

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПП
ОК2

ЗАТВЕРДЖУЮ



Проректор з науково-педагогічної
роботи, к.т.н., доцент

С.О. Слободян

_____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

**МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ ОБ'ЄКТІВ І ПРОЦЕСІВ
ЗАХИСТУ ІНФОРМАЦІЇ**

**Modeling and Optimization of Information
Protection Objects and Processes**

Рівень вищої освіти другий (магістерський)
Тип дисципліни обов'язкова
Мова викладання українська

Миколаїв 2025 рік

Робоча програма навчальної дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» є однією із складових комплексної підготовки фахівців галузі знань F «Інформаційні технології», спеціальності F5 «Кібербезпека та захист інформації», освітня програма «Системи технічного захисту інформації, автоматизація її обробки»
«21» 04 2025 р. – 43 с.

Розробник: Турти М.В., доцент кафедри Комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» узгоджено з гарантом освітньої програми

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»
д.т.н., професор»

 В.І. Передерій

Проект робочої програми навчальної дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» розглянуто на засіданні кафедри КТІБ.

Протокол від «21» 04 2025 р. № 12.

Завідувач кафедри КТІБ, к.т.н., доцент

 С.М. Нужний

Проект робочої програми навчальної дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від «15» 05 2025 р. № 5.

Заступник голови МР ННІАЕ,
к.т.н., доцент

 С.М. Новогрецький

Проект робочої програми навчальної дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» погоджено з навчальним відділом.

Начальник навчального відділу, к.т.н., доцент

 А.В. Лабарткава

Робочу програму навчальної дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» затверджено Навчально-методичною радою НУК ім. адм. Макарова.

Протокол від «21» 05 2025 р. № 5.

Голова Навчально-методичної ради
НУК ім. адм. Макарова, к.т.н., доцент

 С.О. Слободян

ЗМІСТ

Вступ.....	4
1. Опис навчальної дисципліни	5
2. Мета навчальної дисципліни	6
3. Передумови для вивчення навчальної дисципліни	8
4. Очікувані результати навчання	8
5. Програма навчальної дисципліни	8
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування.....	28
7. Форми поточного та підсумкового контролю	30
8. Критерії оцінювання результатів навчання.....	32
9. Засоби навчання	38
10. Рекомендовані джерела інформації.....	39

ВСТУП

Анотація

Навчальна дисципліна «Моделювання та оптимізація об'єктів і процесів захисту інформації» є дисципліною загальної підготовки магістрів за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» галузі знань F «Інформаційні технології», спеціальності F «Кібербезпека та захист інформації». Дана дисципліна є обов'язковим компонентом освітньої програми, який забезпечує формування умінь використовувати різноманітні методи оптимізації для побудови ефективних систем захисту інформації і досліджувати процеси захисту інформаційних ресурсів обмеженого доступу на математичних моделях. Отримані слухачами курсу теоретичні знання та практичні навички є базовим програмним результатом навчання та формують фахову компетентність.

Важливість засвоєння теоретичних знань і здобуття практичних навичок оптимізації та дослідження на математичних моделях систем технічного захисту інформації обумовлена необхідністю їх динамічного вдосконалення з метою адаптації до високих темпів змін умов експлуатації таких систем у кіберпросторі. Основна увага в процесі викладання дисципліни приділяється вивченню методів вирішення актуальних прикладних задач інформаційної безпеки.

Ключові слова: оптимізація, математичне програмування, системи масового обслуговування, теорія ігор, мережі Петрі, управління проектами, захист інформаційних ресурсів обмеженого доступу, математична модель.

Abstract

The educational discipline "Modeling and Optimization of Information Protection Objects and Processes" is a discipline of general master's training under the educational program "Systems of technical protection of information, automation of its processing" of the field of knowledge F "Information technologies", specialty F5 "Cybersecurity and information protection". This discipline is a mandatory component of the educational program, which provides the formation of the ability to use various optimization methods to build effective information protection systems and research the processes of protecting information resources with limited access using mathematical models. The theoretical knowledge and practical skills acquired by the students of the course are the basic program outcome of the study and form professional competence.

The importance of acquiring theoretical knowledge and acquiring practical skills of optimization and research on mathematical models of technical information protection systems is due to the need for their dynamic improvement in order to adapt to the high rates of changes in the operating conditions of such systems in cyberspace. The main attention in the process of teaching the academic discipline is given to the study of methods of solving actual applied problems of information security.

Keywords: optimization, mathematical programming, mass service systems, game theory, Petri nets, project management, protection of restricted access information resources, mathematical model

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 9	Галузь знань F «Інформаційні технології» Спеціальність: F5 «Кібербезпека та захист інформації»	Обов'язкова	
Модулів – 3	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 4		1-й	1-й
		Семестр	
Загальна кількість годин – 270		1-ий, 2-ий	1-ий, 2-ий
Тижневих годин для денної форми навчання: 1-ий семестр: Аудиторних – 3 Самостійної роботи: – 3. 2-ий семестр: Аудиторних – 3; Самостійної роботи: – 9.	Рівень вищої освіти: другий (магістерський)	Лекції, год	
		30 год.	8 год.
		Лабораторні роботи, год	
		30 год.	10 год.
		Практичні роботи, год	
		30	8
		Самостійна робота, год	
		180	244
		Вид контролю: 1-ий семестр – екзамен 2-ий семестр – екзамен, курсова робота	
		Форма контролю: усна, письмова	

2. Мета навчальної дисципліни

Метою вивчення навчальної дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» є оволодіння здобувачами вищої освіти теоретичними методами і практичними методиками моделювання та оптимізації процесів в системах технічного захисту інформації

Завданнями дисципліни є теоретична та практична підготовка студентів для вирішення конкретних фахових питань, зокрема: обґрунтування прийняття рішень при побудові систем обробки інформації обмеженого доступу і оцінці їх ефективності, при проектуванні технічних засобів захисту інформації на основі системного підходу, системного аналізу, як основних методів створення моделей систем; вивчення методик дослідження багаторівневих ієрархічних систем, дослідження узгодженості та координованості у багаторівневих ієрархічних системах управління, методик створення математичних моделей управління в ієрархічних системах; вивчення концепцій проектування комплексних систем захисту інформації, технологій, життєвих циклів, моделей та методів проектування; засобів оптимізації об'єктів і процесів в системах захисту інформації; здобуття практичних навичок прийняття рішень в галузі ТЗІ на основі діючої нормативно-правової бази (для студентів, що мають форму допуску до складу нормативно-правової бази включені документи з обмеженим доступом) при побудові систем обробки інформації обмеженого доступу і оцінці ефективності їх захисту; здобуття практичних навичок обґрунтованого вибору методів побудови моделей безпеки і розповсюдження прав доступу, побудови систем захисту від загроз порушення інформаційної безпеки для формування наступних компетентностей:

Інтегральна компетентність:

– Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки

Загальні компетентності

- (ЗК-2) Здатність проводити дослідження на відповідному рівні;
- (ЗК-3) Здатність до абстрактного мислення, аналізу та синтезу;
- (ЗК-4) Здатність оцінювати та забезпечувати якість виконуваних робіт;

Фахові компетентності:

– (КФ-1) Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки;

- (КФ-5) Здатність до дослідження, системного аналізу та забезпечення

безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

– (КФ-10) Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки;

– (КФ-15) Здатність адмініструвати системи, мережі та системи безпеки інформації.

Компетентності, набуті здобувачами вищої освіти за ОПП «Системи технічного захисту інформації, автоматизація її обробки» спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» в результаті вивчення дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» відповідають:

– Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затверджену наказом Міністерства освіти і науки України від 18.03.2021 року №332 (згідно з Постановою Кабінету міністрів України №1392 від 16.12.2022 р. – за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології»; згідно з Постановою Кабінету міністрів України №1021 від 30.08.2024 р. – за спеціальністю F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології»);

– Професійному стандарту «Фахівець сфери захисту інформації», затверджену Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації №715 від 25.11.2022 р. (професійна кваліфікація – провідний фахівець сфери захисту інформації)

Відповідність компетентностей, набутих здобувачами вищої освіти в результаті вивчення дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації», Стандарту вищої освіти зі спеціальності і Професійним стандартам

№ з/п	ОПП «Системи технічного захисту інформації, автоматизація її обробки»	Стандарт вищої освіти зі спеціальності	ПС «Фахівець сфери захисту інформації»
1	ЗК-2	КЗ-2	—
2	ЗК-3	КЗ -3	ЗК.04
3	ЗК-4	КЗ -4	ЗК.03
4	КФ-1	КФ1	А1

№ з/П	ОПП «Системи технічного захисту інформації, автоматизація її обробки»	Стандарт вищої освіти зі спеціальності	ПС «Фахівець сфери захисту інформації»
5	КФ-5	КФ5	A2
6	КФ-10	КФ10	Д
7	КФ-15	КФ15	A8

3. Передумови для вивчення навчальної дисципліни

Передумовами для вивчення дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» є наступні дисципліни першого (бакалаврського) рівня вищої освіти.

- Інформаційні технології в захисті інформації та кібербезпеці;
- Управління інформаційною безпекою;
- Безпека інформаційних та комунікаційних систем;
- Методи і засоби захисту інформації;
- Технічні засоби охорони об'єктів;
- Захист програмного продукту;
- Комплексні системи захисту інформації;
- Моделювання об'єктів і процесів технічного захисту інформації.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» є:

- (РН2) Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах;
- (РН3) Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі;
- (РН4) Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки;
- (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та/або кібербезпеки в цілому;

- (РН16) Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень;
- (РН17) Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання;
- (РН19) Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності;
- (РН21) Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки;
- (РН22) Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки;
- (РН24) Приймати обґрунтовані рішення з виконання передпроектних робіт щодо систем та комплексів захисту інформації, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

Результати навчання з дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» здобувачів вищої освіти за ОПП «Системи технічного захисту інформації, автоматизація її обробки» спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» відповідають:

- Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затверджені наказом Міністерства освіти і науки України від 18.03.2021 року №332 (згідно з Постановою Кабінету міністрів України №1392 від 16.12.2022 р. – за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології»; згідно з Постановою Кабінету міністрів України №1021 від 30.08.2024 р. – за спеціальністю F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології»);
- Професійному стандарту «Фахівець сфери захисту інформації», затверджені Наказом Адміністрації Державної служби спеціального зв'язку та

захисту інформації №715 від 25.11.2022 р. (професійна кваліфікація – провідний фахівець сфери захисту інформації).

