

Міністерство освіти і науки України  
Харківський національний університет імені В.Н. Каразіна  
Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”



Проректор з науково – педагогічної роботи

Олександр ГОЛОВКО

” \_\_\_\_\_ 2022 р.

Робоча програма навчальної дисципліни

**“Криптографічні методи в кібербезпеці”**

рівень вищої освіти другий (магістерський)  
галузь знань 012 - Інформаційні технології  
спеціальність 125- Кібербезпека  
освітня програма Безбезпека інформаційних і комунікаційних систем  
вид дисциплін обов’язкова  
факультет комп’ютерних наук

2022 / 2023

Програму обговорено та рекомендовано до затвердження вченою радою факультету комп'ютерних наук "28" червня 2022 року, протокол №10

РОЗРОБНИКИ ПРОГРАМИ:

Горбенко Іван Дмитрович, доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій.

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій

Протокол від "23" червня 2022 року № 10

Завідувач кафедри безпеки інформаційних систем і технологій



Сергій Рассомахін

Гарант освітньої (професійної/наукової) програми

(керівник проєктної групи) Єсін Віталій Іванович

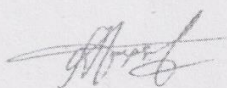


Віталій Єсін

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "24" червня 2022 року №9

Голова методичної комісії факультету комп'ютерних наук



Анатолій Бердников

## ВСТУП

Програма навчальної дисципліни “Криптографічні методи в кібербезпеці” складена відповідно до освітньо-професійної програми підготовки магістра. Спеціальності - 125 Кібербезпека. Освітня програма - Безпека інформаційних і комунікаційних систем .

### 1. Опис навчальної дисципліни

#### 1.1. Мета викладання навчальної дисципліни

**Мета дисципліни** – закласти термінологічний та методологічний фундаменти, виявленню та аналізу сучасних проблем криптографічного захисту інформації, навчання студентів основам побудови та аналізу криптосистем, застосуванню крипто систем для кіберзахисту, створенню та застосуванню постквантових криптосистем та нормативному регулюванню і стандартизації криптосистем.

Магістранти, що спеціалізуються в цьому напрямку, мають можливість використовувати одержані компетенції, знання та уміння при проведенні досліджень та виконанні наукової роботи, а також на практиці, що передуює розробці магістерської роботи.

#### 1.2. Основні завдання вивчення дисципліни

У цьому курсі передбачається формування у студентів компетенцій, знань та умінь з теорії та практики побудови, аналізу та стандартизації криптосистем, а також їх застосування в існуючих додатках для надання електронних довірчих послуг.

#### 1.3. Кількість кредитів - 6

#### 1.4. Загальна кількість годин - 180

1.5. Характеристика навчальної дисципліни	
Нормативна / за вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	1-й
Семестр	
1-й	1-й
Лекції	
16 год.	16 год.
Практичні, семінарські заняття	
8 год.	8 год.
Лабораторні заняття	
8 год.	8 год.
Самостійна робота	
148 год.	148 год.
У т.ч. індивідуальні завдання (курсова робота 20 год та наукові дослідження 20 год)	

#### 1.6. Заплановані результати навчання

**МАТИ КОМПЕТЕНЦІЇ:**

#### **Загально – професійні**

базові явлення про основні положення організації та функціонування захищених інформаційних систем(ІС), телекомунікаційних систем(ТС) та інформаційно -

телекомунікаційних систем різного призначення, в тому числі хмарних обчислень, а також інфраструктур відкритого ключа(ІВК);

здатність обґрунтовувати та використовувати стандартизовані криптографічні системи, комплекси, інфраструктури відкритого ключа, криптографічні примітиви та протоколи захисту інформації державних інформаційних ресурсів та персональних даних, в тому числі в пост квантовий період;

володіння стандартизованими на міжнародному, національному та регіональних рівнях методами, механізмами, системами, протоколами та засобами криптографічного захисту інформації при наданні електронних транскордонних довірчих послуг юридичним та фізичним особам та захисту інформаційних ресурсів і персональних даних; в тому числі для хмарних сервісів.

здатність будувати, здійснювати аналіз та порівняння криптографічних систем та криптографічних протоколів, а також засобів криптографічного захисту інформації(КЗІ) з використанням обґрунтованих критеріїв та показників, в тому числі відносно хмарних сервісів.

### **Спеціалізовано – професійні**

базові явлення про загрози та надання користувачам в ІС, ТС, ІТС та ІВК базових, в тому числі транскордонних електронних довірчих послуг, з безпеки інформації та інформаційних ресурсів, в тому числі для хмарних сервісів та в пост квантовий період;

здатність використовувати професійно профільовані знання й практичні навички при проектуванні, експертизі, дослідній експлуатації та застосуванні систем захисту інформації (СЗІ) та інформаційних ресурсів в ІТС та ІВК, в тому числі в пост квантовий період;

здатність використовувати існуючу міжнародну, регіональну та національну нормативно – правову базу при обґрунтуванні вимог до захисту інформації та ресурсів в ІС, ТС, ІТС та ІВК, в тому числі відносно хмарних сервісів та у пост квантовий період;

володіння основними спеціалізованими апаратними, апаратно програмними та програмними засобами захисту інформації та інформаційних ресурсів, програмними пакетами та спеціалізованими бібліотеками, інтерфейсами та технічними специфікаціями що стосуються КЗІ, в тому числі для хмарних сервісів та у постквантовий період;

уміння практичного застосування ІС, ТС, ІТС та ІВК, в яких забезпечується необхідний рівень безпеки інформації надання електронних, в тому числі транскордонних, довірчих послуг, захисту інформаційних ресурсів та персональних даних, в тому числі в пост квантовий період.

