Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Проректор з науково – педагогічної роботи

Олександр ГОЛОВКО

“____”_____2022 р.

Робоча програма навчальної дисципліни

«Математичні основи проектування та оптимізації інформаційно-комутаційних систем»

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

2022 / 2023

2

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

РОЗРОБНИК ПРОГРАМИ:
Кошман Сергій Олександрович, доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій
Протокол від " 23 " червня 2022 року № 10

Завідувач кафедри безпеки інформаційних систем і технологій

Сергій Рассомахін

Гарант освітньої (професійної/наукової) програми

(керівник проектної групи) Єсін Віталій Іванович

Віталій Єсін

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "24 "червня 2022 року №9

Голова методичної комісії факультету комп'ютерних наук

Анатолій Бердников

ВСТУП

Програма навчальної дисципліни "Математичні методи моделювання та оптимізації процесів" складена відповідно до освітньо-професійної програми підготовки **магістра** спеціальності **125** – Кібербезпека.

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Навчальна дисципліна відображає в собі основні відомості методологічні та математичні основи проектування та реалізації математичних моделей складних інформаційно-комунікаційних систем, систем захисту інформації та їх компонентів; математичні методи оптимізації в лінійних та нелінійних, однокритеріальних та багатокритері-альних, цілочисельних та нецілочисельних завдань з метою одержання найкращих характеристики функціонування засобів та систем.

Метою викладання навчальної дисципліни є оволодіння основами класичної теорії моделювання та оптимізації, яка базується на багатьох математичних методах рішення задач різних класів, формування у студентів певних професійних компетенцій, знань та вмінь у галузі дослідження та оцінки ефективності засобів захисту інформації, вивчення основних положень теорії ефективності технічних систем, математичного та імітаційного моделювання, методів експертного оцінювання та методів розкиду системних показників.

Програма навчальної дисципліни складається з таких розділів: Математичні методи моделювання систем та процесів; Математичні методи оптимізації.

1.2. Основні завдання вивчення дисципліни

Формування у студентів знань про: принципи класифікації методів моделювання та оптимізації процесів та систем; методологічні й математичні основи формульовання та вирішення завдань різних класів, програмну реалізацію багатьох класів задач моделювання та оптимізації. Студенти мають оволодіти уміннями усебічного аналізу та вибору методів моделювання і оптимізації складних систем і процесів. Вивчення курсу "Математичні методи моделювання та оптимізації процесів" базується на знаннях, отриманих при вивченні таких курсів як вища математика, фізика, інформаційні технології, пакети прикладного програмування, теорія ймовірностей, прикладна криптологія, теорія алгоритмів, об'єктне орієнтоване програмування, спеціалізовані мови програмування тощо. Вивчення дисципліни здійснюється у 1 та 2 семестрі навчання і передбачає : лекції, практичні заняття, самостійну роботу студентів та проведення поточного контролю в межах загального обсягу годин..

1.3. Кількість кредитів – 7 (з повного обсягу 13).

1.4. Загальна кількість годин – 210

1.5. Характеристика навчальної дисципліни	
Нормативна / за вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	
Семестр	
2-й	
Лекції	
40 год	
Практичні, семінарські заняття	
40 год	

Лабораторні заняття	
-	-
Самостійна робота	
130 год	
Індивідуальні завдання	
Курсова робота	

1.6. Заплановані результати навчання

Компетенції: професійні за фундаментальною підготовкою:
комплексні уявлення про номенклатуру та здібності базових методів моделювання складних технічних та організаційних систем; методики формульовання та вирішення однокритеріальних та багатокритеріальних завдань безумовної та умовної оптимізації та вміння застосовувати їх в професійної діяльності.

