Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної

роботи

Антон ПАНТЕЛЕЙМОНОВ

"_____" 2020 р.

Робоча програма навчальної дисципліни

Криптографічні методи в кібербезпеці

рівень вищої освіти другий (магістри)

галузь знань 12 «Інформаційні технології»

спеціальність 125 – «Кібербезпека»

освітня програма Безпека інформаційних і комунікаційних систем .

спеціалізація

вид дисципліни обов'язкова

факультет комп'ютерних наук

2020 / 2021 навчальний рік

Програму рекомендовано до затвердження вченою радою факультету (інституту, центру)

"31" серпня 2020 року, протокол № 12

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 "31" серпня 2020 року № 1

Завідувач кафедри безпеки інформаційних систем і технологій

_____ Рассомахін С.Г.
(підпис) (прізвище та ініціали)

Програму погоджено з гарантом освітньої (професійної/наукової) програми (керівником проектної групи) Безпека інформаційних і комунікаційних систем
назва освітньої програми

Гарант освітньої (професійної/наукової) програми
(керівник проектної групи) Єсін Віталій Іванович

_____ Єсін В.І.
(підпис) **(прізвище та ініціали)**

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "31" серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

_____ Бердніков А. Г.

ВСТУП

Програма навчальної дисципліни "Криптографічні методи в кібербехпеці " 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, навчанню 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 проведені досліджень та виконанні наукової роботи, а також на практиці, що передує 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 постківантовий 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 крипто протоколів в ІТС та ІВК, в тому числі в пост квантовий період, включаючи хмарі сервіси.

УМІТИ:

складати моделі загроз безпеці інформації, визначати задачі захисту та розробляти тактико-технічні вимоги до криптосистем та крипто протоколів, 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 випробовуваннях 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 потокових 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 інкапсуляціє ключів Особливості проектування та застосування криптосистем, в тому числі для кібебрзахисту та у постквантовий період.

Тема 3. Методи побудування та основи аналізу ЕП. Порівняльний аналіз тап 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. Національні 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
Тема 1. Введення в дисципліну. Основи побудування та дослідження криптосистем на основі блокових та потокових симетричних шифрів	18	2		4		12
Тема 2. Класифікація, основні вимоги, стандартизація та дослідження асиметричних криптосистем шифрування та інкапсуляціє ключів	18	2		2		14
Тема 3. Методи побудування та основи аналізу ЕП. Функції гешування, вимоги, стандартизація та застосування.	18	2		2		14
Тема 4. . Побудування та аналіз засобів криптографічного захисту інформації.	18	2	2			14
Тема 5. Методи, механізми та засоби криптографічного захисту інформації в ІТС.	18	2	2			14
Тема 6 Електронні довірчі послуги, сутність особливості надання. Основи побудови ІВК.	16	2	2			12
Тема 7. Генерування, сертифікація та застосування асиметричних ключів в ІВК. .	18	2	2			14
Тема 8. Методи аналізу та порівняння криптографічних систем та протоколів. Проблеми кіберзахисту на основі стандартизованих криптопримітивів.	16	2				14
Індивідуальне завдання(курсова робота 20 год та наукові дослідження 20 год) **(за рахунок С.Р.)***	40				40*	
Усього годин	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 потокових симетричних шифрів. Методики проведення крипто аналізу та оцінки властивостей криптосистем на основі БСШ.		4
2	Дослідження асиметричних криптосистем шифрування та інкапсуляціє 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 електроннного 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 крипто аналізу потокових симетричних шифрів.
6. Методи та алгоритми крипто аналізу блокових симетричних шифрів.
7. Дослідження перспективних криптографічних механізмів та протоколів встановлення ключів.
8. Розробка та аналіз систем захисту від НСД на основі методів багатофакторної автентифікації.

5. Завдання для самостійної робота

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

	електронного цифрового підпису(ЕЦП) та направленого 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 багатофакторної 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
	Разом:	**148**

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 моделюванні та порівнянні».

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 кафедру.

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 зайнятті здійснюється шляхом концентрації уваги студентів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

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

На практичному зайнятті 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 дисципліні складає 100 балів.