### **ЗНАТИ:**

національну та міжнародну нормативно правову базу, науково-методичні та технічні принципи організації та виконання виготовлення, дослідження, впровадження та застосування криптографічних систем в ІС, ТС, ІТС та ІВК, включаючи хмарні обчислення;

моделі порушників та типові загрози безпеці інформації в ІС, ТС, ІТС та ІВК, що можуть виникати при застосуванні криптосистем, порядок їх аналізу та оцінки в процесі розробки, дослідження та застосування , а також особливості загроз ключам користувачів в хмарах.

критерії та показники оцінки стійкості, складності тощо реалізації криптосистем та безпечності криптографічних протоколів, включаючи хмарні сервіси;

методи, методики та засоби дослідження стійкості криптосистем та засобів КЗІ, особливості їх розробки та експертизи на національному та міжнародному рівнях;

типові вимоги до систем та засобів управління ключовими даними в криптосистемах, включаючи криптосистеми ІВК, та шляхи їх виконання в процесі побудування криптосистем та засобів КЗІ, в тому числі в пост квантовий період;

стандартизовані криптографічні примітиви, порядок їх розробки та застосування при захисті інформації з обмеженим доступом та наданні електронних транскордонних довірчих послуг в ІТС та ІВК, в тому числі у пост квантовий період;

типові стандартизовані криптосистеми та засоби криптографічного захисту інформації в ІС, ТС, ІТС та ІВК, вимоги до них та особливості побудування в ІТС та ІВК, в тому числі в пост квантовий період;

проблеми, стан та перспективи створення та застосування криптосистем та криптопротоколів в ІТС та ІВК, в тому числі в пост квантовий період, включаючи хмарні сервіси.

#### *УМІТИ:*

складати моделі загроз безпеці інформації, визначати задачі захисту та розробляти тактико-технічні вимоги до криптосистем та криптопротоколів, включаючи моделі загроз відносно користувачів хмарних сервісів;

розробляти технічні та часткові технічні завдання на криптосистеми та засоби КЗІ при їх побудові;

застосовувати отримані знання при експертизі, тематичних дослідженнях та сертифікаційних випробуваннях криптосистем та засобів КЗІ, в тому числі в пост квантовий період;

обґрунтувати та проектувати стандартні криптографічні системи, засоби, криптографічні примітиви та протоколи захисту інформації та інформаційних ресурсів в ІТС, включаючи хмарні сервіси;

здійснювати загальну оцінку якості захисту інформації та правомірність застосування криптосистем систем та засобів КЗІ в ІТС;

визначати основні функціональні та криптографічні вимоги до системи сертифікації та ТДС різного призначення, включаючи хмарні сервіси;

виконувати та аналізувати обов'язки посадових осіб служб інформаційної безпеки захищених ІТС(ІС) та центрів сертифікації ключів(ЦСК) згідно діючих регламентів чи діючих політик безпеки.

моделювати та досліджувати на ПЕОМ та безпосередньо з використанням засобів КЗІ процеси криптографічного захисту інформації та інформаційних ресурсів, криптографічних перетворень, криптографічного аналізу, управління ключами та криптографічні протоколи в ІТС та ІВК, в тому числі користувачам хмарних сервісів.

## **2. Тематичний план навчальної дисципліни**

Тема 1. Введення в дисципліну. Основи застосування криптосистем та засобів КЗІ при наданні електронних довірчих послуг. . Класифікація, основні вимоги та побудування криптосистем на основі блокових та поточкових симетричних шифрів. Застосування систем КЗІ для кіберзахисту. Вимоги до стандартизованих симетричних криптоперетворень в постквантовий період.

Тема 2. Класифікація, основні вимоги, стандартизація та принципи побудування асиметричних криптосистем шифрування та інкапсуляції ключів Особливості проектування та застосування криптосистем, в тому числі для кіберзахисту та у постквантовий період.

Тема 3. Методи побудування та основи аналізу ЕП. Порівняльний аналіз та застосування стандартизованих ЕП. Функції гешування, вимоги, стандартизація та застосування. Перспективні ЕП та ФГ для кіберзахисту та у постквантового періоду.

Тема 4. Побудування та аналіз засобів криптографічного захисту інформації.

Основні етапи проектування, побудови, експертизи, впровадження та експлуатації засобів КЗІ. Особливості проектування та застосування засобів КЗІ для кіберзахисту.

Тема 5. Методи, механізми та засоби криптографічного захисту інформації в ІТС. Основні додатки криптосистем та крипто протоколів, в тому числі відносно хмарних сервісів. Методи кіберзахисту від НСД на основі криптографічних перетворень.

Тема 6. Електронні довірчі послуги, сутність електронних довірчих послуг та особливості реалізації. Основи побудови ІВК. Електронні довірчі послуги на основі ЕЦП та АСШ. Особливості побудови ІВК для хмарних сервісів.

Тема 7. Генерування, сертифікація та застосування асиметричних ключів в ІВК. Життєві цикли приватних (особистих) ключів та сертифікатів відкритих ключів. Формати та технічні специфікації асиметричних пар ключів в ІВК.

Тема 8. Методи аналізу та порівняння криптографічних систем та протоколів. Національна система надання електронних довірчих послуг. Проблеми кіберзахисту на основі стандартизованих криптопримітивів. Основні проблеми КЗІ в перехідний та пост квантовий періоди.

