

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Прикарпатський національний університет імені Василя Стефаника»

Факультет математики та інформатики
Кафедра алгебри та геометрії

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ПРИКЛАДНА КРИПТОЛОГІЯ

Освітня програма: Прикладна математика

Спеціальність: 113 Прикладна математика

Галузь знань: 11 Математика та статистика

Затверджено на засіданні кафедри
Протокол №1 від 31 серпня 2020 р.

ЗМІСТ

1. Загальна інформація
2. Анотація до курсу
3. Мета та цілі курсу
4. Компетентності
5. Результати навчання
6. Організація навчання курсу
7. Система оцінювання курсу
8. Політика курсу
9. Рекомендована література

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

Назва дисципліни	Прикладна криптологія
Викладач(-і)	Мазуренко Н.І.
Контактний телефон	(0342)596016
E-mail	nataliia.mazurenko@pnu.edu.ua
Формат дисципліни	Лекції та лабораторні заняття
Обсяг дисципліни	3 кредити
Консультації	Вівторок, 15 ⁰⁰

2. АНОТАЦІЯ ДО КУРСУ

Курс прикладної криптології відповідає потребам студента, майбутнього фахівця у сфері захисту інформації, якому розуміння теорії потрібно для її практичного застосування у питаннях менеджменту інформаційної безпеки, побудови та експертизи комплексних систем захисту інформації тощо.

Гармонійне поєднання в цьому курсі математичного аспекту криптології з акцентом на її прикладний характер, робить його особливо привабливим для практиків.

3. МЕТА ТА ЦІЛІ КУРСУ

Формування у студента навичок практичної оцінки якостей шифрів, вміння використовувати основні методи й способи розв'язання конкретних задач синтезу та аналізу криптографічних систем (зокрема, це стосується забезпечення конфіденційності, цілісності та авторства інформації за допомогою класичних симетричних криптосистем та криптосистем з відкритим ключем).

Формування навичок дослідника: «навчити вчитися» студента на конкретних задачах, показати, як користуватися наявним «інструментарієм», який метод може допомогти у розв'язанні проблеми.

4. КОМПЕТЕНТНОСТІ

Відповідно до освітньо-професійної програми «Прикладна математика» для першого (бакалаврського) рівня вищої освіти:

- ЗК1.** Здатність до абстрактного мислення, аналізу та синтезу, до застосування теорії у практичних ситуаціях;
- ЗК2.** Здатність до пошуку та інтерпретації інформації, засвоєння нових знань, генерування та викладу ідей, зокрема, з застосуванням інформаційних технологій;
- ЗК3.** Здатність працювати як автономно, так і у складі наукового, зокрема, інтернаціонального, колективу фахівців з усвідомленням відповідальності за результати роботи;
- ЗК4.** Здатність вести дослідницьку діяльність, включаючи оцінку актуальності дослідження, аналіз проблем, вибір способу й методів дослідження, а також оцінку якості результатів.
- ПК1.** Цілісне уявлення про математику, її сучасний стан, виникнення і шляхи розвитку, її місце у системі наукових знань людства;
- ПК2.** Здатність зрозуміти постановку завдання, пов'язаного із застосуванням методів прикладної математики, сформульовану на мові певної предметної галузі;
- ПК3.** Здатність математично формалізувати проблему прикладного характеру, розпізнати стандартні об'єкти і властивості аналізу, звичайних диференціальних рівнянь, рівнянь математичної фізики, дискретної математики, теорії керування, методів оптимізації, алгебри, геометрії;
- ПК4.** Здатність обирати та застосовувати математичні методи для розв'язування практичних задач дослідження, моделювання, аналізу, керування, прийняття рішень;
- ПК7.** Уміння ефективно співпрацювати, розподіляти роботу і спілкуватись з колегами в процесі командного виконання дослідницьких та програмних проектів;
- ПК9.** Здатність використовувати методи системного аналізу та математичного моделювання для побудови моделей у різних галузях;
- ПК13.** Здатність до побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення та аналізу алгоритмів, оцінювання їх ефективності та складності для адекватного моделювання предметних областей і створення програмних та інформаційних систем;
- ПК14.** Здатність застосовувати теоретичні та практичні основи методології та технології моделювання, реалізовувати алгоритми моделювання для дослідження характеристик і поведінки складних об'єктів і систем,

