Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

Кафедра методики навчання математики та методики навчання інформатики

НАВЧАЛЬНА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Вибрані питання математики

(назва навчальної дисципліни)

підготовки здобувачів ступеня вищої
освіти *бакалавр*
(назва рівня вищої освіти)
напряму підготовки 6.040201 Математика*
(шифр і назва напряму підготовки)
спеціалізації *інформатика*
(назва спеціалізації)

Слов'янськ – 2017 р.

РОЗРОБЛЕНО ТА ВНЕСЕНО КАФЕДРОЮ МЕТОДИКИ НАВЧАННЯ МАТЕМАТИКИ ТА МЕТОДИКИ НАВЧАННЯ ІНФОРМАТИКИ ФІЗИКО-МАТЕМАТИЧНОГО ФАКУЛЬТЕТУ ДВНЗ «ДДПУ»

УКЛАДАЧІ ПРОГРАМИ:

Пащенко З.Д. − кандидат фізико-математичних наук, доцент,
Турка Т.В. − кандидат фізико-математичних наук, доцент.

РЕЦЕНЗЕНТИ:

Беседін Борис Борисович, кандидат педагогічних наук, доцент кафедри методики навчання математики та методики навчання інформатики ДВНЗ «ДДПУ»;

Чуйко Олексій Сергійович, кандидат фізико-математичних наук, доцент кафедри математики та інформатики ДВНЗ «ДДПУ».

Рекомендовано до впровадження
науково-методичною радою
Державного вищого навчального закладу
«Донбаський державний педагогічний університет»

«21» вересня 2017 р.
протокол № 2

Перший проректор _____ Набока О.Г.

ВСТУП

Навчальна програма вивчення дисципліни «*Вибрані питання математики*» складена відповідно до освітньо-професійної програми підготовки бакалавра напряму 6.040201 Математика* .

Предметом вивчення навчальної дисципліни є криптологія. Криптологія має три складові: криптографію – науку про збереження інформації, криптоаналіз – науку про проникнення у таємницю тексту та математичний апарат, за допомогою якого реалізуються поставлені задачі.

Міждисциплінарні зв'язки: алгебра, дискретна математика, теорія чисел, числові системи, інформатика.

Програма навчальної дисципліни містить такі змістові модулі:
Змістовний модуль 1. Вибрані питання теорії чисел.
Змістовний модуль 2. Основи криптографії.

1. Мета й завдання навчальної дисципліни

1.1. Мета викладання дисципліни: вивчення математичних та теоретичних основ криптозахисту даних, ознайомлення з предметом, методами та завданнями захисту даних, ознайомлення з загальними принципами захисту мереж і баз даних, ознайомлення з основними методами математичного перетворення інформації та способи її відтворення.

1.2. Основними завданнями вивчення дисципліни є:

– розкрити місце і значення знань з криптології у загальній і професійній освіті людини, з'ясувати психолого-педагогічні аспекти засвоєння предмета, взаємозв'язки курсу криптології з іншими навчальними предметами, зокрема інформатикою, алгеброю і теорією чисел, числовими системами, теорією імовірностей, іншими математичними і нематематичними дисциплінами, розкрити зв'язки класичної симетричної і сучасної асиметричної криптографії, показати теоретичну і практичну значимість методики та застосувань криптографії при розв'язуванні найрізноманітніших гуманітарних, наукових і технічних проблем;

– забезпечити ґрунтовне вивчення і засвоєння студентами тих понять і методів криптології, які можуть бути використані ними при викладання окремих тем шкільних курсів інформатики,

– виховати у майбутніх вчителів творчий підхід до викладання основ інформатики і обчислювальної техніки, математики, зокрема з використанням засобів сучасної інформаційної технології, сформувати знання, вміння і навички, необхідні для самостійного аналізу проблем інформатизації навчального процесу, розвитку логічного і творчого мислення учнів, гуманітаризації освіти,

гуманізації навчання, розвинути здатність і відчуття необхідності постійної самоосвіти, самовдосконалення, наукового пошуку шляхів удосконалення змісту освіти, управління навчальним процесом, формування основ інформаційної і загальної культури учнів, активізації їх пізнавальної діяльності, творчої активності, надання навчальній діяльності дослідницького характеру, практичної значимості результатам навчання. З цієї точки зору важливого значення набуває організація самостійної роботи студентів, їх участь у науково-дослідний роботі кафедр, широке використання в навчальному процесі засобів НІТ, в тому числі і систем штучного інтелекту, для розв'язування задач навчального і дослідницького характеру.

1.3. За результатами вивчення дисципліни у здобувачів повинні бути сформовані такі компетентності:

*загальні**:*** знання математичного апарату сучасної криптології (теорія чисел, теорія конгруенцій, скінченні поля), методики захисту важливої інформацію від несанкціонованого доступу, основні напрямки використання криптографічних методів.

