## Загальні відомості про дисципліну

| | |
|---|---|
| Назва дисципліни | **Криптографічні методи захисту інформації** |
| Освітній ступінь | магістр |
| Галузь знань | 12 Інформаційні технології |
| Спеціальність | 124 Системний аналіз |
| Освітня програма | Інформаційні технології та бізнес-аналітика (Data Science) |
| Навчальний рік | 2021-2022,2022-2023 |
| Семестр | 1-3 |
| Факультет | ФІТ |
| Курс | 1,2 |
| Підсумковий контроль | екзамен |

## Місце дисципліни в освітній програмі

| | |
|---|---|
| Фахові компетентності | СК1. Здатність інтегрувати знання та здійснювати системні дослідження, застосовувати методи математичного та інформаційного моделювання складних систем та процесів різної природи.<br>СК2. Здатність проєктувати архітектуру інформаційних систем.<br>СК4. Здатність оцінювати ризики, розробляти алгоритми управління ризиками в складних системах різної природи.<br>СК8. Здатність розробляти і реалізовувати наукові та прикладні проєкти в галузі інформаційних технологій та дотичні до неї міждисциплінарні проєкти.<br>СК9. Здатність здійснювати захист прав інтелектуальної власності, комерціалізацію результатів досліджень та інновацій.<br>СК10. Здатність до самоосвіти та професійного розвитку. |
| Програмні результати навчання | РН1. Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері системного аналізу та інформаційних технологій і є основою для оригінального мислення та проведення досліджень.<br>РН2. Будувати та досліджувати моделі складних систем і процесів застосовуючи методи системного аналізу, математичного, комп'ютерного та інформаційного моделювання.<br>РН10. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефахівців, зокрема до осіб, які навчаються<br>РН11. Вільно презентувати та обговорювати усно і письмово результати досліджень та інновацій, інші питання професійної діяльності державною та англійською мовами. |
| Передумови вивчення дисципліни | знання:<br>• безпека баз даних;<br>• безпека операційних систем;<br>• основи кіберпезпеки;<br>• правове забезпечення інформаційної безпеки держави;<br>• теорії чисел;<br>• теорії ймовірностей та математичної статистики;<br>• математичного аналізу;<br>• комп'ютерної дискретної математики;<br>• економічної інформатики (стандартне програмне забезпечення персональних комп'ютерів);<br>• архітектури комп'ютера;<br>• захист систем електронних комунікацій;<br>• об'єктно-орієнтованого програмування;<br>• іноземної мови за професійним спрямуванням;<br>вміння: вільно працювати:<br>• з офісними додатками Microsoft;<br>• з хмарними сервісами Office 365;<br>• з технологіями розробки та тестуванням ПЗ;<br>• з пошуковою системою Google. |

## Забезпечення дисципліни

| | |
|---|---|
| Основні джерела | Основи криптографічного захисту інформації : підручник / авт.: Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2011. – 94 с. |
| | Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с. |
| | Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с. |
| | Бабак В. П. Теоретичні основи захисту інформації : підручник // Бабак В. П. – Книжкове видавництво НАУ, 2008. – 752 с. |

## Аудиторні заняття

Лектор - к. т. н., доц. Савченко Т. В.

| № | Тема лекції |
|---|---|
| 1 | Історичний огляд криптографічних методів захисту інформації |

| | |
|---|---|
| 2 | Шифри та їх види |
| 3 | Сучасні криптографічні методи захисту інформації |
| 4 | Симетричні та асиметричні методи шифрування |
| 5 | Криптографія та криптоаналіз. |
| 6 | Криптографічні протоколи |
| 7 | Електронний цифровий підпис та поділ секрету |
| 8 | Протоколи аутентифікації (ідентифікації) |
| 9 | Управління криптографічними ключами |
| 10 | Стеганографічний захист інформації |
| | **Загальний обсяг лекцій: 20 год** |

Викладач - к. т. н., доц. Савченко Т. В.

| № | Тема практичного заняття | Бали |
|---|---|---|
| 1 | Шифрування.Шифр Цезаря | 10 |
| 2 | Частотний аналіз криптограм | 10 |
| 3 | Блокові шифри | 10 |
| 4 | Блочне шифрування даних ДСТУ ГОСТ 28147:2009 | 10 |
| 5 | Аутентифікація доступу | 10 |
| 6 | Криптосистеми | 10 |
| 7 | Цифровий підпис | 10 |
| 8 | Криптографічні ключи для захисту інформації | 10 |
| 9 | Проектування систеи безпеки на основі технології блокчейн | 10 |
| 10 | Стенографічний канал | 10 |
| | **Загальний обсяг практичних занять 20 год** | **100** |

## Політика дисципліни

| | |
|---|---|
| Відвідування занять | Відвідування лекційних та практичних занять з дисципліни є обов'язковим для всіх студентів |
| Відпрацювання пропущених занять | Студент, який пропустив практичне заняття, самостійно вивчає матеріал за наведеними в силабусі джерелами, виконує завдання і здає його викладачу. За умови неповажної причини |
| Допуск до екзамену | Згідно з Положенням про організацію освітнього процесу всі студенти допускаються до іспиту |
| Підсумкова модульна оцінка | Підсумкова модульна оцінка за семестр є сумою оцінок, отриманих студентом за виконання практичних завдань. Максимальна модульна оцінка становить 100 балів.<br>Студент, який отримав підсумкову модульну оцінку менше за 20 балів, при будь-якій екзаменаційній оцінці не може отримати задовільну підсумкову оцінку з дисципліни і буде ліквідовувати академічну заборгованість під час додаткової сесії. |
| Екзаменаційна оцінка | Максимальна екзаменаційна оцінка становить 100 балів |
| Підсумкова оцінка з дисципліни | Підсумкова оцінка з дисципліни обчислюється як середнє арифметичне підсумкової модульної та екзаменаційної оцінки. |