галузі.

5. Міждисциплінарні зв'язки. Дисципліна є вибірковою компонентою освітньо-наукової програми «Комп'ютерна інженерія» і базується на знаннях, отриманих під час вивчення дисциплін: «ІТ в практиці наукових досліджень», «Теорія і методи зеленої ІТ-інженерії», «Теорія і технології критичного комп'ютингу», «Наукові англомовні комунікації», «Теорія планування експерименту», що є обов'язковими компонентами.

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для підготовки дисертаційної роботи .

3. Програма навчальної дисципліни
Модуль 1

Змістовний модуль 1. Основи безпеки критичної інфраструктури

Тема 1. Базові поняття про критичну інфраструктуру та її захист.

Об'єкти критичної інфраструктури. Критерії віднесення об'єктів до критичної інфраструктури. Категорії об'єктів критичної інфраструктури. Безпека критичної інфраструктури.

Тема 2. Структура критичних систем.

Структура критичних систем. Складові елементи критичних систем. Моделі критичних систем. Інформаційна безпека в критичних інфраструктурах. Вразливі елементи критичних систем, що потребують захисту. Способи захисту критичної інфраструктури.

Тема 3. Ризики та загрози для об'єктів критичної інфраструктури.

Поняття ризику та його види. Аналіз можливих ризиків. Оцінка ризиків. Визначення ризиків та способи їх попередження, долання та усунення. Поняття загрози та її види. Аналіз загроз. Оцінка загроз на основі ризиків. Запобігання загрозам.

Модульний контроль.

Змістовний модуль 2. Захист критичної інфраструктури.

Тема 4. Система захисту об'єктів критичної інфраструктури.

Математичні моделі захисту об'єктів критичної інфраструктури. Сучасні системи захисту. Види систем захисту. Застосування у різних областях критичних систем відповідних до них систем захисту.

Тема 5. Кібербезпека критичних інфраструктур.

Аналіз існуючих загроз і атак на ІТ- критичні інфраструктури. Моделі атак на ІТ- критичні інфраструктури. Методи оцінки загроз кібербезпеці. Моделі кібербезпеки об'єктів (систем) критичної інфраструктури. Методи забезпечення кібербезпеки.

Тема 6. Проектування систем захисту об'єктів критичної інфраструктури.

Вибір об'єктів критичної інфраструктури. Визначення та оцінка загроз та ризиків. Вибір способів захисту. Формалізований опис захисту. Складання математичної моделі системи захисту. Вибір способів реалізації системи захисту. Перспективи розвитку систем захисту критичної інфраструктури.

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
Модуль 1					
Змістовний модуль 1. Основи безпеки критичної інфраструктури.					
Тема 1. Базові поняття про критичну інфраструктуру та її захист.	26	6		6	14
Тема 2. Структура критичних систем.	26	6		6	14
Тема 3. Ризики та загрози для об'єктів критичної інфраструктури.	25	6		5	14
Модульний контроль.	1			1	
Разом за змістовним модулем 1	**78**	**18**		**18**	**42**
Змістовний модуль 2. Захист критичної інфраструктури.					
Тема 5. Система захисту об'єктів критичної інфраструктури.	24	6		6	12
Тема 6. Кібербезпека критичних інфраструктур.	24	6		4	14
Тема 7. Проектування систем захисту об'єктів критичної інфраструктури.	23	4		5	14
Модульний контроль	1			1	
Разом за змістовним модулем 2	**72**	**16**		**16**	**40**
Усього годин за дисципліною	**150**	**34**		**34**	**82**

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено*	
2		
	Разом	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено*	4
2		
	Разом	

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Моделі об'єктів критичної інфраструктури	6
2	Оцінка ризиків та загроз для об'єктів критичної інфраструктури	6
3	Моделі систем захисту об'єктів критичної інфраструктури	6
4	Моделі атак IT- критичні інфраструктури	6
5	Моделі кібербезпеки об'єктів (систем) критичної інфраструктури	4
6	Проектування систем захисту об'єктів критичної інфраструктури	6
	Разом	**34**