Відповідність результатів навчання з дисципліни «Моделювання та оптимізація об'єктів і процесів захисту інформації» Стандарту вищої освіти і Професійному стандарту «Фахівець сфери захисту інформації»

№ з/п	ОПП «Системи технічного захисту інформації, автоматизація її обробки»	Стандарт вищої освіти	ПС «Фахівець сфери захисту інформації»	
			Знання	Уміння
1	РН-2	РН2	В1.31	В1.У1
2	РН-3	РН3	Г1.31	А1.У4 Г1.У4 Г2.У3
3	РН-4	РН4	Г1.31	А1.У4
4	РН-14	РН14	А1.35 А2.31 Б1.34 В4.31 Г1.33	А1.У4 А3.У1
5	РН-16	РН16	А1.35 Б1.31 В1.31 Г1.33 Д1.32 Д2.32	В1.У1
6	РН-17	РН17	Г1.31	А3.У5
7	РН-19	РН19	А2.34 Б2.35 Г1.31	А3.У5 Г2.У3
8	РН-21	РН21	А2.34	А1.У4
9	РН-22	РН22	А2.34 Г1.31	А1.У5 А3.У5
10	РН-24	РН24 (А5)	А2.34 В1.31	В1.У1

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Моделювання і аналіз складних ієрархічних систем

Тема 1. Класифікація і методи аналізу систем. Процедури оптимізації в інформаційній безпеці. [4]: с.95-109; [5]: с.7-68, 189-191; [7]: с.13-169; [8]: с.8-14; [9]: с.46-57, 76-82

Перелік питань, що виносяться на вивчення за темою:

Поняття «складна система», «дослідження операцій», «системний аналіз», «системний підхід», «системний синтез», «системотехніка»

Складні системи та їх характеристики: класифікації складних систем, матеріальні та нематеріальні складні системи, розвиток складних систем, мета системи, структурна схема складної системи, емерджентність, синергізм, життєвий цикл системи, простір станів системи.

Моделі складних систем: класифікації моделей складних систем, модель “чорної скрині”, модель складу і модель структури системи, структурна схема складної системи, моделі, що містять проблем у і моделі, що містять розв’язок проблеми, динамічні моделі систем, імітаційні моделі систем.

Декомпозиція складних систем і агрегування: моделі систем, як основа декомпозиції, алгоритмізація процедури декомпозиції, модель дерева цілей, що побудована методом декомпозиції, види агрегування, конфігуратор, агрегати-оператори, функція декількох змінних як агрегат.

Теорія прийняття рішень: загальна характеристика, ентропійна інтерпретація прийняття рішень, всхідна і спадна стратегії проектування, етапи системного розв’язку проблеми, етапи системного аналізу, альтернативи, сценарії.

Методи оптимізації: метод градієнтного спуску, виявлення локальних і глобальних оптимумів заданої функції багатьох змінних, Парето-оптимальні рішення задач оптимізації, засоби визначення бажаних сценаріїв, політики.

Функція мети: принципи визначення, вагові коефіцієнти в складових мети, функція мети в системах захисту інформації.

Критерії оптимізації: загальна характеристика, критерії оптимізації в умовах невизначеності, критерій Гурвіца, критерій Лапласа, критерій Севіджа, критерій Вальда, критерії оптимізації в інформаційній безпеці, стандартні профілі захищеності як критерії оптимальності системи захисту, критерії захищеності.

Тема 2. Метод аналізу ієрархій і його розширення. Методи комбінаторно-морфологічного аналізу і синтезу. [5]: с.103-113, 159-188, 233-241; [7]: с.170-208, 253-285

Перелік питань, що виносяться на вивчення за темою:

Метод аналізу ієрархій: типи ієрархій за характером зв’язків критеріїв та альтернатив, методи порівняння альтернатив, ієрархія з однаковою кількістю і функціональним складом альтернатив під критеріями, локальні пріоритети і методи їх отримання, визначення пріоритетів за матрицею попарних порівнянь, оцінювання послідовності тверджень експертів, алгоритм синтезу глобальних пріоритетів альтернатив, оцінювання однорідності ієрархії, динамічні переваги і пріоритети, функції, що апроксимують динамічні твердження, врахування тверджень декількох експертів, порівняння об’єктів із стандартами, порівняння об’єктів методом копіювання, багатокритеріальний вибір на ієрархіях з різною кількістю та функціональним складом критеріїв оцінювання альтернатив.

Метод ELECTRE

Морфологія.

Метод систематичного покриття поля.

Метод морфологічної скрині.

Етапи морфологічних досліджень.

Обробка інформації для аналізу і синтезу систем.

Морфологічні таблиці.

Синтез раціональних систем на морфологічних множинах.

Міри подібності і відмінності. Міра включення.

Пряма, оптимізаційна і апроксимаційна кластеризація.

Врахування при синтезі різного впливу підсистем.

Синтез систем на основі якісних класифікаційних ознак.

Синтез варіантів за прототипом.
 Метод деревоподібного синтезу.
 Метод лабіринтного синтезу.
 Метод блочно-лабіринтного синтезу.

Тема 3. Математичні моделі типових задач лінійного програмування і методи їх розв'язку. [5]: с.70-84; [8]: с.15-90, 248-254; [9]: с.83-90, 100-108

Перелік питань, що виносяться на вивчення за темою:
 Математичне програмування.
 Область припустимих рішень.
 Форми області припустимих рішень задачі лінійного, нелінійного і дискретного програмування в багатовимірному просторі
 Формалізація задачі математичного програмування. Види обмежень.
 Графоаналітичний метод розв'язку задачі лінійного програмування..
 Графоаналітичний розв'язок багатокритеріальної задачі лінійного програмування.
 Загальна, стандартна і канонічна форми задачі лінійного програмування.
 Задача про планування випуску продукції при обмежених ресурсах.
 Задача про суміші.
 Оптимальний розподіл однотипних виробничих завдань..
 Оптимальне використання потужності підприємства за визначений термін..
 Максимізація прибутку в часі.
 Метод Жордана-Гауса. Перетворення нерівностей-обмежень на рівності. Базисні і вільні змінні.
 Симплексна таблиця.. Вирішальний рядок. Вирішальний стовпчик. Опорний план.
 Правила перетворення симплексної таблиці.
 Оптимальний план. Псевдоплан. Вироджена задача лінійного програмування. Ознаки відсутності рішення задачі лінійного програмування. Ознаки протирічності обмежень в задачі лінійного програмування.
 Складання двоїстої задачі лінійного програмування.
 Основні теореми двоїстості.
 Рішення прямої і двоїстої задачі.
 Двоїстий симплексний метод.: умови використання, алгоритм, умови несумісності і лінійної залежності обмежень, псевдо план, ознака наявності опорних планів

Тема 4. Аналіз дискретних систем і нелінійних систем. Транспортна задача. Комбінаторно-граничні методи. [5]: с.84-94; [8]: с.91-196; [9]: с.16-19, 108-111, 131-150; [26]

Перелік питань, що виносяться на вивчення за темою:
 Задачі цілочисельного програмування: математична модель задачі цілочисельного програмування, методи рішення задач цілочисельного програмування.
 Метод Гоморі: алгоритм для цілком цілочисельних задач, умови наявності рішення, правила перетворення симплекс-таблиці, алгоритм для частковоцілочисельних задач, умови наявності рішення, правила перетворення симплекс-таблиці.
 Транспортна задача: математична модель транспортної задачі, закрыта і відкрита транспортні задачі, математична модель задачі про призначення, методи початкового розподілу постачання (метод «північно-західного кута», метод найменших втрат споживачів, метод найменших втрат постачальників, метод Фогеля), метод потенціалів, цикли, перерозподіл постачання

Задачі нелінійного програмування: метод множників Лагранжа, інтерпретація множників Лагранжа, метод конфігурацій, метод штрафних функцій.

Задачі динамічного програмування: математична модель задачі динамічного програмування, принцип оптимальності Беллмана, задача про зміну стану системи, метод гілок та меж.

Типові задачі: задача рюкзака, задача розподілу обмежених коштів, задача заміни обладнання, задача забезпечення кадрами, задачі розкрою

Використання типових задач дослідження операцій в системах технічного захисту інформації.

Змістовий модуль 2. Методологія аналізу і синтезу оптимальних об'єктів і процесів КСЗІ

Тема 5. Аналіз процесів функціонування систем кібербезпеки за допомогою графів. [5]: с.299-308; [7]: с.286-322; [25]

Перелік питань, що виносяться на вивчення за темою:

Графи і їх характеристики: види графів, кущі і дерева, орієнтовані і неорієнтовані графи, основні характеристики дуг, змістовне навантаження дуг і вузлів, типові задачі аналізу графів, визначення зв'язності, повнозв'язна система, багаторівневі графи, багатокольорові графи, розмітка графів, матричне представлення графів.

Дерева: дерево цілей, дерево рішень, дерево проблем, дерево напрямків розвитку, дерево відмов: загальна характеристика, бінарне дерево, покривне дерево, правила побудови дерева цілей.

Метод PATTERN: етапи, принципи, коефіцієнти відносної важливості, коефіцієнти взаємної корисності, коефіцієнт «стан-строк», матриця «цілі-засоби», прийоми конкретизації верхніх рівнів дерева цілей.

Когнітивні карти: аналіз систем за допомогою когнітивних карт (визначення, концепти, графічне відображення), методи побудови когнітивних карт, визначення поведінки шляхів та циклів на когнітивних картах, проблема передбачення наслідків прийняття рішення за когнітивними картами, пояснення результатів і прийняття рішення за когнітивними картами.

Таблиця рішень.

Функціонально-вартісний аналіз.

