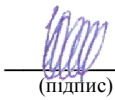
Міністерство освіти і науки України

Національний аерокосмічний університет ім. М.Є. Жуковського
“Харківський авіаційний інститут”

Кафедра математичного моделювання та штучного інтелекту (№304)

ЗАТВЕРДЖУЮ

Керівник проектної групи



_____ О.Г.Ніколаєв
(підпис) (ініціали та прізвище)

«_01_» __09__ 2020 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації
(назва навчальної дисципліни)

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

Спеціальність: 124 «Системний аналіз»
(код та найменування спеціальності)

Освітня програма: «Системний аналіз і управління»
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Харків 2020 рік

Робоча програма «Захист інформації» для студентів
(назва навчальної дисципліни)
за спеціальністю: 124 «Системний аналіз» освітньою програмою: «Системний аналіз і управління»

«27» серпня 2020 р. – 10 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 № 1 від « 28 » серпня 2020 р.

Завідувач кафедри д.т.н., проф _____ 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 – 4,5</td><td rowspan="12">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальність
124 «Системний аналіз»
(код та найменування)

Освітня програма
«Системний аналіз і управління»
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td colspan="2">вибіркова</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">2020/ 2021</td></tr>
<tr><td>Індивідуальне завдання -</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 135
денна – 54/81</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 – 3,4
самостійної роботи студента – 5,1</td><td colspan="2">24 годин</td></tr>
<tr><td colspan="2">Практичні, семінарські[1)]</td></tr>
<tr><td colspan="2">30 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">81
година</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 – 54/135.

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.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні терміни та визначення, принципи побудови профілю захисту;
- основні міжнародні та національні стандарти з захисту інформації;
- основні принципи організації захисту інформації в інформаційних системах;
- механізми та протоколи забезпечення конфіденціальності інформації;
- механізми й протоколи забезпечення аутентичності інформації в інформаційних системах;
- механізми та протоколи цілісності даних в інформаційних системах;
- основні види атак, принципи криптоаналізу;
- основні напрямки розвитку сучасної криптографії.

вміти:

- визначати вимоги та формувати профіль захисту в інформаційних системах;
- ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів і протоколів захисту інформації в інформаційних системах;
- визначати механізми та протоколи для забезпечення аутентичності інформації;
- визначати криптографічні системи для забезпечення конфіденціальності даних в інформаційних системах;
- вибирати механізми та протоколи для забезпечення цілісності даних, проводити розрахунки їх потрібних показників;
- забезпечувати грамотний підбір програмно-апаратних і програмних засобів для забезпечення необхідного рівня захисту інформації;
- аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники інформаційної системи в цілому;
- оформлювати прийняті технічні рішення щодо забезпечення захисту інформації у вигляді комплекту технічної документації, враховуючи необхідний рівень безпеки даних в інформаційної системі фактори можливих атак, а також необхідну кількість механізмів і протоколів захисту під час розробки системи безпеки інформаційних систем.
- проводити об'єктивний аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних і наукових завдань, які виникають під час розробки та дослідження механізмів.

***мати уявлення*:**

- про класичні і сучасні методи захисту інформації.

Згідно з вимогами освітньо-професійної програми студенти повинні набути такі компетентності:

інтегральна:

здатність розв'язувати складні спеціалізовані задачі та практичні проблеми системного аналізу у професійній діяльності або в процесі навчання, що передбачають застосування теоретичних положень та методів системного аналізу та інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні:

ЗК1 – здатність до абстрактного мислення, аналізу та синтезу.

ЗК2 – здатність застосовувати знання у практичних ситуаціях.

ЗК4 – здатність знати та розуміти предметну область і професійну діяльність.

ЗК7 – здатність до пошуку , оброблення та аналізу інформації з різних джерел.

ЗК8 – здатність бути критичним і самокритичним.

ЗК14 – здатність оцінювати та забезпечувати якість виконуваних робіт

Фахові:

ФК1 – здатність використовувати системний аналіз як сучасну міждисциплінарну методологію, що базується на прикладних математичних методах та сучасних інформаційних технологіях і орієнтована на вирішення задач аналізу і синтезу технічних, економічних, соціальних, екологічних та інших складних систем.