проводити експерименти за програмою моделювання з обробкою й аналізом результатів;

ПК16. Здатність опанувати сучасні технології математичного моделювання об'єктів, процесів і явищ, розробляти обчислювальні моделі та алгоритми чисельного розв'язання задач математичного моделювання з урахуванням похибок наближеного чисельного розв'язання професійних задач;

ПК17. Здатність застосовувати основні методи та алгоритми прийняття рішень в умовах наявності нечіткої вхідної інформації, здійснювати аналіз отриманих результатів.

5. РЕЗУЛЬТАТИ НАВЧАННЯ

- демонструвати знання й розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці, а також гуманітарних дисциплін підготовки фахівця (P1);
- володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та аналітичної геометрії, теорії диференціальних рівнянь, рівнянь математичної фізики, теорії ймовірностей, математичної статистики та випадкових процесів, числовими методами, методами оптимізації. (P2);
- знати де виникають оптимізаційні задачі, основні етапи операційного дослідження (математичного моделювання) і основні принципи ефективної формалізації таких задач (P3);
- самостійно працювати над дослідницькою темою, обґрунтовувати і створювати програмну реалізацію розроблених методів. (P4);
- уміти розробляти математичні моделі об'єктів і процесів, які досліджуються, використовуючи процедури формального уявлення про систему та результати дослідження реальних природничих та соціально-економічних процесів. (P5);
- проводити аналітичне дослідження математичних моделей об'єктів і процесів на предмет існування та єдиності їх розв'язку. (P6);
- уміти розробляти нові і удосконалювати існуючі математичні моделі та алгоритми моделювання природничих, соціально-економічних систем та проводити комп'ютерне моделювання. (P7);
- знати основні поняття криптології, способи захисту інформації та найпростіші методи шифрування. Знати функціональні можливості застосування сучасних

пакетів програмної реалізації криптографічних перетворень та криптографічних бібліотек (P23);

- уміти проводити наукові дослідження, грамотно викладати і представляти опрацьований матеріал і власні результати, в тому числі і з сучасними можливостями візуалізації, створювати комп'ютерну реалізацію розроблених методів (P25).

6. ОРГАНІЗАЦІЯ НАВЧАННЯ КУРСУ

Обсяг курсу	
Вид заняття	Загальна кількість годин
Лекції	14
Лабораторні	16
Самостійна робота	60

Ознаки курсу				
Спеціальність, освітня програма	Рівень освіти	Курс (рік навчання)	Семестр	Нормативна/ вибіркова
113 Прикладна математика	Бакалавр	4 ^{ий}	7 ^{ий}	вибіркова

Тематика курсу (7 семестр)

Тема, план	Форма заняття	Література	Завдання, год	Вага оцінки	Термін виконання
Класична криптографія. Інформаційно-теоретична стійкість шифрів	лекція	[1, 3, 4, 8]	Опрацювати матеріал лекції з рекомендованою літературою, 4 ауд. год., 4 год. с. р.	–	1 ^{ий} – 2 ^{ий} тижні
Класичні шифри заміни та перестановки, блокові шифри	лабораторна	[1, 3]	Реалізувати програмними засобами основні класичні шифри, 4 ауд. год., 4 год. с. р.		1 ^{ий} – 2 ^{ий} тижні
Блокове та потокове шифрування	лекція	[1, 3, 8]	Опрацювати матеріал лекції з рекомендованою літературою, 4 ауд. год., 8 год. с. р.	–	3 ^{ій} – 4 ^{ий} тижні
Алгоритми блокових та поточкових шифрів	лаб	[1, 3, 4, 8]	Реалізувати програмними засобами типові алгоритми блокових та поточкових шифрів чи їх фрагменти		3 ^{ій} – 4 ^{ий} тижні