Дерево відмов: потенційне джерело шкоди; поняття «безпека», «небезпека», «носій небезпеки», «надзвичайна подія»; критерії класифікації надзвичайних подій; надзвичайні ситуації природного, техногенного, соціально-політичного і військового характеру; надзвичайні ситуації загальнодержавного, регіонального, об'єктового рівнів та рівня об'єкта інформаційної діяльності; поняття критичної інфраструктури; нормативно-правове забезпечення визначення ризиків і критичності подій, концепція припустимого ризику

Ризик-орієнтований підхід в управлінні безпекою

Якісний аналіз небезпек: загальна характеристика, типи аналізу, методи аналізу

Попередній якісний аналіз небезпек: загальна характеристика, алгоритм, принципи визначення критичних елементів, базові питання, шкала для встановлення тяжкості наслідків відмов, якісні оцінки частоти виникнення небезпек, матриця визначення рангу небезпеки, особливості якісного аналізу небезпек і галузі захисту інформації

Кількісний аналіз відмов: загальна характеристика, структура і принципи побудови дерева відмов, умовні позначення логічних операцій і подій на дереві відмов, розрахункові вирази для логічних операцій І та АБО, структура робочого аркушу кількісного аналізу видів, наслідків і критичності відмов

Мережі Петрі: визначення, структура, графічне відображення, виконання мереж Петрі, маркування, послідовність маркувань, послідовність переходів, множина досяжності,

моделювання одночасності засобами мереж Петрі, моделювання конфліктів засобами мереж Петрі, непримітивні події, задача про взаємне виключення, узагальнення мереж Петрі

Управління проектами: класифікація проектів, зовнішні чинники управління проектами, внутрішні чинники управління проектами, цілі та принципи управління проектами, життєвий цикл проекту, функції управління проектами, мережний граф, вхідні дані для побудови мережних графів, правила побудови мережних графів, нумерація вузлів мережного графа, мінімальний і максимальний час настання події, критичний час проекту, повний і робочий резерв часу роботи, коефіцієнт критичності роботи, критичний шлях, підкритичний шлях, діаграми Ганта, правила побудови лінійних діаграм, варіанти представлення інформації про ресурсні обмеження і потреби, розв'язок задачі планування робіт при обмежених ресурсах на лінійних діаграмах.

Автоматизовані системи управління проектами: функції автоматизованих систем управління проектами, функції систем календарно-мережного планування, класифікація автоматизованих систем управління проектами, загальна характеристика моделі проекту в автоматизованих системах управління проектами, Microsoft Project (загальна характеристика, дії при створенні нового проекту, введення і кодування задач, декомпозиція робіт, залежності між задачами, оцінювання тривалості задачі, управління ресурсами, витратами і ризиками, методи визначення задач з високим ризиком, визначення ресурсів з високим ризиком, відстеження змін, обмін даними між учасниками проекту, завершення проекту, Microsoft ProjectCentral.com), Open Plan Professional, Sure Trek Project Manager, Primavera Project Planner, Basecamp

Задача комівояжера: задача комівояжера для орієнтованої і для неорієнтованої мережі, метод редукції рядків та колонок для задачі комівояжера, метод осереднених коефіцієнтів для задачі комівояжера, спрощені методи рішення задачі комівояжера.

Задача виходу з лабіринту. Рішення задачі виходу з лабіринту на графі.

Визначення шляхів в мережі: визначення найдовшого і найкоротшого шляху в орієнтованій мережі, визначення найкоротшого шляху в неорієнтованій мережі.

Визначення максимального потоку в мережі.

Тема 6. Теорія масового обслуговування. Теорія ігор. [5]: с.94-103; [8]: с.197-247; [9]: с.13-16, 69-76, 92-100, 195-223; [10]

Перелік питань, що виносяться на вивчення за темою:

Імітаційне моделювання

Теорія масового обслуговування: математична модель системи масового обслуговування, розподіл Пуассона, задачі аналізу систем масового обслуговування, Статичний режим систем масового обслуговування

Неперервні і дискретні марківські ланцюги

Теорія розкладів.

Теорія ігор: загальна характеристика, класифікація ігор, матрична гра, ігри з сідловою точкою, ігри з природою (статистичні ігри), оцінювання гри, нижня і верхня ціни гри, чисті та змішані стратегії, представлення матричної гри як задачі лінійного програмування, принципи аналізу систем на ігрових моделях, отримання висновків за ігровими моделями, використання теорії ігор при аналізі систем захисту інформації, моделювання інформаційної безпеки корпоративних систем підприємств з використанням теорії ігор і марковських процесів, моделювання інформаційного протистояння засобами теорії ігор, оцінювання життєздатності інформаційної системи засобами теорії ігор

Тема 7. Засоби штучного інтелекту. [5]: с.119-122; [22]; [23]; [9]: с.155-195

Перелік питань, що виносяться на вивчення за темою:

Засоби штучного інтелекту.

Обробка і представлення експертної інформації.

Нечіткі знання. Нечіткі множини.
 Методи формування функцій приналежності.
 Теорія однозначних нечітких систем
 Структура експертних систем.
 Засоби створення експертних систем.
 Алгоритм роботи механізмів висновку в експертних системах.
 Технології отримання висновку в експертних системах.
 Правила отримання висновку на нечітких даних.
 Міра впевненості у гіпотезі та уточнення міри впевненості.
 Використання нечітких даних в інформаційній безпеці: загальна характеристика, біометричні СКД, криптологія, виявлення атак, управління інформаційною безпекою.

Тема 8. Методи аналізу і синтезу об'єктів і процесів КСЗІ. [4]: с.102-104, 167-181; [5]: с.113-136, 193-296; [9]: с.19-30, 111-131, 151-154

Перелік питань, що виносяться на вивчення за темою:
 Проблеми моделювання в сфері інформаційної безпеки
 Вирішення задач менеджменту інформаційної безпеки на математичних моделях
 Алгоритм побудови математичної моделі протистояння
 Моделі оцінювання інвестицій в інформаційну безпеку
 Моделі втрат інформації і процесі антагоністичного протистояння
 Дослідження на математичних моделях ефективності розвідки при протистоянні двох сторін в інформаційній сфері
 Оптимізація сумарних втрат у сфері захисту інформації
 Методологія IDEF
 Прийняття рішень в умовах невизначеності: особливості застосування нечітких множин і стохастичного підходу при обґрунтуванні та прийнятті управлінських рішень в умовах невизначеності, статистичний і аналітичний методи оцінювання ризику при прийнятті управлінських рішень
 Методи комплексного оцінювання результатів прийнятих управлінських рішень: метод сум, метод геометричної середньої, метод коефіцієнтів, методи суми місць та суми балів, метод відстаней, таксонометричний метод.
 Оцінювання альтернативних варіантів побудови систем автоматизації
 Оцінювання альтернативних варіантів автоматизованих робочих місць в інформаційних системах
 Оцінювання якості та конкурентоспроможності систем електронного документообігу
 Нормативно-правова база системного аналізу систем захисту інформації.
 Моделювання об'єктів і процесів захисту інформації (загальна характеристика).
 Вимоги до програмних продуктів для аналізу об'єктів і процесів кібербезпеки.
 Програмні продукти для аналізу об'єктів і процесів кібербезпеки: Засоби MS Office, CASE-технології, пакети статистичної обробки.
 Характеристики об'єктів інформаційної діяльності.
 Модель загроз.
 Модель порушника.
 Моделі засобів захисту.
 Системи підтримки прийняття рішень в галузі захисту інформації.

Модуль 2

Змістовий модуль 3. Теорія захисту інформаційних ресурсів та кібервузлів обмеженого доступу

Тема 9. Основні поняття теорії захисту інформаційних ресурсів обмеженого доступу. [3]: с.13-52; [4]: с.130-167; [20]

Перелік питань, що виносяться на вивчення за темою:

Етапи розвитку парадигм захисту інформації.

Основні поняття теорії захисту інформаційних ресурсів обмеженого доступу: об'єкт захисту, інформаційна технологія, інформаційна система, автоматизована система, комп'ютерна система, обчислювальна система

Помилки під час розроблення систем захисту інформації як причина появи вразливостей

Класифікація вразливостей: критерії класифікації, класифікація вразливостей за стадіями життєвого циклу обчислювальної системи

Типи каналів потенційного порушення інформаційної безпеки.

Поняття гарантовано захищеної інформаційної технології

Взаємозв'язок між несанкціонованим і нелегітимним доступом.

Основні принципи розробки системи захисту

Основи розробки гарантовано захищених інформаційних технологій: концепція ієрархічної декомпозиції, доказовий підхід до побудови систем захисту, теорема про безпеку системи, теорема про достатність системи захисту, модель політики безпеки, модель безпеки, нормативний підхід до побудови систем захисту, взаємозв'язок доказового і нормативного підходів до побудови системи захисту, НД ТЗІ 2.5-004-99 як приклад доказового підходу до побудови систем захисту, довірча обчислювальна база, концепція диспетчера доступу, розмежування і керування доступом, правила розмежування доступу, об'єкти доступу, суб'єкти доступу, схема функціонування диспетчера доступу, монітор авторизації, ядро захисту, концепція ізоляції.

Основи розробки гарантованих систем захисту: моделі, методи і засоби забезпечення заданого рівня гарантій; система документів із забезпечення заданого рівня гарантій; перспективні напрями розвитку гарантованих систем захисту.

Тема 10. Загальні моделі опису процесів захисту інформації [3]: с.53-86

Перелік питань, що виносяться на вивчення за темою:

Типи моделей опису функціонування комп'ютерної системи.

Суб'єктно-об'єктна модель: об'єкт, об'єкт-користувач, об'єкт – процес, пасивний об'єкт, суб'єкт, домен комп'ютерної системи, потік інформації, доступ до інформації, типи доступів та їх нотації

Автоматна суб'єктно- об'єктна модель: мова опису, об'єкт відносно мови, процес, домен системи, статус «керування», опис взаємодії об'єктів в системі, опис стану системи та процесів його змін, фазовий простір системи, формулювання задачі захисту інформації, інформаційні потоки в системі, характеристики інформаційних потоків.