За результатами вивчення дисципліни студенти повинні
ЗНАТИ:

1. Основні принципи класифікації видів задач моделювання та оптимізації систем та процесів.
2. Методологічні основи розробки та складення алгоритмів і моделей.
3. Математичні моделі типових процесів в інфокомунікаційних системах і системах захисту інформації.
4. Уявлення про різні класи завдань оптимізації в лінійних та нелінійних системах.
5. Об'єкти і завдання дослідження захищеності інформаційно-телекомунікаційних систем (ІТС). Ключові поняття та визначення теорії ефективності технічних систем;
6. Математичні основи дослідження ефективності технічних систем. Особливості дослідження і оцінки ефективності засобів захисту інформації;
7. Показники та критерії ефективності технічних систем. Показники та критерії ефективності засобів захисту інформації;
8. Методи експертного оцінювання та методи розкиду системних показників;
9. Математичні моделі технічних систем. Імітаційні моделі дослідження ефективності, апарат оцінки якості моделей та планування експериментів.
10. Моделі та методи статистичного дослідження і оцінки ефективності засобів захисту інформації.
11. Моделі та методи статистичного дослідження ефективності криптоалгоритмів із застосуванням зменшених моделей, зокрема, методи статистичних досліджень диференційних та лінійних властивостей блокових симетричних шифрів (БСШ), колізійних властивостей функцій ґешування та кодів автентичності повідомлень (Message Authentication Code – MAC).

ВМІТИ:

1. моделювати динамічні процеси використовуючи методи опису та дослідження складних динамічних систем;
2. розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації;
3. розробляти стохастичні моделі та будувати стохастичні оцінки для випадкових змінних в умовах проведення експериментів за допомогою методу статистичного моделювання випадкових та неперервних величин;

4. розробляти та тестувати імітаційні моделі, використовуючи мову імітаційного моделювання;
5. проектувати моделюючі алгоритми, використовуючи методи сумісної роботи аналітичних та імітаційних компонентів;
6. використовувати математичні методи оптимізації з метою одержання найкращих характеристик функціонування засобів та систем. Проводити класифікацію об'єктів та задач дослідження захищеності ІТС. Використовувати сучасні методики дослідження ефективності технічних систем із врахуванням особливостей побудови сучасних засобів захисту інформації;
7. розробляти показники та критерії ефективності технічних систем. Використовуючи різні концепції раціональної поведінки розробляти показники та критерії ефективності засобів захисту інформації;
8. розробляти узагальнені (системні) показники ефективності технічних систем. Практично визначати вплив вагових коефіцієнтів на величину узагальнених оцінок ефективності. Визначати часткові і узагальнені системні показники, проводити оцінку розкиду загальносистемних показників;
9. організовувати та проводити експертне оцінювання за визначеною методикою. Обробляти результати експертного опитування. Проводити оцінку узгодженості думок експертів;
10. розробляти математичні та імітаційні моделі технічних систем, зокрема проводити дослідження їхньої ефективності. Проводити оцінку якості моделей та планування експериментів;
11. розробляти моделі та проводити статистичні дослідження та оцінку ефективності засобів захисту інформації;
12. використовувати моделі та методи статистичного дослідження ефективності криптоалгоритмів із застосуванням зменшених моделей, зокрема, проводити статистичні дослідження диференційних та лінійних властивостей БСШ, колізійних властивостей функцій ґешування та МАС.

2. Тематичний план навчальної дисципліни

Розділ 1. Математичні методи моделювання систем та процесів.

Тема 1. Методологічні основи моделювання.

Основні визначення математичного моделювання. Аналітичне та імітаційне моделювання. Принципи реалізації математичних моделей.

Тема 2. Моделювання детермінованих процесів в криптографії.

Програмно-аналітична модель лінійної структури БСШ. Програмно-аналітична модель типового нелінійного блоку замін. Моделювання алгоритмів та функцій хешування. Мала модель елементарного послідовно-ітеративного хешування. Моделювання потокових симетричних шифрів. Комбінаційні схеми ПСШ. Приклади моделювання та аналізу ПСШ.

Тема 3. Моделювання випадкових величин.

Загальна характеристики методів моделювання випадкових величин. Моделювання гауссових процесів на основі центральної граничної теореми. Метод зворотних функцій. Метод кусочной апроксимації. Метод суперпозиції. Метод Неймана.

Розділ 2. Математичні методи оптимізації.

Тема 4. Основні визначення теорії оптимізації і дослідження операцій.

Методи формалізації задач оптимізації. Однокритеріальна та багатокритеріальна оптимізація. Безумовна та умовна оптимізація.

