Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Навчально-науковий інститут лазерної та біомедичної інженерії
(повна назва)

Кафедра Фізичних основ електронної техніки
(повна назва)

ЗАТВЕРДЖУЮ
В.о. директора ННІ ЛБІ

_____ Олександр ГАЛАТ
«_27_» ___серпня___20_26_ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Квантовий захист інформації»
(назва навчальної дисципліни)

рівень вищої освіти магістерський
(бакалаврський, магістерський, освітньо-науковий)

спеціальність G6 Інформаційно-вимірювальні технології
(код і повна назва спеціальності)

освітньо-професійна програма
(професійна або наукова)
«Інженерія оптоінформаційних та лазерних систем»
(повна назва програми)

Харків – 2026 р.

Розробник: Є.М. Одаренко, професор каф.ФОЕТ, д. ф.-м. н., с.н.с
(ініціали, прізвище, посада, науковий ступінь, вчене звання)

Робочу програму схвалено на засіданні кафедри ФОЕТ

Протокол від «27» серпня 2026 р. № 9

Завідувач кафедри _____ Олександр ГНАТЕНКО
(підпис) (Власне ім'я, прізвище)

Гарант освітньої програми _____ Євген ОДАРЕНКО
(підпис) (Власне ім'я, прізвище)

Схвалено методичною комісією ННІ ЛБІ

Протокол від «27» серпня 2026 р. № 5

Голова методичної комісії _____ Олександр ГАЛАТ
(підпис) (Власне ім'я, прізвище)

1 ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Характеристика навчальної дисципліни*</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС* - 5</td><td colspan="2">Вибіркова</td></tr>
<tr><td rowspan="2">Змістових модулів - 2</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>1-й</td><td>1-й</td></tr>
<tr><td>Індивідуальних завдань*:
РГЗ та КР - 0
курс. робота (проєкт) - 0</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="4">Загальна кількість годин* - 150</td><td>1-й та 2-й</td><td>1-й та 2-й</td></tr>
<tr><td colspan="2">Кількість годин</td></tr>
<tr><td>55</td><td>37</td></tr>
<tr><td colspan="2">Навчальні заняття:
1) лекції, год</td></tr>
<tr><td rowspan="15">Мова навчання
українська</td><td>30 год</td><td>8 год</td></tr>
<tr><td colspan="2">2) практичні, год</td></tr>
<tr><td>16 год</td><td>6 год</td></tr>
<tr><td colspan="2">3) лабораторні, год</td></tr>
<tr><td>4 год</td><td>8 год</td></tr>
<tr><td colspan="2">4) консультації, год</td></tr>
<tr><td>5 год</td><td>15 год</td></tr>
<tr><td colspan="2">Самостійна робота, год</td></tr>
<tr><td>95 год</td><td>113 год</td></tr>
<tr><td colspan="2">в тому числі: 1) РГЗ та КР., год</td></tr>
<tr><td>-</td><td>1,2 год.</td></tr>
<tr><td colspan="2">2) курсова робота(проект), год</td></tr>
<tr><td>-</td><td></td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Примітка.

* Відомості з навчального плану.

2 МЕТА ДИСЦИПЛІНИ ТА ОЧІКУВАНІ РЕЗУЛЬТАТИ З ЇЇ ВИВЧЕННЯ

2.1 Мета вивчення дисципліни:

Ознайомлення з основними принципами застосування квантових об’єктів в новітніх системах захисту інформації в каналах передачі даних, методами та засобами технічної реалізації пристроїв квантової криптографії.

2.2 Результати навчання:

за результатом вивчення дисципліни студенти повинні:

знати: сучасні методи наукових досліджень, організації та планування експерименту, комп’ютеризованих методів дослідження та опрацювання результатів вимірювань;

основні поняття теорії вимірювань, застосовувати на практиці та при комп’ютерному моделюванні об’єктів та явищ;

сучасні методи та методики проектування і дослідження, а також аналізу отриманих результатів;

основні принципи криптографічного захисту інформації та застосування для цього досягнень квантової фізики.

вміти: виконувати аналіз інженерних продуктів, процесів і систем за встановленими критеріями, обирати і застосовувати найбільш придатні аналітичні, розрахункові та експериментальні методи для проведення досліджень, інтерпретувати результати досліджень;

аналізувати склад та елементи систем квантової криптографії для визначення фізичних принципів їх функціонування та методів захисту інформації в оптичних лініях зв’язку;

застосовувати апаратні та програмні засоби сучасних інформаційних технологій для вирішення задач в сфері метрології та інформаційно-вимірювальної техніки.