9. Схема нарахування балів

Бали за поточний контроль знань по темам 1- 8 протягом 5 семестру				В т.ч компютерний тест	Курсова робота	Разом сума балів у семестрі	Іспит	Загальна сума балів
Т1-Т2	Т3-Т4	Т5-Т6	Т7 – Т84					
8	8	10	10	4	20	60	40	100

Т1, Т2, Т3, Т4 – теми занять.

5 семестр

Рівень знань, продемонстрований студентами, оцінюється таким чином:
- за темою 1(Т1) – 7 балів: виконання 1 ЛР, 1 експрес-опитування;
- за темою 2(Т2) – 5 балів, виконання 1 ЛР;
- за темою 3(Т3) – 4 балів: виконання 1 ЛР, 1 експрес-опитування;
- за темою 4(Т4) – 4 бали: виконання 1 ПЗ;
- за темою 5(Т5) – 5 балів: виконання 1 ПЗ, 1 експрес-опитування;
- за темою 6(Т6) – 5 балів, виконання 1 ПЗ, 1 експрес-опитування;
- за темою 7(Т7) – 4 балів, виконання 1 ПЗ, 1 експрес-опитування;
- за темою 8(Т8) – 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	4

знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	
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

10.1 Основна література

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

10.2 Допоміжна література

1. В.И.Долгов, И.В.Лисицкая. Блочные симметричные шифры. Методология оценки стойкости к атакам дифференциального и линейногокриптоанализа. Монография. Харков, ХНУРЭ, Форт, 2014 р., 455 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. Есин В. И. Безопасность информационных систем и технологий / В. И. Есин, А. А. Кузнецов, Л. С. Сорока. – Х. : ООО «ЭДЭНА», 2010. – 656 с.
5. Шеннон К. Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – 830 с. (Раздел – Теория связи в секретных системах).
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: «Триумф», 2002. – 797 с.
7. Шнайер Б. Безопасность данных в цифровом мире. – СПб: Питер, 2003. – 367 с.
8.Ю. Юдін О.К, Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К. Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.
9. В.В. Яновский. Квантовая механика алгоритмов. - Харьков: «ИСМА», 2009.- 272с.

10. Думачев В.Н. Математические основы криптографии: учебник/В.Н. Думачев,- Воронеж: Воронежский институт МВД России, 2008, -240с.

10.3 Інформаційні ресурси

1. Висновки Ради щодо плану дій європейського електронного Уряду 2011-2016 роки, 3093rd, Засідання Ради транспорту, телекомунікацій та енергетики, Брюссель, 27 травня 2011 року.
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. Формуваннятаперевіряння».
4. ДСТУ ITU-TRec.X.509 | ISO/IEC 9594-8:2006 «Інформаційнітехнології. 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 15946-4. «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 4: Цифровіпідписизвідновленнямповідомлень».
12. ДСТУ ISO/IEC 15946-3:2006 Інформаційні технології. Методи захисту. Криптографічні методи, що грунтуються на еліптичних кривих. Частина 3. Установлення ключів
13. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.
14. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.
208. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV.
15. 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).
16. 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)(COM (2012) 0238 - C7-0133/2012 - 2012 / 0146 (COD))
17. 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.
18. 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.
19. Требования к форматам, структуре и протоколам средств ЭЦП. Совместный приказ Министерства Юстиции Госспецсвязи № 1236/5/453 от 20.08.2012.
20. American National Standard for Financial Services ANSI X9.98-2010 Lattice Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry[Електронний ресурс]. – 202.
21. FIPS-186-3. Digital signature standard: 2009 [Text]. 2009 – 07 – 19 - Gaithersburg, MD 20899-8900 - 2009
22. FIPS PUB 186-1994.Digital signature standard.National Institute of standard and technology, 1994.
23. Fips 197 «Advanced Encryption Standard», 2001.
24. FIPS PUB 186-2-2000. Digital signature standard.National Institute of standard and technology, 2000.
25. FIPS PUB 186-3-2009. Digital signature standard: 2009. National Institute of standard and technology. – 2009.
26. ISO/IEC 18031:2011 Information technology – Security techniques – Random bit generation.
27. ISO/IEC 9594-8:2008 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
28. ISO/IEC 18033-1:2005 Information technology – Security techniques – Encryption algorithms – Part 1: General
29. ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric cipher
30. ISO/IEC 9594-8:2008 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
31. ISO/IEC 9796-2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms
32. ISO/IEC 9796-3:2006 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms
33. ISO/IEC 15946-2:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures.
34. ISO/IEC 14888-1:2008 Information technology – Security techniques – Digital signatures with appendix – Part 1: General
35. ISO/IEC 14888-2:2008 Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms
36. ISO/IEC 14888-3:2006 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms
37. ISO/IEC 15946-1:2008 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General
38. ISO/IEC 9798-1:2010. Information technology – Security techniques – Entity authentication – Part 1: General
39. ISO/IEC 13888-1:2004, IT security techniques – Non-repudiation – Part 1:General.
40. 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.
41. ДСТУ ISO/IEC 9796-2:2014. 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. Вперше.

