Дисципліна «Криптографічні методи захисту інформації»

Лектор, науковий ступінь, вчене звання, посада	Фесенко А.О., канд. техн. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання	Здобуття теоретичних знань та практичних навичок математичного аналізу сучасних криптоалгоритмів симетричного та асиметричного методів шифрування інформації, роботи змережею Фейстеля та створенню алгоритмів на її основі, роботи з криптопровайдерами сучасних операційних систем та їх використання у практичному створенні систем захисту інформації, програмної реалізації зазначених методів шифрування, можливості комбінації основних методів захисту інформації та створенню власних алгоритмів.
Зміст	Історія розвитку засобів криптографічного захисту інформації від Стародавнього світу до сучасності. Загальні визначення та поняття криптографії. Теорія криптографічних систем. Мережа Фейстеля, конструкція блочного шифру, сучасні шифри, що базуються на ній. Симетричні системи шифрування інформації. Асиметричні системи шифрування інформації: RSA, DES та інші. Система обміну ключами Діффі-Хелмана. Криптосистеми Мессі-Омури та Ель-Гамаля для передачі повідомлень. Електронний цифровий підпис. Основні світові та вітчизяні криптостандарти. Алгоритми та їх практична програмна реалізація. Призначення та особливості застосування CryptoAPI, його основні функції. Функції та призначення криптопровайдерів, основні криптопровайдери Microsoft. Аналіз існуючого програмного забезпечення, що використовується для криптографічного захисту інформації: PGP, ACE та інші.