Державний вищий навчальний заклад

“Ужгородський національний університет”

Математичний факультет

Кафедра кібернетики і прикладної математики

ЗАТВЕРДЖУЮ

Проректор з наукової роботи

_____ проф. Студеняк І.П.

“ ” _____2019 р.

“

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні та комп’ютерні основи криптології

Рівень вищої освіти	**третій (освітньо-науковий)**
за спеціальністю	111 «Математика»
галузі знань	11 «Математика і статистика»
Статус дисципліни	Обов’язкова
Мова навчання	Українська

Ужгород 2019

Робоча програма «Математичні та комп'ютерні основи криптології» для аспірантів за спеціальністю 111 «Математика»

Розробники: Повідайчик М. М., доцент кафедри кібернетики і прикладної математики, к.е.н.

Робочу програму схвалено на засіданні кафедри кібернетики і прикладної математики.

Протокол від "27" червня 2019 року № 13

Завідувач кафедри кібернетики і прикладної математики

_____ (проф. Гече Ф.Е.)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань
11–математика та статистика
(шифр і назва)</td><td colspan="2">Нормативна
(за вибором)</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність:
111–математика</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів – 2</td><td>1-й</td><td>-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання _____
(назва)</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – 90</td><td>1-й</td><td>-й</td></tr>
<tr><td colspan="2" rowspan="13">Освітньо-науковий ступінь:
доктор філософії</td><td colspan="2">Лекції</td></tr>
<tr><td>22 год.</td><td>год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>54 год.</td><td>год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td></td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Мета вивчення дисципліни «Математичні та комп'ютерні основи криптології» – ознайомлення студентів з основними криптографічними методами захисту даних та методами криптоаналізу.

Завдання дисципліни «Математичні та комп'ютерні основи криптології» полягають у формуванні у студентів знань, умінь та навичок розробки алгоритмів захисту даних та їх криптоаналізу.

Загальні компетентності:

- **ЗК-1**. Здатність до абстрактного мислення, аналізу та синтезу на основі логічних аргументів та перевірених фактів.
- **ЗК-4.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- ЗК-6. Здатність визначати, формулювати та розв'язувати проблеми, приймати обґрунтовані рішення.
- **ЗК-8.** Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків.

Фахові компетентності:

- **ФК-1.** Володіти найбільш передовими концептуальними та методологічними знаннями в галузі науково-дослідної та/або професійної діяльності і на межі предметних галузей і дослідницькими математичними методами та вміннями
- **ФК-3.** Розроблення та реалізація проектів, включаючи власні дослідження в галузі математики, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику, і розв'язання проблем.
- **ФК-4.** Здатність інтерпретувати результати досліджень, брати участь у семінарах, наукових конференціях, дискусіях із досвідченими науковцями-математиками стосовно наукового значення та потенційних наслідків отриманих результатів.
- **ФК-6.** Здатність формулювати наукову проблему, робочі гіпотези досліджуваної проблеми, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми «Математика» (третього освітньо-наукового рівня вищої освіти), вивчення даної навчальної дисципліни повинно забезпечити досягнення здобувачами ступеня вищої освіти: доктор філософії / Doctor Philosophy (Ph.D) таких програмних результатів навчання (ПРН):

- **ПРН-2.** Здобуття знань і розумінь поглибленого рівня у математиці та споріднених областях, включаючи методики проведення доведень і побудови математичних моделей, рівень цих знань повинен бути достатнім для проведення наукових досліджень на рівні останніх світових досягнень і направленим на їх розширення та поглиблення.

- **ПРН-9.** Обізнаність та здатність взаємодіяти інтелектуально з найновішими математичними дослідженнями в спеціальній області дослідження.
- **ПРН-10.** Досягнення відповідних знань, розумінь та здатностей використання методів аналізу даних і статистики на найсучаснішому рівні.
- **ПРН-11.** Здатність створювати крупні програмні продукти на різних мовах програмування відповідно до потреб дисертаційного дослідження, а також адаптувати, удосконалювати та вбудовувати програмні продукти, початково призначені для іншої мети.
- **ПРН-12.** Здатність планувати оригінальний вклад на основі дослідження до математичних знань, пов'язаних з важливою задачею, який є відповідної якості для друку.