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. ДСТУ ISO/IEC 9798-1: 2014. Вперше
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. Вперше.
48. ДСТУ ISO/IEC 9798-4:2014. Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 4. Методи на базі криптографічних контрольних функцій. Вперш.
49. ДСТУ ISO/IEC 9798-5: 2014. Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 5. Механізми, що використовують методи нульової обізнаності. Вперше.
50. ДСТУ ISO/IEC 10116:2014. Інформаційні технології. Методи забезпечення безпеки. Режими роботи для N-розрядного блочного шифру. Вперше.
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. захисту. 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. Вперше.
56. ДСТУ ISO/IEC 11770-5:2014. Інформаційні технології. Методи забезпечення безпеки. Керування ключами. Частина 5. Група керування ключами. Вперше.
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 14888-3:20. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням Частина 3. Механізми на основі сертифікатів. На заміну ДСТУ ISO/IEC 14888-3:2002.

62. ДСТУ ISO/IEC 14888-2:2014. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням Частина 2. Механізми на основі ідентифікаторів. На заміну ДСТУ ISO/IEC 14888-2:2002.
63. 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.
64. ДСТУ ISO/IEC 15946-5:2014. Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 1. Генерація еліптичних кривих. Вперше.
65. 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.
66. 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.
67. 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.
68. ДСТУ ISO/IEC 19790:2014. Інформаційні технології. Методи захисту. Вимоги щодо захисту криптографічних модулів. На заміну ДСТУ ISO/IEC 19790:2009
69. ДСТУ ISO/IEC 29115:2014. Інформаційні технології. Методи забезпечення безпеки. Схема забезпечення автентифікації об'єкта. Вперше.
70. ДСТУ ISO/IEC 29191:2014. Інформаційні технології. Методи захисту. Вимоги до частково анонімної, частково роз'єднаної автентифікації. Вперше.
71. ДСТУ CWA 14167-1:2014 Вимоги безпеки для надійних систем управління сертифікатами для електронних підписів. Частина 1. Вимоги безпеки системи. Вперше.
72. ДСТУ CWA 14167-2:2014 Криптографічний модуль для операцій підписування CSP з резервуванням. Частина 2. Профіль захисту CMCSOB.Вперше
73. ДСТУ CWA 14167-4:2014. Криптографічний модуль для операцій підписування CSP. Частина 4. Профіль захисту CMCSO. Вперше.
74. RFC 2631 "Diffie-Hellman Key Agreement Method", June 1999.
75. RFC 2785 Methods for Avoiding the «Small-Subgroup» Attacks on the Diffie-Hellman Key Agreement for S/MIME, March 2000.
76. RFC 3279 "Algorithms and Identifiers for the Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.
77. RFC 3281 "An Internet Attribute Certificate Profile for Authorization", April 2002.
78. RFC 3370 "Cryptographic Message Syntax (CMS) Algorithms", August 2002.
79. RFC 3394 "Encryption Standard (AES) Key Wrap Algorithm", September 2002.
80. RFC 3852 "Cryptographic Message Syntax (CMS)", July 2004.
81. RFC 5008 "Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)", September 2007.
82. RFC 5480 "Elliptic Curve Cryptography Subject Public Key", March 2009.
83. RFC 5652 "Cryptographic Message Syntax (CMS)", September 2009.