спеціальні: набуття умінь і навичок, пов'язаних ***з*** застосовування механізму шифрування інформації за допомогою існуючих методів шифрування, володіння навичками розв'язування проблемних задач, які вимагають використання криптографічних методів.

На вивчення навчальної дисципліни відведено 180 годин / 5 кредитів ECTS.

2. Інформаційний обсяг навчальної дисципліни

Змістовний модуль 1. *Вибрані питання теорії чисел.*

ТЕМА 1. Теорія подільності
1. Алгоритм Евкліда. Прості числа. Алгоритми визначення простоти.
2. Розподіл простих чисел.

ТЕМА 2. Теорія конгруенцій.
1. Конгруенції. Квадратичні лишки. Первісні корені за простим модулем.
2. Розпізнавання квадратичності і добування квадратних коренів.

ТЕМА 3. Складність функцій та алгоритмів
1. Поняття про складність задач та алгоритмів. Важкооборотні функції.
2. Дискретний логарифм. Складність дискретного логарифмування.

ТЕМА 4. Скінченні поля.
1. Кільце класів лишків. Скінченні поля.
2. Кільце многочленів. Звідність многочленів.

Змістовний модуль 2. ОСНОВИ КРИПТОЛОГІЇ.

ТЕМА 1. Основи класичної криптографії.

1. Проблеми захисту інформації. Основні поняття і терміни. Історичний огляд. Загальна схема системи зв'язку з таємним ключем. Моделі джерел відкритого тексту, ентропія на символ джерела.
2. Теорія Шеннона. Теоретична та практична секретність. Байєсівський підхід у криптоаналізі.

ТЕМА 2. Класичні схеми шифрування.

1. Моноалфавітні підстановки. Методи криптоаналізу. Поліалфавітні системи. Визначення періоду.
2. Перестановки як елемент криптосистем. Роторні системи.

ТЕМА 3. Булеві функції та їх криптографічні властивості.

1. Визначення, класифікація та основні криптографічні властивості булевих функцій.
2. Критерії оцінки криптографічних властивостей булевих функцій.

ТЕМА 4. Системи блочного шифрування.

1. Блочні шифри та принципи їх побудови. Схема OE8. Методи криптоаналізу системи OE8. Система ГОСТ 28147-89.
2. Режими використання блочних алгоритмів. Інші алгоритми блочного шифрування.

ТЕМА 5. Криптографічні властивості випадкових послідовностей та їх оцінка.

1. Різні підходи до визначення випадкової послідовності. Псевдовипадкові послідовності, методи генерації.
2. Статистичні методи оцінки якості випадкових послідовностей. Структурні методи оцінки якості випадкових послідовностей.

ТЕМА 6. Несиметричні криптографічні системи.

1. Схема відкритого розповсюдження ключів Діффі - Хеллмана. Системи шифрування на базі дискретного логарифмування. Система RSA. Інші несиметричні системи.
2. Загальна схема криптосистем з відкритим ключем. Методи генерації простих чисел. Схеми цифрового підпису. Хеш - функції.

ТЕМА 7. Основні криптографічні протоколи.

1. Ідентифікація, автентифікація, механізми підтвердження справжності. 2. Протоколи розподілу секретів, доведення без розголошення, сліпий підпис.

ТЕМА 8. Нові напрямки в криптології.

Криптографічні системи на еліптичних кривих. Імовірнісне шифрування. Квантова криптографія. Багаторівнева криптографія.

3. Рекомендована література

1. Вербіцький О.В. Вступ до криптології. - Львів: Науково-технічна література, 1998.-248с.

2. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.:Единая Европа, 1994. - 564с.

3. Диффи У., Хеллман М. Защищенность и имитостойкость. // ТИИЭР."- 1979.- Т.67,№3.-С.71-109.

4. Месси Дж.Л. Введение в современную криптологию. // ТИИЭР. - 1988. - Т.76,№5.-С.24-42.

5. Саломаа А. Криптография с открытым ключом. - М.: Мир, 1996. - 318с.

6. Шеннон К.З. Теория связи в секретных системах. // В кн.: Шеннон К.З. Работы по теории информации и кибернетике. - М.: ИЛ, 1963. - С.243-332

7. Гери М., Джонсон Д. Вычислительные машины и труднорешаемые задачи.-М.: Мир, 1982.-416с.

8. Биркгоф Г., Барти Т.. Современная прикладная алгебра. - М. Мир, 1976.

9. Нечаев В. И. Злементы криптографии (основи защиты информации). -Москва: Высшая школа, 1999. -109с.

10. Коблиц Н. Курс теории чисел и криптографии. - М.:, 2001.

11. Ященко В. В. Введение в криптографию.

12. Сидельников В. М. Криптография и теория кодирования. - М.:, 2000.

13. Романец Ю. В., Тимофеев П. А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.:, 2001.

4. Форма підсумкового контролю успішності навчання

Залік, залік

5. Засоби діагностики результатів навчання

Поточне оцінювання, виконання індивідуальних завдань.