Перелік сформованих компетентностей (відповідно до освітньо-професійної програми):

загальні компетентності:

ЗК1. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність проведення досліджень на відповідному рівні.

ЗК5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК8. Здатність працювати в міжнародному контексті.

спеціальні (фахові, предметні) компетентності:

ФК3. Знання і розуміння наукових фактів, концепцій, теорій, принципів і методів експериментальної інформатики.

ФК4. Здатність застосовувати системний підхід до вирішення науково-технічних завдань метрології та інформаційно-вимірювальної техніки.

ФК7. Здатність застосовувати комплексний підхід до вирішення експериментальних завдань із застосуванням засобів інформаційно-вимірювальної техніки та прикладного програмного забезпечення.

ФК14. Здатність розробляти фізично та математично обґрунтовані моделі складних оптоелектронних систем та проектувати лазерне метрологічне обладнання.

ФК17. Здатність продемонструвати сучасні знання побудови систем лазерної та оптоелектронної техніки.

ФК19. Здатність дотримуватись професійної та академічної доброчесності при провадженні професійної діяльності.

Програмні результати навчання:

ПРН1. Знати і розуміти сучасні методи наукових досліджень, організації та планування експерименту, комп’ютеризованих методів дослідження та опрацювання результатів вимірювань.

ПРН3. Розуміти міждисциплінарні зв’язки та контексти спеціальності.

ПРН8. Володіти сучасними методами та методиками проектування і дослідження, а також аналізу отриманих результатів.

ПРН15. Вміти користуватися відкритими науковими базами даних, «хмарними» та інтернет-технологіями та іншими сучасними джерелами інформації.

ПРН17. Вміти розробляти вірогідні фізичні та математичні моделі оптоелектронних елементів інформаційно-вимірювальних систем та користуватися ними для розроблення новітніх приладів та пристроїв.

ПРН20. Вміти застосовувати сучасні інформаційно-вимірювальні технології для досягнення Цілей Сталого Розвитку.

ПРН21. Знати принципи академічної доброчесності та мати навички їх застосування.

2.3 Передумови для вивчення дисципліни:

Передумовою вивчення дисципліни є раніше здобуті компетентності та результати навчання, що перевіряються під час єдиного фахового вступного випробування зі спеціальності на основі Програми фахового вступного випробування, що затверджується головою приймальної комісії ХНУРЕ.

Загальна структура предметного тесту передбачає чотири основних розділи: Сучасні методи вимірювань та обробки результатів вимірювання, Основи технічного регулювання, Вища математика, Основи електротехніки та електроніки.

3 ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. Фізичне та технічне підґрунтя для квантової криптографії

Тема 1. Основні поняття квантової фізики.

Тема 2. Поляризація електромагнітних хвиль.

Тема 3. Волоконно-оптичні лінії зв’язку.

Тема 4. Однофотонні джерела випромінювання.

Змістовий модуль 2. Основи квантової криптографії

Тема 1. Криптографічні методи захисту інформації.

Тема 2. Застосування квантових принципів для захисту інформації.

Тема 3. Технічна реалізація квантових криптографічних систем.

4 СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	Усього	у тому числі					Усього	у тому числі				
		л	п	лб	конс	с.р.		л	п	лб	конс	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Фізичне та технічне підґрунтя для квантової криптографії												
Тема 1 Основні поняття квантової фізики	14	4				10		1			1	10
Тема 2. Поляризація електромагнітних хвиль	16	4	2			10		1		4	2	10
Тема 3. Волоконно-оптичні лінії зв’язку	33	4	4		1	20		1	2		2	20
Тема 4. Однофотонні джерела випромінювання	19	4	4	4	1	10		1	2	4	2	20
Разом за зміст. мод. 1	**82**	**16**	**10**	**4**	**2**	**50**		**4**	**4**	**8**	**7**	**60**
Змістовий модуль 2. Основи квантової криптографії												
Тема 1. Криптографічні методи захисту інформації	27	6			1	20		1			2	13
Тема 2. Застосування квантових принципів для захисту інформації	17	4	2		1	10		1	1		2	20
Тема 3. Технічна реалізація квантових криптографічних систем	24	4	4		1	15		2	1		4	20
Разом за зміст. мод. 2	**68**	**14**	**6**		**3**	**45**		**4**	**2**		**8**	**53**
Усього годин за семестр	**150**	**30**	**16**	**4**	**5**	**95**	**150**	**8**	**6**	**8**	**15**	**113**