В результаті вивчення даного курсу здобувач повинен

знати: історію розвитку криптографії, докомп'ютерні методи захисту даних, основні симетричні криптосистеми та криптосистеми з відкритим ключем;

вміти: використовувати програмну реалізацію вивчених алгоритмів з метою захисту даних.

4. ЗАСОБИ ОЦІНЮВАННЯ ТА МЕТОДИ ДЕМОНСТРУВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

11. Методи контролю

1. Поточний контроль – фронтальне опитування, виконання практичних завдань.
2. Модульний контроль – виконання контрольних робіт та тестових завдань.
3. Підсумковий контроль – виконання тестових і практичних завдань.

Оцінка успішності студента є рейтинговою і виставляється за стобальною шкалою з урахуванням оцінок засвоєння окремих модулів.

Розподіл балів, які отримують студенти

<table>
<tr><td colspan="10">Поточне тестування та самостійна робота</td><td>Сума</td></tr>
<tr><td colspan="10">Модуль №1</td><td rowspan="6">100</td></tr>
<tr><td colspan="10">Змістовий модуль №1</td></tr>
<tr><td>Т 1</td><td>Т 2</td><td>Т 3</td><td>Т 4</td><td>Т 5</td><td>Т 6</td><td>Т 7</td><td></td><td></td><td></td></tr>
<tr><td>6</td><td>6</td><td>6</td><td>6</td><td>6</td><td>6</td><td>6</td><td></td><td></td><td></td></tr>
<tr><td colspan="10">Модуль №2</td></tr>
<tr><td colspan="10">Змістовий модуль №1</td></tr>
<tr><td>Т 1</td><td>Т 2</td><td>Т 3</td><td>Т 4</td><td>Т 5</td><td>Т 5</td><td>Т 7</td><td>Т 8</td><td>Т 9</td><td>Т10</td></tr>
<tr><td>6</td><td>6</td><td>6</td><td>6</td><td>6</td><td>6</td><td>6</td><td>6</td><td>5</td><td>5</td></tr>
</table>

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Критерій оцінювання з дисципліни

"Відмінно" (90 та вище балів) заслуговує здобувач, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії.

"Добре" (82-89 балів) заслуговує здобувач, який виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисциплін і здатний до самостійного доповнення, але під час відповіді допустив деякі неточності.

"Добре" (74-81 балів) заслуговує здобувач, що виявив не цілком повне знання програмного матеріалу, не завжди успішно виконує передбачені програмою завдання, частково засвоїв основну літературу, рекомендовану програмою, виявив не систематичний характер знань з дисциплін і не завжди здатний до їх самостійного доповнення і під час відповіді допускає деякі неточності.

"Задовільно" (64-73 балів) заслуговує здобувач, що виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка "задовільно" виставляється здобувачам, що допустили помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача.

“Задовільно” (60-63 балів) заслуговує здобувач, що виявив часткове знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою. Як правило, оцінка “достатньо" виставляється здобувач, що допустили грубі помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які частково володіють необхідними знаннями для їх усунення за допомогою викладача.

“Незадовільно з можливістю повторного складання” (35-59 балів) виставляється здобувач, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

“Незадовільно з обов’язковим повторним вивченням дисципліни” (1-34 балів) виставляється здобувачу коли протягом семестру він допустив грубі помилки у виконанні передбачених програмою завдань.

При виставленні оцінки можуть враховуватися результати навчальної роботи здобувача протягом семестру.

Іспит виставляється (без складання) у випадку набору кількості балів, що відповідає мінімальній оцінці “достатньо” (E).

Протягом семестру проводиться не менше двох модулів або колоквіумів чи контрольних робіт або інших видів контролю. Максимальна кількість балів, яка встановлюється для цих видів контролю, а також відповідність оцінок FX та F у шкалі ECTS, у балах та національній шкалі визначається Вченими радами факультетів або кафедрами, які забезпечують викладання відповідних дисциплін.

