Міністерство освіти і науки України

Національний аерокосмічний університет ім. М.Є. Жуковського
"Харківський авіаційний інститут"

Кафедра математичного моделювання та штучного інтелекту (№304)

ЗАТВЕРДЖУЮ»

Голова НМК

_____ Д.М. Крицький
(підпис) (ініціали та прізвище)

«_31_» _____08_____ 2021 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і назва галузі)

Спеціальність: 122 «Комп'ютерні науки»
(код та найменування спеціальності)

Освітня програма: «Інтелектуальні системи та технології»
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Харків 2021 рік

Робоча програма «Захист інформації» для студентів
(назва навчальної дисципліни)
для студентів за спеціальністю: 122 «Комп'ютерні науки»
освітньою програмою: «Інтелектуальні системи та технології»

«27» серпня 2021 р. – 9 с.

РОЗРОБНИК ПРОГРАМИ:
Чумаченко Д.І., доцент кафедри 304, к. т. н., доцент _____
(прізвище та ініціали, посада, наукова ступень та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри математичного моделювання та штучного інтелекту
(назва кафедри)
Протокол № 2 від «27» серпня 2021 р.

Завідувач кафедри д.т.н., доц. _____ А. Г. Чухрай
(наукова ступінь та вчене звання) (підпис) (ініціали та прізвище)

Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="14">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальність
122 «Комп’ютерні науки»
(код та найменування)

Освітня програма
«Інтелектуальні системи та технології»
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td colspan="2">Цикл загальної підготовки</td></tr>
<tr><td>Кількість модулів – 1</td><td colspan="2">Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td colspan="2">2021/ 2022</td></tr>
<tr><td>Індивідуальне завдання -</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150
денна – 60/150</td><td colspan="2">8-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 3,75
самостійної роботи студента – 5,625</td><td colspan="2">24 годин</td></tr>
<tr><td colspan="2">Практичні, семінарські[1)]</td></tr>
<tr><td colspan="2">36 годин</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td colspan="2">-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td colspan="2">90 годин</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">залік</td></tr>
</table>

Примітка

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання – 60/90.

2. Мета та завдання навчальної дисципліни

.

Мета – навчання студентів принципам побудови систем захисту інформації на основі використання алгоритмів симетричної та несиметричної криптографії, МАС-кодів та хеш-функцій щодо забезпечення аутентичності, цілісності та конфіденціальності інформації в інформаційних системах.

Завдання – оволодіти знаннями та вміннями, які створять теоретичний і практичний фундамент, необхідний для аналізу загроз виникаючих при зберіганні, обробленні та передачі інформації; побудові системи захисту інформації на основі використання методів традиційної криптографії та криптографії з відкритим ключем.

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких **компетентностей**:

ЗК4. Здатність до абстрактного мислення, аналізу та синтезу на відповідних рівнях.

ЗК9. Креативність, здатність до системного мислення.

ЗК20. Здатність аналізувати та синтезувати науково-технічну, природничо-наукову та загальнонаукову інформацію.

ФК4. Базові знання в області системних досліджень і вміння застосовувати їх під час управління ІТ-проектами, здійснення моделювання систем, проведення системного аналізу об’єктів інформатизації, прийняття рішень, розробки методів і систем штучного інтелекту.

Програмні результати навчання:

ПРН17. Знання теоретичних і практичних основ методології системного аналізу для дослідження складних міждисциплінарних проблем різної природи, методів формалізації системних завдань, що мають суперечливі цілі, невизначеності та ризики, уміння вирішувати практичні науково-технічні та соціально-економічні завдання міждисциплінарного характеру.

Міждисциплінарні зв'язки: алгебра та геометрія, математичний аналіз, теорія імовірностей та математична статистика, теорія алгоритмів та математична логіка, алгоритми і структури даних, методи обчислень, програмування та алгоритмічні мови, паралельні та розподілені обчислювання, проектування програмних систем, системи та методи прийняття рішень.