5 ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№	Назва теми	Кількість годин	
		денна	заочна
1	Розрахунки поляризаційних характеристик електромагнітних хвиль.	2	
2	Розрахунки електродинамічних характеристик волоконно-оптичних ліній передачі.	4	2
3	Формування однофотонних джерел випромінювання.	4	2
4	Схеми каналів передачі інформації із застосуванням квантової криптографії.	2	1
5	Структура систем квантового захисту інформації.	4	1
	Загальна кількість, год.	**16**	**6**

6 ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№	Назва теми	Кількість годин	
		денна	заочна
1	Моделювання фотонно-кристалічного резонатору, що містить квантовий об'єкт, та застосовується для формування однофотонного джерела випромінювання.	4	4
2	Моделювання поляризаційних станів фотонів.		4
	Загальна кількість, год.	**4**	**8**

7 САМОСТІЙНА РОБОТА

№	Назва теми	Кількість годин	
		денна	заочна
1	Вивчення теоретичного матеріалу з використанням конспектів і навчальної літератури	35	40
2	Підготовка до лабораторних занять	5	10
3	Підготовка до практичних занять	24	25
4	Пошук і систематизація науково-технічної літератури за напрямами, що стосуються квантової криптографії	15	20
5	Підготовка доповідей та інформаційних повідомлень на конференції та наукові семінари	16	18
	Загальна кількість, год.	**95**	**113**

8 ІНДИВІДУАЛЬНІ ЗАВДАННЯ

8.1 Згідно з навчальним планом розрахунково-графічні завдання (РГЗ) та контрольні роботи (КР) не передбачено.

8.2 Згідно з навчальним планом курсова робота (проєкт) не передбачена.

9 МЕТОДИ НАВЧАННЯ ТА ЗАСОБИ ОЦІНЮВАННЯ

Основні методи навчання – словесний (лекція), практичний (проведення лабораторних робіт та практичних занять), наочний (метод ілюстрацій і метод демонстрацій); робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); перевірка знань та умінь (за результатами заліку).

10 МЕТОДИ КОНТРОЛЮ ТА РЕЙТИНГОВА ОЦІНКА ЗА ДИСЦИПЛІНОЮ

10.1 Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Вид заняття / контрольний захід	Оцінка $O_{\text{сем}}$
Пз № 1-4	(5…10) × 4 = 20…40
Лб № 1	20…30
Контрольна точка 1	**40…..70**
Пз № 5-6	(10…15) × 2 = 20…30
Контрольна точка 2	**20…..30**
Всього за семестр	**60…..100**

Для підсумкового контролю у формі заліку для оцінювання роботи студента протягом семестру використовується підсумкова рейтингову оцінку $O_{\text{сем}} = \sum O_{\text{і}}$. Оцінка за семестр $O_{\text{сем}}$ обчислюється як сума оцінок за різні види занять та контрольні заходи.

10.2 Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки.

1. Основні постулати квантової фізики та їх застосування до створення сучасних систем захисту інформації.
2. Принцип невизначеності Гейзенберга.
3. Двійчаста природа світла. Корпускулярно-хвильовий дуалізм.
4. Поняття поляризації електромагнітних хвиль.
5. Методи керування та контролю поляризації світлових хвиль.
6. Структура та фізичні властивості оптоволоконних ліній передачі.
7. Поляризаційні властивості оптоволоконних ліній передачі.
8. Сучасні технології побудови однофотонних джерел випромінювання.
9. Фізичні принципи функціонування однофотонних джерел випромінювання.
10. Основні поняття сучасної криптографії: шифри, ключі, криптосистеми, криптографічні атаки, компрометація тощо.
11. Основні застосування сучасної криптографії.
12. Симетричні та асиметричні методи шифрування інформації.
13. Керування ключами шифрування. Складові частини цього процесу та їх особливості.
14. Протокол квантової криптографії BB84.
15. Протокол квантової криптографії на парадоксі Ейнштейна-Подольського-Розенберга.
16. Методи апаратної реалізації протоколів квантової криптографії.
17. Різновиди атак на канали передачі даних та методи боротьби з ними.
18. Основні технічні проблеми апаратної реалізації протоколів квантової криптографії.

Необхідний обсяг умінь для одержання позитивної оцінки.