Орієнтований перелік питань, що виносяться на залік

1. Математичні моделі стандартних блочних систем.
2. Криптосистема DES і її властивості.
3. Криптосистема IDEA.
4. Криптосистема ГОСТ 28147-89.
5. Загальна структура алгоритму Rijndael.
6. Криптосистеми з відкритим ключем.
7. Описання RSA-Криптосистеми.
8. Стійкість RSA.
9. Пошук секретного ключа і факторизація модуля.
10. Система Рабина.
11. Ранцевий метод шифрування.
12. Стійкість ранцевого шифру.
13. Електронний цифровий підпис.
14. Узагальнена модель ЕЦП.
15. Схема ЕЦП Рабина.
16. Схема Діффі-Лампорта.

17. Імовірнісна схема підпису Рабина.
18. Стандарт ЕЦП DSS.
19. Схема ЕЦП Ель-Гамаля.
20. Задача дискретного логарифмування.

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Докомп'ютерна криптографія.

Тема 1. Докомп'ютерний захист інформації.

Основні поняття криптографії. Шифри підстановки. Шифр Цезаря. Модулярний шифр. Гомофонічне шифрування. Поліграмне шифрування. Шифр Плейфера. Багатоалфавітне підстановочне шифрування. Шифр Віженера. Шифр Вернама.

Тема 2. Арифметичні основи криптографії.

Алгоритм ділення з остачею. Найбільший спільний дільник. Взаємно прості числа. Найменше спільне кратне. Прості числа. Порівняння. Класи лишків. Функція Ейлера. Порівняння першого степеня. Первісні корені. Існування первісних коренів. Індекси за модулем p^k і $2p^k$. Символ Лежандра. Квадратичний закон взаємності. Символ Якобі.

Тема 3. Алгебраїчні основи криптографії.

Поняття групи. Підгрупи груп. Циклічні групи. Гомоморфізм груп. Групи підстановок. Дії групи на множині. Кільця і поля. Підкільця. Гомоморфізм кілець. Евклідові кільця. Прості і максимальні ідеали. Скінченні розширення полів. Поле розкладу. Скінченні поля. Порядки незвідних многочленів. Лінійні рекурентні послідовності. Послідовності максимального періоду.

Тема 4. Поняття про еліптичні криві.

Рівняння Вейєрштрасса, дискримінант і j-інваріант. Додавання точок еліптичної кривої. Еліптичні криві над скінченними полями.

Тема 5. Ймовірнісно-статистичні моделі повідомлень та їхні ентропійні властивості.

Джерела дискретних повідомлень та їхні ймовірнісні моделі. Функціонал ентропії та його властивості. Умовна ентропія та її властивості. Питома ентропія стаціонарної символьної послідовності. Ентропійні характеристики марківських символьних послідовностей. Джерела неперервних повідомлень і їхні ентропійні властивості. Оптимізація функціонала ентропії на класі ймовірнісних розподілів.

Тема 6. Методи теорії інформації у криптографії.

Асимптотичні властивості стаціонарного джерела дискретних повідомлень. Ентропійна стійкість випадкових символьних послідовностей. Кількість інформації за Шенноном і її властивості. Шенноновські моделі криптосистем. Теоретико-інформаційні оцінки стійкості симетричних криптосистем.

Тема 7. Статистичне тестування випадкових і псевдовипадкових послідовностей.

Рівномірно розподілена випадкова послідовність і її властивості. Універсальний алгоритм статистичного тестування випадкових і

псевдовипадкових послідовностей. Тест n-серій. Тест інтервалів. Узагальнений покер-тетст. Тест «збирача купонів». Тест перестановок. Тест перетинаючихся n-грам. Тест, заснований на рангах двійкових матриць. Спектральні тести. Тест випадкового блуждання. Універсальний статистичний тест Мауера. Тест на основі прирощеної ентропії. Тест, заснований на алгоритмі стиснення Лемпеля-Зіва. Тест, заснований на лінійній складності. Тест на основі екстремальної статистики скалярного добутку. Тест на основі екстремальної статистики дельта-добутку. Алгоритмічне визначення випадковості.

Модуль 2

Змістовий модуль 1. Комп'ютерні методи криптографії.

Тема 1. Алгоритми генерування випадкових і псевдовипадкових послідовностей.

