МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА»

Факультет математики та інформатики

Кафедра математичного і функціонального аналізу

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Ймовірнісні методи захисту інформації

Освітня програма “Прикладна та теоретична статистика”

Спеціальність 112 “Статистика”

Галузь знань 11 “Математика та статистика”

Затверджено на засіданні кафедри
Протокол № 1 від “27” серпня 2020 р.

м. Івано-Франківськ - 2020

ЗМІСТ

1. Загальна інформація	
Назва дисципліни	Ймовірнісні методи захисту інформації
Рівень вищої освіти	Другий (магістерський)
Викладач (-і)	Слободян С.Я.
Контактний телефон викладача	+380501574456
E-mail викладача	slobodian_s@ukr.net
Формат дисципліни	Вибіркова навчальна дисципліна
Обсяг дисципліни	6 кредитів ЄКТС / 180 год.
Посилання на сайт дистанційного навчання	
Консультації	

2. Анотація до курсу

Курс " Методологія та організація наукових досліджень " входить до переліку вибіркових дисциплін. Згідно навчального плану передбачено 180 навчальних годин, з яких 32 години лекційних, 28 години практичних і 120 годин самостійної підготовки. Студенти отримують фундаментальні знання з теорії ймовірнісних методів захисту інформації, основ криптографічного захисту інформації.Завершується курс заліком.

3. Мета та цілі курсу

Метою даного курсу є формування системи теоретичних і практичних знань у сфері теоретичної криптографії та криптоаналізу, а також ознайомлення з основними принципами роботи криптографічних систем, математичними моделями джерел інформації, поняттями стійкості криптоалгоритмів. Завдання: − вивчити алгоритмічні аспекти ймовірнісних методів і їх застосування в сучасній теорії захисту інформації, вивчити сучасні методи криптографічного захисту інформації; вивчити основи криптографічних протоколів.

4. Результати навчання та компетентності

В результаті вивчення дисципліни студент повинен наступне.

- Знати принципи функціонування та моделювання природничих, економічних та соціальних процесів (ПРН-4);
- Уміти будувати математичні моделі систем і явищ з елементами випадковості, працювати з імовірнісними розподілами, що застосовуються в прикладних сферах досліджень (ПРН-5);
- Уміти інтегрувати знання з різних галузей для розв’язання теоретичних та практичних задач і проблем (ПРН-13)
- Мати здатність до використання принципів, методів та організаційних процедур дослідницької та практичної діяльності (ФК-4)
- Мати здатність здійснювати дослідницьку або професійну діяльність у міжнародному середовищі (ФК-10).

Компетентності:

- Здатність до професійного спілкування зі спеціалістами з інших галузей знань (ЗК-9).
- Здатність застосовувати та розвивати методи теорії ймовірностей і математичної статистики для побудови й дослідження математичних моделей стохастичних систем і явищ (ФК-2).
- Здатність застосовувати ймовірнісно-статистичні методи в міждисциплінарному контексті (ФК-5).
- Здатність подавати статистичні процедури та результати їхнього застосування у формі, придатній для цільової аудиторії (ФК-6).

Обсяг курсу					
Вид заняття				Загальна кількість годин	
Лекції				32	
семінарські заняття / практичні / лабораторні				28	
самостійна робота				120	
Ознаки курсу					
Семестр	Спеціальність		Курс (рік навчання)		Нормативний / вибірковий
1	**Статистика**		1		Нормативний
Тематика курсу					
Тема, план	Форма заняття	Література	Завдання, год	Вага оцінки	Термін виконання
Тема 1. Складність арифметичних дій. Алгоритм Евкліда і його складність.	Лекція (2 год), практичне заняття (1 год)	[1]-[5]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 2. Прості числа. Числа Марсенна. Числа Ферма.	Лекція (2 год), практичне заняття (1 год)	[1]-[5]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 3. Порівняння і кільця лишків.	Лекція (2 год), практичне заняття (1 год)	[1]-[5]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 4. Огляд теорії полів. Скінченні поля. Поле Галуа	Лекція (2 год), практичне заняття (1 год)	[1]-[5]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 5. Функція Ейлера. Властивості функції Ейлера. Теорема Ейлера.	Лекція (2 год), практичне заняття (1 год)	[1]-[5]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 6. Алгебраїчні порівняння с одним	Лекція	[1]-[5]	Опрацювання лекційного матеріалу		