Опис базових операцій в системі на основі суб'єктно- об'єктної моделі: породження суб'єктів (властивості суб'єктів, відмінність понять «користувач» і «суб'єкт», аксіома породження суб'єктів, об'єкт- джерело для суб'єкта, активізуючий суб'єкт для суб'єкта, процедури породження суб'єктів та інформаційні потоки, асоціювання об'єктів із суб'єктами, потік інформації між об'єктами і типи потоків, доступ суб'єкта до об'єкта, правила розмежування доступу суб'єкт до об'єкта, тотожність об'єктів та тотожність суб'єктів, монітор звернень (змістовий монітор, індикаторний монітор) та монітор безпеки

Підходи до формування моделі загроз: класифікація загроз, методи реалізації загроз, розподіл методів реалізації загроз за рівнями доступу до інформації

Підходи до формування моделі порушника: типи моделей порушника, еталонні моделі, диференційовані моделі, класифікація порушників за НД ТЗІ.

Підходи та моделі опису цінності інформації: поняття «цінність інформації», «ціна інформації», «оцінка цінності інформації»; адитивна модель цінності інформації; порядкова шкала цінностей; модель решітки цінностей; MLS-решітка

Тема 11. Політика безпеки. [1]: с.686-689; [3]: с.87-105; [6]: с. 28

Перелік питань, що виносяться на вивчення за темою:

Поняття політики безпеки

Гранулювання захисту

Політики управління доступом: мандатна політика безпеки, дискреційна політика безпеки, рольова політика безпеки, адміністративна політика безпеки, довірча політика безпеки

Матриці доступів

Домен безпеки

Атрибути доступу

Підходи до керування доступом, визначені НД ТЗІ: довірче і адміністративне керування доступом; сталість атрибутів доступу; створення нових об'єктів, експорт та імпорт об'єктів

Моделі опису політики безпеки: мета створення моделей політики безпеки, формалізовані і неформалізовані моделі політики безпеки, галузі застосування моделей політики безпеки, базові положення моделей безпеки, класифікація моделей безпеки за типами загроз, класифікація моделей безпеки за типами захисту (моделі узагальненого аналізу захищеності, моделі дослідження політики безпеки, спеціалізовані моделі)

Теоретико-емпіричний підхід до оцінювання інформації

Аналітичні моделі: модель порушення фізичної цілісності інформації, модель отримання несанкціонованого доступу до інформації

Тема 12. Стандартизовані моделі. [3]: с.265-409; [11-21], [31]

Перелік питань, що виносяться на вивчення за темою:

Модель, що є основою стандарту ISO 7498-2: ієрархічна декомпозиція в моделі OSI/ISO, модель взаємодії відкритих систем; взаємодія на прикладному, представницькому, сеансовому, транспортному, мережевому, каналному і фізичному рівнях; взаємодія рівнів ієрархії; примітиви послуг; загрози в архітектурі відкритих мереж; засоби захисту, рекомендовані для моделі взаємодії відкритих систем процедури захисту, сервісні служби захисту, реалізація захисту, адміністрування засобів безпеки

Модель, що є основою стандарту ISO 15408: структура ISO 15408, основні компоненти безпеки, загальна методологія оцінки безпеки інформаційних технологій, кваліфікаційний аналіз, потенційні загрози безпеці, типові завдання захисту, вимоги до політики безпеки, порівняння продукту інформаційних технологій і системи обробки інформації, профіль захисту, проект захисту, структура функціональних вимог безпеки, класи функціональних вимог, декомпозиція класів функціональних вимог, вимоги гарантій безпеки, декомпозиція класів гарантій, рівні гарантій безпеки, види тестувань, напівформальні і формальні методи верифікації розробки та тестування.

Модель, що є основою НД ТЗІ 2.5-004 і НД ТЗІ 2.5-005: загальні положення моделі, класифікація автоматизованих систем, функціональні критерії безпеки, послуги безпеки, функції безпеки, критерії гарантій безпеки, функціональні профілі захищеності інформації

Вимоги до моделі порушника, моделі загроз та політики безпеки за НД ТЗІ 1.4-001-2000

Опис вразливостей, загроз і порушників за ISO 27005:

Змістовий модуль 4. Моделі безпеки

Тема 13. Моделі розмежування доступу. [1]: с.682-686, 689-691; [3]: с.105-141; [6]: с.29-39

Перелік питань, що виносяться на вивчення за темою:

Моделі дискреційного доступу: загальна характеристика

Модель Харрісона-Руссо-Ульмана: призначення і базові принципи, формалізований опис, примітивні оператори, опис функціонування системи, умови застосування примітивних операторів, наслідки застосування примітивних операторів, команди, теорема Харрісона, граничні теореми в рамках моделі HRU, розвиток моделі HRU

Модель Take-Grant: призначення і базові принципи, формалізований опис, опис функціонування системи, правила перетворення графу доступів, правила де-юре моделі Take-Grant, правила де-факто моделі Take-Grant, моделювання санкціонованого одержання прав доступу, моделювання викрадення прав доступу, розширена модель Take-Grant, підходи до визначення вартості шляхів в розширеній моделі Take-Grant

Моделі мандатного доступу: загальна характеристика

Модель Белла-ЛаПадули: правила контролю доступу, формалізований опис, безпечні стани системи, основна теорема безпеки Белла-ЛаПадули, недоліки моделі Белла-ЛаПадули, розширення моделі Белла-ЛаПадули, основна теорема безпеки Мак-Ліна

Моделі з динамічною зміною рівнів суб'єктів та об'єктів: загальна характеристика, модель Low-Water-Mark (базові принципи, основні операції і умови їх дозволів, опис функціонування системи), модель підвищення рівня суб'єкта, модель зниження рівня суб'єкта

Спеціалізовані моделі безпеки: загальна характеристика моделі Лендвера, основні поняття моделі Лендвера (класифікація інформації, міра довіри до користувача, ідентифікатор користувача, роль, об'єкт, контейнер, сутність, вимоги міри довіри об'єктів, ідентифікатор сутності, пряме і непряме посилення на сутність, операція правила безпеки, обмеження безпеки

Інформаційні моделі: загальна характеристика, модель інформаційних потоків, модель невтручання, модель невиводимості

Ймовірнісні моделі: загальна характеристика, модель системи безпеки з повним перекриттям, ігрова модель, ланкова модель, модель Хартсона

Тема 14. Моделі забезпечення цілісності. [1]: с.691-693; [3]: с.141-149

Перелік питань, що виносяться на вивчення за темою:

Модель Бібі: основні принципи, взаємозв'язок моделі Бібі і моделі Белла-ЛаПадули, Варіації моделі Бібі, правила NRU і NWD моделі Бібі, формальний опис моделі Бібі, моделі із змінними рівнями суб'єктів та об'єктів (загальна характеристика, модель підвищення рівня суб'єкта, модель зниження рівня об'єкта), переваги і недоліки моделі Бібі

Модель Кларка-Вільсона: дані CDI та UDI, операції IVP та TP, правила моделі Кларка-Вільсона, порівняння моделі Кларка Вільсона з моделями Бібі і Белла-ЛаПадули

Модель контролю цілісності ядра системи: сегменти моделі, дескриптори, лічильники, привілеї процедур, умови преривань, дозволи звернень

Тема 15. Моделі забезпечення доступності. [3]: с.149-160

Перелік питань, що виносяться на вивчення за темою:

Загальна характеристика моделей забезпечення доступності

Основні поняття моделей забезпечення доступності: відмова у доступі, максимальний час очікування послуги та його трактовки, визначення мінімального часу очікування, визначення загрози на основі мінімального часу очікування

Мандатна модель забезпечення доступності: загальна характеристика, правила моделі, переваги і недоліки моделі

Модель Міллена розподілення ресурсів: загальна характеристика, порівняння моделі Міллена з моделями Бібі і Белла-ЛаПадули, формальний опис моделі Міллена, правила моделі Міллена, опис стратегій на основі моделі Міллена

Тема 16. Застосування моделей безпеки [1]: с. 682-683; [2]: с.501-528; [3]: с.160-196; [15]; [24]

Перелік питань, що виносяться на вивчення за темою:

Моделі захисту централізованих і розподілених операційних систем: модель операційної системи ADEPT-50, модифікація дискреційної моделі доступу для базової моделі безпеки операційної системи Unix, модифікація дискреційної моделі доступу для базової моделі безпеки операційних систем Windows

Моделі безпеки типових технологій обробки інформації: модель безпеки електронного каталогу за ІТУ-Т X.500 (загальна характеристика; об'єкти, їх ідентифікатори та атрибути; протоколи доступу; атрибути доступу; автономні області; зміст операцій над об'єктами, типами атрибутів та значеннями атрибутів; стандартні типи запитів до довідника, групування суб'єктів і об'єктів доступу; вибір пріоритетів ACL, алгоритм обчислення вирішальної функції), модель безпеки електронного каталогу на основі моделі забезпечення цілісності Кларка-Вільсона (базові принципи забезпечення цілісності, відповідність правил моделі Кларка-Вільсона базовим принципам забезпечення цілісності, коректність транзакцій, мінімізація привілеїв, розмежування функціональних обов'язків, аудит подій, об'єктивний контроль, управління передачею привілеїв

Модель безпеки інформаційної системи на базі технологій IoT

Модель багаторівневого захисту інформаційної системи організації

Методика синтезу моделей безпеки

Синтез гарантовано захищеної автоматизованої системи: моделювання автоматизованої системи (мова, об'єкти, загальні ресурси системи, суб'єкти, активізовані суб'єкти, умови активізації суб'єктів, опис функціонування системи), модель безпеки інформаційної системи (опис витоку інформації по каналах пам'яті, опис небезпечних дій користувача, умови відсутності каналів витоку, умови надання доступу), моделювання умов виконання вимог політики безпеки, реалізація гарантовано захищеної автоматизованої системи

Доведення гарантованості захищеності автоматизованих систем за допомогою моделей безпеки: загальна характеристика

Модуль 3

Індивідуальне науково-дослідне завдання (ІНДЗ):

курсowa робота за тематикою "Дослідження об'єктів і процесів інформаційної безпеки на регресійній моделі".