Класифікація алгоритмів генерування. Лінійні і мультиплікативні конгруентні генератори. Нелінійні конгруентні генератори. Рекуренти у скінченному полі. Послідовності, породжені лінійними регістрами здвигу зі зворотнім зв'язком. Генератори Фібоначчі. Криптостійкі генератори на основі односторонніх функцій. Криптостійкі генератори, засновані на проблемах теорії чисел. Методи «покращення» псевдовипадкових послідовностей. Комбінування алгоритмів генерації методом Макларена-Марсальї. Комбінування LFSR-генераторів. Конгруентний генератор з випадковими параметрами.

Тема 2. Потокові криптосистеми.

Основні поняття. Рекурентні послідовності. Лінійні рекурентні послідовності. Оцінка параметрів і розпізнавання ЛРП. Лінійна складність. Визначення початкового стану ЛРП. Комбінування послідовностей. Кореляційний криптоаналіз.

Тема 3. Математичні моделі стандартних блочних криптосистем.

Криптосистема DES і її властивості. Криптосистема IDEA. Криптосистема ГОСТ 28147-89. Загальна структура алгоритму Rijndael. Використання алгебри поліномів у алгоритмі Rijndael.

Тема 4. Математичні методи криптоаналізу симетричних систем.

Завдання та принципи криптоаналізу. Метод «опробування» і його обчислювальна складність. Методи криптоаналізу на основі теорії статистичних рішень. Різницевий криптоаналіз. Лінійний криптоаналіз.

Тема 5. Криптосистеми з відкритим ключем.

Описання RSA–криптосистеми. Можливі атаки на криптосистему RSA. Стійкість RSA проти методу повторного шифрування. Пошук секретного ключа d і факторизації модуля N. Біти в RSA-криптосистемі. Система Рабина. Ранцевий метод шифрування. Стійкість ранцевого шифру. Теорема Вінера про малий секретний ключ. Арифметика великих чисел. Модулярна арифметика. Ознака простоти. Алгоритми генерації простих чисел. Задача факторизації.

Тема 6. Функції хешування.

Визначення і властивості. Блочно-ітераційні функції хешування. Використання блочних криптосистем. Атака «днів народження». Криптосистеми аутетифікації. Функція хешування СТБ 1176.1-99.

Тема 7. Електронний цифровий підпис.

Узагальнена модель ЕЦП. Схема ЕЦП Рабина. Схема Діффі-Лампорта. Імовірнісна схема підпису Рабина. Стандарт ЕЦП DSS. Схема ЕЦП Ель Гамаля. Арифметичні властивості російського стандарту цифрового підпису. Еквівалентність задач фальсифікації підпису в DSS схемою Ель Гамаля. Електронний цифровий підпис СТБ 1176.1-99. Задача дискретного логарифмування.

Тема 8. Еліптичні криві у криптографії.

Цифровий підпис на еліптичних кривих. Особливості скалярного множення на еліптичних кривих. Обчислення порядку еліптичної кривої.

Тема 9. Протоколи управління криптографічними ключами.

Протоколи генерації ключів. Протоколи взаємної аутентифікації. Протоколи прямого обміну ключами. Протоколи розподілу сеансових ключів з використанням центру розподілу ключів.

Тема 10. Нові напрямки у криптографії.

Можливості квантової криптографії. Математичне розділення секрету. Стенографія і її застосування. Активний криптоаналіз.

Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	Усього	У тому числі					Усього	у тому числі				
		лек.	пр.	лаб.	інд. р.	сам. р.		лек.	пр.	лаб.	інд. р.	сам. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Модуль 1												
Змістовий модуль 1. Докомп'ютерна криптографія.												
Тема 1. Докомп'ютерний захист інформації.	7	2	1			4						
Тема 2. Арифметичні основи криптографії.	7	2	1			4						
Тема 3. Алгебраїчні основи криптографії.	7	2	1			4						
Тема 4. Поняття про еліптичні криві.	7	2	1			4						
Тема 5. Ймовірнісно-статистичні моделі повідомлень та їхні ентропійні властивості.	7	2	1			4						
Тема 6. Методи теорії інформації у криптографії.	7	2	1			4						