Тема 5. Метоли рішення завдань дослідження операції для оптимізації складних систем.

Лінійне програмування: графічне та симплексне рішення завдань. Табличний алгоритм симплекс методу. *Цілочисельне лінійне програмування. Метод Гоморі. Метод гілок і меж. Динамічне програмування. Принцип оптимальності. Етапи рішення завдань динамічного програмування.*

Тема 6. Методи одновимірної оптимізації.

Оптимальний пасивний пошук. Методи послідовного пошуку. Мінімізація випуклих функцій.

Тема 7. Чисельні методи безумовної оптимізації.

Алгоритми методу градієнтного спуску. Метод Ньютона і його модифікації. Алгоритми прямого спуску. Метод Франка-Вульфа

Тема 8. Аналітичні методи нелінійного програмування.

Оптимальний пасивний пошук. Методи послідовного пошуку. Мінімізація одно модальних та багато модальних функцій. Формульювання завдань нелінійного програмування. Аналітичний метод нелінійного програмування. Теорема Куна-Такера. Метод невизначених множників Лагранжа. Задачі з обмеженнями-рівностями і нерівностями.

Розділ 3. Методологічні основи дослідження ефективності технічних систем

Тема 9. Ключові поняття та визначення теорії ефективності технічних систем

Структура та зміст дисципліни, її зв'язок з іншими дисциплінами навчального плану. Ключові поняття та визначення теорії ефективності технічних систем

Тема 10. Показники та критерії ефективності технічних систем

Показники ефективності технічних систем. Форми показників ефективності технічних систем. Концепції раціональної поведінки . Критерій ефективності технічних систем. Показники та критерії захищеності ІТС

Тема 11. Оцінка ефективності методом розкиду системних показників

Визначення показників ефективності технічних систем. Метод оцінки розкиду системних показників

Тема 12. Метод експертних оцінок при дослідженні ефективності технічних систем

Метод експертних оцінок, його організація та проведення. Обробка результатів експертного опиту. Оцінка узгодженості думок експертів.

Тема 13. Метод аналізу ієрархій

Призначення методу аналізу ієрархій. Дерево цілей та позначення, що використовуються. Алгоритм попарного порівняння. Процедура обробки матриць попарних порівнянь. Розрахунок значущості альтернатив для цілі верхнього рівня. Процедура вибору та впорядкування альтернатив

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин (денна форма)					
	усього	у тому числі				
		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7
Розділ 1. Математичні методи моделювання систем та процесів.						
Тема 1. Методологічні основи моделювання.	8	2	2			4
Тема 2. Моделювання детермінованих процесів в криптографії.	16	2	6			8
Тема 3. Моделювання випадкових величин.	12	2	2			8
Разом за розділом 1	36	6	10			20
Розділ 2. Математичні методи оптимізації						
Тема 4 Основні визначення теорії оптимізації і дослідження операцій	4	2				2
Тема 5. Метоли рішення завдань дослідження операції.	16	6	2			8
Тема 6. Методи одновимірної оптимізації.	8	2	2			4
Тема 7. Чисельні методи безумовної оптимізації.	14	2	4			8
Тема 8. Аналітичні методи нелінійного програмування.	12	2	2			8
Разом за розділом 2	54	14	10			3066
Розділ 3. Методологічні основи дослідження ефективності технічних систем						
Тема 9. Ключові поняття та визначення теорії ефективності технічних систем	18	4	4			10
Тема 10. Показники та критерії ефективності технічних систем	18	4	4			10
Тема 11. Оцінка ефективності методом розкиду системних показників	18	4	4			10
Тема 12. Метод експертних оцінок при дослідженні ефективності технічних систем	18	4	4			10
Тема 13. Метод аналізу ієрархій	18	4	4			10
Курсова робота	30				30	
Разом за розділом 3	120	20	20		30	50
Усього годин	210	40	40		30	100

4. Теми практичних і лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Побудова аналітичних моделей на основі словесного опису процесу.	2
2.	Побудова малої моделі БСШ на основі структури мережі Фейстеля.	2
3.	Моделювання елементів формування шифрів гамування і найпростіших алго-	2

