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 ПЛЕЙМОНОВ

_____2020 р.

Робоча програма навчальної дисципліни

Прикладна криптологія

рівень вищої освіти __перший (бакалаврський)__

галузь знань 12 «Інформаційні технології»

спеціальність 125 – «Кібербезпека»

освітня програма Кібербезпека

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, професо 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) Кібербезпека
назва освітньої програми

Гарант освітньої (професійної/наукової) програми
(керівник проектної групи) Рассомахін Сергій Геннадійович

_____ Рассомахін С. Г.
(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 «Прикладна криптологія» складена відповідно до освітньої програми підготовки першого (бакалаврського) рівня за спеціальністю 125 «Кібербезпека».

1. Опис навчальної дисципліни

1.1. Мета навчальної дисципліни

Дисципліна має на меті: закласти математичний та термінологічний фундамент в галузі криптології, навчити студентів основним методам, механізмам, алгоритмам та протоколам криптографічного захисту інформації при забезпеченні кібербезпеки з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз та проведення криптографічного аналізу зі сторони потенційних порушників.

1.2. Основні завдання дисципліни:

Основними завданнями вивчення дисципліни є:

вивчення основних методів, механізмів, алгоритмів та протоколам криптографічного захисту інформації з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз та проведення криптографічного аналізу зі сторони потенційних порушників.

1.3. Кількість кредитів – 9

1.4. Загальна кількість годин – 270

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
3-й	-й
Семестр	
5-й	-й
Лекції	
32 год.	год.
Практичні, семінарські заняття	
8 год.	год.
Лабораторні заняття	
24 год.	год.
Самостійна робота	
41 год.	год.
Рік підготовки	
3-й	-й
У т.ч. індивідуальні завдання: курсова робота-20год та розрахункові роботи 8 год.	
Семестр	
6-й	-й
Лекції	

32 год.	год.
Практичні, семінарські заняття	
8 год.	год.
Лабораторні заняття	
24 год.	год.
Самостійна робота	
101 год.	год.
У т.ч. індивідуальні завдання: курсова робота-20год та розрахункові роботи 8 год.	

1.6. Заплановані результати навчання:

У результаті вивчення даного курсу студент повинен:

знати:

1. Канали уразливості та витоку інформації, явища, що притаманні їх прояву та існуванню.
2. Основні методи, механізми, протоколи та алгоритми криптографічного захисту інформації.
3. Критерії та показники оцінки якості криптографічного захисту інформації.
4. Методи криптографічних перетворень інформації та способи їх здійснення.
5. Методи та засоби аналізу та крипто аналізу асиметричних та симетричних крипто перетворень.
6. Методи, механізми та протоколи безпечного встановлення, узгодження, підтвердження, розподілення і транспортування ключів та розподілення таємниці;
7. Основні протиріччя, проблеми, тенденції та напрями розвитку теорії та практики криптографічного захисту інформації, прогнозування їх можливостей та можливостей порушників(крипто аналітиків);
8. Функціональні можливості та порядок застосування сучасних пакетів програмної реалізації криптографічних перетворень та криптографічних бібліотек.

уміти:

1. Обґрунтовувати, вибирати та застосовувати критерії та показники оцінки стійкості криптографічних перетворень та безпечності криптографічних протоколів.
2. Розробляти вимоги та обирати для застосування криптографічні перетворення та протоколи, що мінімізують впливи порушників.
3. Розробляти моделі загроз безпеці інформації, вирішувати завдання аналізу та синтезу криптографічних алгоритмів та протоколів захисту інформації.
4. Моделювати крипто аналітичні атаки та здійснювати крипто аналіз.
5. Аналізувати криптографічні протоколи на їх рівень безпечності (повноту, коректність та нульове розголошення тощо).
6. Ооцінювати захищеність від несанкціонованого доступу до інформації.
7. Обґрунтовувати вимоги до ключових даних та ключової інформації, здійснювати аналіз їх властивостей.
8. Застосовувати стандартні пакети при розв’язанні прикладних задач моделювання криптографічних перетворень, ключових даних та протоколів.

