МЕТОДИ АНАЛІЗУ ТА ПОБУДОВИ КРИПТОСИСТЕМ

Тип дисципліни	Обов'язкова
Освітній рівень	Другий (магістерський)
Мова викладання	Українська
Семестр	Другий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Денна

Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати*, *інтегрувати*, *розробляти* та *удосконалювати* сучасні інформаційні технології для провадження інноваційної діяльності в сфері інформаційної безпеки та/або кібербезпеки, криптографічного захисту інформації у кіберпросторі та вирішення складних інженерно-прикладних задач інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик; *досліджувати* та *розробляти* засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури; *досліджувати*, *розробляти*, *впроваджувати* та *використовувати* методи та засоби криптографічного захисту інформації бізнес/операційних процесів, а також *аналізувати* і *надавати* оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

Зміст навчальної дисципліни. Огляд основних задач реалізації криптографічних систем. Дослідження і розробка криптографічних протоколів. Концептуальні підходи до створення інфраструктури відкритих ключів. Створення центру сертифікації ключів. Дослідження та розробка малоресурсних криптографічних систем. Дослідження та застосування методів криптоаналізу систем. Підхід до побудови криптостійких алгоритмів та протоколів. Криптосистеми в хмарних технологіях.

Пререквізити – вихідна

Кореквізити – проєктування та супровід систем інформаційної безпеки

Запланована навчальна діяльність: лекції – 18 год., лабораторні заняття – 36 год., самостійна робота – 96 год.; разом – 150 год.

Форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, проблемні, контекстні, тренінгові, навчання у співпраці, моделювання, застосування інформаційно-комп'ютерних технологій.

Форми оцінювання результатів навчання: захист лабораторних робіт, письмова контрольна робота, підсумковий контрольний захід.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». Тернопіль. 2020. 380 с.
2. Досконала форма системи залишкових класів: методи побудови та застосування: монографія/ М. М. Касянчук. Тернопіль: ТНЕУ, 2019. 223 с.
3. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
4. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua.
5. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладач: д.т.н., доцент Касянчук М.М.