О:

Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

назва дисципліни	**Основи криптології**
факультет	**фізико-математичний**
кафедра	**методики навчання математики та методики навчання інформатики**
спеціальність	**014 Середня освіта (Інформатика)**
освітня програма	**Середня освіта (Інформатика)**
рівень вищої освіти	**перший (бакалаврський)**

О:

Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

ПІБ викладача	**Кайдан Наталія Володимирівна**
науковий ступінь, вчене звання	**кандидат фізико-математичних наук, доцент** (за кафедрою алгебри)
профайл викладача	**офіційна web-сторінка кафедри** https://ddpu.edu.ua/index.php/kafedra-mnm-ta-mni
e-mail викладача	kaydannv@gmail.com
сторінка курсу в Moodle	http://ddpu.edu.ua:9090/moodle/course/view.php?id=1649
розклад консультацій	**щочетверга з 15^{00} до 16^{00} (аудиторія №502)**

Анотація до дисципліни

Предметом вивчення дисципліни є:

основи криптології, дисципліна присвячена вивченню основ криптології та криптографічного аналізу, що застосовуються до захисту інформації в інформаційних системах.

Міждисциплінарні зв'язки

Для опанування даної дисципліни необхідне вивчення дисциплін: «Математичний аналіз», «Лінійна алгебра», «Дискретна математика», «Інформатика». В свою чергу, дана дисципліна повинна забезпечити ґрунтовну основу для вивчення курсів «Захист інформації», «Математичні основи криптології», «Сучасні методи криптографічного захисту інформації».

Мета вивчення дисципліни

– ознайомлення з основами математичної теорії криптології;
– придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації;
– розуміння суті інформаційних процесів в криптографічних системах;
– розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення;
– застосування комп'ютерів для вирішення завдань шифрування і дешифрування.

О: **Державний вищий навчальний заклад «Донбаський державний педагогічний університет»**

основні завдання: *компетентності*, які будуть сформовані у здобувачів за результатами вивчення:

загальні

Здатність вчитися і оволодівати сучасними знаннями.
Здатність застосовувати знання у практичних ситуаціях.
Знання і розуміння предметної області та розуміння професійної діяльності.

спеціальні

Здатність до організації позакласної й позашкільної роботи з інформатики в закладах загальної середньої освіти (рівень базової середньої освіти).
Здатність використовувати знання наукових фактів, концепцій, теорій, принципів і методів інформатики у практиці навчання інформатики в базовій середній школі.
Здатність застосовувати системні знання з математики в професійній діяльності.
Здатність застосовувати відповідні кількісні математичні, наукові і технічні методи, а також комп'ютерне програмне забезпечення для вирішення професійних завдань.

очікувані результати навчання

Знає основні історичні етапи розвитку предметної області.
Знає та розуміє фізичні, логічні та математичні основи інформаційних технологій.
Знає та розуміє способи двійкового кодування текстової, числової, графічної, звукової та відео інформації.
Знає та розуміє етико-правові засади використання інформаційно-комунікаційних технологій; уміє впроваджувати засоби й методи захисту інформації та безпеки в мережі Інтернет.
Уміє створювати інформаційні моделі, реалізовувати їх засобами інформаційно-комунікаційних технологій, здійснювати дослідження, інтерпретувати, аналізувати та узагальнювати його результати.

О:

Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

Перелік тем – інформаційний обсяг навчальної дисципліни

Тема 1	Основні поняття кріптології.
Тема 2	Класичні шифри перестановки.
Тема 3	Класичні шифри заміни.
Тема 4	Математичні основи кріптографії.
Тема 5	Шифри аналітичних перетворень.
Тема 6	Псевдовипадкові числа.
Тема 7	Шифри з використанням гамування.
Тема 8	Стандарт шифрування даних DES.
Тема 9	Асиметричні кріптосистеми.
Тема 10	Ідентифікація та аутентифікація.
Тема 11	Електронний цифровий підпис.
Тема 12	Управління кріптографічними ключами.
Тема 13	Основи «довгої» арифметики.