ТЕОРІЯ ТА ПРОЄКТУВАННЯ ЗАХИЩЕНИХ СИСТЕМ

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

Результати навчання. 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, технічного 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 технічного 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. Визначення комплексу методів та засобів захисту інформації в залежності від задачі, які покладаються на проектовану систему. Аналіз підходів до розробки захищених операційних систем. Організаційні засади, методи та засоби забезпечення безпеки мережевої інфраструктури. Дослідження та проєктування технологій Honeypot та Deception. Захист передачі конфіденційних повідомлень. Захист від витоку конфіденційних файлів. DLP-системи. Складові безпеки веб-ресурсів. Концептуальні засади інформаційної безпеки України. Основні підходи до розробки гарантовано захищених інформаційних систем. Забезпечення гарантій виконання вимог політик безпеки. Аутсорсинг інформаційної безпеки.

Пререквізити – вихідна

Кореквізити – проєктування та супровід систем інформаційної безпеки

Запланована навчальна діяльність: лекції – 17 год., лабораторні заняття – 34 год., самостійна робота – 99 год.; разом – 150 год.

Форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, проблемні, контекстні, навчання у співпраці, 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. Технології забезпечення безпеки мережевої інфраструктури / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с.
2. Основи кібербезпеки та кібероборони: підручник/ Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.
3. Захищені операційні системи: Конспект лекцій /Укладачі Ю. В. Баришев, О. В. Дмитришин, В. А. Каплун. Вінниця: ВНТУ, 2018. 161 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.

Викладачі: д.т.н., професор Савенко О.С., д.т.н., професор Андрощук О.С.