ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРНЕТИКИ І ПРИКЛАДНОЇ МАТЕМАТИКИ

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
_____ / Студеняк І.П./
«___» _____ 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні та комп'ютерні основи криптології

Рівень вищої освіти	**Третій (освітньо-науковий)**
Галузь знань	**11 – Математика і статистика**
Спеціальність	**113 – Прикладна математика**
Освітні програми	**Прикладна математика**
Статус дисципліни	**Нормативна**
Мова навчання	**Українська**

Ужгород 2020

Робоча програма навчальної дисципліни «**Математичні та комп'ютерні основи криптології**» для здобувачів вищої освіти на третьому (освітньо-науковому) рівні: доктор філософії/Doctor Philosophy (Ph.D) галузі знань – математика і статистика.

Розробник:

Повідайчик М.М., доцент, кандидат економічних наук, доцент кафедри кібернетики і прикладної математики

Робочу програму розглянуто на засіданні

Кафедри кібернетики і прикладної математики

протокол № 10 від «26» червня 2020 р.

Завідувач кафедри _____ Гече Ф.Е.

Схвалено науково-методичною комісією **факультету математики та цифрових технологій**

протокол № 8 від «03» липня 2020 р.

Голова науково-методичної комісії _____ Мулеса О.Ю.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування
Показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Очна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 120</td><td>1-ий</td><td></td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="5">Тижневих годин
для очної форми навчання: 9

аудиторних – 3

самостійної роботи здобувача – 6</td><td>1-ий</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>28</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>20</td><td></td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: залік</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю:
усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>72</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни «Математичні та комп'ютерні основи криптології» є формування у студентів знань теоретичних основ криптології, а також практичних умінь та навичок застосування математичних моделей та методів у цій галузі. Об'єктом вивчення навчальної дисципліни – є теоретико-прикладні основи криптології. Предметом вивчення навчальної дисципліни – є математичні моделі та методи криптології.

Згідно вимог освітньої програми підготовки доктора філософії (PhD), здобувачі повинні знати: основні методи докомп'ютерної криптології, основні симетричні криптосистеми та криптосистеми з відкритим ключем.

Здобувачі повинні вміти: застосувати криптосистеми для захисту даних.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню для здобувачів ступеня вищої освіти: доктор філософії / Doctor Philosophy (Ph.D) таких компетентностей:

1. загальні компетентності:

- **ЗК-1.** Креативність, здатність до абстрактного мислення, аналізу і синтезу.
- **ЗК-2.** Здатність проведення досліджень на відповідному рівні.
- **ЗК-3.** Здатність до адаптації та дії в новій ситуації, здатність застосовувати знання у практичних ситуаціях, розуміння предметної області та розуміння професії.
- **ЗК-4.** Навички використання інформаційних і комунікаційних технологій, здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- **ЗК-5.** Здатність приймати обґрунтовані рішення.
- **ЗК-7.** Здатність вчитися і бути сучасно навченим.
- **ЗК-8.** Здатність бути критичним і самокритичним, поважати різноманітність та мультикультурність, діяти соціально-відповідально та громадянсько свідомо.

2. фахові компетентності:

- **ФК-1.** Здатність розробляти та вдосконалювати методи і засоби математичного та комп'ютерного моделювання, які призначені для дослідження та управління процесами та системами у різних галузях людської діяльності.
- **ФК-5.** Розробка математичних моделей та методів аналізу природничо-наукових, технічних, економічних та соціальних систем.
- **ФК-6.** Використання нових інформаційних технологій для моделювання та аналізу складних систем.
- **ФК-7.** Здатність до пошуку та аналізу науково-технічної, природничо-наукової та загальнонаукової інформації.