Назва розділів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		Л	ПЗ	Лаб.	Інд.	С.Р.
1	2	3	4	5	6	7
<b>Тема 1.</b> Введення в дисципліну. Основи побудування та дослідження криптосистем на основі блокових та поточкових симетричних шифрів	18	2		4		12
<b>Тема 2.</b> Класифікація, основні вимоги, стандартизація та дослідження асиметричних криптосистем шифрування та інкапсуляції ключів	18	2		2		14
<b>Тема 3.</b> Методи побудування та основи аналізу ЕП. Функції гешування, вимоги, стандартизація та застосування.	18	2		2		14
<b>Тема 4.</b> . Побудування та аналіз засобів криптографічного захисту інформації.	18	2	2			14
<b>Тема 5.</b> Методи, механізми та засоби криптографічного захисту інформації в ІТС.	18	2	2			14
<b>Тема 6</b> Електронні довірчі послуги, сутність особливості надання. Основи побудови ІВК.	16	2	2			12
<b>Тема 7.</b> Генерування, сертифікація та застосування асиметричних ключів в ІВК. .	18	2	2			14
<b>Тема 8.</b> Методи аналізу та порівняння криптографічних систем та протоколів. Проблеми кіберзахисту на основі стандартизованих криптопримітивів.	16	2				14
<b>Індивідуальне завдання( курсова</b>	40				40*	

робота 20 год та наукові дослідження 20 год) (за рахунок С.Р.)*						
<b>Усього годин</b>	180	16	8	8	40 *	108

#### 4. Теми практичних та лабораторних занять

№ з/п	Назва теми семінарських (практичних) занять	Кількість годин
1	Побудування та аналіз засобів криптографічного захисту інформації.	2
2	Нормативно – правова база. Стан стандартизації. Вимоги до засобів КЗІ згідно діючих стандартів. Особливості проектування та застосування засобів КЗІ	2
3	Електронні довірчі послуги, сутність особливості надання. Основи побудови ІВК	2
4	Проблеми кіберзахисту на основі стандартизованих криптопримітивів.	2
	Разом	8

№ з/п	Назва теми лабораторних занять	Кількість годин
1	Побудування та дослідження криптосистем на основі блокових та поточкових симетричних шифрів. Методики проведення криптоаналізу та оцінки властивостей криптосистем на основі БСШ.	4
2	Дослідження асиметричних криптосистем шифрування та інкапсуляції ключів Дослідження та порівняльний стандартів електронного цифрового підпису( ЕЦП).	2
3	Інсталяція та дослідження АЦСК, аналіз систем управління та сертифікація ключів, моніторинг безпеки, виконання планової та аварійної заміни ключів, порядок ведення експлуатаційної та ключової документації	2
3*	Альтернатива 3. Інсталяція та дослідження системи захисту IP – sec(TCP) , аналіз процесів управління ключами та шифраторами в режимах планової та аварійної заміни, моніторинг безпеки, особливості ведення експлуатаційної та ключової документації	
	Разом	8

#### Додаткові лабораторні роботи (за вибором студента)

1. Дослідження постквантових проектів стандартів асиметричного шифрування та інкапсуляції ключів.
2. Дослідження постквантових проектів стандартів електронного підпису.
3. Розроблення програмних моделей та дослідження перспективних криптографічних перетворень типу електронний цифровий підпис
4. Розроблення програмних моделей та дослідження перспективних функцій гешування.
5. Методи та алгоритми криптоаналізу поточкових симетричних шифрів.
6. Методи та алгоритми криптоаналізу блокових симетричних шифрів.
7. Дослідження перспективних криптографічних механізмів та протоколів встановлення ключів.
8. Розробка та аналіз систем захисту від НСД на основі методів багатofакторної автентифікації.

### 5. Завдання для самостійної роботи

<i>№з/п</i>	Види, зміст самостійної роботи	<i>Кількість годин</i>
1	<p>Класифікація, основні вимоги та побудування криптосистем на основі блокових симетричних шифрів(БСШ). Управління ключами в криптосистемах на основі БСШ.</p> <p>Класифікація, основні вимоги та побудування криптосистем на основі поточкових симетричних шифрів(ПСШ). Механізми автентифікації, розподілу, узгодження та встановлення ключів в симетричних криптосистемах на основі ПСШ.</p>	12
2	<p>Основні вимоги та принципи побудування асиметричних криптосистем. Порівняльний аналіз асиметричних крипто систем по критеріям складності та криптографічної стійкості</p> <p>Створення(побудування) та особливості застосування асиметричних крипто перетворень при побудуванні асиметричних криптосистем та криптографічних протоколів. Побудування та аналіз систем управління ключами в асиметричних криптосистемах</p>	14
3	<p>Вимоги до засобів КЗІ. Стандартизація та уніфікація вимог до засобів КЗІ. Методи побудови програмних, апаратно – програмних та апаратних засобів КЗІ.</p> <p>Основні етапи проектування, побудови, експертизи, впровадження та експлуатації засобів КЗІ. Вимоги до мови управління засобами КЗІ та їх реалізація. Сутність та вимоги до бібліотек криптографічних перетворень</p>	14
4	<p>Системи захисту IP – sec в робочому стані, управління ключами та шифраторами режимах, планової та аварійної заміни, ведення експлуатаційної та ключової документації з використанням БСШ.</p> <p>Системи захисту з'єднань, управління ключами та шифраторами режимах, планової та аварійної заміни, ведення експлуатаційної та ключової документації з використанням БСШ та ПСШ</p>	14
5	<p>Політики сертифікації. Нормативно правова база надання електронних довірчих послуг. Міжнародна національна стандартизація. Моделі загроз та порушника ІВК. Принципи побудування та застосування ІВК.</p> <p>Основні принципи побудування та застосування систем та засобів надання електронних довірчих послуг.</p>	14
6	<p>Нормативно правова база управління ключами. Основні функції систем управління ключами. Управління ключами в основних додатках КЗІ. Криптографічна живучість систем управління ключами. Криптографічні механізми та протоколи встановлення,</p>	12