ФК8 – здатність використовувати сучасні інформаційні технології для комп'ютерної реалізації математичних моделей та прогнозування поведінки конкретних систем, а саме: об'єктно - орієнтований підхід при проектуванні складних систем різної природи, прикладні математичні пакети, застосування баз даних і знань, використання моделей алгоритмічних обчислень, оцінювання їх ефективності та складності для адекватного моделювання предметних областей.

ФК9 – здатність організувати роботу з аналізу та проектуванню складних систем, створення відповідних інформаційних технологій та програмного забезпечення.

Програмні результати навчання:

ПРН10 – знати архітектуру сучасних обчислювальних систем і комп'ютерних мереж.

ПРН11 – знати і вміти застосовувати на практиці системи управління базами даних і знань та інформаційні системи.

ПРН13 – проектувати, реалізовувати, тестувати, впроваджувати, супроводжувати, експлуатувати програмні засоби роботи з даними і знаннями в комп'ютерних системах і мережах.

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, 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	14	2	2	–	10
Тема 2. Найпростіші методи шифрування із закритим ключем	16	4	4	–	8
Тема 3. Принципи побудови блокових шифрів з закритим ключем. Алгоритми DES і AES	14	2	2	–	10
Тема 4. Режими роботи блокових алгоритмів. Алгоритм криптографічного перетворення даних ГОСТ 28147-89. Криптографічні хеш-функції	16	4	4	–	8
Модульний контроль	2		2		
Разом за змістовим модулем 1	62	12	14		36
Модуль 2					
Змістовий модуль 2.					
Тема 5. Потокові шифри і генератори псевдовипадкових чисел	16	2	2	–	12
Тема 6. Криптографія з відкритим ключем	17	4	4	–	9
Тема 7. Електронний цифровий підпис	16	2	4	–	10
Тема 8. Цілком таємні системи. Шифрування, завадостійке кодування і стиснення інформації	22	4	4	-	14
Модульний контроль	2		2		
Разом за змістовим модулем 1	73	12	16		45
Усього годин	135	24	30	0	81

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.	2
2	Симетричні криптосистеми	4
3	Програмна реалізація шифру DES	2
4	Український стандарт шифрування ГОСТ 28147-89	4
5	Вивчення псевдовипадкових генераторів	2
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	30

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Програмна реалізація шифрів підстановки	10
2	Класичні алгоритми симетричного шифрування	8
3	Програмна реалізація шифру AES	10
4	Режими шифрування алгоритму ГОСТ 28147-89	8
5	Програмна реалізація псевдовипадкових алгоритмів	6
6	Генерація чисел	6
7	Обмін ключами алгоритмом RSA	9
8	Обмін ключами алгоритмом Ель-Гамаля	10
9	Реалізація завадостійких кодів	6
10	Реалізація алгоритмів стиснення даних	8
	Разом	81

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 іспиту.

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 всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		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 . -

14. Рекомендована література

Базова

1. 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 .
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.

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. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.
4. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос, 2001. - 264 с : ил.
5. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. 452с., ил.
6. Домарев В. В. Безопасность информационных технологий: Системный подход: - К.: ООО "ТИД ДС", 2004. – 992с.
7. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энциклопедия компьютерных вирусов. - М.: «СОЛОН-Р», 2001.

8. Конев И. Р., Беляев А. В. Информационная безопасность предприятия.- СПб.: БХВ - Петербург, 2003, 752с.: ил.
9. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. - М: Горячая линия-Телеком, 2004. -280 с. ил.
10. Малюк А. А., Пазизин С. В., Погожин Н.С. Введение в защиту информации в автоматизированных Системах. - М.: Горячая линия-Телеком, 2001. - 148 с: ил.
11. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб.: Питер, 2002.- 848 с.: ил.
12. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.- 368с.:ил.
13. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Переклад В.Ф.Писаренко)
14. 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.
15. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил.

15. Інформаційні ресурси

Сайт бібліотеки ХАІ: http://library.khai.edu