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Прикладна математика»** (третього освітньо-наукового рівня вищої освіти)**,** вивчення навчальної дисципліни «**Математичні та комп'ютерні основи криптології**» повинно забезпечити досягнення здобувачами ступеня вищої освіти: доктор філософії / Doctor Philosophy (Ph.D) таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	**Шифр ПРН**
Розробляти та вдосконалювати методи і засоби математичного та комп'ютерного моделювання, обчислювальні методи, призначені для використання при всебічному дослідженні і створенні об'єктів та систем технічного призначення.	1.1
Знання теоретичних і методологічних основ та інструментальних засобів використання інформаційних технологій у різних галузях людської діяльності.	1.2
Уміння генерувати нові ідеї і варіант розв'язання задач, комбінування та експериментування, оригінальність, конструктивність, економічність	2.1

рішень.	
Уміння адаптуватися до роботи за конкретною професією чи спеціальністю, до нових факторів середовища, уміння розв’язувати складні практичні задачі на основі системного аналізу, синтезу нових підходів у тому числі в умовах неповноти інформації або невизначеності.	2.3
Уміння виявляти, ставити та вирішувати проблеми з урахуванням багатофакторності та динаміки середовища.	2.5
Уміння розробляти та вдосконалювати методи і засоби математичного та комп'ютерного моделювання, обчислювальні методі, призначені для використання при всебічному дослідженні і створенні об'єктів та систем технічного призначення.	2.9
Уміння виконувати всі етапи наукових досліджень складних систем, накопичувати та обробляти науково-технічну інформацію, ставити та обробляти результати наукового експерименту.	2.12
Уміння розробляти математичну модель системи відповідно до поставленої задачі дослідження, здійснювати аналіз та вибір математичного апарату для дослідження математичної моделі.	2.13
Ініціювати наукові та інноваційні комплексні проекти в галузі прикладної математики, лідерство та автономність під час їх реалізації.	4.1
Діяти, дотримуючись принципів соціальної відповідальності, на основі етичних міркувань (мотивів).	4.2
Самовдосконалюватися, нести відповідальність за новизну наукових досліджень та прийняття експертних рішень.	4.3
Приймати обґрунтовані рішення, мотивувати людей та рухатися до спільної мети.	4.4

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «**Математичні та комп’ютерні основи криптології**»:

Очікувані результати навчання з дисципліни	Шифр ПРН
Уміння здійснювати пошук наукової інформації (наукових публікацій, відомостей про наукові видання, наукові заклади та окремих науковців) що у загальнодоступних науково-пошукових сервісах відповідно до власних наукових інтересів.	1.1 2.1 4.1
Уміння використовувати сервіси, які дозволяють здійснювати комунікацію в міжнародній науковій спільноті з метою обміну науковими ідеями, пошуку однодумців тощо.	4.1 4.2 4.3 4.4
Уміння користуватися хмарними та онлайн ресурсами, призначеними для пошуку, індексації, систематизації, збереження та обміну даними, а також пакетами прикладних програм та спеціальними онлайн-ресурсами, призначеними для створення наукових текстів та роботи з ними	1.2 2.3
Уміння користуватися пакетами прикладних програм та онлайн ресурсами, які призначені для аналізу результатів наукових досліджень та їх презентації у різних формах; здійсненню іншої науково-педагогічної діяльності	4.1 4.3 4.4
Уміння розробляти та вдосконалювати методи і засоби математичного та комп'ютерного моделювання, обчислювальні методі, призначені для використання при всебічному дослідженні і створенні об'єктів та систем технічного призначення.	1.1 1.2 2.5

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- залік;
- виконання практичних робіт;
- виконання індивідуальних та групових завдань;
- презентація результатів виконаної індивідуальної роботи студента.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: виступ на семінарських заняттях, виконання практичних робіт, презентація та захист групових проєктів.

Модульне контрольне оцінювання: контрольна робота.

Контроль самостійної роботи: перевірка виконаних завдань на практичних заняттях, перевірка домашніх завдань.

Підсумковий семестровий контроль: залік.

