Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

назва дисципліни	**Вибрані питання математики, інформатики та методики їх навчання: «Елементи теорії чисел»**
факультет	**фізико-математичний**
кафедра	**методики навчання математики та методики навчання інформатики**
спеціальність	**014 Середня освіта (Математика)**
освітня програма	**Середня освіта (Математика)**
рівень вищої освіти	**перший (бакалаврський)**

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

ПІБ викладача	**Турка Тетяна Вікторівна**
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	tvturka@gmail.com
сторінка курсу в Moodle	http://ddpu.edu.ua:9090/moodle/course/view.php?id=1031
розклад консультацій	**щочетверга з 15^{00} до 16^{00} (аудиторія №503)**

Анотація до дисципліни

Курс присвячений питанням математичних основ криптографії. У ньому розглядаються необхідні розділи теорії чисел, деякі блокові й потокові шифри. Основна увага приділяється криптосистемам з відкритим ключем і першочерговими задачами, які розв’язуються із залученням таких криптографічних алгоритмів, як шифрування даних, цифрові підписи, схеми ідентифікації та ін.

Міждисциплінарні зв’язки

Для опанування даної дисципліни необхідне вивчення дисциплін: «Алгебра», «Дискретна математика», «Теорія чисел», «Числові системи», «Інформатика».

Мета вивчення дисципліни

полягає у вивченні 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

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

загальні

Здатність до самовдосконалення та саморозвитку
Здатність вчитися і оволодівати сучасними знаннями.

спеціальні

Здатність використовувати системні знання з математики, педагогіки, методики навчання математики, історії їх виникнення та розвитку.
Здатність ефективно застосувати ґрунтовні знання змісту шкільної математики.
Здатність аналізувати математичну задачу, розглядати різні способи її розв'язування.
Здатність ефективно планувати та організовувати різні форми позакласної роботи з математики.
Здатність розв'язувати задачі шкільного курсу математики різного рівня складності та формувати відповідні уміння в учнів.
Здатність забезпечити умови для набуття учнями досвіду застосування математичних знань та умінь, формування їхнього позитивного ставлення до вивчення систематичних курсів алгебри та геометрії.
Здатність забезпечувати розвиток прийомів розумової діяльності та просторової уяви учнів, усвідомлюючи й реалізуючи специфічні можливості процесу навчання математики для розвитку логічного та алгоритмічного мислення.

очікувані результати навчання

Здатний продемонструвати та застосувати знання з математики.
Розуміє і здатний застосувати основні теоретичні положення методики навчання математики на рівні, необхідному для досягнення інших результатів освітньої програми.
Здатний виокремлювати компоненти професійної (педагогічної або математичної) задачі, пояснювати їх взаємозв'язки та розробляти, пропонувати різні шляхи розв'язування задачі.
Уміє розв'язувати задачі різних рівнів складності шкільного курсу математики.
Здатний спроектувати і провести на належному рівні урок математики в основній школі.
Володіє методикою підготовки учнів до математичних олімпіад та турнірів.
Здатний виявляти помилки та недоліки в математичних знаннях та уміннях, в логіці міркувань, пояснювати різницю між фактами і наслідками.
Здатний оцінювати, реконструювати та модифікувати власні професійні знання та уміння, беручи на себе відповідальність за прийняття рішень.
Здатний проектувати конкретні напрями власного професійного розвитку та аргументувати відповідальне ставлення до нього як до неперервного процесу.

Перелік тем – інформаційний обсяг навчальної дисципліни

Тема 1	Теорія подільності.
Тема 2	Теорія конгруенцій
Тема 3	Складність функцій та алгоритмів.
Тема 4	Скінченні поля.
Тема 5	Основи класичної криптографії.
Тема 6	Класичні схеми шифрування.
Тема 7	Булеві функції та їх криптографічні властивості
Тема 8	Системи блочного шифрування.
Тема 9	Криптографічні властивості випадкових послідовностей та їх оцінка.
Тема 10	Несиметричні криптографічні системи.
Тема 11	Основні криптографічні протоколи.
Тема 12	Нові напрямки в криптології.

Ос