	ритмів аналізу параметрів псевдовипадкових послідовностей	
4.	Моделювання випадкових величин.	2
5.	Лінійне програмування, геометричний та симплекс методи.	2
6.	Метод Гоморі рішення цілочисельних задач	2
7.	Метод гілок і меж.	2
8.	Динамічне програмування.	2
9.	Метод Франка-Вульфа.	2
10.	Аналітичний метод нелінійного програмування. Метод множників Лагранжа.	2
11.	Контрольна робота	2
12.	Ключові поняття та визначення теорії ефективності технічних систем	2
13.	Показники та критерії ефективності технічних систем	4
14.	Оцінка ефективності методом розкиду системних показників	4
15.	Метод експертних оцінок при дослідженні ефективності технічних систем	4
16.	Метод аналізу ієрархій	4
5	**Разом за курсом**	40

5. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Підготовка до лекцій.	20
1.1	Повторення основних положень аналітичного моделювання	20
1.2	Вивчення положень теоріх дослідження операцій	10
2	Підготовка до практичних занять.	20
2.1	Вивчення табличного алгоритму симплекс-методу ЛП	10
2.2	Вивчення методу зворотних функцій	10
3	Читання додаткової літератури.	10
4	Курсова робота	30
	Разом	130

6. Індивідуальні завдання

Індивідуальні завдання студентів пов’язані з вивченням окремих, в тому іноземних джерел, за тематикою дисципліни, проведенням аналізу існуючих та перспективних засобів захисту інформації, дослідженням рівнів стійкості, розробленням імітаційних моделей та дослідженням ефективності в тому числі із застосуванням принципу масштабування. Теми індивідуальних завдань, як правило, пов’язуються з науковими та науково - методичними дослідженнями, які веде кафедра та інші підрозділи університету чи інші підприємства чи заклади тощо, фірми.

Основними формами реалізації результатів виконання індивідуального завдання є:

- доповідь чи виступ на семінарських чи практичних заняттях;
- доповідь на тематичних науково - практичних конференціях з опублікуванням тез чи доповідей;
- підготовка та опублікування наукових та науково - практичних статей;
- підготовка та подання результатів досліджень для використання в НДР та ДКР кафедри;
- участь в розробці науково - методичних та навчальних матеріалів;
- підготовка патентів на винаходи та корисні моделі;

– розробка та опис програмних продуктів та моделей тощо.

Під час вивчення навчальної дисципліни передбачається проведення **курсової роботи в** межах загального обсягу годин, передбаченого на самостійну підготовку. Індивідуальні завдання курсового проектування видаються викладачем під час проведення першого практичного заняття, на якому наголошуються основні критерії оцінки. Типові завдання курсового проектування наведено у додатку А.

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

Для оперативного контролю степені засвоєння матеріалу протягом семестру застосовуються наступні заходи:

– контроль присутності студентів (пропуск лекції без поважної причини – "мінус" один бал);

– контроль і оцінка виконання індивідуального завдання практичного заняття – перевірка роботи комп'ютерної програми та усна співбесіда;

– контроль звітів про виконання практичної роботи та знання відповідей на контрольні питання;

– контроль повноти та якості конспектів (до 10 балів).

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

Підсумковий контроль здійснюється шляхом проведення іспиту.

Екзаменаційний квиток включає два теоретичних і одне практичне питання. Теоретичні питання оцінюються в 10 балів кожен, практичний - в 20.

Максимальна кількість балів за результатами іспиту складає 40 балів.

Максимальна кількість балів за результатами вивчення дисципліні складає 100 балів.