Під час **оцінювання індивідуальної роботи** враховується самостійність, творчий підхід, правильність виконання завдань та максимальне залучення при цьому всіх доступних програмних ресурсів.

Основні форми та методи організації навчального процесу, під час викладання дисципліни «Математичні та комп'ютерні основи криптології»:

- Словесні: лекція, бесіда, обговорення.
- Наочні: ілюстрація, демонстрація (з використанням фотоілюстрацій, таблиць та схем, електронних презентацій).
- Практичні: опитування на практичних заняттях; виконання практичних завдань; виконання індивідуальних завдань; контрольні роботи.
- Інтерактивні методи навчання.

Викладач використовує наступні групи методик контролю знань аспірантів, які вивчають дисципліну «Математичні та комп'ютерні основи криптології»:

1. Методи усного контролю: відповідь здобувача на окреме питання теми практичного заняття; запитально-відповідна бесіда під час роз'яснення проблемного питання на практичному занятті.
2. Методи практичного контролю: перевірка правильності виконання практичних завдань; залік, який включає у себе практичні завдання.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота							**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	50	100

8	7	7	7	7	7	7		

Т1, Т2 ... – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота							**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	50	100
7	7	7	8	7	7	7		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Кількість	Максимальна кількість балів (сумарна)
Практичні (семінарські) заняття	10	20
Виконання індивідуальних завдань	2	20
Виконання та презентація групових завдань	2	10
Модульна контрольна робота	2	50
Разом		**100**

Критерії оцінювання модульної контрольної роботи.

Модульна контрольна робота проводиться у формі практичних завдань, які виконуються в аудиторії. Варіант модульної контрольної роботи складається з двох блоків.

Перший блок складається з теоретичних питань (25 балів).

Другий блок присвячений розв’язанню задач (25 балів).

Критерії оцінювання підсумкового семестрового контролю

Відповідно до ***«Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університеті»*** (затверджено Наказом Ректора ДВНЗ «УжНУ» № 698/01-17 від

08.05.2015 р.), знання здобувачів оцінюється як з теоретичної, так і з практичної підготовки за такими критеріями:

оцінку «відмінно» (90-100 балів, А) заслуговує здобувач, який:

- всебічно і глибоко володіє навчально-програмовим матеріалом;
- вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;
- засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;
- засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;
- вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;
- самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

оцінку « добре» (82-89 балів, В) – заслуговує здобувач, який:

- повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання в достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;
- має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування

проблем професійного спрямування;

- під час відповіді допустив деякі неточності, які самостійно виправив, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, С) заслуговує здобувач, який:

- в цілому навчальну програму засвоїв, але відповідає на екзамені з певною кількістю помилок;

- вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

- опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) – заслуговує здобувач, який:

- знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

- виконує завдання непогано, але зі значною кількістю помилок;

- ознайомлений з основною літературою, яка рекомендована програмою;

- допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

оцінку «задовільно» (60-63 бали, E) – заслуговує здобувач, який:

- володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) – виставляється здобувачу, який: виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінка «незадовільно» (35 балів, F) – виставляється здобувачу, який:

- володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;

- допускає грубі помилки при виконанні завдань, передбачених програмою;

- не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

При виставленні оцінки враховуються результати навчальної роботи здобувача протягом семестру.

Таблиця відповідності оцінок за різними шкалами

Оцінка за 100-бальною шкалою	Оцінка ЄКТС	Оцінка за національною шкалою	
		Диференційована	Недиференційована
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	незараховано з можливістю повторного складання
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	незараховано з обов'язковим повторним вивченням дисципліни

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст 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. 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 5. 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 6. 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.

Тема 7. 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.

Модуль 2

Змістовий модуль 1. Комп’ютерні методи криптографії.

Тема 1. 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 2. 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 3. 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 4. 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 5. Функції хешування.

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

Тема 6. 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 9. Протоколи управління криптографічними ключами.