Примітка 1. Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів.

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Денна форма					Заочна форма				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
л		п	лаб	с.р	л		п	лаб	с.р	
Модуль 1 (М1)										
Змістовий модуль 1. Моделювання і аналіз складних ієрархічних систем										
Тема 1. Класифікація і методи аналізу систем. Процедури оптимізації в інформаційній безпеці	8	2	-	2	4	8	2	-	1	5
Тема 2. Метод аналізу ієрархій і його розширення. Методи комбінаторно-морфологічного аналізу і синтезу	8	2	-	2	4	8		-	1	7
Тема 3. Математичні моделі типових задач лінійного програмування і методи їх розв'язку	9	2	2	-	5	9	2	2	-	7
Тема 4. Аналіз дискретних систем і нелінійних систем. Транспортна задача. Комбінаторно-граничні методи.	20	2	4	4	10	20		-	-	20
Разом за змістовим модулем 1	45	8	6	8	23	45	2	2	2	39
Змістовий модуль 2. Методологія аналізу і синтезу оптимальних об'єктів і процесів КСЗІ										
Тема 5. Аналіз процесів функціонування систем кібербезпеки за допомогою графів	19	2	4	4	9	19	2	2	-	15
Тема 6. Теорія масового обслуговування. Теорія ігор	12	2	2	2	6	12		-	1	11
Тема 7. Засоби штучного інтелекту	8	2	2	-	4	8		-	-	8
Тема 8. Методи аналізу і синтезу об'єктів і процесів КСЗІ.	6	1	1	1	3	6	2	-	1	5
Разом за змістовим модулем 2	45	7	9	7	22	45	2	2	2	39
Разом за модулем 1	90	15	15	15	45	90	4	4	4	78

Назви змістових модулів і тем	Денна форма					Заочна форма				
	Кількість годин									
	усього	у тому числі				усього	у тому числі			
л		п	лаб	с.р	л		п	лаб	с.р	
Модуль 2 (М2)										
Змістовий модуль 3. Теорія захисту інформаційних ресурсів та кібервузлів обмеженого доступу										
Тема 9. Основні поняття теорії захисту інформаційних ресурсів обмеженого доступу.	9	2	2	-	5	9	2	-	-	7
Тема 10. Загальні моделі опису процесів захисту інформації	10	2	2	-	6	10		-	-	10
Тема 11. Політика безпеки	16	2	2	4	8	16		2	2	12
Тема 12. Стандартизовані моделі	10	2	2	-	6	10		-	-	10
Разом за змістовим модулем 3	45	8	8	4	25	45	2	2	2	39
Змістовий модуль 4. Моделі безпеки										
Тема 13. Моделі розмежування доступу	18	2	2	6	8	18	2	2	2	12
Тема 14. Моделі забезпечення цілісності	11	2	2	2	5	11			1	10
Тема 15. Моделі забезпечення доступності	11	2	2	2	5	11		-	-	11
Тема 16. Застосування моделей безпеки	5	1	1	1	2	5		-	1	4
Разом за змістовим модулем 4	45	7	7	11	20	45	2	2	4	37
Разом за модулем 2	90	15	15	15	45	90	4	4	6	76
Модуль 3 (М3)										
ІНДЗ – Курсова робота	90	–	–	–	90	90	–	–	–	90
Разом за модулем 3	90	–	–	–	90	90	–	–	–	90
Разом (М1+М2+М3)	270	30	30	30	180	270	8	8	10	244

Для студентів заочної форми навчання читаються оглядові лекції за темами змістових модулів в обсягах відповідно до вищенаведеної таблиці.

Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		ДФН	ЗФН
Модуль 1			
Змістовий модуль 1. Моделювання і аналіз складних ієрархічних систем			
1	Симплексний метод і двоїсті задачі лінійного програмування	2	2
2	Методи рішення задач цілочисельного програмування	2	-
3	Транспортна задача	2	-
Змістовий модуль 2. Методологія аналізу і синтезу оптимальних об'єктів і процесів КСЗІ			
4	Засоби визначення і дослідження оптимального складу і структури систем захисту інформації	2	-
5	Управління проектами в галузі розробки і впровадження систем захисту інформації	2	2
6	Теорія ігор	2	-
7	Нечіткі данні	2	-
8	Оцінювання управлінських рішень	1	-
Модуль 2			
Змістовий модуль 3. Теорія захисту інформаційних ресурсів та кібервузлів обмеженого доступу			
9	Класифікація несанкціонованого доступу	2	-
10	Класифікація загроз інформаційної безпеки	2	-
11	Поняття доступу і моніторингу безпеки	2	2
12	Нормативно-правові засади захисту інформаційних ресурсів обмеженого доступу	2	-
Змістовий модуль 4. Моделі безпеки			
13	Побудова систем захисту від загрози порушення конфіденційності інформації	2	2
14	Побудова систем захисту від загрози порушення цілісності інформації	2	-
15	Побудова систем захисту від загрози відмови в доступі до ресурсів	2	-
16	Побудова систем захисту від загрози розкриття параметрів інформаційних систем	1	-
Разом		30	8

Студенти заочної форми виконують практичні роботи № 1, 5, 11, 13

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		ДФН	ЗФН
Модуль 1			
Змістовий модуль 1. Моделювання і аналіз складних ієрархічних систем			
1	Методи оптимізації систем і засоби оптимізаційних розрахунків	2	1
2	Метод аналізу ієрархій і його розширення	2	1
3	Задачі нелінійного програмування	2	-
4	Задачі динамічного програмування	2	-
Змістовий модуль 2. Методологія аналізу і синтезу оптимальних об'єктів і процесів КСЗІ			
5	Опис та аналіз систем захисту інформації за допомогою дерев	2	-
6	Мережі Петрі	2	-
7	Системи масового обслуговування	2	1
8	Система комплексного захисту інформації	1	1
Модуль 2			
Змістовий модуль 3. Теорія захисту інформаційних ресурсів та кібервузлів обмеженого доступу			
9	Моделювання політики безпеки	2	1
10	Побудова матриці доступів	2	1
Змістовий модуль 4. Моделі безпеки			
11	Модель розповсюдження прав доступу Take-Grant	2	1
12	Модель системи безпеки Белла-Лападула	2	1
13	Модель Low-Water-Mark	2	
14	Моделі цілісності	2	1
15	Моделі доступності	2	
16	Побудова систем захисту інформації	1	1
Разом		30	10

Студенти заочної форми виконують лабораторні роботи № 1, 2, 7, 8, 9, 10, 11, 12, 14, 16 із розрахунку 1 год./ 1 лаб. роботу.

Самостійна робота

Самостійна робота здобувача вищої освіти є однією з форм організації навчання, основною формою оволодіння навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних, практичних і лабораторних заняттях. Самостійна робота проводиться в лабораторіях НУК, читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, виноситься на підсумковий контроль поряд з навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

В рамках самостійної роботи також виконується індивідуальне науково-дослідне завдання у формі курсової роботи.

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 0,25 – 0,5 год. / 1 заняття;
- підготовка до лабораторних робіт – 0,25 – 1 год. / 1 заняття;
- підготовка до практичних робіт – 0,25 – 1 год. / 1 заняття
- підготовка до модульних контрольних робіт 6 год на 1 роботу
- підготовка до екзаменів – 11 год. на 1 захід.

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 0,5 год. / 1 заняття (на 1 лекцію);
- самостійне опрацювання окремих тем навчальної дисципліни (які не викладаються на лекціях) – 1-3 год. / 1 заняття;
- підготовка до лабораторних робіт – 1 – 3 год. / 1 заняття;
- підготовка до практичних робіт – 1 – 3 год. / 1 заняття;
- підготовка до модульних контрольних робіт 11 год на 1 роботу
- підготовка до екзаменів – 30 год. на 1 захід.

Розподіл годин самостійного опрацювання окремих тем навчальної дисципліни

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н	З.Ф.Н.
Модуль 1			
1	До теми 1. Підбір параметру в Excel	0,25	1,0

№ з/п	Назва теми	Кількість годин	
		Д.Ф.Н.	З.Ф.Н.
2	До теми 2. Метод ELECTRE	0,5	1,0
3	До теми 3. Максимізація прибутку в часі	0,25	1,0
4	До теми 4. Метод Фогеля	0,5	1,0
5	До теми 5. Метод PATTERN	0,25	1,0
6	До теми 6. Microsoft Project	0,5	1,0
7	До теми 7. Неперервні і дискретні марківські ланцюги	0,5	1,0
8	До теми 8. Методологія IDEF	0,25	1,0
Усього годин за модуль 1		3	8
Модуль 2			
9	До теми 9. НД ТЗІ 2.5-004-99	0,25	1,0
10	До теми 10. Класифікація порушників за НД ТЗІ	0,5	1,0
11	До теми 11. Підходи до керування доступом, визначені НД ТЗІ	0,25	1,0
12	До теми 12. Вимоги до моделі порушника, моделі загроз та політики безпеки за НД ТЗІ 1.4-001-2000	0,5	1,0
13	До теми 13. Модель Хартсона	0, 5	1,0
14	До теми 14. Порівняння моделі Кларка Вільсона з моделями Бібі і Белла-ЛаПадули	0,25	1,0
15	До теми 15. Порівняння моделі Міллена з моделями Бібі і Белла-ЛаПадули	0,25	1,0
16	До теми 16. ITU-T X.500	0,5	1,0
Усього годин за модуль 2		3	8
Разом		6	16

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		ДФН	ЗФН
Модуль 1			
1	Підготовка до лекцій	4	4
2	Підготовка до лабораторних робіт	7	6
3	Підготовка до практичних робіт	8	8
4	Підготовка до модульних контрольних робіт	12	22
5	Самостійне опрацювання окремих тем навчальної дисципліни	3	8
6	Підготовка до екзамену	11	30
Усього годин за модуль 1		45	78
Модуль 2			
1	Підготовка до лекцій	4	4
2	Підготовка до лабораторних робіт	8	6

№	Вид роботи	Кількість годин	
		ДФН	ЗФН
3	Підготовка до практичних робіт	7	6
4	Підготовка до модульних контрольних робіт	12	22
5	Самостійне опрацювання окремих тем навчальної дисципліни	3	8
6	Підготовка до екзамену	11	30
Усього годин за модуль 2		45	76
Модуль 3			
1	Виконання курсової роботи	90	90
Усього годин за модуль 2		90	90
Разом за курсом		180	244

Індивідуальне науково-дослідне завдання

Індивідуальне навчально-дослідне завдання (ІНДЗ) виконується здобувачем під керівництвом викладача і полягає у виконанні курсової роботи.

