Одеський національний університет імені І.І.Мечникова
Факультет математики, фізики та інформаційних технологій

Кафедра комп'ютерної алгебри та дискретної математики

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи

_____О.В.Запорожченко

_____2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Основи криптографії

Рівень вищої освіти перший (освітньо-науковий) рівень - бакалавр.

Галузь знань: 10 –"Природничі науки".

Спеціальність: 105 - Прикладна фізика та наноматеріали.

Освітньо-наукова програма: " Прикладна фізика та наноматеріали ".

Факультет математики, фізики та інформаційних технологій

Одеса – 2020 рік

Програму рекомендовано до затвердження Вченою Радою факультету математики, фізики та інформаційних технологій «03» вересня 2020року.
Протокол № 1.

Розробники програми:
Кандидат фізико-математичних наук, доцент Сімонова І.Г.

Начальна програма затверджена на засіданні кафедри комп'ютерної алгебри та дискретної математики .
Протокол № 1 від «3» вересня 2020 року.

Завідувач кафедри _____Варбанець П.Д.

Програму погоджено навчально-методичною комісією (НМК) ФМФІТ:
Протокол № 1 від «03» вересня 2020 року

Голова НМК _____ Ніщук Ю.А.

ВСТУП

Програма навчальної дисципліни «Криптографія» складена відповідно до освітньо-наукової програми підготовки першого (освітньо-наукового) рівня вищої освіти (бакалавр). Галузь знань: 10 –"Природничі науки".
Спеціальність: 105 – Прикладна фізика та наноматеріали. Освітньо-наукова програма: " Прикладна фізика та наноматеріали ".

1. Опис навчальної дисципліни

1.1. Метою викладання навчальної дисципліни є:
надати майбутнім бакалаврам з фізики та астрономії необхідного мінімуму попередніх відомостей щодо методів та алгоритмів криптографії, ознайомлення студентів з сучасними засобами захисту інформації. Для цього до програми також входять деякі питання з алгебри і теорії алгоритмів, які не вивчались на молодших курсах, і які в свою чергу є елементами базової підготовки по математичним основам криптографічного захисту інформації.

1.2. Основними завданнями вивчення дисципліни є:
засвоєння студентами сучасних засобів захисту інформації методами криптографії та успішне використання їх на практиці.

Інтегральна компетентність (ІК)
- Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми прикладної фізики та наноматеріалів, що передбачає застосування сучасних засобів захисту інформації методами криптографії й характеризується комплексністю та невизначеністю умов.

Загальні компетентності згідно з освітньо-професійною програмою «Прикладна фізика та наноматеріали» спеціальності 105 – «Прикладна фізика та наноматеріали»:
- Здатність застосовувати знання у практичних ситуація, ЗК1.
- Знання та розуміння предметної області та розуміння професійної діяльності, ЗК2.
- Здатність спілкуватися державною мовою як усно, так і письмово, ЗК3.
- Здатність спілкуватися іноземною мовою, ЗК4.
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел, ЗК9.
- Здатність працювати автономно, ЗК9.

Спеціальні (фахові) компетентності згідно з освітньо-професійною програмою «Прикладна фізика та наноматеріали» спеціальності 105 – «Прикладна фізика та наноматеріали»:
- Здатність використовувати теоретичні уявлення сучасних засобів захисту інформації методами криптографії (ФК 6),
- Здатність використовувати методи і засоби теоретичного дослідження та математичного моделювання в професійній діяльності (ФК 7).

2. Тематичний план навчальної дисципліни
4-й рік, VII семестр

Тема 1. *Початкові поняття криптології1. Вступ до криптології.*
Проблема захисту інформації в сучасному суспільстві. Поняття про криптографію та криптоаналіз. Задачі криптографії. Класична криптографічна схема. Принцип Керкхоффса. Теорія Шеннона секретного зв'язку. Ідея відкритого ключа. Задача управління ключами.
2. *Історична криптографія*
Шифри заміни. Шифри Цезаря та Августа. Квадрат Полібія. Частотний метод. Шифр чотирьох квадратів. Шифри перестановки. Шифр Сцитали. Шифри Кардано і Ришельє. Поліалфавітні шифри. Шифри Тритеміуса та Віженера. Шифр Вернама. Композиція шифрів. Шифр ADFGVX.