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Нормативне регулювання безпеки критичної інфраструктури	14
2	Критична інфраструктура в ЄС та США	14
3	Моделі ризиків та загроз об'єктам критичної інфраструктури	14
4	Методи фізичного захисту об'єктів критичної інфраструктури	12
5	Методи пентестінгу об'єктів критичної інфраструктури	14
6	Методи забезпечення кібербезпеки об'єктів критичної інфраструктури	14
	Разом	**82**

9. Індивідуальні завдання

Не передбачено навчальним планом

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота аспірантів за відповідними матеріалами.

11. Методи контролю

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

12. Критерії оцінювання та 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
Змістовний модуль 1			
Робота на лекціях	0…2	9	0…18
Виконання лабораторних робіт	0...4	4	0...16
Модульний контроль	0…16	1	0…16
Змістовний модуль 2			
Робота на лекціях	0…2	8	0…16
Виконання лабораторних робіт	0...4	4	0...16
Модульний контроль	0…18	1	0…18
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту 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 одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- знати базові поняття безпеки об'єктів критичної інфраструктури;
- знати основні способи захисту критичної інфраструктури;
- знати основні підходи щодо оцінки ризиків та загроз для критичної інфраструктури;
- знати основні способи захисту критичної інфраструктури.

Необхідний обсяг вмінь для одержання позитивної оцінки:

- уміти оцінювати ризиків та загроз для критичної інфраструктури ;
- уміти розробляти моделі об'єктів критичної інфраструктури;
- уміти розробляти моделі захисту об'єктів критичної інфраструктури.

12.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь, виконати 60% лабораторних завдань. Знати базові поняття, що стосуються оцінки безпеки критичної інфраструктури, а також методів захисту об'єктів критичної інфраструктури

Добре (75-89). Твердо знати теоретичний мінімум, опанувати матеріали всіх лекцій і виконати не менше 75% лабораторних завдань. Показати вміння виконувати всі практичні завдання в обумовлений викладачем строк з обгрунтуванням рішень та заходів, які наведено у методичних посібниках з практичних занять.

Відмінно (90-100). Повно знати основний та додатковий матеріал. Знати усі теми. Виконати не менше 90% лабораторних завдань. Орієнтуватися у підручниках та посібниках. Досконально знати та володіти способами оцінки стану критичної інфраструктури, вміти розробляти моделі, необхідні для проектування систем захисту, та використовувати методи захисту критичної інфраструктури.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Фесенко Г.В. Аспекти безпеки критичної інфраструктури: навчальний посібник / Фесенко Г.В., Клюшніков І.М., Харченко В.С.. – Х.: НАКУ «ХАІ», 2021. – 108 с.

14. Рекомендована література

Базова

2. Єсін В.І. Безпека інформаційних систем і технологій: навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.

3. Developing The Critical Infrastructure Protection System in Ukraine:monograph / [S. Kondratov, D. Bobro, V. Horbulin et al.]; general editor O. Sukhodolia. – Kyiv : NISS, 2017. – 184 p.

Допоміжна

1. Бурячок В. Л., Соколов В. Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів : Монографія. Київ : КУБГ, 2019. 164 с.

2. Taj Dini M., Sokolov V. Yu. Internet of Things Security Problems. Сучасний захист інформації. 2017. №1. С. 120–127. DOI: 10.5281/zenodo.2528814. arXiv: 1902.08597.

3. Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест - Київ : Дніпро, 364 с.

15. Інформаційні ресурси

1. Homeland Security. Energy Sector. [Електронний ресурс]. – URL: http://www.dhs.gov/energy-sector.

2. National Security Strategy. – Washington: The White House, Feb, 2015 [Електронний ресурс]. – URL: https://nssarchive.us/wp-content/uploads/2020/04/2015.pdf

3. European Programme for Critical Infrastructure Protection. [Електронний ресурс]. – URL: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terror i sm/l33260_en.htm.