Індивідуальні завдання на курсову роботу видаються студентам на другому тижні першого семестру.

Виконання курсової роботи створює умови для якнайповнішої реалізації творчих можливостей студентів і має на меті поглиблення, узагальнення та закріплення знань, які здобувачі одержують у процесі навчання, а також застосування знань на практиці.

Індивідуальні завдання виконуються самостійно і не входять до тижневого аудиторного навантаження здобувача. Викладач контролює виконання індивідуального завдання на консультаціях. Студент несе особисту відповідальність за прийняті в роботі рішення і правильність виконання і оформлення роботи.

Приймає курсову роботу викладач або комісія у складі трьох осіб, склад якої визначається завідувачем кафедри комп'ютерних технологій та інформаційної безпеки і фіксується у відповідному протоколі.

Курсова робота складається з розрахунково-пояснювальної записки та графічної частини (остання - на аркушах формату А3 або А4). Тематика та зміст курсової роботи спрямовані на здобуття студентами практичних навичок дослідження базових рядів даних, визначення параметрів регресійної моделі, перевірки статистичної значимості параметрів моделі і адекватності моделі в цілому, перевірки відповідності даних припущенням методу найменших квадратів і перетворення даних в разі необхідності, прогнозування за побудованою моделлю і надання рекомендацій щодо напрямку зміни впливових

факторів з метою наближення до оптимуму залежної змінної, що характеризує систему технічного захисту інформації.

Індивідуальне завдання курсової роботи може бути пов'язане з тематикою наукової діяльності студента.

Вхідні дані для курсового проектування отримуються як результат аналізу літературних джерел або проведених експериментальних досліджень за тематикою магістерської наукової роботи або обираються за номером варіанту в тому випадку, коли дипломна робота студента не пов'язана з обробкою числових рядів даних.

Метою курсової роботи є формування практичних навичок побудови і використання регресійних моделей для дослідження об'єктів і процесів інформаційної безпеки та прогнозування за отриманими моделями, результати котрих використовуються при управлінні інформаційною безпекою.

Змістом курсової роботи є виконані в будь-якому програмному середовищі розрахунки за наведеними у даних методичних вказівках формулами для визначення параметрів рядів даних, параметрів регресійної моделі, інтервальних та точкових прогнозів значень незалежних і залежних змінних, а також ряду тестових параметрів.

Програмне середовище для виконання розрахунків обирається студентом самостійно.

До складу курсової роботи входять зміст; вступ, в якому коротко наводиться аргументація актуальності задачі та аргументація обраних засобів її розв'язку; розрахункова частина, виконана студентом у відповідності до індивідуального завдання в будь-якому програмному середовищі, вибір якого повинен бути аргументований у першому підрозділі розрахункової частини; висновки та перелік посилань, оформлені за вимогами до курсових проектів/робіт.

В курсовій роботі мають бути продемонстровані системний підхід до розв'язку задачі та відповідність знань та вмінь студента з дисципліни “Математичні методи моделювання та оптимізації процесів кібербезпеки та інформаційного захисту інформації” вимогам даної робочої програми.

Тематика курсових робіт стосується дослідження на регресійних моделях об'єктів і процесів інформаційної безпеки:

1. Аналіз впливу певних факторів на показники якості систем захисту інформації, наприклад, аналіз впливу витрат на технічне обслуговування служби безпеки і витрат на підвищення кваліфікації її співробітників на кількість випадків витоку інформації / на ризики інформаційної безпеки

2. Виявлення факторів впливу на ефективність системи захисту

інформації в локальній мережі інституту/ університету / фірми, що має ліцензію на надання послуг в галузі інформаційної безпеки / медичної установи / районного суду / судноплавної компанії / порту / судна / кампуса тощо.

3. Виявлення факторів впливу на ефективність системи захисту IP-телефонії кафедри / інституту/ університету / фірми, що має ліцензію на надання послуг в галузі інформаційної безпеки / медичної установи / районного суду / судноплавної компанії / порту тощо.

4. Дослідження на регресійній моделі процесів технічного захисту інформації на певних об'єктах інформаційної діяльності / сайтах

5. Дослідження на регресійній моделі процесів технічного захисту інформації у складових системи оброблення /захисту інформації, наприклад, пристроях мобільного зв'язку / системах автоматизованого документообігу / електронній пошті / системі шифрування / системі контролю доступу / системі антивірусного захисту тощо з метою виявлення впливових факторів, визначення ступеня і напряму їх впливу на показники якості оброблення / захисту інформації, прогнозування на заданий термін часу подій та інцидентів інформаційної безпеки / показників якості оброблення/захисту інформації / прогнозування порушення конфіденційності/ цілісності/ доступності/ спостереженості інформації, розроблення рекомендацій щодо поліпшення показників якості оброблення / захисту інформації.

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

Методами навчання є:

- пояснення, демонстрування;
- лекція, відеометод;
- робота з літературою;
- лабораторна робота;
- практична робота;
- інструктаж (інструктаж з техніки безпеки та пожежної безпеки проводиться одноразово на першому занятті в лабораторії);
- виконання індивідуальних завдань;
- репродуктивний метод;
- проблемного викладу.

При вивченні дисципліни використовуються 3 групи методів навчання:

I група методів - методи організації та здійснення навчально-пізнавальної діяльності:

- словесні: розповідь-пояснення, лекція;
- наочні: ілюстрація, презентація, демонстрація;
- практичні: лабораторні роботи, практичні роботи;
- індуктивні методи: узагальнення, пов'язані із проведенням експериментів;
- дедуктивні методи: розвиток абстрактного мислення для засвоєння навчального матеріалу на основі узагальнень;
- репродуктивні методи: робота за готовими прикладами;
- творчі, проблемно-пошукові методи: самостійна, творча пізнавальна діяльність;
- навчальна робота студентів під керівництвом НПП;
- самостійна робота студентів.

II група методів - методи стимулювання й мотивації навчально-пізнавальної діяльності:

- методи стимулювання інтересу до навчання: створення ситуації інтересу при викладанні матеріалу; аналіз життєвих ситуацій;
- методи стимулювання обов'язку й відповідальності: роз'яснення мети навчального предмета; вимоги до вивчення предмета; заохочення та покарання в навчанні;

III група методів - методи контролю (самоконтролю, взаємоконтролю), корекції (самокорекції, взаємокорекції) за ефективністю навчально-пізнавальної діяльності:

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних і практичних робіт;
- командні проєкти; індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- захист курсового проєкту;
- екзаменаційна робота;
- комплексна контрольна робота (за необхідністю).

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних і практичних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

Поточний контроль проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних і практичних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка екзаменаційних робіт;
- перевірка та захист звітів з лабораторних робіт;
- перевірка та захист звітів з практичних робіт;
- проведення та перевірка модульних контрольних робіт;
- контроль виконання розділів індивідуального науково-дослідного завдання;
- контрольна робота на заочній формі навчання;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звітів з лабораторних і практичних робіт включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звітів з лабораторних і практичних робіт включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання за змістом є об'єднаним представленням модульних контрольних робіт, які проводяться для здобувачів

денної форми навчання, і має відповідати тим самим вимогам. Контрольна робота на заочній формі навчання виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку результатів знань студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.

Процедура захисту звіту з індивідуального науково-дослідного завдання (курсової роботи) включає наступні елементи:

- надання пояснювальної записки звіту з індивідуального науково-дослідного завдання (курсової роботи) в електронному вигляді;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях, лабораторних і практичних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 35 балів, яку студент повинен набрати у разі виконання всіх елементів модулів (60% від максимальної суми балів - 60, яку студент може набрати за семестр).

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді **екзаменів** в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав протягом семестру за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише семестрову екзаменаційну роботу (проводиться у письмовій формі), до якої він допускається, якщо захистив курсову роботу і має за виконання всіх передбачених елементів модулів не менше 35 балів. Максимальна кількість балів за семестрову підсумкову залікову роботу (екзамен) становить 40 балів.

Студенти заочної форми навчання пишуть підсумкову залікову роботу обов'язково.

Підсумкова оцінка з дисципліни від 60 до 100 балів визначається як сума балів за змістовими модулями та семестрової залікової роботи (у разі її написання).

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8. Критерії оцінювання результатів навчання

8.1 Критерії оцінювання практичних робіт

При оцінюванні практичних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну практичну роботу для ДФН у першому семестрі – 3 бала, у другому семестрі – 2 бали.

Максимальна оцінка за кожну практичну роботу для ЗФН у першому семестрі – 8 балів, у другому семестрі – 5 балів.

Максимальна сумарна кількість балів за практичні роботи для студентів ДФН становить:

- у першому семестрі: $8 \times 3 = 24$ бали;
- у другому семестрі: $8 \times 2 = 16$ балів.

Максимальна сумарна кількість балів за практичні роботи для студентів ЗФН становить:

- у першому семестрі: $2 \times 8 = 16$ балів;
- у другому семестрі: $2 \times 5 = 10$ балів.

Критерії оцінювання практичних робіт

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
Модуль 1	
3 (8)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
2,4 (6,4)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
1,8 (4,8)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
1,2 (3,2)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
0,6 (1,6)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 24 бали (8 робіт по 3 бали). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 16 балів (2 роботи по 8 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,2 бала.	
Модуль 2	
2 (6)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
1,6 (4,8)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
1,2 (3,6)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
0,8 (2,4)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
0,4 (1,2)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 16 балів (8 роботи по 2 бали). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 10 балів (2 роботи по 5 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,2 бала.	