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

5.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Змістовий модуль 1. Докомп'ютерна криптографія.						
Тема 1. Докомп'ютерний захист інформації.	9	2	2			5
Тема 2. Арифметичні основи криптографії.	9	2	1			6
Тема 3. Алгебраїчні основи криптографії.	8	2	1			5
Тема 4. Ймовірнісно-статистичні моделі повідомлень та їхні ентропійні властивості.	8	2	1			5
Тема 5. Методи теорії інформації у криптографії.	8	2	1			5
Тема 6. Статистичне тестування випадкових і псевдовипадкових послідовностей.	8	2	1			5
Тема 7. Алгоритми генерування випадкових і псевдовипадкових послідовностей.	8	2	1			5
Разом за змістовий модуль 1	58	14	8			36
Модульна контрольна робота № 1	2		2			
Усього годин за модуль 1	60	14	10			36
Модуль 2						
Змістовий модуль 1. Комп'ютерні методи криптографії.						
Тема 1. Потокові криптосистеми.	8	2	1			5
Тема 2. Математичні моделі стандартних блочних криптосистем.	8	2	1			5
Тема 3. Математичні методи криптоаналізу симетричних систем.	9	2	1			6
Тема 4. Криптосистеми з відкритим ключем.	9	2	2			5
Тема 5. Функції хешування.	8	2	1			5
Тема 6. Електронний цифровий підпис.	8	2	1			5
Тема 9. Протоколи управління криптографічними ключами.	8	2	1			5
Разом за змістовий модуль 1	58	14	8			36
Модульна контрольна робота № 2	2		2			
Усього годин за модуль 2	60	14	10			36
Усього годин	120	28	20			72

5.3. Теми практичних занять

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

5.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
15.	Докомп’ютерний захист інформації.	5
16.	Арифметичні основи криптографії.	6
17.	Алгебраїчні основи криптографії.	5
18.	Ймовірнісно-статистичні моделі повідомлень та їхні ентропійні властивості.	5
19.	Методи теорії інформації у криптографії.	5
20.	Статистичне тестування випадкових і псевдовипадкових послідовностей.	5
21.	Алгоритми генерування випадкових і псевдовипадкових послідовностей.	5
22.	Потокові криптосистеми.	5
23.	Математичні моделі стандартних блочних криптосистем.	5
24.	Математичні методи криптоаналізу симетричних систем.	6
25.	Криптосистеми з відкритим ключем.	5
26.	Функції хешування.	5
27.	Електронний цифровий підпис.	5
28.	Протоколи управління криптографічними ключами.	5

6. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Бауэре Н., Гербер Х., Джане Д., Неебитт С., Хикман Дж. Актуарная математика. Перев. сангл. / Под ред. В. К. Малиновского. – М.: Янус-К, 2001. - 656 С., илл.
2. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 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. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М: Постмаркет. – 2001. 187 с.
8. Мак Т. Математика рискового страхования / Пер. с нем. – М.: ЗАО «Олимп-Бизнес», 2005. – 432 с.
9. 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.
10. Нильс Фергюсон, Брюс Шнайер Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems – М.: Диалектика, 2004. – 432 с.

Допоміжна література

1. Гребенніков В.В. Історія криптології & секретного зв'язку. Ужгород. – 803 с.
2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004.
3. Слюсарчук П.В. Теорія ймовірності та математична статистика. – Ужгород: Карпати, 2005. – 184 с.
4. 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.

Результати перегляду
робочої програми навчальної дисципліни

Робоча програма перезатверджена на 20___ / 20___ н.р.   без змін;   зі змінами (Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р.   Завідувач кафедри _________ ____________
(підпис)   (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р.   без змін;   зі змінами (Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р.   Завідувач кафедри _________ ____________
(підпис)   (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р.   без змін;   зі змінами (Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р.   Завідувач кафедри _________ ____________
(підпис)   (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р.   без змін;   зі змінами(Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р.   Завідувач кафедри _________ ____________
(підпис)   (Прізвище ініціали)