3. Програма навчальної дисципліни

Змістовий модуль 1

Тема 1. Основні поняття криптографії

Визначаються предмет і завдання криптографії, формулюються основоположні визначення курсу і вимоги до криптографічних систем захисту інформації, дається історична довідка про основні етапи розвитку криптографії як науки. Також розглядається приклад найпростішого шифру, на основі якого пояснюються сформульовані поняття і тези.

Тема 2. Найпростіші методи шифрування із закритим ключем

Розглядається загальна схема симетричного шифрування, а також дається класифікація найпростіших методів симетричного шифрування. Опис кожного із зазначених в класифікації шифрів супроводжується прикладом

Тема 3. Принципи побудови блокових шифрів з закритим ключем. Алгоритми DES і AES

Розглядаються принципи побудови сучасних блокових алгоритмів: операції, які використовуються в блокових алгоритмах симетричного шифрування; структура блочного алгоритму; вимоги до блокового алгоритму шифрування. Дається поняття мережі Фейстеля. Крім того в цій лекції пояснюється, що таке алгоритм DES "дворазовий DES", атака "зустріч

посередині" і способи її усунення. У цій же лекції коротко розглядається новий стандарт США на блоковий шифр - алгоритм Rijndael.

Тема 4. Режими роботи блокових алгоритмів. Алгоритм криптографічного перетворення даних ГОСТ 28147-89. Криптографічні хеш-функції

Розглянуто вітчизняний стандарт на блоковий алгоритм шифрування. У лекції докладно розглядається структура ГОСТ 28147-89, а також режими шифрування даних з використанням алгоритму криптографічного перетворення даних ГОСТ 28147-89.

Модульний контроль

Змістовий модуль 2

Тема 5. Потокові шифри і генератори псевдовипадкових чисел

Шифрування при передачі даних в режимі реального часу. Сформульовано принципи використання генераторів псевдовипадкових ключів при потоковому шифруванні. Розглядаються деякі найпростіші генератори псевдовипадкових чисел: лінійний конгруентний, генератор за методом Фібоначчі з запізненням, генератор псевдовипадкових чисел на основі алгоритму BBS. Опис кожного з алгоритмів супроводжується прикладом, в якому пояснюються особливості використання того чи іншого методу генерації псевдовипадкових чисел.

Тема 6. Криптографія з відкритим ключем

Асиметрична криптографія. Які математичні функції називаються односторонніми і як вони використовуються для шифрування, формування секретних ключів і цифрового підпису на електронних документах. Викладені найбільш відомі криптографічні алгоритми з відкритим ключем: RSA, алгоритм Діффі-Хеллмана, алгоритм Ель-Гамаля. Опис кожного з алгоритмів супроводжується докладним прикладом. Сформульовані принципи роботи криптографічних систем на еліптичних кривих.

Тема 7. Електронний цифровий підпис

Основні підходи до формування цифрового підпису на основі різних алгоритмів з відкритим ключем. Крім того, розглядаються вітчизняні та зарубіжні стандарти на алгоритми цифрового підпису, що застосовуються в даний час.

Тема 8. Цілком таємні системи. Шифрування, завадостійке кодування і стиснення інформації

Основні ідеї теорії Шеннона, дізнаємося, як розраховуються ентропія і невизначеність повідомлень, норма мови, надмірність повідомлень і відстань єдиності шифру. Сформульовані основні підходи до використання завадостійких кодів і алгоритмів стиснення даних, необхідних на практиці.

Модульний контроль

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	денна форма				
	усього	у тому числі			
		л	п	лаб	с.р.
Модуль 1					
Змістовий модуль 1.					
Тема 1. Основні поняття криптографії	18	2	4	–	12
Тема 2. Найпростіші методи шифрування із закритим ключем	18	4	4	–	10
Тема 3. Принципи побудови блокових шифрів з закритим ключем. Алгоритми DES і AES	16	2	4	–	10
Тема 4. Режими роботи блокових алгоритмів. Алгоритм криптографічного перетворення даних ГОСТ 28147-89. Криптографічні хеш-функції	20	4	6	–	10
Разом за змістовим модулем 1	72	12	18		42
Модуль 2					
Змістовий модуль 2.					
Тема 5. Потокові шифри і генератори псевдовипадкових чисел	16	2	4	–	10
Тема 6. Криптографія з відкритим ключем	20	4	4	–	12
Тема 7. Електронний цифровий підпис	20	2	4	–	14
Тема 8. Цілком таємні системи. Шифрування, завадостійке кодування і стиснення інформації	22	4	6	-	12
Разом за змістовим модулем 1	78	12	18		48
Усього годин	150	24	36	0	90