бути ознайомленим:

з сучасними напрямками розвитку теорії прикладної криптології та практичного застосування устаткування

2. Тематичний план навчальної дисципліни

Тема 1. Математичні основи прикладної криптології

Предмет і завдання дисципліни. Місце прикладної криптології при забезпеченні кіберзахисту. Основні поняття теорія чисел та груп, скінченні поля Галуа, еліптичні групи та спарювання точок ЕК. Основи застосування математичних методів в криптографії. Проблеми пост квантової криптографії.

Тема 2 .Симетричні криптографічні системи

Основи теорії секретних систем (конфіденційності). Класифікація, критерії та методи оцінки властивостей. Вимоги до симетричних криптоперетворень. Симетричні криптографічні перетворення та їх властивості. Джерела ключів та ключової інформації, вимоги до них.

Тема 3. Асиметричні криптографічні системи

Вступ в теорію асиметричних крипто перетворень. Класифікація, критерії та методи оцінки властивостей. Асиметричні крипто перетворення в групах точок еліптичних кривих. Пост квантові асиметричні крипто перетворення. Джерела ключів асиметричних криптосистем та вимоги до них. Сертифікація ключів та застосування сертифікатів.

Тема 4. Методи автентифікації інформації.

Методи та механізми автентифікації в криптосистемах, класифікація та застосування.. Критерії та методи оцінки властивостей механізмів автентифікації. . Аналіз та застосування функцій гешування. Методи та механізми захисту від несанкціонованого доступу. Методи та механізми імітозахисту.

Тема 5. Цифровий підпис та його властивості

Класифікація та загальна характеристика цифрових (електронних) підписів. Електронні цифрові підписи з додатком. Електронні цифрові підписи з відновлення повідомлень. Особливості механізмів пост квантових ЕП. Властивості та основи застосування електронних цифрових підписів.

Тема 6. Криптографічні протоколи

Криптографічні механізми та протоколи управління ключами. Критерії та методи оцінки властивостей. Криптографічні механізми та протоколи автентифікації. Синтез та аналіз криптографічних протоколів. Синтез постквантових протоколів інкапсуляції ключів. Квантові механізми аналізу безпечності криптографічних протоколів.

Тема 7. Криптографічний аналіз асиметричних криптосистем

Вступ в теорію та практику крипто аналізу. Критерії та методи оцінки стійкості асиметричних криптоперетворень. . Методики крипто аналізу асиметричних криптосистем. Методи та алгоритми крипто аналізу асиметричних криптографічних перетворень. Методи та системи квантового криптоаналізу асиметричних криптоперетворень. Порівняльний аналіз та застосування методів криптоаналізу.

Тема 8. Криптографічний аналіз симетричних криптосистем

Вступ в теорію крипто аналізу симетричних криптосистем. Критерії та методи оцінки стійкості симетричних криптоперетворень.. Методи крипто аналізу блокових симетричних криптосистем. Методи крипто аналізу потокових симетричних криптосистем. Методи та системи квантового криптоаналізу симетричних криптоперетворень. Проблеми прикладної криптології та їх вирішення.

3. Структура навчальної дисципліни

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. Предмет і завдання дисципліни. Місце прикладної криптології при забезпеченні кіберзахисту. Основи застосування математичних методів в криптографії. Проблеми пост квантової криптографії.	20	6	6			10
Тема 2. Основи теорії секретних систем. Класифікація, критерії та методи оцінки властивостей. Вимоги до симетричних криптоперетворень. Симетричні криптографічні перетворення та їх властивості. Джерела ключів та ключової інформації, вимоги до них.	30	10	4	8		10
Тема 3 Вступ в теорію асиметричних крипто перетворень. Класифікація, критерії та методи оцінки властивостей. Асиметричні крипто перетворення в групах точок еліптичних кривих. Пост квантові асиметричні крипто перетворення. Джерела ключів асиметричних криптосистем та вимоги до них.	33	8	3	6	8	10
Тема 4. Методи та механізми автентифікації в криптосистемах, класифікація та застосування.. Критерії та методи оцінки властивостей механізмів автентифікації. . Аналіз та застосування функцій гешування. Методи та механізми захисту від несанкціонованого доступу. Методи та механізми імітозахисту.	23	8	1	6		10
Тема 5. Класифікація та загальна характеристика електронних (цифрових) підписів. Електронні	29	10	2	8		10

