ПРЕЗЕНТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Освітня програма, рівень вищої освіти:		Прикладна математика Бакалавр					
Статус дисципліни:		Нормативна					
Кредити ECTS	4	**Навч. рік:**	2020-21	**Рік навчання**	3	**Тижні**	14
Кількість годин	120	**Кількість змістових модулів**[1]	3	**Лекційні заняття – 14** **Практичні заняття – 28** **Самостійна робота – 78**			
Вид контролю:		залік					
Посилання на курс в Moodle			https://moodle.znu.edu.ua/course/view.php?id=6888				
Консультації: *час консультація за розкладом консультацій (розміщено на стенді кафедри) Moodle (форум курсу), Zoom*							

ОПИС КУРСУ

Курс є необхідною складовою частиною базової теоретичної та практичної підготовки студента, що навчається за освітньою програмою «прикладна математика», а також є основою для подальшого вивчення спеціальних дисциплін.

Програму курсу укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Курс «Математичні основи криптографії» складається з 3-х змістових модулів: 1.Основні поняття криптографії та захисту інформації. Математичні основи; 2. Криптосистеми на базі кілець; 3.Асиметричні криптосистеми на базі полів.

***Основною метою** викладання курсу є отримання компетентностей в області криптографії, криптографічного захисту інформації.*

*Основними **завданнями** курсу є: надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації; формування у студентів категоріальних понять з основ математики симетричної та асиметричної криптографії; формування у студентів умінь обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів; стимулювання студентів до активної аналітико-пошукової роботи.*

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

*У разі успішного завершення курсу студент **зможе**:*

- *застосовувати на практиці набуті знання про джерела і способи дії загроз на об'єкти інформаційної безпеки ;*
- *використовувати фундаментальні та спеціальні знання з математики до розв'язання прикладних задач в галузі шифрування, кодування даних, захисту інформації, кібербезпеки;*
- *володіти алгоритмами шифрування інформаційних текстів та застосовувати їх;*
- *працювати з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів;*
- *створювати засобами стандартного програмного забезпечення елементи захисту інформації.*

Використання новітніх програмних засобів під час виконання практичних та лабораторних завдань розвине як загальні, так і професійні компетенції слухачів.

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, плани занять, методичні рекомендації до виконання індивідуальних та практичних завдань, групових творчих проектів розміщені на платформі Moodle: https://moodle.znu.edu.ua/course/view.php?id=6888