8.2 Критерії оцінювання лабораторних робіт

При оцінюванні лабораторних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу для ДФН у першому семестрі – 2 бала, у другому семестрі – 3 бали.

Максимальна оцінка за кожну лабораторну роботу для ЗФН у першому семестрі – 6 балів, у другому семестрі – 5 балів.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ДФН становить:

- у першому семестрі: $8 \times 2 = 16$ балів;
- у другому семестрі: $8 \times 3 = 24$ бали.

Максимальна сумарна кількість балів за лабораторні роботи для студентів ЗФН становить:

- у першому семестрі: $4 \times 6 = 24$ балів;
- у другому семестрі: $6 \times 5 = 30$ балів.

Критерії оцінювання лабораторних робіт

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
Модуль 1	
2 (6)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
1,6 (4,8)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
1,2 (3,6)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
0,8 (2,4)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
0,4 (1,2)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 16 балів (8 робіт по 2 бали). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 24 бали (4 роботи по 6 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,2 бала.</i>	
Модуль 2	
3 (5)	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
2,4 (4)	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
1,8 (3)	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.

Кількість балів (в дужках для ЗФН)	Критерії оцінювання
1,2 (2)	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
0,6 (1)	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0 (0)	Робота не виконана.
	<i>Максимальна сумарна оцінка студента за даний компонент програми для ДФН – 24 бали (8 роботи по 3 бали). Максимальна сумарна оцінка студента за даний компонент програми для ЗФН – 30 балів (6 робіт по 5 балів). При незначних відхиленнях від вказаних критеріїв оцінка може доповнюватись знаками «-» або «+», що при підсумовуванні відповідає 0,2 бала.</i>

8.3 Критерії оцінювання модульних контрольних робіт

Для поточного модульного контролю студентами виконуються 4(чотири) модульні контрольні роботи (МКР) за матеріалами змістовних модулів.

Критерієм оцінювання МКР є відсоток правильних відповідей на питання модульної контрольної роботи.

Максимальна кількість балів за кожну МКР для студентів ДФН і ЗФН становить 10 балів.

Загальна сума балів за модульні контрольні роботи для студентів ДФН і ЗФН становить:

- у першому семестрі: $2 \times 10 = 20$ балів;
- у другому семестрі: $2 \times 10 = 20$ балів.

Критерії оцінювання задач та практичних завдань в МКР

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	10	9	8	7	6	5	4	3	2	1

8.4 Критерії оцінювання курсової роботи

Критеріями оцінювання курсової роботи є:

- самостійність виконання завдання;
- правильність виконання завдання;
- вчасність оформлення звіту з курсової роботи;
- правильність оформлення звіту з курсової роботи;
- правильність відповідей на питання при захисті курсової роботи.

Максимальна кількість балів за курсову роботу становить 100 балів.

Розподіл максимально можливої кількості балів за курсову роботу

Звіт з курсової роботи	Захист курсової роботи	Сума
50	50	100

Критерії оцінювання пояснювальної записки і графічної частини курсової роботи

виконання роботи, %	Критерії оцінювання пояснювальної записки і графічної частини курсової роботи	бал
100	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Графічна частина виконана відповідно до вимог.	50
70 - 99	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках і/або у графічній частині курсової роботи.	40
59 - 69	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Графічна частина містить незначні некоректності в оформленні.	30
40 - 58	Завдання виконано у повному об'ємі але з помилками. Звіт (в тому числі графічна частина) містить неточності у висновках та окремі помилки.	20
20 - 39	Завдання виконано не у повному об'ємі. Надано звіт, що містить неточності і помилки. Графічна частина містить помилки.	10
1 - 20	Робота не виконана.	0

Критерії оцінювання захисту курсової роботи

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	50	45	40	35	30	25	20	15	10	5

8.5 Критерії оцінювання екзаменаційної роботи

Максимальна оцінка за екзаменаційні роботи – 40 балів.

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	40	36	32	28	24	20	16	12	8	4

8.6 Розподіл оцінки за змістовними модулями та видами контролю

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
Модуль 1					
ЗМ1	T1	Лабораторна робота 1	2	Лабораторні роботи 1	6
	T2	Лабораторна робота 2	2	Лабораторна робота 2	6
	T3	Практична робота 1	3	Практична робота 1	8
	T4	Лабораторні роботи 3, 4	4	-	-
		Практичні роботи 2, 3	6	-	-
	МКР1	Тест	10	Тест	10
ЗМ2	T5	Лабораторні роботи 5, 6	4	-	-
		Практичні роботи 4, 5	6	Практична робота 5	8
	T6	Лабораторна робота 7	2	Лабораторна робота 7	6
		Практична робота 6	3	-	-

		Денна форма		Заочна форма	
		Вид роботи	Кількість балів	Вид роботи	Кількість балів
	T7	Практична робота 7	3	-	-
	T8	Лабораторна робота 8	2	Лабораторна робота 8	6
		Практична робота 8	3	-	-
	МКР2	Тест	10	Тест	10
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100	100	
Модуль 2					
ЗМ3	T9	Практична робота 9	2	-	-
	T10	Практична робота 10	2	-	-
	T11	Лабораторні роботи 9, 10	6	Лабораторні роботи 9, 10	10
		Практична робота 11	2	Практична робота 11	5
	T12	Практична робота 12	2	-	-
	МКР3	Тест	10	Тест	10
ЗМ4	T13	Лабораторні роботи 11, 12, 13	9	Лабораторні роботи 11, 12	10
		Практична робота 13	2	Практична робота 13	5
	T14	Лабораторна робота 14	3	Лабораторна робота 14	5
		Практична робота 14	2	-	-
	T15	Лабораторна робота 15	3	-	-
		Практична робота 15	2	-	-
	T16	Лабораторна робота 16	3	Лабораторна робота 16	5
		Практична робота 16	2	-	-
МКР4	Тест	10	Тест	10	
Підсумковий семестровий контроль		екзамен	40	екзамен	40
Всього			100	100	
Модуль 3					
Курсова робота	Звіт		50	Звіт	50
	Захист		50	Захист	50
Всього			100	100	

**Рівні підсумкової оцінки екзамену з дисципліни
(перерахунковий коефіцієнт – 0,4)**

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82-89 (високий рівень)/(high level)	B (дуже добре) / (very good)
74-81 (добрий рівень)/(good level)	C (добре) / (good)

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
64-73 (середній рівень)/(average level)	D (посередньо) / (average)
60-63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35-59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1-34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) із доступом до Інтернет.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає: операційну систему (Windows); програмне забезпечення для інженерних розрахунків ризиків (Excel, Mathcad); текстовий редактор та редактор растрових зображень (для підготовки звітів з лабораторних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному вигляді); браузер для доступу до Інтернет-ресурсів.

При очній формі навчання використовуються апаратні та програмні можливості лабораторій №129, №130 і №134 кафедри КТІБ ННІАЕ НУК. В цьому випадку в процесі проведення лекцій, практичних і лабораторних робіт для демонстрації тематичних презентацій і прикладів використовується наявне в лабораторіях мультимедійне обладнання.

При дистанційній формі навчання використовуються апаратні та програмні можливості домашніх персональних комп'ютерів (настільних комп'ютерів або ноутбуків) та мобільних пристроїв із доступом до Інтернет. Заняття проводиться в Zoom. Необхідна студентам інформація (робоча програма дисципліни, методичні вказівки, рекомендована література, інформація щодо поточної набраної кількості балів) викладається на google-диск кафедри КТІБ, до якого студенти отримують доступ без права редагування. Виконані студентами роботи надсилаються на кафедральну пошту ktib@nuos.edu.ua. Під час воєнного стану допускається виконання звітів з лабораторних робіт і модульних контрольних робіт в рукописному вигляді без дотримання стандартів оформлення. Такі звіти надсилаються у вигляді графічних зображень (фотографій). Відповідно, для

дистанційної форми навчання додатково використовуються Zoom, e-mail і відеокамери мобільних пристроїв.

10. Рекомендовані джерела інформації

Основна література

Навчально-методична література

1. Бабак В.П. Теоретичні основи інформаційно-вимірювальних систем: Підручник / В.П. Бабак, С.В. Бабак, В.С. Єременко та ін.; за ред. чл.-кор. НАН України В.П. Бабака / 2-е вид., перероб. і доп. — К.: Ун-т новітніх технологій; НАУ, 2017. — 496 с. URL: <https://ela.kpi.ua/handle/123456789/31505>
2. Бобало Ю.Я. Інформаційна безпека: навч. посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С.Войтусік, А.Я. Гропенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, С.І. Яковенко, В.І.Отенко, І.Я. Тишик; за заг.ред. Ю.А. Бобала, І.В. Горбатого. — Львів:Вид-во Львівської політехніки, 2019. — 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
3. Богуш В.М. Теоретичні основи захищених інформаційних технологій / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. — К.: ДУІКТ, 2009. — 292 с. URL: <https://studfile.net/preview/5367403>
4. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа. — Львів.: «Магнолія 2006», 2018. — 320 с. URL: <https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf>
5. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / — К.:ДУТ, 2015. — 345 с. URL: https://duikt.edu.ua/uploads/l_1242_54311567.pdf
6. Гапак О. М., Глебена М. І. Захист інформації в комп'ютерних системах. — Ужгород: УЖНУ, 2021. — 184 с. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36506/1/%d0%9f%d0%86%d0%94%d0%a0%d0%a3%d0%a7%d0%9d%d0%98%d0%9a%20%d0%97%d0%86%d0%9a%d0%a1_2021.pdf
7. Катренко А. В. Системний аналіз об'єктів та процесів комп'ютеризації: навч. посіб. для студ. вищ. закл. освіти / А. В. Катренко. — Львів : Новий світ-2000, 2003. — 424 с.
8. Кутковецький В.Я. Дослідження операцій: Навчальний посібник. — Миколаїв: Вид-во МДГУ ім. П. Могили, 2003. — 260 с. URL: <https://lib.chmnu.edu.ua/pdf/pidruchniku/14/1.pdf>
9. Левченко Є.Г., Швець В. А., Демчишин М.В. Економіка інформаційної безпеки: Навчальний посібник. — К.: НАУ, 2012. — 225 с. URL: https://er.nau.edu.ua/bitstream/NAU/10221/1/Ekonom_bezp.pdf
10. Толубко В.Б. Імітаційне моделювання систем масового обслуговування: навч. посіб. [для студентів техн. спец. вищ. навч. закл.] / В. Б. Толубко, А.Д. Кожухівський, В.В. Вишнівський, Г.І. Гайдур, О.А. Кожухівська. — Київ: ДУТ, 2018. - 175 с. URL: https://duikt.edu.ua/uploads/p_303_81677701.pdf?file=p_303_81677701.pdf