1. Застосування постулатів квантової фізики для пояснення фізичних явищ, притаманних мікро- та нанооб’єктам.
2. Визначення характеристик хвильових електромагнітних процесів.
3. Визначення поляризації світлових хвиль та розуміння методів керування нею.
4. Розуміння закономірностей прояву корпускулярної та хвильової природи світла.
5. Визначення характеристик взаємодії когерентних та некогерентних світлових хвиль.
6. Визначення характеристик волоконно-оптичних ліній передачі, в тому числі поляризаційних.
7. Характеризувати основні фізичні процеси та явища, що використовуються при розробленні однофотонних джерел випромінювання.
8. Складати блок-схеми пристроїв для отримання одиничних фотонів на основі різноманітних підходів та методів.
9. Орієнтуватися в сучасних криптографічних протоколах та алгоритмах їх застосування.
10. Вільно орієнтуватися у найбільш поширених сучасних протоколах квантової криптографії.
11. Використовувати знання основних принципів квантової фізики для побудови схем, що реалізують алгоритми квантової криптографії.
12. Застосовувати оптичні елементи для керування та визначення поляризаційних характеристик світла.

Критерії оцінювання роботи студента протягом семестру.

Задовільно, D, E (60-74). Мати мінімум знань і умінь. Відпрацювати всі практичні заняття та лабораторні роботи. Знати основні постулати квантової фізики, на яких базуються методи квантової криптографії, та принципи квантового захисту інформації. Уміти визначати поляризаційні характеристики світлових хвиль.

Добре, C (75-89). Твердо знати мінімум. Орієнтуватися в основних поняттях криптографії. Знати схеми побудови систем квантової криптографії та принципи їх функціонування.

Відмінно, A, B (90-100). Знати всі теми. Вільно орієнтуватися в рекомендованих підручниках. Уміти застосовувати отриману інформацію для аналізу фізичних процесів в системах квантової криптографії, у тому числі в різноманітних за принципом дії однофотонних джерелах випромінювання.

Здобувачам вищої освіти, які в день, визначений за розкладом для складання контрольного заходу, отримали оцінки «не зараховано», «незадовільно» або позначки «не з'явився/не з'явилася» може бути надано право покращення результатів підсумкового контролю з відповідного освітнього компонента незалежно від кількості отриманих незадовільних оцінок з інших дисциплін в період екзаменаційної сесії, тобто перескладання екзамену протягом екзаменаційної сесії відповідно до графіків консультацій викладачів, встановлених кафедрою. Оцінка, отримана при повторному складанні контрольного заходу, вважається як отримана здобувачем вищої освіти поза терміном, за виключенням випадків навчання здобувачів вищої освіти за індивідуальним графіком виконання ІНП.

Шкала оцінювання: національна та ЄКТС

Оцінка з дисципліни	Оцінка ЄКТС	Оцінка за національною шкалою	
		екзамен, курсовий проект (робота), практика	залік
96–100	A	5 (відмінно)	зараховано
90–95	B		
75–89	C	4 (добре)	
66–74	D	3 (задовільно)	
60–65	E		
35–59	FX	2 (незадовільно)	не зараховано
0-34	F		

11 МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ТА РЕКОМЕНДОВАНА ЛІТЕРАТУРА

11.1 Базова література

1. Остапов С.Е., Добровольський Ю.Г. Квантова інформатика та квантові обчислення / С.Е.Остапов. Ю.Г. Добровольський - Чернівці: ЧНУ, 2021. 99 с.
2. Карлаш Г.Ю. Квантові інформаційні системи: навчальний посібник для спеціальності «Прикладна фізика та наноматеріали». Київ: факультет радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, 2018. 77 с.
3. Rogers A. Polarization in Optical Fibers. Artech House, 2008. 273 p.
4. Quantum Communications and Cryptography / edited by Alexander V. Sergienko. – Taylor&Francis, 2006. 232 p.

11.2 Допоміжна література

5. Lydersen L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination // Nature Photonics. 2010. 4. P. 686–689.

6. J. McKeever, A. Boca, A. D. Boozer et al. Deterministic Generation of Single Photons from One Atom Trapped in a Cavity // Science Reports. 2004. Vol. 303. P. 1992–1994.
7. Hardware-Based Computer Security Techniques to Defeat Hackers. From Biometrics to Quantum Cryptography. Wiley, 2008. 227 p.

12 ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ

1. Пакет комп’ютерної алгебри та математичного моделювання Scilab.