цифрові підписи з додатком. Електронні цифрові підписи з відновлення повідомлень. Особливості механізмів пост квантових ЕП. Властивості та основи застосування електронних цифрових підписів						
Тема 6 Криптографічні механізми та протоколи управління ключами. Критерії та методи оцінки властивостей. Криптографічні механізми та протоколи автентифікації. Синтез та аналіз криптографічних протоколів. Синтез постквантових протоколів інкапсуляції ключів. Квантові механізми аналізу безпечності криптографічних протоколів..	27	10	2	8	8	12
Тема 7 Вступ в теорію та практику крипто аналізу. Критерії та методи оцінки стійкості асиметричних криптоперетворень. . Методики крипто аналізу асиметричних криптосистем. Методи та алгоритми крипто аналізу асиметричних криптографічних перетворень. Методи та системи квантового криптоаналізу асиметричних криптоперетворень. Порівняльний аналіз та застосування методів криптоаналізу.	24	6	4	6		12
Тема 8 Вступ в теорію крипто аналізу симетричних криптосистем. Критерії та методи оцінки стійкості симетричних криптоперетворень.. Методи крипто аналізу блокових симетричних криптосистем. Методи крипто аналізу потокових симетричних криптосистем. Методи та системи квантового криптоаналізу симетричних криптоперетворень. Проблеми прикладної криптології та їх вирішення.	20	4	2	6		12
курсові роботи					40	
розрахункові роботи					16	
Усього годин	210	64	16	48	56	86

4. Теми практичних та лабораторних занять

№ з/п	Назва теми	Кількість годин
	Теми практичних занять	
1	Аналіз методів криптографічних перетворень, критерії та показники оцінки якості крипто перетворень, умови реалізації безумовно стійких, обчислювально стійких та ймовірно стійких шифрів.	2
2	Аналіз методів симетричних крипто перетворень, блокові та потокові симетричні шифри та методичні основи їх порівняння. Елементарні шифри та їх властивості.	2
3	Аналіз асиметричних криптографічних перетворень. Моделі загроз та порушника. Синтез крипто перетворень. Направлені шифри пост квантового періоду та їх реалізація.	2
4	Методи генерування випадкових та псевдовипадкових послідовностей. Детерміновані генератори псевдовипадкових послідовностей. Вимоги до генераторів ключів та ключової інформації.	2
5	Аналіз загроз обману. Методи забезпечення цілісності та справжності інформації при застосуванні симетричних крипто перетворень. Методи захисту від несанкціонованого доступу.	2
6	Класифікація цифрових підписів. Цифрові підписи з додатком. Основні загрози та протидія їм. Оцінка стійкості цифрових підписів з додатком. Стандартизація цифрових підписів пост квантового періоду.	2
7	Аналіз протоколів управління ключами. Основні механізми та протоколи. Критерії та показники оцінки та порівняльного аналізу. Стандартизація протоколів управління ключами.	2
8	Криптографічні механізми та протоколи автентифікації. Протоколи автентифікації з використанням симетричних та асиметричних крипто перетворень. Інтерактивні та протоколи зь нульовим розголошенням.	2
9	Методи та системи крипто аналізу асиметричних криптосистем. Складність крипто аналізу перетворень типу цифровий підпис та направлене шифрування групі точок еліптичних кривих.	2