9. Схема нарахування балів

Поточне тестування та самостійна робота													Контрольна робота	Курсова робота	Разом	Екзамен	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13					
2	2	2	3	3	3	3	3	3	3	3	3	3	5	20	60	40	100

Критерії оцінювання

Критерії оцінювання знань студентів за виконання практичної роботі

Визначення	Кількість балів
Завдання по практичної роботі виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При	3

захисті роботи показано розуміння суті і змісту проведених досліджень	
Завдання по практичної роботі виконане самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При перевірці та захисті роботи були виявлені незначні помилки у знанні теоретичного матеріалу	2
Завдання по практичної роботі виконане в повному обсязі. Звіт оформлений достатньо акуратно, в оформленні роботи є незначні недоліки. При захисті роботи були виявлені незначні помилки у знанні теоретичного матеріалу	2,5
Завдання по практичної роботі виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу	2
Завдання по практичної роботі виконане не повному обсязі. Звіт оформлений з суттєвими помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу	1

Критерії оцінювання знань студентів за виконання контрольній 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	5
У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за наявності незначних помилок зроблені достатньо повні і правильні висновки	4
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	3
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	3
У відповідях на показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки	1

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	25-34

помилками, завдання вирішене правильно з незначними помилками. Зроблені неповні висновки	
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

Критерії оцінювання знань студентів за виконання курсової роботі

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

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 література

1. М.П.Медіченко, О.В. Потій Основи теорії систем та системного аналізу: Навч. посібник – Х.: ХНУРЕ, 2006.- Стор. 28-3015.
2. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
3. НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу"
4. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»
5. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 04.07.2008 N 112.
6. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»
7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
8. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2012 р., 878 с

Допоміжна література

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. Радіотехніка. Всеукраїнський міжвідомчий збірник. Харків, ХНУРЕ, 2000 – 2015 рр.
5. Прикладная радиоелектроника. Научн. техн. журнал. Академія наук прикладної радіоелектроніки, ХНУРЕ. Тематические выпуски «Безопасность информации» 2006 – 2015 рр.
6. Зайченко Ю. П. Дослідження операций: Учеб. посібник для студентів вузів. — 2-е изд., – Киев: Вища школа, 1979. – 392 с.

Рекомендоване методичне забезпечення

1. Електронні комп'ютерні слайди за дисципліною "Моделювання та оцінка ефективності засобів захисту інформації". Електронний ресурс кафедри БІСТ.
2. Методичні вказівки до практичних робіт з дисципліни "Моделювання та оцінка ефективності засобів захисту інформації". Електронний ресурс кафедри БІСТ.
3. Плани проведення консультацій (друкований та електронній варіанти).
4. Навчальна програма з дисципліни "Моделювання та оцінка ефективності засобів захисту інформації". Електронний ресурс кафедри БІСТ.
5. Завдання до контрольних робіт (3 роботи). Електронний ресурс кафедри БІСТ.
6. Перелік питань до екзамену за дисципліною "Моделювання та оцінка ефективності засобів захисту інформації". Електронний ресурс кафедри БІСТ.
7. Екзаменаційні білети за дисципліною "Моделювання та оцінка ефективності засобів захисту інформації". Електронний ресурс кафедри БІСТ.

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

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. www.world.std.com/~franl/crypto.html
15. www.cryptonessie.org
16. www.osti.gov/eprints

Додаток А

Рекомендовані теми курсових робіт за дисципліною

1. Аналіз та порівняльні дослідження криптографічно стійких генераторів псевдовипадкових послідовностей для пост-квантового застосування
2. Програмна реалізація та дослідження властивостей генератору псевдовипадкових послідовностей QUAD
3. Програмна реалізація та дослідження властивостей генератору псевдовипадкових послідовностей SYND
4. Програмна реалізація та дослідження властивостей генератору псевдовипадкових послідовностей Fischer-Stern
5. Аналіз та порівняльні дослідження схем електронного цифрового підпису для пост-квантового застосування
6. Програмна реалізація та дослідження властивостей схеми електронного цифрового підпису CFS
7. Програмна реалізація та дослідження властивостей схеми електронного цифрового підпису Parallel-CFS
8. Програмна реалізація та дослідження властивостей схеми електронного цифрового підпису pqsigRM
9. Програмна реалізація та дослідження властивостей схеми електронного цифрового підпису RaCoSS
10. Програмна реалізація та дослідження властивостей схеми електронного цифрового підпису RankSign
11. Програмна реалізація та дослідження властивостей схеми інкапсуляції ключів Classic McElice
12. Дослідження моделей та вимог нерозрізненості шифртекстів (IND-CPA, IND-CCA1, IND-CCA2) для пост-квантових криптоалгоритмів
13. Порівняльні дослідження пост-квантових схем інкапсуляції ключів за нерозрізненістю шифртекстів (IND-CPA, IND-CCA1, IND-CCA2)
14. Порівняльні дослідження пост-квантових схем направленого шифрування за нерозрізненістю шифртекстів (IND-CPA, IND-CCA1, IND-CCA2)
15. Аналіз та порівняльні дослідження схем ідентифікації для пост-квантового застосування