невідомим. Розв'язок лінійних порівнянь	(2 год), практичне заняття (1год)		(3 год), виконання вправ (4 год)		
Тема 7. Системи порівнянь першого степеню. Китайська теорема про лишки.	Лекція (2 год),	[1]-[5]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Контрольна робота	Практичне заняття (2 год)		Підготовка до контрольної роботи (4 год)	0,5	5 тиждень
Тема 8. "Класична" криптографія. Класичні криптосистеми та їх криптоаналіз	Лекція (2 год), практичне заняття (2 год)	[1], [6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 9. Афінні шифри.	Лекція (2 год), практичне заняття (2 год)	[6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 10. Сучасні стандарти симетричного шифрування. DES	Лекція (2 год), практичне заняття (2 год)	[6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 11. Сучасні стандарти симетричного шифрування. AES	Лекція (2 год), практичне заняття (2 год)	[1], [6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 12. Режими шифрування. Задачі режиму шифрування.	Лекція (2 год), практичне заняття (2 год)	[1], [6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 13. Методи та алгоритми	Лекція	[1], [6]-[11]	Опрацювання лекційного матеріалу		

асиметричної криптографії	(2 год), практичне заняття (2 год)		(3 год), виконання вправ (4 год)		
Тема 14. Задачі електронного цифрового підпису. ЕЦП RSA	Лекція (2 год), практичне заняття (2 год)	[1], [6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 15 Основні криптографічні протоколи	Лекція (2 год), практичне заняття (2 год)	[1], [6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Тема 16 Проблеми інформаційного захисту банківських та комерційних систем. Нові напрямки в криптології	Лекція (2 год), практичне заняття (2 год)	[1], [6]-[11]	Опрацювання лекційного матеріалу (3 год), виконання вправ (4 год)		
Контрольна робота	Практичне заняття (2 год)		Підготовка до контрольної роботи (4 год)	0,5	10 тиждень

6. Система оцінювання курсу	
Загальна система оцінювання курсу	Підсумковим контролем в курсі є письмовий залік із можливим захистом виконань його завдань. Проміжним контролем є дві аудиторні контрольні роботи. Оцінювання проводиться в шкалі, яка передбачає: відмінну оцінку (A) за 90 — 100% правильних результатів, дуже добру оцінку (B) за 80 — 89% правильних результатів, добру оцінку (C) за 70 — 79% правильних результатів, задовільну оцінку (D) за 60 — 69% правильних результатів, достатню оцінку (E) за 50 — 59% правильних результатів, недостатню оцінку (FX) за 25 — 59% правильних результатів та незадовільну оцінку (F) за менше, ніж 25% правильних результатів.
Вимоги до письмової роботи	Контрольні письмові роботи виконуються студентом в призначений час в аудиторії протягом двох академічних годин. Робота містить теоретичні та практичні завдання загальною кількістю достатньою для досягнення її мети.
Семінарські заняття	Практичні заняття проводяться після лекцій з відповідної теми. Змістом практичних занять є виконання завдань під керівництвом викладача

Умови допуску до підсумкового контролю	1. Відвідування не менше 50% лекційних і не менше 75% семінарських занять. 2. Виконання контрольної робіт з оцінкою, що становить не менше 25% від максимальної оцінок.

7. Політика курсу

Лекції читаються лектором із залученням студентів до обговорення окремих питань. На практичних заняттях студенти виконують запропоновані викладачем завдання з його допомогою. Самостійна робота студента передбачає вивчення теоретичних положень дисципліни та виконання завдань, заданих викладачем на лекціях та практичних заняттях. Кожна контрольна робота виконуються студентом самостійно без використання друкованих та електронних засобів доступу до інформації. Пропущена контрольна робота повинна бути виконана не пізніше, ніж через два тижні після пропуску. Час виконання таких робіт встановлюється викладачем окремо за заявою студента.

8. Рекомендована література

1. О. В. Вербіцький Вступ до криптології. ВНТА. Львів.1998 – 247с.
2. Н. Коблиц. Курс теории чисел и криптографии. М.: ТВП, 2001.
3. О. Н. Василенко. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.
4. А. В. Черемушкин. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.
5. А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А. А. Часовских. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: 2006.
6. Б. Анин Защита компьютерной информации СПБ: БХВ – СанктПетербург. 2000. –384с.
7. Б. С.Люцарев, К. В. Ермаков, Е. Б. Рудный, И. Е. Ермаков. Безопасность компьютерных сетей на основе Windows NT. 1998. –340с. «Channel Tr. Ltd»
8. В. В. Домарѐв Защита информации и безопасность компьютерных систем. Diasoft. Киев. 1999. –453с.
9. В. Ємець, А. Мельник, Р. Попович. Сучасна криптографія. Основні погяття. Львів-2003, “Бак”, -144с.
10. Т. Корнієнко, А. Мельник, В. Мельник. Алгоритм та процеси симетричного блокового шифрування. Львів-2003, “Бак”, -168с.
11. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. –К. : Видавничий дім "СофтПрес", 2005. –316 с.

Викладач _____