10	Методи крипто аналізу симетричних шифрів. Оцінка стійкості блочних симетричних шифрів. Крипто аналітичні системи та їх застосування.	2
	Теми лабораторних робіт	
1	Джерела ключів. Методи та засоби формування випадкових та псевдовипадкових послідовностей. Дослідження властивостей випадкових та псевдовипадкових послідовностей.	4
2	Дослідження властивостей симетричних крипто перетворень. Методи та засоби генерування ключів в симетричних криптосистемах	6
3	Дослідження властивостей асиметричних крипто перетворень типу асиметричний шифр.	6
4	Дослідження властивостей джерел ключів асиметричних криптосистем та аналіз виконання вимог до таких ключів.	4
5	Розроблення програмних засобів та дослідження методів гешування та автентифікації.	4
6	Дослідження перспективних криптографічних перетворень типу електронний цифровий підпис.	4
7	Розроблення програмних моделей та дослідження стандартизованих криптографічних перетворень типу електронний цифровий підпис.	4
9	Програмне моделювання та аналіз стандартизованих блокових симетричних шифрів.	4
10	Програмне моделювання та аналіз потокових симетричних шифрів.	4
11	Програмне моделювання постквантових криптоперетворень	4
	Разом	64

Альтернативні лабораторні роботи (за вибором студента)

1. Розроблення програмних моделей та дослідження перспективних криптографічних перетворень типу ЕП зі спарюванням точок еліптичних кривих
2. Розроблення програмних моделей та дослідження перспективних функцій гешування.
3. Дослідження властивостей перспективних асиметричних крипто перетворень направленого шифрування пост квантового періоду
4. Дослідження стандартизованих міжнародних алгоритмів блокового симетричного перетворення.

5. Дослідження стандартизованих міжнародних алгоритмів потокового симетричного перетворення.
6. Дослідження стандартизованих міжнародних функцій гешування.
7. Розроблення програмних моделей генерування загальних параметрів для асиметричних криптоперетворень.
8. Розроблення програмних моделей генерування загальних параметрів для асиметричних постквантових криптоперетворень
9. Дослідження механізмів асиметричного шифрування та інкапсуляції ключів.
10. Дослідження перспективних криптографічних механізмів та протоколів встановлення ключів в групі точок ЕК.

5. Завдання для самостійної роботи

№ з/п	Види та зміст завдання	Кількість годин
1	Підготовка до лекцій	5
1.1	Повторення основних положень теорії груп, полів, кілець та еліптичних кривих	2
2	Підготовка до практичних занять та лабораторних робіт	5
3	Виконання домашніх завдань	10
4	Підготовка до комп'ютерного тестування	4
5	Виконання курсової роботи 2шт	40
6	Виконання розрахункових робот 2шт	16
	Разом	82

6. Індивідуальні завдання

Індивідуальне завдання – курсова робота по розділам 2-6 за темами «Побудування та порівняльний аналіз класичних та постквантових криптоперетворень».

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 завданні на курсову роботу, завданням якої є проведення дослідження з подальшою підготовкою наукової доповіді чи наукової статі. В цьому випадку курсова робота може бути розширеним варіантом доповіді чи статі. Така курсова робота може оцінюватись, як провило, 20 балами.

Бали за виконання розрахункових робот складаються з розрахунку: 2 бал за акуратність оформлення розрахункової робот, 8 балів за результат без помилок, з незначними помилками 7 балів, з певною кількістю помилок 5 балів, грубі помилки, нерозуміння суті роботи 0 балів .Максимальна кількість балів за курсову роботу складає 10 балів.

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 2 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 4 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- 4 протягом 5 семестру				Контрольна робота, передбачена навчальним планом	розрахункових робота	Курсова робота	Разом сума балів у семестрі	Іспит	Загальна сума балів
Т1	Т2	Т3	Т4						
5	6	6	5	8	10	20	60	40	100

Т1, Т2, Т3, Т4 – теми занять.

5 семестр

Рівень знань, продемонстрований студентами, оцінюється таким чином:
- за темою 1(Т1) – 6 балів: 6 занять, виконання ПЗ, 1 експрес-опитування;
- за темою 2(Т2) – 6 балів: 8 занять, захист ЛР, виконання ПЗ, 1 комп'ютерне опитування;
- за темою 3(Т3) – 5 балів: 7 занять, захист ЛР, виконання ПЗ, 1 експрес-опитування;
- за темою 4(Т4) – 10 балів: 7 занять, захист ЛР, виконання ПЗ, 1 комп'ютерне опитування;
- за контрольну роботу (Т1 – Т4) – 8 балів;
- за присутність на заняттях – 8 балів.