	транспортування та передавання ключів. Порядок оцінки систем управління та сертифікації ключів.	
7	Класифікація та порівняльний аналіз національних стандартів електронного цифрового підпису( ЕЦП) та направленою шифрування (НШ). Синтез та аналіз криптографічних протоколів автентифікації, розподілу, узгодження та встановлення ключів. Оцінка безпеки криптографічних протоколів.	14
8	Асиметричні криптографічні перетворення перехідного та пост квантового періодів. Моделі та методи побудування. Особливості побудування загальних параметрів та генерування ключів. Побудування та аналіз механізмів та протоколів КЗІ на основі пост квантових криптотопримітивів. Методи захисту від НСД на основі криптографічних перетворень. Порівняльний аналіз та оцінка захищеності від НСД на основі методів багатofакторної автентифікації. Основні додатки криптосистем та крипто протоколів. Побудування та аналіз систем КЗІ на фізичному, прикладному, IP та TCP – рівня Проблеми теорії та практики криптографічного захисту інформації	14
9	Проведення наукових досліджень та підготовка наукових доповідей та наукових статей	20
10	Виконання курсової роботи	20
<b>Разом:</b>		<b>148</b>

#### 5. Завдання для самостійної роботи

№ з/п	Види та зміст завдання	Кількість годин
1	Підготовка до лекцій	8
1.1	Вивчення та аналіз національних та міжнародних стандартів КЗІ	32
2	Підготовка до практичних занять та лабораторних робіт	16
3	Виконання домашніх завдань	16
4	Підготовка до комп'ютерного тестування	4
5	Виконання курсової роботи	20
6	Переклад та аналіз додаткової літератури	32
	Проведення наукових досліджень та підготовка наукових доповідей та наукових статей	20
	Разом	148

#### 6. Індивідуальні завдання

Індивідуальне завдання – курсова робота по розділам 1-6 за темами «Побудування та порівняльний аналіз класичних та постквантових криптосистем».

Суть завдання, що виконується в курсовій роботі, полягає у обґрунтуванні вимог до симетричних та асиметричних криптоперетворень, вибору критеріїв та показників оцінки криптоперетворень, аналізу та оцінці сутності криптоперетворень, математичному чи програмному моделюванню та порівнянню».

Допускається виконання індивідуального завдання, основою якого є проведення дослідження з подальшою підготовкою наукової доповіді чи наукової статі, удосконалення дослідницьких лабораторних робіт, а також подача результатів досліджень на кафедрі.

## 7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom).

## 8. Методи контролю

Контроль засвоєння студентами навчального матеріалу на лекційному занятті здійснюється шляхом концентрації уваги студентів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

Присутність студента на занятті оцінюється в 0,25- 0.5 балів. Максимальна кількість балів за присутність студента на занятті складає 8 балів в семестр.

На практичному занятті контроль знань студентів робиться методом проведення експрес-опитувань (письмово), в тому числі вирішенні задач за тематикою ПЗ. Рівень знань, продемонстрований студентами на кожному експрес-опитуванні оцінюється, як правило, максимально 4 балами.

На лабораторних роботах контроль засвоєння студентами навчального матеріалу здійснюється шляхом оцінки якості оформлення звіту і його захисту. Рівень знань, продемонстрований студентами при оформленні і захисті звітів по лабораторних роботах оцінюється максимально 8 балами.

Контроль засвоєння студентами навчального матеріалу здійснюється на контрольних роботах (комп'ютерних тестах), що передбачена навчальним планом. Завдання на контрольну роботу включає два практичні питання(задачі). Рівень знань, продемонстрований студентами на контрольній роботі оцінюється максимально 8 балами (як правило 4 бала за кожне практичне питання).

При виконанні курсової роботи контролюється рівень полягає у обґрунтуванні вимог до симетричних та асиметричних криптоперетворень, вибору критеріїв та показників оцінки криптоперетворень, аналізу та оцінці сутності криптоперетворень, математичному чи програмному моделюванні та порівнянні альтернатив.

Бали за курсову роботу складаються з розрахунку: 3 бал за акуратність оформлення розрахунково-пояснювальної записки (відповідно до вимог методичних вказівок по оформленню курсової роботи), 12 балів за результат та 5 балів за захист курсової роботи. Максимальна кількість балів за курсову роботу складає 20 балів.

Максимальна кількість балів за результатами контролю поточної успішності за семестр складає 60 балів.

Згідно рішення кафедри безпеки інформаційних системі технологій до іспиту не допускаються студенти, що не захистили звіти по лабораторних роботах, не брали участь у виконанні контрольних робіт і не захистили курсову роботу.

Підсумковий контроль здійснюється шляхом проведення письмового іспиту.

Екзаменаційний квиток включає два теоретичних і одне практичне питання. Теоретичні питання оцінюються до 10 балів кожне, практичне – до 20 балів.

Максимальна кількість балів за результатами іспиту складає 40 балів.

Максимальна кількість балів за результатами вивчення дисципліни складає 100 балів.

