Силабус курсу

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ступінь вищої освіти - бакалавр
Галузь знань 12 "Інформаційні технології"
Спеціальність – 122 «Комп'ютерні науки»
Освітньо-професійна програма: «Штучний інтелект»

Рік навчання: IV**, Семестр:** 7

Кредитів: 5 **Мова викладання:** українська

Керівник курсу

ПІП	**к.т.н., доцент Биковий Павло Євгенович**
Контактна інформація	pb@wunu.edu.ua

Опис дисципліни

Метою вивчення дисципліни «Методи та засоби забезпечення інформаційної безпеки» є формування знань, умінь і навичок у студентів щодо основних понять та категорій комп'ютерної безпеки, вивчення принципів побудови комплексних систем захисту інформації, розробки, дослідження та застосування механізмів захисту інформації, що ґрунтуються на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій.

Структура курсу

Години (лек./лаб.)	Тема	Результати навчання	Завдання
4/-	Тема 1. Поняття інформаційної безпеки та захисту інформації.	Знати основні складові інформаційної безпеки, важливість і складність проблеми інформаційної безпеки. Розуміти загрози приступності, цілісності, конфіденційності. Знати шкідливе програмне забезпечення.	Питання
2/-	Тема 2. Рівні забезпечення інформаційної безпеки	Знати законодавчий рівень, адміністративний рівень, процедурний рівень, програмно технічний рівень.	Питання
4/-	Тема 3. Технічні канали витоку інформації. Методи та засоби їх блокування.	Знати загальний підхід до технічного захисту інформації. Вміти застосовувати організаційно-технічні заходи. Знати методи несанкціонованого зняття інформації. Знати класифікацію каналів витоку інформації. Знати засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації.	Питання
2/2	Тема 4. Програмні засоби загрози інформаційній безпеці.	Знати поняття перехоплювачів паролів, троянських програм. Вміти використовувати утиліти скритого адміністрування. Знати інформацію про	Питання, лабораторна робота

		комп'ютерні віруси. Вміти використовувати антивірусні програми, пакетні фільтри.	
4/2	Тема 5. Вступ до криптографії. Класичні техніки шифрування	Знати шифри перестановок (зокрема, шифр частоколу, матричний шифр, шифр Першої світової війни - ADFGVX). Знати шифри підстановок (зокрема, шифр Цезаря, шифр пар, квадрат Полібія, шифр Play-Fair, шифр Віженера). Вміти використовувати елементи теорії зв'язку в секретних системах	Питання, лабораторна робота
2/2	Тема 6. Сучасні криптосистеми	Знати симетричні криптосистеми (зокрема, блокові шифри, особливості стандарту DES, особливості стандарту ГОСТ 28147-89, міжнародний стандарт шифрування даних IDEA, особливості стандарту AES. потокові шифри). Знати асиметричні криптосистеми (зокрема, криптосистема RSA. криптосистема Ель-Гамаля).	Питання, лабораторна робота
2/2	Тема 7. Електронний цифровий підпис	Знати функції хешування, алгоритми MD2, MD4, MD5, алгоритм SHA-1. Вміти використовувати алгоритми електронного цифрового підпису DSA, стандарти цифрового підпису ГОСТ Р 34.10-94 і ГОСТ Р 34.10-2001	Питання, лабораторна робота
4/2	Тема 8. Елементи криптоаналізу	Знати про атаки на криптосистему RSA. Знати елементи частотного, різницевого та лінійного криптоаналізу.	Питання, лабораторна робота
2/2	Тема 9. Огляд способів захисту на рівні IP.	Знати сфери застосування IPSec. Вміти здійснювати захист електронної пошти. Знати систему PGP, стандарт S/MIME.	Питання, лабораторна робота
4/2	Тема 10. Захист у Web.	Знати проблеми захисту у Web. Вміти здійснювати захист потоку даних у Web. Знати протоколи SSL та TLS, протокол захищених електронних транзакцій (SET), основні засади роботи SNMP, архітектуру SNMP.	Питання, лабораторна робота

Літературні джерела

Основна література

1. Вишня В. Б., Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки: навч. посібник. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2020. 128 с.
2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.
4.Остапов С.Е., Євсеєв С.П., Король О.Г.. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: «Новий Світ-2000», 2020 . 678 с.

Додаткова література

1. Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography, 3rd Edition. Chapman and Hall/CRC. 2020, 628 p.
2. Daswani, N., & Elbayadi, M. Big Breaches: Cybersecurity Lessons for Everyone. 1st ed. Apress. 2021, 331 p.
3. Derek Fisher. Application Security Program Handbook: A guide for software engineers and team leaders. Manning. 2022, 296 p.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Модуль 1		Модуль 2	Модуль 3
40 %	40%	5 %	15 %
Поточне оцінювання	Модульний контроль	Тренінг	Самостійна робота
Середня оцінка за виконання та захисту лабораторних робіт	Модульна контрольна робота (20 тестів, 1 практичне завдання)	Середня оцінка за виконання 3 завдань під час тренінгу	Оцінка за виконання наскрізного завдання для самостійної роботи

Шкала оцінювання:

За шкалою ЗУНУ	За національною шкалою	За шкалою ECTS
90-100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)