			4 ауд. год., 8 год. с. р.		
Криптографія з відкритим ключем. Електронний цифровий підпис, криптографічні протоколи.	лекція	[1, 3, 4]	Опрацювати матеріал лекції з рекомендованою літературою, 6 ауд. год., 6 год. с. р.	–	6 ^{ий} – 8 ^{ий} тижні
Основні алгоритми криптосистем з відкритим ключем	лаб	[1, 3, 4]	Реалізувати програмними засобами основні криптосистеми з відкритим ключем або їх фрагменти, 6 ауд. год., 6 год. с. р.		6 ^{ий} – 8 ^{ий} тижні
Криптографічні інструменти - важкооборотні функції - генератори псевдовипадкових бітів	сам. роб.	[1, 6, 7]	Опрацювати матеріал за рекомендованою літературою, 6 год. с. р.	–	9 ^{ий} – 12 ^{ий} тижні
Тематичний контроль	контрольна робота	[1–8]	Підготовка до к. р., 6 год. с. р. Індивід. завдання, 2 ауд. год.	25	13 ^{ий} тиждень
Практикум з криптології	сам. роб.	[1–8]	Індивідуальні завдання, 10 год. с. р.	50	9 ^{ий} – 14 ^{ий} тижні
Тематичний контроль	тест	[1–8]	Підгот. до тесту, 8 год. с. р.	25	15 ^{ий} тиждень
Підсумковий контроль	залік			100	

7. СИСТЕМА ОЦІНЮВАННЯ КУРСУ

Загальна система оцінювання	Підсумкова оцінка з дисципліни у є сумою оцінок за кожен з таких видів робіт: аудиторна робота (активна робота на практичних заняттях), самостійна робота (практикум та опрацювання окремих тем), тематичний контроль (контрольна робота і тест). Підсумкова оцінка визначається відповідно до поданої нижче таблиці оцінювання за різними шкалами (100-бальна, ECTS, національна).
Аудиторна робота	Максимальна оцінка за активну і змістовну участь у розв'язуванні задач з криптології на практичних заняттях становить 5 балів.
Самостійна робота	Практикум з лінійного/дискретного програмування містить по 5 завдань у кожному з 25 варіантів. Максимальна оцінка за виконання і захист завдань практикуму становить 10 балів за кожне завдання.
Тематичний контроль	Кожен варіант контрольної роботи містить 7 завдань на застосування методів криптографії та криптоаналізу. Максимальна оцінка становить 25 балів. Тест з криптології містить від 15 до 25 завдань закритого типу на розуміння основних понять, методів та алгоритмів криптології. Максимальна оцінка за тест становить 25 балів.

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

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
80 – 89	B	добре	
70 – 79	C		
60 – 69	D	задовільно	
50 – 59	E		
26 – 49	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-25	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

8. ПОЛІТИКА КУРСУ

Усі види навчальної роботи слід виконувати вчасно, щоб зберегти загальний темп курсу, котрий сприяє ефективному засвоєнню матеріалу без шкоди здоров'ю. Наслідками пропущених занять без поважних причин, зазвичай, стають додаткові завдання для самостійної роботи.

При проходженні курсу вітаються комунікативність, активність, креативність, самостійність. Плагіат та інші види академічної недоброчесності не принесуть користі, тому є недоречними.

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Вербіцький О. В. Вступ до криптології. - Львів: ВНТЛ, 1998. - 248с.
2. Берегуляк І. Я. Класичні методи криптивання. - Львівський університет, 1997.
3. Бабенко Т.В., Гулак Г.М., Сушко С.О., Фомичова Л.Я. Криптологія у прикладах, тестах і задачах: навч. посібник / Д.: Національний гірничий університет, 2013. - 318 с.
4. Барычев С. Г., Серов Р. Е. Основы современной криптографии.
5. Яценко В.В. Введение в криптографию.
6. Виноградов И. М. Основы теории чисел. - М.: Наука. - 1981.
7. ван дер Варден Б. Л. Алгебра. - М.: Наука. - 1979.
8. Тилборг ван Х. К. А. Основы криптологии / Тилборг ван Х. К.А. – М. : Мир, 2006. - 471 с.

Викладач Мазуренко Н. І.