Бали за поточний контроль знань по темам 5-8 Протягом 5 семестру				Контрольна робота, передбачена навчальним планом	розрахун ков их робота	Курсова робота	Разом сума балів у семестр і	Іспит	Загальн а сума балів
Т5	Т6	Т7	Т8	4	10	20	60	40	100
6	6	6	8						

6 семестр
- за темою 5 (Т5) – 8 балів: 8 занять, захист ЛР, виконання ПЗ,1 експрес-опитування;
- за темою 5 (Т6) – 8 балів: 8 занять, захист ЛР, виконання ПЗ, 1 комп'ютерне опитування;
- за темою 6 (Т7) – 8 балів: 7 занять, захист ЛР, виконання ПЗ, 1 експрес-опитування;
- за темою 6 (Т8) – 8 балів: 5 занять, захист ЛР , виконання ПЗ, 1 комп'ютерне опитування;
- за присутність на заняттях – 4 бали;
- за контрольну роботу (Т5 – Т6) – 4 балів;
- за курсову роботу (Т3–Т7) – 20 балів

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	3

обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу	
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 виконання контрольної роботи

Визначення	Кількість балів
Дані повні відповіді на кожне практичне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	8
У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки	5-7
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	2-4
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 знань студентів за виконання розрахункової роботи

Визначення	Кількість балів
Робота виконана в повному обсязі, розрахунки виконані без помилок , показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки.	10
Робота виконана в повному обсязі, розрахунки виконані с незначними помилками , показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки.	8
Робота виконана в повному обсязі, розрахунки виконані при наявності суттєвих помилок, показано достатньо знання навчального матеріалу при наявності, зроблені висновки	6
Робота виконана в повному обсязі, розрахунки виконані при наявності принципових помилок, відсутні висновки	4
Робота виконана в повному обсязі, розрахунки виконані при наявності принципових помилок, відсутні висновки. Показано слабкі знання навчального матеріалу.	2

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

Базова

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2013 р., 1 та 2 видання, 878 с.

2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 868 с.

3. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2012 р.

4. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004 – 368 с.

5. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Харків. Форт. 2010, 593 с.

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

7. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний носій до підручника. Харків, ХНУРЕ, 2012 р.

Допоміжна

1. Задірака В. Комп’ютерна криптологія. Підручник. К, 2002, 504 с.

2. NIST IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi- Kai Liu // – Режим доступу: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf.

3. Bruce Schneier Applied Cryptography. Protocols, Algorithms, and Source Code in C. John Wiley & Sons. 1996. 784 p.

4. William Stallings Cryptography and Network Security: Principles and Practice (6th Edition). Pearson. 2013. 752 p.

5. Claude E. Shannon The Mathematical Theory of Communication (16th Edition). The University of Illinois Press. 1971. 144 p.

6. Federal Office for Information Security IT-Grundschutz-Compendium. Final Draft, 1 February 2022. 960 p.

1. **Інформаційні ресурси**

1. Закон України від 15 грудня 2005 року № 3200-IV "Про основи національної безпеки України".

2. Закон України "Про інформацію". Із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР.

3. Закон України "Про Національну програму інформатизації" Із змінами, внесеними згідно із Законом від 13.09.2001 № 2684-III-ВР.

4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV.

5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.

6. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.

7. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.

8. Правила посиленої сертифікації, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3, зареєстровані 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).

9. 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».

10. ISO/IEC 15946-2:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures.

11. ДСТУ ISO/IEC 15946-2:2006 (проект) «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 2: Електроні цифрові підписи».

12. ISO/IEC 13888-1:2004, IT security techniques – Non-repudiation – Part 1:General.

13. ДСТУ ISO/IEC 13888-1:1997 «Інформаційні технології. Методи захисту. Неспростовність. Частина 1: Загальні положення» (переглянуто у 2004 році).