Нормативні документи

11. ISO/IEC 15408-1:2009. Informational technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model. URL: <https://www.iso.org/standard/50341.html>
12. ISO/IEC 15408-2:2008. Informational technology. — Security techniques — Evaluation criteria for IT security. — Part 2: Security functional requirements. URL: <https://www.iso.org/standard/46414.html>
13. ISO/IEC 15408-3:2008. Informational technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirement. URL: <https://www.iso.org/standard/46413.html>

14. ISO 27005:2018 Information technology -- Security techniques -- Information security risk management. URL: <https://www.iso.org/standard/75281.html>
15. Recommendation ITU-T X.500 (10/2019). Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. Series X: Data networks, open system communications and security. URL: <https://www.itu.int/rec/T-REC-X.500-201910-I/en>
16. ДСТУ ISO/IEC 7498-1:2004 Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Еталонна модель
17. ДСТУ ISO 7498-2:2004 Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура захисту інформації ДСТУ
18. ISO/IEC 7498-3:2004 Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 3. Найменування та адресація
19. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. URL: <https://tzi.com.ua/downloads/1.4-001-2000.pdf>
20. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342>
21. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. URL: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

Наукові публікації

22. Корченко А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с. URL: <https://er.nau.edu.ua/bitstream/NAU/38772/1/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F%20%D0%9A%D0%BE%D1%80%D1%87%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%90%D0%BD%D0%BD%D0%B0.pdf>
23. Корченко О.Г., Архипов О.Є., Казмірчук С.В. Аналіз та оцінювання ризиків інформаційної безпеки. - К.: ТОВ «Поліграф-Лазурит», 2013. – 275 с. URL: <https://er.nau.edu.ua/bitstreams/608567f9-7c99-4cb1-ba31-bb66bf7c19c0/download>
24. Мнушка О.В., Савченко В.М. Модель безпеки інформаційної системи на базі технологій IOT// Вісник Національного технічного університету "ХПІ", 2019, № 28 (1353). –С.108-116. URL: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/3f887a4c-32be-4f31-9249-74ab0f249e93/content>
25. Свида І.Ю., Зварич А. О., Бухал Д. А. Методичний підхід щодо оптимального використання пропускну здатності телекомунікаційних мереж // Вісник НТУУ «КПІ». Радіотехніка, радіоапаробудування : збірник наукових праць. – 2018. – Вип. 73. – С. 11–17. URL: <https://ela.kpi.ua/bitstream/123456789/24391/1/4.pdf>
26. Хорошко В.О., Хохлачова Ю.Є. Оптимізація параметрів систем захисту в мережах передачі інформації //Інформатика та математичні методи в моделюванні. – 2013. –Т.3. - №1. - С.74-81. URL: http://immm.op.edu.ua/files/archive/n1_v3_2013/n1_v3_2013.pdf
27. Гладун А.Я., Хала К.О. Таксономія стандартів інформаційної безпеки //Інформаційні технології. – 2017. - №2. – С.53-64. URL: http://nti.ukrintei.ua/wp-content/uploads/2018/05/2017-2_stat7_UA_povn.pdf

Допоміжна література

Навчально-методична література

28. Bishop, M. Computer security: art and science / M. Bishop. 2nd ed. — Addison-Wesley Professional, 2018. — 2865 p. URL: <https://dokumen.pub/qdownload/computer-security-art-and-science-2nbsped-0321712331-9780321712332-0134097173-9780134097176.html>

29. Блінцов В.С., Кінаш А.Т., Хлопенко М.Я. Основні методи оптимального управління електромеханічних систем. - Миколаїв: УДМТУ, 2002
30. Гайвороновський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група ВНУ, 2009
31. Гречко Т.К., Чернова Л.С. Системний аналіз і прийняття інноваційних рішень: Навчально-методичний посібник. - Миколаїв: Торубара В.В., 2015
32. Жерновий Ю.М. Імітаційне моделювання систем масового обслуговування. - Львів: Видавничий центр ЛНУ ім. Івана Франка, 2007
33. Зайченко Ю.П. Дослідження операцій. - К.: ЗАТ «ВІПОЛ», 2000
34. Зайченко Ю.П. Дослідження операцій: Навч. посібник - К.: Вища школа, 1975, 1988
35. Зайченко Ю.П. Дослідження операцій: Збірка задач. - К.: Вища школа, 1984, 1990
36. Зайченко Ю.П. Основи проектування інтелектуальних систем: Навчальний посібник. - К.: Видавничий дім «Слово», 2004
37. Коваленко І. І., Гожий О.П. Методи підтримки прийняття рішень (системні аспекти): Навчальний посібник. - Миколаїв: Іліон, 2007
38. Нефьодов Ю.М. Основи моделювання інтелектуальних систем: Навчальний посібник. - Луганськ: Видавництво СЛУ ім.В.Даля, 2012
39. Приходько С.Б. Індивідуальний комплект навчально-методичних матеріалів з дисципліни "Системний аналіз об'єктів і процесів комп'ютеризації". - Миколаїв: НУК, 2005
40. Самойленко Д. М. Спеціальні розділи математики у кібербезпеці: навч. посібник. - Миколаїв: НУК, 2017
41. Довідник з типових програм моделювання /Під ред. О.Г. Івахненко. - К.: Техніка, 1980
42. Тимченко А.А. Основи системного проектування та системного аналізу складних об'єктів: Підручник. - К.: Либідь, 2003
43. Томашевський В. та ін. Вирішення практичних завдань методами комп'ютерного моделювання. - К.: "Корнійчук", 2001
44. Хлопенко М.Я., Білюк І.С. Збірник задач для контрольних і самостійних робіт з дисципліни «Дослідження операцій електромеханічних систем». - Миколаїв: НУК, 2008
45. Хлопенко М.Я., Білюк І.С., Шевченко В.В. Оптимальне управління об'єктами: Навчальний посібник для студентів ВНЗ (з грифом МОН). - Миколаїв: НУК, 2013
46. Хорошко В.А. Проектування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опіський, Л. Т. Пархуць. Львів: Видавництво Львівської політехніки, 2020. 320 с. - <https://vlp.com.ua/node/20177>

Наукові публікації

47. Антонюк А. О., Жора В. В. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / А. О. Антонюк, В. В. Жора. - Ірпінь Національний університет ДПС України, 2010. - 310 с.
48. Корченко О.Г. Побудова систем захисту інформації на нечітких множинах. Теорія і практичні рішення. - К.: МК-Пресс, 2006

Інформаційні ресурси в Інтернеті

Сайти навчально-методичного забезпечення

1. Презентації з тематики теорії захисту інформаційних ресурсів обмеженого доступу. URL: <https://ppt-online.org/402918>
2. Системи онлайн-освіти. URL: <https://prometheus.org.ua/>, <http://www.udacity.com>, <https://www.coursera.org>

Сайти з нормативно-правового забезпечення

3. Державна служба спеціального зв'язку та захисту інформації.
URL: <https://cip.gov.ua/ua>
4. Діяльність Адміністрації Держспецзв'язку у сфері кіберзахисту.
URL: <https://cip.gov.ua/ua/statics/cyber-protection>
5. Команда реагування на комп'ютерні надзвичайні події України.
URL: <https://cert.gov.ua/>
6. Нормативна база у сфері ТЗІ URL: <http://altersign.com.ua/korysna-informacija/normatyvna-baza-u-sferi-tzi>
7. Офіційний сайт ISO. URL: <https://www.iso.org/standard>
8. Перелік документів міжнародних організацій та країн-партнерів у сфері кіберзахисту. URL: <https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-u-sferi-kiberzakhistu>
9. Портал безпека. URL: <https://www.bezpeka.com/uk/golovna/>

Електронні журнали

10. Безпека інформації. URL: <https://jrn1.nau.edu.ua/index.php/Infosecurity>
11. Безпека інформаційних систем і технологій. URL: <https://ists.knu.ua/index.php/bist>
12. Захист інформації. URL: <https://jrn1.nau.edu.ua/index.php/ZI>
13. Інформаційна безпека людини, суспільства, держави. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=JRN&P21DBN=JRN&S21STN=1&S21REF=10&S21FMT=fullwj&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=I=&S21COLORTERMS=0&S21STR=%D0%96100315
14. Інформаційні технології та комп'ютерна інженерія. URL: <https://itce.vntu.edu.ua/index.php/itce>
15. Інформація та безпека. URL: <http://infobezpeka.in.ua/about.php>
16. Кібербезпека: освіта, наука, техніка. URL: <https://csecurity.kubg.edu.ua/index.php/journal>
17. Сучасний захист інформації. URL: <http://journals.dut.edu.ua/index.php/dataprotect/index>
18. Сучасні інформаційні технології у сфері безпеки та оборони. URL: <http://sit.nuou.org.ua/>
19. Advanced Information Technology = Сучасні інформаційні технології. URL: <https://ait.knu.ua/>
20. Applied Aspects of Information Technology = Прикладні аспекти інформаційних технологій. URL: <https://aait.opu.ua/>
21. Bulletin of modern information technologies = Вісник сучасних інформаційних технологій. URL: <https://hait.opu.ua/>
22. Problems of information technologies = Проблеми інформаційних технологій. URL: <http://journals.kntu.net.ua/index.php/pit>
23. Science Direct URL: <https://www.sciencedirect.com/browse/journals-andbooks?accessType=openAccess&accessType=containsOpenAccess&subject=computer-science>

Зміни та доповнення