16. Програмна реалізація та дослідження властивостей схем ідентифікації на основі кодів, що виправляють помилки
17. Аналіз та порівняльні дослідження протоколів доказу з нульовим розголошенням в умовах пост-квантового середовища
18. Програмна реалізація та дослідження властивостей протоколу доказу з нульовим розголошенням із застосуванням криптосистеми McEliece
19. Аналіз та порівняльні дослідження протоколів ідентифікації в децентралізованих інформаційних системах
20. Аналіз та порівняльні дослідження протоколів консенсусу в децентралізованих інформаційних системах
21. Показники та критерії ефективності децентралізованих інформаційних систем
22. Методи генерації випадкових нелінійних вузлів заміни та дослідження їх властивостей
23. Структурний аналіз нелінійних вузлів заміни криптоалгоритмів «Кузнечік» та «Стрибог»
24. Дослідження властивостей конструкції TKlog для побудови нелінійних вузлів заміни
25. Дослідження властивостей алгоритмів малоресурсної криптографії Simon та Speck.
26. Дослідження нелінійних вузлів ускладнення сучасних алгоритмів потокового шифрування (аналіз відомих схем ускладнення, що використовувалися в алгоритмах з проектів eSTREAM та CRYPTREC, стандартів ISO/IEC 29192-3:2012 та ISO/IEC 18033-4; реалізація всіх варіантів побудови вузлів ускладнення; дослідження властивостей)
27. Дослідження схем нерівномірного управління рухом регістрів зсуву в сучасних потокових шифрах (аналіз відомих методів нерівномірного управління рухом регістрів зсуву, їх реалізація та дослідження властивостей)
28. Аналіз та дослідження схем ініціалізації та завантаження ключових даних сучасних алгоритмів потокового шифрування (аналіз схем ініціалізації та завантаження ключових даних, що використовувалися в алгоритмах з проекту eSTREAM та CRYPTREC, стандартів ISO/IEC 29192-3:2012 та ISO/IEC 18033-4; реалізація всіх варіантів та дослідження властивостей)
29. Аналіз базових структур алгоритмів потокового криптоперетворення та дослідження їх властивостей (аналіз різних базових структур алгоритмів потокового криптоперетворення з проекту eSTREAM та CRYPTREC, стандартів ISO/IEC 29192-3:2012 та ISO/IEC 18033-4; дослідження властивостей у різних варіантах реалізації)
30. Аналіз потокових алгоритмів шифрування що засновані на використанні регістрів зсуву та дослідження їхніх властивостей (аналіз відомих алгоритмів потокового шифрування, які застосовують регістри зсуву; дослідження властивостей регістрів зсуву та їх впливу на характеристики потокового шифру)
31. Розробка зменшених моделей програмно-орієнтованих потокових шифрів з проекту eSTREAM (алгоритми HC-128, Rabbit, Salsa 20, SOSEMANUK)
32. Розробка зменшених моделей апаратно-орієнтованих потокових шифрів з проекту eSTREAM та алгоритму Enocoro зі стандарту ISO/IEC 29192 (алгоритми Grain, MICKEY, Trivium, Enocoro)
33. Розробка зменшених моделей потокових шифрів з проекту CRYPTREC та зі стандарту ISO/IEC 18033-4 (алгоритми KCipher-2 (K2), MUGI, SNOW 2.0)
34. Розробка зменшених моделей потокових шифрів з проекту CRYPTREC та зі стандарту ISO/IEC 18033-4 (алгоритми KCipher-2 (K2), MUGI, SNOW 2.0)
35. Розробка та дослідження алгоритму потокового шифрування KCipher-2