### 9. Схема нарахування балів

Бали за поточний контроль знань по темам 1- 8 протягом 5 семестру				В т.ч комп'ютерни й тест	Курсо ва робота	Разом сума балів у семест рі	Іспит	Загальна сума балів
T1-T2	T3-T4	T5-T6	T7 – T84	4	20	60	40	100
8	8	10	10					

T1, T2, T3, T4 – теми занять.

5 семестр

Рівень знань, продемонстрований студентами, оцінюється таким чином:

- за темою 1(T1) – 7 балів: виконання 1 ЛР, 1 експрес-опитування;
- за темою 2(T2) – 5 балів, виконання 1 ЛР;
- за темою 3(T3) – 4 балів: виконання 1 ЛР, 1 експрес-опитування;
- за темою 4(T4) – 4 бали: виконання 1 ПЗ;
- за темою 5(T5) – 5 балів: виконання 1 ПЗ, 1 експрес-опитування;
- за темою 6(T6) – 5 балів, виконання 1 ПЗ, 1 експрес-опитування;
- за темою 7(T7) – 4 балів, виконання 1 ПЗ, 1 експрес-опитування;
- за темою 8(T8) – 6 балів: 1 комп'ютерне опитування;;
- в тому числі за присутність на заняттях – 4 балів;
- в тому числі за результати досліджень – 4 бали.12

### Критерії оцінювання

#### Критерії оцінювання знань студентів при опитуванні

Визначення	Кількість балів
Відповідь без помилок	2
Виконання відповіді з незначними помилками	1
Відповідь є з певною кількістю помилок, які не заважають достатньо повному висвітленню питання	0,5
Неправильна відповідь, мають місце грубі помилки, нерозуміння суті питання	0

#### Критерії оцінювання знань студентів за виконання лабораторної роботи

Визначення	Кількість балів
Завдання по лабораторній роботі виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захисті звіту показано розуміння суті і змісту проведених досліджень	4
Завдання по лабораторній роботі виконане самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу	3
Завдання по лабораторній роботі виконане в повному обсязі. Звіт оформлений достатньо акуратно, в оформленні звіту є незначні недоліки. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу	2

Завдання по лабораторній роботі виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу	1
---	---

#### Критерії оцінювання знань студентів за комп'ютерний тест

Визначення	Кількість балів
Дані повні відповіді на кожне практичне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	4
У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки	3
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	2
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	1
У відповідях на показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки	0,5

#### Критерії оцінювання знань студентів за виконання курсової роботи

Визначення	Кількість балів
Завдання на курсову роботу виконано акуратно в повній відповідності з вимог методичних вказівок. Студент показав тверде знання навчального матеріалу, вміння чітко і стисло викладати основні результати дослідження.	20
Завдання на курсову роботу виконано досить акуратно, але не в повній відповідності з вимогами методичних вказівок. Студент показав достатньо тверде знання навчального матеріалу і вміння стисло викладати основні результати дослідження.	12-19
Завдання на курсову роботу виконано не в повній відповідності з вимогами методичних вказівок. Студент показав не достатньо тверде знання навчального матеріалу і вміння викладати основні результати дослідження.	4-11
Завдання на курсову роботу виконано не в повній відповідності з вимогами методичних вказівок. Студент показав слабке знання навчального матеріалу і невміння викладати основні результати дослідження. У розрахунково-пояснювальній записці є присутніми помилки	1-4

## Критерії оцінювання екзаменаційних робіт студентів

Визначення	Кількість балів
При відповіді на екзаменаційний квиток теоретичні питання освітлені повністю, завдання вирішене правильно, зроблені висновки	40
При відповіді на екзаменаційний квиток теоретичні питання достатньо освітлені, завдання вирішене правильно з незначними помилками, зроблені висновки	35-39
При відповіді на екзаменаційний квиток теоретичні питання освітлені з помилками, завдання вирішене правильно з незначними помилками. Зроблені неповні висновки	25-34
При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене з помилками. Зроблені неповні висновки	15-24
При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене частково або не повністю. Висновки неповні або відсутні	1-14

## Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для чотирирівневої шкали оцінювання (іспит)
90 – 100	відмінно
70-89	добре
50-69	задовільно
1-49	незадовільно

**10. Рекомендована література****Основна література**

1. Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації. Монографія За редакцією Горбенко І.Д. Горбенко Ю.І.. Харків. Форт. 2016, 902 с.
2. Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації. Електронна версія. Монографія. За редакцією Горбенко І.Д. Горбенко Ю.І. Харків. Форт. 2016, 902 с.
3. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010, 593 с.
4. Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження / О. В. Потій, А. В. Леншин, Л. С. Сорока, В. І. Єсін і ін. // . – Дніпропетровськ: Академія митної служби України, 2011. – 202 с.
5. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013 р., 878 с.

**Допоміжна література**

1. Кузнецов О.О., Потій О.В., Полуяненко М.О., Горбенко Ю.І. Потоківі шифри. Монографія. Харків. Форт. 2019 р., 544 с.
2. Задірака В., Олексик О. Комп'ютерна криптологія. – К., 2002. – 502 с.