Тема 7. Статистичне тестування випадкових і псевдовипадкових послідовностей.	7	2	1			4						
Модульна робота	1		1			-						
Модуль 2												
Змістовий модуль 1. Комп'ютерні методи криптографії.												
Тема 1. Алгоритми генерування випадкових і псевдовипадкових послідовностей.	6	1	1			4						
Тема 2. Потокові криптосистеми.	7	1	1			5						
Тема 3. Математичні моделі стандартних блочних криптосистем.	7	1	1			5						
Тема 4. Математичні методи криптоаналізу симетричних систем.	7	2	1			4						
Тема 5. Криптосистеми з відкритим ключем.	7	2	2			3						
Тема 6. Функції хешування.	7	2	1			4						
Тема 7. Електронний цифровий підпис.	7	2	1			4						
Тема 8. Еліптичні криві у криптографії.	7	1	1			5						
Тема 9. Протоколи управління криптографічними ключами.	7	1	1			5						
Тема 10. Нові напрямки у криптографії.	7	1	1			5						
Модульна робота	1		1			-						
Усього годин	**120**	**28**	**20**			**72**						

Теми практичних занять

№ з/п	Назва теми	Кількість годин
1.	Докомп'ютерний захист інформації.	1
2.	Арифметичні основи криптографії.	1
3.	Алгебраїчні основи криптографії.	1
4.	Поняття про еліптичні криві.	1
5.	Ймовірнісно-статистичні моделі повідомлень та їхні	1

	ентропійні властивості.	
6.	Методи теорії інформації у криптографії.	1
7.	Статистичне тестування випадкових і псевдовипадкових послідовностей.	1
8.	Модульна робота	1
9.	Алгоритми генерування випадкових і псевдовипадкових послідовностей.	1
10.	Потокові криптосистеми.	1
11.	Математичні моделі стандартних блочних криптосистем.	1
12.	Математичні методи криптоаналізу симетричних систем.	1
13.	Криптосистеми з відкритим ключем.	2
14.	Функції хешування.	1
15.	Електронний цифровий підпис.	1
16.	Еліптичні криві у криптографії.	1
17.	Протоколи управління криптографічними ключами.	1
18.	Нові напрямки у криптографії.	1
19.	Модульна робота	1
	Разом	20

7. Теми лабораторних занять

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Докомп’ютерний захист інформації.	4
2.	Арифметичні основи криптографії.	4
3.	Алгебраїчні основи криптографії.	4
4.	Поняття про еліптичні криві.	4
5.	Ймовірнісно-статистичні моделі повідомлень та їхні ентропійні властивості.	4
6.	Методи теорії інформації у криптографії.	4
7.	Статистичне тестування випадкових і псевдовипадкових послідовностей.	4
8.	Алгоритми генерування випадкових і псевдовипадкових послідовностей.	4
9.	Потокові криптосистеми.	5
10.	Математичні моделі стандартних блочних криптосистем.	5
11.	Математичні методи криптоаналізу симетричних систем.	4
12.	Криптосистеми з відкритим ключем.	3
13.	Функції хешування.	4
14.	Електронний цифровий підпис.	4
15.	Еліптичні криві у криптографії.	5
16.	Протоколи управління криптографічними ключами.	5
17.	Нові напрямки у криптографії.	5
	Разом	72

Рекомендована література

Базова

1. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. – М.: Гелиос АРВ, 2002. – 240 с.
2. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая линия – Телеком, 2002. – 175 с.
3. Венбо Мао. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice – М.: Вильямс, 2005. – 768 с.
4. Грабарчук В., Зинович З.,Свиць А. Кибернетический подход к проектированию систем защиты информации. – Киев, 2003. – 659 с
5. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 335 с.
6. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел. Наукове видання. – Київ, 2003. – 254 с.
7. Математические и компьютерные основы криптографии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003. – 382 с.
8. Нильс Фергюсон, Брюс Шнайер Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems – М.: Диалектика, 2004. – 432 с.
9. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.
10. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М: Постмаркет. – 2001. 187 с.

Допоміжна

1. Вильям Столлингс. Криптография и защита сетей: принципы и практика. – М.: Вильямс, 2001.
2. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. – СПб.: Лань, 2000.
3. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
4. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004.
5. Ухлинов А. М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1996.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.
7. Ященко В. В. Введение в криптографию. – СПб.: Питер, 2001.
8. Гребенніков В.В. Історія криптології & секретного зв'язку. Ужгород. – 803 с.

15. Інформаційні ресурси

1. https://www.uzhnu.edu.ua/uk/infocentre/60