11. Посиланная на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

11. 1 Посиланная на інформаційні ресурси в Інтернет

1. Європейська комісія : Пропозиція регламенту Європейського Парламенту і Ради щодо електронної ідентифікації та довірчих послуг для електронних операцій на внутрішньому ринку (Текст розроблений для ЄЕП (європейського економічного

простору)). {SWD(2012) 135} {SWD(2012) 136}.

2. A Chosen. Ciphertext Attack against NTRU. – Режим доступу: http://www. iacr. org/archive/crypto2000/18800021/18800021. pdf.

3. IBM Research Advances Device Performance for Quantum Computing [Electronic resource] / NY. IBMnews. – Режим доступу: \www/ URL: – http://www-03. ibm. com/press/us/en/pressrelease/36901. wss - 28. 02. 2012 p.

4. Mandate M460: «Standardisation Mandate to The European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures».

5. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for. [Електронний ресурс]. http://www.bing.com/search?q=NIST+SP+800-22&src=IE-SearchBox&Form=IE8SRC.

6. STORKproject. [Электронный ресурс]. – Режим доступа: https://www. eid-stork. eu/ Дата обращения: 09.06.2014.

7. STORK 2. 0 project. [Електронний ресурс]. – Режим доступу: https://www. eid-stork2. eu/ Дата обращения: 09.06.2014.

8. http://ec. europa. eu/information_society/policy/esignature/eu_legislation/revision.

9. Lockheed Martin piece about D-Wave technology [Електронний ресурс] / Burnaby, British Columbia, Canada Блог компанії D-Wave. – Режим доступу: \www/ URL: – http://dwave. wordpress. com/2013/03/08/lockheed-martin-piece-about-d-wave-technology / Дата обращения: 08.03.2013 р.

10. NTRU: a ring based public key cryptosystem [Електронний ресурс] / J. Hoffstein, J. Pipher, J. H. Silverman // LNCS. –Springer. – 1998. – Vol. 1423. – P.267-288. – Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi

11. Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices [Електронний ресурс] / Damien Stehlé, Ron Steinfeld // Cryptology ePrint Archive. – 2013. – (Report 2013/004). – Режим доступу: http://eprint.iacr.org/2013/004.

12. Обзор методов вичисления дискретного логарифма [Електронний ресурс]. – Режим доступу: Http://WWW. cs. Toronto. edu/~cvs/dlog/research_paper. pdf

13. Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс]. – Режим доступу: http://dstszi. gov. ua/dstszi/control/uk/publish/

14. Технологии аутентификации [Електронний ресурс]. – 2009. – Режим доступу: http://ypn. ru/category/data-protection-technologies/authentication-technologies/

15. Факторизація RSA-768 [Електронний ресурс]. – Режим доступу: Https://eprint. jacr. org/2010/006

16. A hybrid lattice-reduction and. meet-in-the-middle attack against NTRU. Nick Howgrave-Graham. nhowgravegraham@ntru. com. NTRU Cryptosystems, Inc. . . . – Режим доступу: www. iacr. org/archive/crypto2007/46220160/46220160. ps

17. Blake I. F., Seroussi G., Smart N. P. Universiti of BristolAdvances in Elliptic Curve Cryptography/Cambridge University Press. 2005. – P. 281. – Режим доступу: /www. cambridge. Org/9780521604154

18. Bob Hattersley NIST SHA-3 Competition Waterfall Hash Algorithm Specification and Analysis. – Режим доступу: http://ehash. iaik. tugraz. at/uploads/1/19/Waterfall_Specification_1. 0. pdf

19. Christophe De Canni`ere, Bart Preneel «Trivium Specifications» : Доповідь з проекту eSTREAM. URL [Електронний ресурс]. – Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

20. Cryptanalysis of GGH and NTRU Signatures Phong Q. Nguyen?1 and Oded Regev 2 INRIA & _Ecole normale sup_erieure, DI, 45 rue d'Ulm, 75005 Paris, France. – Режим доступу: http://www. di. ens. fr/~pnguyen/

School of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel. – Режим доступу: http://www. cs. tau. ac. il/~odedr/

21. Cryptanalysis of the Revised NTRU Signature Scheme. Craig Gentry1 and Mike Szydlo2. DoCoMo USA Labs, San Jose, CA, USA //. – Режим доступу:cgentry@docomolabs-usa. com. RSA Laboratories, Bedford, MA, USA//. – Режим доступу:mszydlo@rsasecurity. com. Keywords: NSS, NTRU, NTRUSign, Signature Schem

