Загальні відомості про дисципліну

Назва дисципліни	**Безпека Інтернет ресурсів**
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	СК2. Здатність проєктувати архітектуру інформаційних систем. СК3. Здатність розробляти системи підтримки прийняття рішень та рекомендаційні системи. СК7. Здатність управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів. СК13. Здатність розробляти і впроваджувати моделі задач інтелектуального аналізу даних засобами комп'ютерного моделювання.
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. РН4. Розробляти та застосовувати методи, алгоритми та інструменти прогнозування розвитку складних систем і процесів різної природи. РН5. Використовувати міри оцінювання ризиків та застосовувати їх при аналізі багатофакторних ризиків в складних системах. РН8. Здійснювати ідентифікацію та оцінювання параметрів математичних моделей об'єктів керування.
Передумови вивчення дисципліни	Знати: – вимоги нормативних документів України по безпеці в глобальних мережах; – основні положення, організацію та моделі систем захисту інтернет-ресурсів; – класифікацію атак на інтернет-ресурси та міри протидії; – технологію та правила мережевої аутентифікації ресурсів і користувачів; – організацію і правила безпеки при роботі в глобальних мережах; – технологію та правила експлуатації міжмережевих екранів; – основи технології віртуальних захищених мереж VPN; – основи забезпечення захисту в мережевих протоколах передачі. Вміти: – визначати загрози інтернет-ресурсам; – здійснювати моніторинг існуючих мережевих з'єднань і відкритих портів у комп'ютерній мережі; – організувати захищений видалений доступ до інтернет-ресурсів; – аналізувати захищеність інтеренет-ресурсів та виявляти атаки на них; – встановлювати і налагоджувати міжмережеві екрани; – реєструвати порушення режиму безпеки і складати звіти; – розробляти індивідуальні системи управління доступом і захистом інтернет-ресурсів; – створювати захист за допомогою програмних засобів; – організовувати безпечну роботу в глобальних мережах; – використовувати VPN-рішення для побудови захищених мереж; – управляти засобами безпеки інтеренет-ресурсів.

Забезпечення дисципліни

Основні джерела	Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник Чернівці.- Видавничий дом «Родовід», 2017. – 471с.
	Кавун С.В. Інформаційна безпека. Навчальний посібник Харків: ХНЕУ, 2016. - 213с.
	Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль – К., 2015. – 435 с., іл.160.
	Єсін В. І. Безпека інформаційних систем і технологій : навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2015. – 632с.
	КавунС. В. Інформаційна безпека підручник / С. В. Кавун. – Харків : ХНЕУ, 2016. – 368с.

Аудиторні заняття

Лектор - к.т.н., доц. Звєрєв В. П.

№	Тема лекції
1	Основи мережевої безпеки.
2	Основи мережевої безпеки.
3	Технології фільтрації мережевого трафіку.
4	Технології фільтрації мережевого трафіку.
5	Основи технології віртуальних приватних мереж.
6	Основи технології віртуальних приватних мереж.
7	Протоколи мережевої безпеки.
8	Безпека інтернет-ресурсів на прикладному рівні.
9	Аналіз безпеки інтернет-ресурсів.
10	Аналіз безпеки інтернет-ресурсів.
	Загальний обсяг лекцій: 20 год

Викладач - к.т.н., доц. Звєрєв В. П.

№	Тема практичного заняття	Бали
1	Засоби мережного аудиту	10
2	Організація мережевої безпеки за допомогою міжмережевого екрана Outpost Firewall	16
3	Організація мережевої безпеки при використанні засобів виявлення мережевих атак	14
4	Організація мережевої безпеки при використанні засобів VPN	7
5	Організація мережевої безпеки при використанні засобів VPN	7
6	Організація шифрування трафіку при використанні утиліти IPSec	8
7	Організація шифрування трафіку при використанні утиліти IPSec	8
8	Організація безпеки механізму мережевої автентифікації	16
9	Побудова віртуальної машини з ОС Windows	7
10	Побудова віртуальної машини з ОС Windows	7
	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.

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. 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.