3. Потій О.В. Стандартизація та сертифікація в галузі захисту інформації. Стандарти управління ключами / О.В. Потій. – Х. : ХНУРЕ, 2002. – 80 с.
4. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій. Х.: ХНУ імені В. Н. Каразіна, 2013. 632 с.
5. Claude E. Shannon The Mathematical Theory of Communication (16th Edition). The University of Illinois Press. 1971. 144 p.
6. Bruce Schneier Applied Cryptography. Protocols, Algorithms, and Source Code in C. John Wiley & Sons. 1996. 784 p.
7. William Stallings Cryptography and Network Security: Principles and Practice (6th Edition). Pearson. 2013. 752 p.
8. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К. Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

### **Інформаційні ресурси**

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 17 серпня 2022 року N 2163-VIII.
2. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.
3. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».
4. ДСТУ ITU-T Rec.X.509 | ISO/IEC 9594-8:2006 «Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів».
5. ДСТУ ISO/IEC 10118-1:2003 «Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення».
6. ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. Геш-функції. Частина 3: Спеціалізовані геш-функції».
7. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування».
8. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення».
9. ДСТУ ISO/IEC 13888-1:2002. «Інформаційні технології. Методи захисту. Неспростовність. Частина 1. Загальні положення».
10. ДСТУ ISO/IEC TR 13335-1:2003 «Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки ІТ», 2005.
11. ДСТУ ISO/IEC 14888-3:2014 «Інформаційні технології – Методи захисту – Цифрові підписи з доповненням – Частина 3. Механізми, що ґрунтуються на дискретному логарифмі» (ISO/IEC 14888-3:2008, IDT). – 113 с.
12. ДСТУ ISO/IEC 15946-3:2006 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3: Встановлення ключів».
13. Закон України «Про електронні довірчі послуги» від 1 січня 2023 року N 2155-VIII.
14. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.
15. Закон України «Про інформацію» від 1 січня 2023 року N 2657-XII.

16. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 4 червня 2020 року N 681-IX.

17. Правила посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 3 від 3.01.2005, зареєстрованих в Міністерстві юстиції України 27.01.2005 за № 104/10384 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 № 50).

18. РЕГЛАМЕНТ (ЄС) № 910/2014 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ ТА РАДИ від 23 липня 2014 року «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС» (1)(СОМ (2012) 0238 - С7-0133/2012 - 2012 / 0146 (COD)).

19. Резолюція Європейського Парламенту від 21.09.2010 про створення внутрішнього ринку для електронної торгівлі, 21.09.10, P7\_TA (2010) 0320, і Резолюція Європейського Парламенту від 15.06.2010 про управління Інтернетом: наступні кроки, P7\_TA (2010) 0208.

20. Державна служба спеціального зв'язку та захисту інформації України. Наказ від 20.07.2007 №141 «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використанням електронного цифрового підпису» № 862/14129.

21. American National Standard for Financial Services ANSI X9.98-2010 Lattice Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry. – 202 p.

22. FIPS-186-3. Digital signature standard: 2009, 2009-07-19. Gaithersburg, MD 20899-8900, 2009.

23. FIPS PUB 186-1994 Digital signature standard. National Institute of standard and technology, 1994.

24. FIPS 197 «Advanced Encryption Standard», 2001.

25. FIPS PUB 186-2-2000. Digital signature standard. National Institute of standard and technology, 2000.

26. FIPS PUB 186-3-2009. Digital signature standard: 2009. National Institute of standard and technology. 2009.

27. ISO/IEC 18031:2011 Information technology. – Security techniques. – Random bit generation.

28. ISO/IEC 9594-8:2008 Information technology. – Open Systems Interconnection. – The Directory: Public-key and attribute certificate frameworks.

29. ISO/IEC 18033-1:2005 Information technology. – Security techniques. – Encryption algorithms. – Part 1: General.

30. ISO/IEC 18033-2:2006 Information technology. – Security techniques. – Encryption algorithms. – Part 2: Asymmetric cipher.

31. ISO/IEC 9594-8:2008 Information technology. – Open Systems Interconnection. – The Directory: Public-key and attribute certificate frameworks.

32. ISO/IEC 9796-2:2010 Information technology. – Security techniques. – Digital signature schemes giving message recovery. – Part 2: Integer factorization based mechanisms.

33. ISO/IEC 9796-3:2006 Information technology. – Security techniques. – Digital signature schemes giving message recovery. – Part 3: Discrete logarithm based mechanisms.

34. ISO/IEC 15946-2:2002 Information technology. – Security techniques. – Cryptographic techniques based on elliptic curves. – Part 2: Digital Signatures.
35. ISO/IEC 14888-1:2008 Information technology. – Security techniques. – Digital signatures with appendix. – Part 1: General.
36. ISO/IEC 14888-2:2008 Information technology. – Security techniques. – Digital signatures with appendix. – Part 2: Integer factorization based mechanisms.
37. ISO/IEC 14888-3:2006 Information technology. – Security techniques. – Digital signatures with appendix. – Part 3: Discrete logarithm based mechanisms.
38. ISO/IEC 15946-1:2008 Information technology. – Security techniques. – Cryptographic techniques based on elliptic curves. – Part 1: General.
39. ISO/IEC 9798-1:2010 Information technology. – Security techniques. – Entity authentication. – Part 1: General.
40. ISO/IEC 13888-1:2004 IT security techniques. – Non-repudiation. – Part 1:General.
41. ДСТУ ISO/IEC 9594-8:2014 «Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8: Основні положення щодо сертифікації відкритих ключів та атрибутів». На заміну ДСТУ ISO/IEC 9594-8:2006.
42. ДСТУ ISO/IEC 9796-3:2014 «Інформаційні технології. Методи забезпечення безпеки. Цифрові схеми підпису, що забезпечують відновлення повідомлень. Частина 3. Основні механізми дискретного логарифма».
43. ДСТУ ISO/IEC 9797-1:2014 «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 1. Механізми, що використовують блокові шифри». На заміну ДСТУ ISO/IEC 9797-1:2009.
44. ДСТУ ISO/IEC 9797-2:2014 «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що використовують універсальну геш-функцію». На заміну ДСТУ ISO/IEC 9797-2:2009.
45. ДСТУ ISO/IEC 9797-3:2014 «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 3. Механізми, що використовують спеціалізовану геш-функцію».
46. ДСТУ ISO/IEC 9798-1:2014 «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 1. Загальні положення». На заміну ДСТУ ISO/IEC 9798-1:2002.
47. ДСТУ ISO/IEC 9798-2:2014 «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 2. Механізми, що використовують алгоритми симетричного шифрування».
48. ДСТУ ISO/IEC 9798-4:2014 «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 4. Методи на базі криптографічних контрольних функцій».
49. ДСТУ ISO/IEC 9798-5:2014 «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 5. Механізми, що використовують методи нульової обізнаності».
50. ДСТУ ISO/IEC 10116:2014 «Інформаційні технології. Методи забезпечення безпеки. Режими роботи для N-розрядного блочного шифру».
51. ДСТУ ISO/IEC 10118-2:2014 «Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n-бітовий блоковий алгоритм шифрування». На заміну ДСТУ ISO/IEC 10118-2:2003.



