АЛГОРИТМИ ШИФРУВАННЯ ТА ЗАХИСТУ ДАНИХ

Викладач: кандидат фізико-математичних наук, доцент, Зіновєєв Ігор Валерійович
Кафедра: Загальної математики, І корпус, ауд. 21а
E-mail: zinoveev@znu.edu.ua
Телефон: (061) 289-12-54
Інші засоби зв'язку: Moodle (форум курсу, приватні повідомлення)

Освітня програма, рівень вищої освіти:	Інформаційні системи та штучний інтелект, Магістр						
Статус дисципліни:	Обов'язкова						
Кредити ECTS	3	**Навч. рік:**	2023-24 1 семестр	**Рік навчання**	1	**Тижні**	10
Кількість годин	90	**Кількість змістових модулів**	4	**Лекційні заняття – 10** **Лабораторні заняття – 20** **Самостійна робота – 60**			
Вид контролю:	Екзамен						
Посилання на курс в Moodle	https://moodle.znu.edu.ua/course/view.php?id=14746						
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 «Інформаційні системи та штучний інтелект», а також є основою для подальшого вивчення спеціальних дисциплін.

Курс «Алгоритми шифрування та захисту даних» складається з 4-х змістових модулів:

1. Основні поняття криптографії та захисту інформації. Історичний огляд криптографічних методів захисту інформації. Класичні алгоритми симетричного шифрування.;
2. Симетрична та асиметрична криптографія. Класичні алгоритми асиметричного шифрування. Алгоритми на основі мереж Фейстеля та SP-мереж.;
3. Сучасні криптографічні методи захисту інформації. Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі блокового шифрування.
4. Алгоритми захисту даних. Електронний цифровий підпис. Алгоритми та технології аутентифікації.

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

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 даних;
- 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 даних.

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

Змістове наповнення курсу, що викладається на лекційних і лабораторних заняттях та засвоюється студентом під час самостійної роботи, забезпечує набуття **компетентностей**:

ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.
СК 4. Здатність розробляти математичні, інформаційні та комп'ютерні моделі об'єктів і процесів інформатизації.
СК 6. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки
СК 10. Здатність застосовувати методи захисту даних в інформаційних системах

Програмні результати навчання:

РН 1. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.
РН 10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації
РН 12. Розробляти та використовувати методи штучного інтелекту
РН 13. Розробляти та використовувати алгоритми шифрування та захисту даних в інформаційних системах

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=14746