22. Daniel J. Bernstein, «Which eSTREAM ciphers have been broken?» : Доповідь з проекту eSTREAM 2008/010 (оновлений 30.03.2008) URL [Електронний ресурс]. – Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

23. Daniel J. Bernstein, «Which phase-3 eSTREAM ciphers provide the best software speeds?» : Доповідь з проекту eSTREAM 2008/013 URL (оновлений 31.03.2008) [Електронний ресурс]. –Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

24. E. Biham, N. Keller. Cryptanalysis of Reduced Variant of Rijndae. [Електронний ресурс]. – Режим доступу: http://cscr. nist. gov/encryption/aes/round2/conf3/aes3papers. html

25. E. Biham, O. Dunkelman, N. Keller. New Results on Boomerang and Rectangle Attacks. [Електронний ресурс]. – Режим доступу: available from http://eprint. iacr. org/2001/070. ps

26. Evaluation Report on the Discrete Logarithm. Problem over finite fields. Jacques Stern. 1 Introduction. This document is an evaluation of the discrete logarithm . . . [Електронний ресурс]. –Режим доступу: www. ipa. go. jp/security/enc/CRYPTREC/. . . /1027_R5_DLOG. pdf

27. F. Arnault, T. P. Berger, C. Lauradoux. «Update on F-FCSR Stream Cipher»: [Електронний ресурс]. Доповідь з проекту eSTREAM. URL. [Електронний ресурс]. – Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

28. Federal Register Notice published on November 2, 2007. [Електронний ресурс]. – Режим доступу: http://csrc. nist. gov/groups/ST/hash/documents/FR_Notice_Nov07. pdf

29. Grain – A Stream Cipher for Constrained. Environments. Martin Hell1, Thomas Johansson1 and Willi Meier2. 1 Dept. of Information Technology, Lund University. – P. O. Box 118, 221 00 Lund, Sweden/ {martin,thomas}@it. lth. se

30. http://ehash. iaik. tugraz. at/wiki/The_SHA-3_Zoo/

31. IDEA NXT Technical Description, MediaCrypt. [Електронний ресурс]. – Режим доступу: WWW. MEDIACRYPT. COM, 2005.

32. J. H. Silverman, W. Whyte, Estimating Decryption Failure Probabilities for NTRUEncrypt, available from: [Електронний ресурс]. – Режим доступу: http://www. ntru. com/cryptolab/articles. Htm

33. J. H. Silverman, W. Whyte, Timing Attacks on NTRUEncrypt via variation in the number of hash calls, NTRU Technical Report 021, 2007. [Електронний ресурс]. – Режим доступу: http://www. ntru. com/cryptolab/articles. htm

34. Kovtun V., Pelzl J., Kuznetsov A. Software Implementation of Genus-2 Hyperelliptic Curve Cryptosystems Over Prime Fields. [Електронний ресурс]. – Режим доступу: http://eprint. iacr. org/2008/057. pdf

35. Kris Gaj, Gabriel Southern, and Ramakrishna Bachimanchi «Comparison of hardware performance of selected Phase II eSTREAM candidates» : Доповідь з проекту eSTREAM URL. [Електронний ресурс]. – Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

36. Martin Hell, Thomas Johansson, Alexander Maximov, Willi Meier «A Stream Cipher Proposal: Grain-128» : Доповідь з проекту eSTREAM URL [Електронний ресурс]. – Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

37. Martin Hell, Thomas Johansson, Willi Meier. «Grain – A Stream Cipher for Constrained Environments» : Доповідь з проекту eSTREAM URL [Електронний ресурс]. – Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

38. National Institute of Standards and Technology, FIPS 140-3 (DRAFT), Security for cryptographis modules [Електронний ресурс]. – Режим доступу: http://www. nist. gov/cmvp

39. NESSIE security report: Public Report / B. Preneel, A. Biryukov, E. Oswald and others. – Deliverable D 20 [Електронний ресурс]. – Version 1, 2002. – Режим доступу: http://cryptonessie. org

40. N. Howgrave-Graham, J. H. Silverman, A. Singer, W. Whyte, Modified Parameter Attacks: Practical Attacks Against CCA2 Secure Cryptosystems, and Countermeasures. Preprint available [Електронний ресурс]. – Режим доступу: from http://eprint. iacr. org

41. N. Howgrave-Graham, J. H. Silverman, W. Whyte, A meet-in-the-middle attack on an NTRU private key, NTRU Technical Report 004 [Електронний ресурс]. – Version 2, 2003. – Режим доступу: http://www. ntru. com/cryptolab/tech_notes. htm#004.

42. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. – April, 2000. – Режим доступу: http://csrc. nist. gov/publications/nistpubs//SP800-22rev1a. pdf

43. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for. [Електронний ресурс]. – Режим доступу: http://www. itl. nist. gov/div893/staff/soto/jshome. html

44. NTRU Cryptosystems. Technical reports. [Електронний ресурс]. – Режим доступу: http://www. ntru. com, 2003

45. NTRU Encrypt криптосистема будущего? [Електронний ресурс]. – Режим доступу: http://habrahabr. ru/blogs/crypto/127878/

46. Salsa20 speed. Daniel J. Bernstein. Department of Mathematics, Statistics, and Computer Science (M/C 249) [Електронний ресурс]. – The University of Illinois at Chicago. Chicago, IL 60607{7045}. snuffle@box. cr. yp. to

47. T. Good and M. Benaissa «Hardware results for selected stream cipher candidates»: [Електронний ресурс]. Доповідь з проекту eSTREAM. URL [Електронний ресурс]. – Режим доступу: http://www. ecrypt. eu. org/stream/papers. html

48. The NTRU public key cryptosystem // A tutorial. The NTRU Cryptosystems. Inc. URI [Електронний ресурс]. – Режим доступу: http://securityinnovation. com /cryptolab /tutorials. shtml/

49. The stream cipher MICKEY 2.0. [Електронний ресурс] / Steve Babbage. – Vodafone Group R&D, Newbury, UK. steve. babbage@vodafone. com. / Matthew Dodd. Independent consultan . matthew@mdodd. net

50. The Stream Cipher Rabbit1 [Електронний ресурс] / Martin Boesgaard, Mette Vesterager, Thomas Christensen, Erik Zenner. CRYPTICO A/S. Fruebjergvej 3.2100 Copenhagen. Denmark. info@cryptico. com

51. NIST Special Publication 800-38. Block Cipher Modes. [Електронний ресурс]. – Режим доступу: http://csrc. nist. gov/groups/ST/toolkit/BCM/current_modes. html

52. R. Knudsen. Integral Cryptanalysis, NESSIE internal report NES/DOC/UIB/WP5/015/1, 20

11.2 Основні сайти з інформацією по дисципліні

1. www.rsasecurity.com
2. www.nist.gov
3. www.eprint.iacr.org
4. www.citeseer.ist.psu.edu
5. www.ansi.org
6. www.cryptography.org
7. www.iso.org
8. www.linuxiso.org
9. www.cryptography.com
10. www.springerlink.com
11. www.cacr.math.uwaterloo.ca
12. www.financialcryptography.com
13. www.austinlinks.com
14. http://world.std.com/~franl/crypto.html
15. www.cryptonessie.org
16. www.cryptography.ru
17. www.osti.gov/eprints
18. Subscribe to STORK 2.0 Newsletter!
19. Participate & “like” Stork eID Facebook page!
20. “Follow Visit STORK 2.0 website www.eid-stork2.eu !
21. ” us on Twitter @StorkEid !
22. Connect to Stork 2.0 EID LinkedIn page!
23. Register in STORK 2.0 online groups!
24. Contact us at info@eid-stork2.eu !

Професор кафедри БІСТ І. Д. Горбенко

Додаток до робочої програми навчальної дисципліни "Криптографічні методи в кібербехпеці ".
Дію робочої програми продовжено: на 2021/2022 н. р.

Заступник декана факультету з навчальної роботи

_____ Євгенія КОЛОВАНОВА

« » серпня 2021 р.

Голова методичної комісії факультету комп'ютерних наук

_____ Анатолій БЕРДНІКОВ

« » серпня 2021 р.

Програму погоджено з гарантом освітньої програми 125 «Кібербезпека»
Гарант освітньої програми 125 «Кібербезпека»

_____ Віталій ЄСІН