52. ДСТУ ISO/IEC 11770-1:2014 «Управління ключами захисту. Частина 1. Структура». На заміну ДСТУ ISO/IEC 11770-1:2009.
53. ДСТУ ISO/IEC 11770-2:2014 «Інформаційні технології. Методи захисту. Управління ключами захисту. Частина 2. Механізми, що використовують симетричні методи». На заміну ДСТУ ISO/IEC 11770-2:2002.
54. ДСТУ ISO/IEC 11770-3:2014 «Інформаційні технології. Методи захисту. Управління ключами захисту. Частина 3. Механізми, що використовують асиметричні методи розроблення». На заміну ДСТУ ISO/IEC 11770-3:2002.
55. ДСТУ ISO/IEC 11770-4:2014 «Інформаційні технології. Методи захисту. Управління ключами захисту. Частина 4. Механізми, засновані на нестійких секретах».
56. ДСТУ ISO/IEC 11770-5:2014 «Інформаційні технології. Методи забезпечення безпеки. Керування ключами. Частина 5. Група керування ключами».
57. ДСТУ ISO/IEC 13888-1:2014 «Інформаційні технології. Методи захисту. Неспростовність. Частина 1: Загальні положення». На заміну ДСТУ ISO/IEC 13888-1:2002.
58. ДСТУ ISO/IEC 13888-2:2014 «Інформаційні технології. Методи захисту. Неспростовність. Частина 2. Механізми використання симетричних методів». На заміну ДСТУ ISO/IEC 13888-2:2009.
59. ДСТУ ISO/IEC 13888-3:2014 «Інформаційні технології. Методи захисту. Неспростовність. Частина 3. Механізми використання асиметричних методів». На заміну ДСТУ ISO/IEC 13888-3:2002.
60. ДСТУ ISO/IEC 14888-1:2014 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням Частина 1. Загальні положення». На заміну ДСТУ ISO/IEC 14888-1:2002.
61. ДСТУ ISO/IEC 15946-1:2014 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 1. Загальні положення». На заміну ДСТУ ISO/IEC 15946-1:2006.
62. ДСТУ ISO/IEC 15946-5:2014 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 1. Генерація еліптичних кривих».
63. ДСТУ ISO/IEC 18014-1:2014 «Інформаційні технології. Методи захисту. Послуги шпенпелювання часу. Частина 1. Основні положення». На заміну ДСТУ ISO/IEC 18014-1:2006.
64. ДСТУ ISO/IEC 18014-2:2014 «Інформаційні технології. Методи захисту. Послуги шпенпелювання часу. Частина 2. Механізми, що виробляють незалежні токени». На заміну ДСТУ ISO/IEC 18014-2:2006.
65. ДСТУ ISO/IEC 18014-3:2014 «Інформаційні технології. Методи захисту. Послуги шпенпелювання часу. Частина 3. Механізми, що виробляють зв'язані і токени». На заміну ДСТУ ISO/IEC 18014-3:2006.
66. ДСТУ ISO/IEC 19790:2014 «Інформаційні технології. Методи захисту. Вимоги щодо захисту криптографічних модулів». На заміну ДСТУ ISO/IEC 19790:2009.
67. ДСТУ ISO/IEC 29115:2014 «Інформаційні технології. Методи забезпечення безпеки. Схема забезпечення автентифікації об'єкта».
68. ДСТУ ISO/IEC 29191:2014 «Інформаційні технології. Методи захисту. Вимоги до частково анонімної, частково роз'єднаної автентифікації».

69. ДСТУ СВА 14167-1:2014 «Вимоги безпеки для надійних систем управління сертифікатами для електронних підписів. Частина 1. Вимоги безпеки системи».
70. ДСТУ СВА 14167-2:2014 «Криптографічний модуль для операцій підписування CSP з резервуванням. Частина 2. Профіль захисту СМCSOB».
71. ДСТУ СВА 14167-4:2014 «Криптографічний модуль для операцій підписування CSP. Частина 4. Профіль захисту СМCSO».
72. RFC 2631 “Diffie-Hellman Key Agreement Method”, June 1999.
73. RFC 2785 Methods for Avoiding the «Small-Subgroup» Attacks on the Diffie-Hellman Key Agreement for S/MIME, March 2000.
74. RFC 3279 “Algorithms and Identifiers for the Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002.
75. RFC 3281 “An Internet Attribute Certificate Profile for Authorization”, April 2002.
76. RFC 3370 “Cryptographic Message Syntax (CMS) Algorithms”, August 2002.
77. RFC 3394 “Encryption Standard (AES) Key Wrap Algorithm”, September 2002.
78. RFC 3852 “Cryptographic Message Syntax (CMS)”, July 2004.
79. RFC 5008 “Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)”, September 2007.
80. RFC 5480 “Elliptic Curve Cryptography Subject Public Key”, March 2009.
81. RFC 5652 “Cryptographic Message Syntax (CMS)”, September 2009.