Тема 2. *Математичний імператив*
Теорія подільності. Прості числа. Розкладення чисел у непериви дріб. Підходящі дроби. Арифметичні функції. Мультиплікативні функції. Числові конгруєції. Система лишків по модулю *m*. Конгруєції одною змінною. Системи порівнень. Порівнення по простому модулю. Конгруєції другого степеня.

Тема 3.
Симетричні криптосистеми. Криптографія з відкритим ключем
Поняття симетричної криптосистеми. Поточні шифри. Гамування. Блокові шифри. Лінійні та афінні шифри. Загальний опис алгоритмів DES, RC4, ГОСТ- 28147-89. Поняття про криптоаналіз блокових шифрів. Криптосистеми. Концепція криптосистем з відкритим ключем. Поняття про важкозворотні функції. Опис системи RSA.

6. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
	Усього	лекцій	практ.	лаб.	інд	сам. роб.
Тема 1.		10	-	4	-	-
Тема 2.		10	-	4	-	-
Тема 3.		10	-	2	-	-
Всього год.		30	-	10	-	-

4. Теми практичних занять

№	Назва теми	Кількість годин
1	Шифри заміни. Шифри Цезаря та Августа. Квадрат Полібія.	2
2	Шифр чотирьох квадратів. Шифри перестановки	2
3	Теорія подільності. Прості числа. Розкладення чисел у непреривну дріб. Підходящі дроби.	2
4	Арифметичні функції. Мультиплікативні функції. Числові конгруєції. Система лишків по модулю *m*. Конгруєції одною змінною.	2
5	Загальний опис алгоритмів DES, RC4, ГОСТ- 28147-89.	2

8. Теми індивідуальних занять

9. Індивідуальні завдання
Не передбачено навчальним і робочим планом

10. Методи навчання. При викладанні дисципліни використовуються інтерактивні методи навчання, наочні методи навчання. Базовим методом навчання є поєднання лекції та практичних занять. Під час проведення лекцій використовуються наступні методи навчання: пояснювальноілюстративний метод; метод проблемного викладу; частково-пошуковий, або евристичний метод. Під час практичних занять використовуються наступні методи навчання частковопошуковий, або евристичний метод; дискусійний метод. Під час самостійної роботи використовуються наступні методи навчання: дослідницький метод.

11. Методи контролю
Для кожної теми формами контролю навчальних здобутків студентів можуть бути поточний контроль: оцінка активності роботи на лекціях; аудиторне поточне опитування; домашні завдання, модульні контрольні роботи, підсумкові залікові та екзаменаційні роботи. Підсумкові бали для оцінки знань студентів за розділ розрахуються таким чином:

№	Вид роботи	Форма контролю	Максимальне число балів
	Аудиторна активність студента		2
	Виконання класних і домашніх завдань, самостійної роботи	Письмові розв'язки, письмові та усні відповіді	4
	Сума		6

12. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завдання				Підсумкова контрольна робота (залік)	Підсумковий бал*
Розділ 1	Розділ 2	Розділ 3	Індивідуальні заняття		
35	30	35	-	100	100

* Обчислюється як середнє від двох балів: балу поточного контролю за активністю студента (включаючи самостійну роботу та індивідуальні завдання) та балу за підсумкову контрольну роботу.

13. Методичне забезпечення
Посібники, контрольні питання і завдання до тем, роздаткові матеріали до лекцій

1. Белозьоров Г.С. Криптографія. Посібник.
2. Шпінарьова І.М. Методичні вказівки до виконання контрольної роботи.

14. Рекомендована література
Базова
Література:

1. Алферов А.П. и др. Основы криптографии. М.: Гелиос АРВ, 2001.
2. Вербіцький О.В. Вступ до криптології. Львів: вид. наук.-техн. літ., 1998.
3. Молдовян А.А. и др. Криптография. СПб.: Лань, 2000.
4. Смарт Н. Криптография. М.: Техносфера, 2006.
5. Иванов М.А. Криптография, М.: Кудиц-образ, 2001.
6. Ященко В.В. и др. Введение в криптографию. СПБ.: МЦНМО Питер, 2001.