ISO/IEC 13888-3:1998, Information Technology – Security Techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.

14. ДСТУ ISO/IEC 13888-3:1998. «Інформаційні технології. Методи захисту. Неспростовність. Частина 3: Методи, що ґрунтуються на використанні асиметричних алгоритмів».

15. ISO/IEC 11770-3: 2008 Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.

16. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 3: Протоколи, що ґрунтуються на асиметричних криптографічних перетвореннях».

17. ISO/IEC 9798-3 Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques.

18. ДСТУ ISO/IEC 9798-3 «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 3: Механізми, що ґрунтуються на використанні алгоритмів цифрового підпису».

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

20. ДСТУ ISO/IEC 18033-2 (проект) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2: Асиметричні шифри».

21. ISO/IEC 15946-4:2004 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery.

22. ДСТУ ISO/IEC 15946-4 (проект) «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 4: Цифрові підписи із відновленням повідомлень».

23. ISO/IEC 9796-3:2006 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms (містить 5 механізмів з ISO/IEC 15946-4:2004).

24. ISO/IEC 15946-1:2002, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General.

25. ДСТУ ISO/IEC 15946-1:2006 «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 1. Основні положення».

26. ISO/IEC 15946-1:2008 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General.

ISO/IEC CD 15946-5:2008 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation.

27. ISO/IEC 14888-3:2006 Information technology – Security techniques – Digital signatures with appendix Part 3: Discrete logarithm based mechanisms (містить 3 механізми з ISO/IEC 15946-2:2002).

28. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».

29. ISO/IEC 15946-3:2002 Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.

30. ДСТУ ISO/IEC 15946-3:2006 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3: Установлення ключів».

31. ДСТУ ISO/IEC 10118-3:2005 «Інформаційні технології. Методи захисту. Геш-функції. Частина 3: Спеціалізовані геш-функції».

32. IEEE P 1363-2000. Standard Specification for public key cryptography. 2000.

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

34. American National Standard X9.62-1999. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm, 1999.

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

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

37. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

38. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

39. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22.

2. Основні сайти з інформацією по дисципліні «Прикладна криптологія»

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

ДОДАТОК А

КУРСОВА РОБОТА

А.1 Тематика курсових робіт

1. Обґрунтування та розробка методики аналізу криптопримітивів за безумовними критеріями.
2. Обґрунтування та розробка методики аналізу криптопримітивів за умовними критеріями.
3. Обґрунтування та розробка методики аналізу криптопримітивів за прагматичними критеріями.
4. Обґрунтування та розробка методики аналізу електронних підписів за безумовними критеріями.
5. Обґрунтування та розробка методики аналізу електронних підписів за умовними критеріями.
6. Обґрунтування та розробка методики аналізу електронних підписів за прагматичними критеріями.
7. Обґрунтування та розробка методики аналізу асиметричних шифрів за безумовними критеріями.
8. Обґрунтування та розробка методики аналізу асиметричних шифрів за умовними критеріями.
9. Обґрунтування та розробка методики аналізу асиметричних шифрів за прагматичними критеріями.
10. Обґрунтування та розробка методики аналізу протоколу інкапсуляції ключів за безумовними критеріями.
11. Обґрунтування та розробка методики аналізу протоколу інкапсуляції ключів за умовними критеріями.
12. Обґрунтування та розробка методики протоколу інкапсуляції ключів за прагматичними критеріями.
13. Порівняльний аналіз математичних методів розроблення асиметричних шифрів.
14. Порівняльний аналіз математичних методів розроблення електронних підписів.
15. Порівняльний аналіз математичних методів розроблення протоколів інкапсуляції ключів.
16. Обґрунтування методу ЕП на основі алгебраїчних решіток.
17. Обґрунтування методу АСШ на основі алгебраїчних решіток.
18. Порівняльний аналіз постквантових ЕП на основі алгебраїчних решіток.
19. Порівняльний аналіз постквантових ЕП Crystals-Dilithium та Falcon.
20. Порівняльний аналіз постквантових ЕП Crystals-Dilithium та Rainbow.
21. Порівняльний аналіз постквантових ЕП Falcon та Rainbow.
22. Порівняльний аналіз постквантових ЕП GeMSS та Picnic.
23. Порівняльний аналіз постквантових ЕП SPHICS+ та Picnic.
24. Порівняльний аналіз постквантових ЕП GeMSS та SPHICS+.