#### **11. Основні сайти з інформацією по дисципліні «Криптографічні методи в кібербезпеці»**

1. <https://csrc.nist.gov/Projects/post-quantum-cryptography/>
2. [www.nist.gov](http://www.nist.gov)
3. <https://www.etsi.org/standards#Pre-defined%20Collections>
4. [https://www.bsi.bund.de/DE/Home/home\\_node.html](https://www.bsi.bund.de/DE/Home/home_node.html)
5. [www.ansi.org](http://www.ansi.org)
6. [www.cryptography.org](http://www.cryptography.org)
7. [www.iso.org](http://www.iso.org)
8. [www.linuxiso.org](http://www.linuxiso.org)
9. [www.cryptography.com](http://www.cryptography.com)
10. [www.cacr.math.uwaterloo.ca](http://www.cacr.math.uwaterloo.ca)
11. [www.financialcryptography.com](http://www.financialcryptography.com)
12. [www.cryptonesia.org](http://www.cryptonesia.org)

## КУРСОВА РОБОТА

### А.1 Тематика курсових робіт

1. Обґрунтування та розробка методик порівняльного аналізу існуючих та перспективних криптосистем.
2. Обґрунтування та вибір критеріїв та показників оцінки та порівняння криптосистем та криптопротоколів.
3. Методики порівняльного аналізу криптосистем (блокові симетричні шифри; потокові симетричні шифри; електронні підписи; направлені шифри; криптографічні протоколи).
4. Методики, системи та засоби здійснення криптоаналізу на основі класичних комп'ютерів та математичних методів (метод Шора, метод Гровера, методи Ксінга тощо).
5. Методики, системи та засоби здійснення криптоаналізу на основі квантових комп'ютерів та квантових алгоритмів.
6. Моделі порушників криптосистем.
7. Моделі загроз існуючим та перспективним криптосистемам.
8. Моделі безпеки існуючих та перспективних криптосистем.
9. Аналіз криптографічної стійкості хмарних сервісів.
10. Дослідження безпечності систем управління ключами клієнтів хмарних сервісів.
11. Розробка та дослідження програмних моделей та бібліотек існуючих та перспективних криптосистем.
12. Аналіз стану створення та застосування квантових комп'ютерів для вирішення задач криптології.
13. Аналіз та порівняння методів криптоаналізу симетричних та асиметричних криптосистем.
14. Обґрунтування вимог та механізмів побудови постквантових криптосистем.
15. Аналіз стану та напрямів створення постквантових криптосистем.
16. Дослідження механізмів побудови ЕП на основі геш-функцій.
17. Дослідження механізмів побудови ЕП на основі алгебраїчних решіток.
18. Обґрунтування та розробка методики аналізу криптопримітивів за безумовними, умовними та прагматичними критеріями.
19. Обґрунтування та розробка методики аналізу асиметричних шифрів за безумовними, умовними та прагматичними критеріями.
20. Обґрунтування та розробка методики аналізу електронних підписів за безумовними, умовними та прагматичними критеріями.
21. Обґрунтування та розробка методики аналізу протоколу інкапсуляції ключів за безумовними, умовними та прагматичними критеріями.
22. Обґрунтування та розробка пропозицій з побудови постквантових механізмів асиметричного шифрування.
23. Розробка та порівняння програмних моделей та бібліотек сучасних та перспективних постквантових криптосистем.
24. Дослідження механізмів та методів забезпечення криптоживучості перспективних постквантових криптосистем.

25. Класифікація та узагальнена оцінка ЕП постквантового періоду.
26. Класифікація та узагальнена оцінка АСШ постквантового періоду.
27. Аналіз та оцінка алгоритму електронного підпису, що є переможцем конкурсу NIST PQC, Crystals-Dilithium.
28. Аналіз та оцінка алгоритму асиметричного шифрування, що є переможцем конкурсу NIST PQC, Crystals-Kyber.
29. Аналіз та оцінка алгоритму електронного підпису, що є переможцем конкурсу NIST PQC, Falcon.
30. Аналіз та оцінка алгоритму електронного підпису, що є переможцем конкурсу NIST PQC, SPHINCS+.
31. Аналіз та оцінка алгоритму асиметричного шифрування, що переходить до четвертого раунду конкурсу NIST PQC, BIKE.
32. Аналіз та оцінка алгоритму асиметричного шифрування, що переходить до четвертого раунду конкурсу NIST PQC, Classic McEliece.
33. Аналіз та оцінка алгоритму асиметричного шифрування, що переходить до четвертого раунду конкурсу NIST PQC, HQC.
34. Аналіз та оцінка алгоритму асиметричного шифрування, що переходить до четвертого раунду конкурсу NIST PQC, SIKE.
35. Порівняльний аналіз стійкості ДСТУ 7624:2014 з міжнародно визнаними стандартами.
36. Порівняльний аналіз стійкості ДСТУ 7564:2014 з міжнародно визнаними стандартами.
37. Синтез та аналіз елементів криптографічних засобів.

**Цей перелік тем не є вичерпним. Можливим є узгодження зі студентам індивідуальних тем для курсової роботи.**