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1		
2		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Симетричні криптосистеми. Підстановка Цезаря.	4
2	Симетричні криптосистеми	4
3	Програмна реалізація шифру DES	4
4	Український стандарт шифрування ГОСТ 28147-89	4
5	Вивчення псевдовипадкових генераторів	4
6	Генерація простого великого числа	4
7	Обмін ключами за схемою Діффі-Хеллмана	4
8	Алгоритм шифрування RSA	4
9	Програмна реалізація електронних цифрових підпис	4
	Разом	36

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Програмна реалізація шифрів підстановки	8
2	Класичні алгоритми симетричного шифрування	8
3	Програмна реалізація шифру AES	8
4	Режими шифрування алгоритму ГОСТ 28147-89	8
5	Програмна реалізація псевдовипадкових алгоритмів	8
6	Генерація чисел	10
7	Обмін ключами алгоритмом RSA	10
8	Обмін ключами алгоритмом Ель-Гамаля	10
9	Реалізація завадостійких кодів	10
10	Реалізація алгоритмів стиснення даних	10
	Разом	90

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, індивідуальні консультації (при необхідності), самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники), проведення олімпіад.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, фінальний контроль у вигляді екзамену.

12. Розподіл балів, які отримують студенти (залік)

Поточне тестування і самостійна робота									Сума	Підсумковий тест (залік) у разі відмови від балів поточного тестування та за наявності допуску до заліку
Змістовий модуль 1				Змістовий модуль 2				Індивідуальне завдання		
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8			
12	12	12	14	12	12	12	14		100	100

Т1, Т8 – теми змістових модулів

Шкала оцінювання: національна та ECTS

Сума балів за	Оцінка	Оцінка за національною шкалою

всі види навчальної діяльності	ECTS	для екзамену, курсового проекту (роботи), практики	для заліку
90-100	**A**	відмінно	зараховано
83-89	**B**	добре	
75-82	**C**		
68-74	**D**	задовільно	
60-67	**E**		
01-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

13. Методичне забезпечення

1. Чумаченко Д.І. Захист інформації в інформаційно-компьютерних системах : навч. посіб. до лаб. практикуму / Д. І. Чумаченко ; М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харк. авіац. ін-т". - Харків. - Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харк. авіац. ін-т", 2017. - 66 с . - http://library.khai.edu/library/fulltexts/metod/

14. Рекомендована література

Базова

1. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.
2. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
3. Домарев В. В. Безопасность информационных технологий: Системный подход: - К.: ООО "ТИД ДС", 2004. – 992с.
4. Конев И. Р., Беляев А. В. Информационная безопасность предприятия.- СПб.: БХВ - Петербург, 2003, 752с.: ил.

Допоміжна

1. Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. Основы информационной безопасности. Учебное пособие для вузов - М.: Горячая линия - Телеком, 2006. - 544 с: ил.
2. Биячуев Т. А. / под ред. Л. Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
3. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос, 2001. - 264 с : ил.
4. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. 452с., ил.
5. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. - М: Горячая линия-Телеком, 2004. -280 с. ил.
6. Малюк А. А., Пазизин С. В., Погожин Н.С. Введение в защиту информации в автоматизированных Системах. - М.: Горячая линия-Телеком, 2001. - 148 с: ил.

7. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб.: Питер, 2002.- 848 с.: ил.
8. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.- 368с.:ил.
9. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Перевод В.Ф.Писаренко)
10. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энциклопедия компьютерных вирусов. - М.: «СОЛОН-Р», 2001.
11. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина.-2-е изд., перераб. и доп.-М.: Радио и связь, 2001.-376 с: ил.
12. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил.

15. Інформаційні ресурси

Сайт кафедри k304.khai.edu