25. Порівняльний аналіз постквантових АСШ Classic McEliece та Crystals-Kyber.
26. Порівняльний аналіз постквантових АСШ Classic McEliece та NTRU.
27. Порівняльний аналіз постквантових АСШ Classic McEliece та Saber.
28. Порівняльний аналіз постквантових АСШ NTRU та Crystals-Kyber.
29. Порівняльний аналіз постквантових АСШ NTRU та Saber.
30. Порівняльний аналіз постквантових АСШ Saber та Crystals-Kyber.
31. Порівняльний аналіз постквантових АСШ BIKE та FrodoKEM.
32. Порівняльний аналіз постквантових АСШ BIKE та HQC.
33. Порівняльний аналіз постквантових АСШ BIKE та NTRUPrime.
34. Порівняльний аналіз постквантових АСШ BIKE та SIKE.
35. Порівняльний аналіз постквантових АСШ FrodoKEM та HQC.
36. Порівняльний аналіз постквантових АСШ FrodoKEM та NTRUPrime.
37. Порівняльний аналіз постквантових АСШ FrodoKEM та SIKE.
38. Порівняльний аналіз постквантових АСШ HQC та NTRUPrime.
39. Порівняльний аналіз постквантових АСШ HQC та SIKE.
40. Аналіз алгоритму генерації загальних параметрів ЕП Crystals-Dilithium та їх оцінка.
41. Аналіз алгоритму генерації загальних параметрів ЕП Falcon та їх оцінка.
42. Аналіз алгоритму генерації загальних параметрів ЕП Rainbow та їх оцінка.
43. Аналіз алгоритму генерації загальних параметрів АСШ Classic McEliece.
44. Аналіз алгоритму генерації загальних параметрів АСШ Crystals-Kyber.
45. Аналіз алгоритму генерації загальних параметрів АСШ NTRU.
46. Аналіз алгоритму генерації загальних параметрів АСШ Saber.
47. Аналіз та оцінка алгоритму генерації ключів ЕП Crystals-Dilithium.
48. Аналіз та оцінка алгоритму генерації ключів ЕП Falcon.
49. Аналіз та оцінка алгоритму генерації ключів ЕП Rainbow.
50. Аналіз та оцінка алгоритму генерації ключів АСШ Classic McEliece.
51. Аналіз та оцінка алгоритму генерації ключів АСШ Crystals-Kyber.
52. Аналіз та оцінка алгоритму генерації ключів АСШ NTRU.
53. Аналіз та оцінка алгоритму генерації ключів АСШ Saber.
54. Аналіз можливостей реалізації моделі безпеки ЕП EUF-CMA.
55. Аналіз можливостей реалізації моделі безпеки ЕП SUF-CMA.
56. Аналіз можливостей реалізації моделей безпеки АСШ IND-CPA, IND-CCA, IND-CCA2.
57. Розробка моделі загроз постквантовим алгоритмам ЕП.
58. Розробка моделі загроз постквантовим алгоритмам АСШ.
59. Розробка моделі порушника постквантовим алгоритмам ЕП.
60. Розробка моделі порушника постквантовим алгоритмам АСШ.
61. Алгоритм зведення решітки для ЕП Crystals-Dilithium.
62. Алгоритм зведення решітки для ЕП Falcon.
63. Класифікація та узагальнена оцінка ЕП постквантового періоду.
64. Класифікація та узагальнена оцінка АСШ постквантового періоду.

65. Обґрунтування та побудова системи сертифікації відкритих ключів на основі дерева Мерклі.

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