МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І. МЕЧНИКОВА
Кафедра математичного забезпечення комп'ютерних систем

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
_____
"_____" _____ 20___ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК29 Захист інформації в комп'ютерних системах
(назва навчальної дисципліни)

Рівень вищої освіти *Перший (бакалаврський)*

Галузь знань: *12 – Інформаційні технології*

Спеціальність *123 – Комп'ютерна інженерія*
(код і назва спеціальностітей)

Освітньо-професійна програма *Комп'ютерна інженерія*
(назва ОПП/ОНП)

ОНУ – 2022

Робоча програма навчальної дисципліни «Захист інформації в комп'ютерних системах». – Одеса:ОНУ, 2022. – 12 с.

Розробники: Шпінарева І.М., к.фіз.-м. наук, доцент кафедри МЗКС

Робоча програма затверджена на засіданні кафедри математичного забезпечення комп'ютерних систем

Протокол № 1 від. "25" 08 2022 р.

Завідувач кафедри _____ (Євгеній МАЛАХОВ)
(підпис) (Ім'я ПРІЗВИЩЕ)

Погоджено із гарантом ОПП/ОНП Комп'ютерна інженерія

_____ (Людмила ВОЛОЩУК)
(Ім'я ПРІЗВИЩЕ)

Схвалено навчально-методичною комісією (НМК) з ІТ спеціальностей факультету МФІТ

Протокол № 2 від. "31" 08 2022 р.

Голова НМК _____ (Алла РАЧИНСЬКА)
(підпис) (Ім'я ПРІЗВИЩЕ)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____" _____ 20__ р.

Завідувач кафедри _____ (_____)
(підпис) (Ім'я ПРІЗВИЩЕ)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____" _____ 20__ р.

Завідувач кафедри _____ (_____)
(підпис) (Ім'я ПРІЗВИЩЕ)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, 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 rowspan="13">Загальна кількість:
кредитів – 4

годин – 120

змістових модулів –3</td><td rowspan="13">Галузь знань
<u>12 – Інформаційні технології</u>
(шифр і назва)

Спеціальність
<u>123 – Комп’ютерна інженерія</u>
(шифр і назва)

Рівень вищої освіти:
<u>Перший (бакалаврський)</u></td><td colspan="2">Нормативна / за вибором (ВНЗ/студента)</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td>3-й</td><td>4-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>6-й</td><td>7-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>34 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>18 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>68 год.</td><td>106 год.</td></tr>
<tr><td colspan="2">у т.ч. ІНДЗ*:</td></tr>
<tr><td colspan="2">Форма підсумкового контролю:
іспит</td></tr>
</table>

* – за наявності

2. Мета та завдання навчальної дисципліни

Метою курсу є формування теоретичних знань та практичних навичок у використанні методів та засобів забезпечення безпеки в комп'ютерних системах, отримання досвіду у використанні криптографічних методів для запобігання протиправним діям щодо знищення, модифікації та блокування комп'ютерної інформації

Задачі дисципліни:

– отримати знання основних аспектів проблеми забезпечення безпеки інформації;

– отримати знання методів та засобів забезпечення безпеки інформації для вирішення практичних завдань в комп'ютерних системах, які виникають при зберіганні, обробці та передаванні інформації;

– оволодіти знаннями побудови систем захисту з використанням методів традиційної криптографії;

– використовувати методи контролю цілісності і автентичності інформації, у тому числі протоколи аутентифікації та електронного підпису.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей** (згідно ОПП «Комп'ютерна інженерія» від **2019** р.):

a) загальних: -

b) фахових:

КС4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

КС10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

Програмні результати навчання (ПРН):

ПР1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПР6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПР16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

ПР20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

ПР21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

Очікувані результати навчання. У результаті вивчення навчальної дисципліни студент повинен

знати: *основні поняття, методи та засоби забезпечення безпеки інформації для вирішення практичних завдань в комп'ютерних системах, які виникають при зберіганні, обробці та передаванні інформації.*

вміти:*забезпечувати конфіденційність, цілісність та доступність інформації, забезпечувати автентичність, відстежуваність та надійність інформації в умовах неповноти та невизначеність вихідних даних, розробляти криптосистеми за допомогою криптографічних бібліотек OpenSSL та CryptoAPI.*

3. Зміст навчальної дисципліни

Змістовний модуль 1. Основні положення теорії інформаційної безпеки та захисту інформації. Сучасні алгоритми криптографії

Тема 1. Основні визначення і поняття теорії захисту інформації. Методи захисту інформації. Види загроз, їх системна класифікація. Комп'ютерні віруси та їх властивості.
Література: [1, 2, 3, 4, 5].

Тема 2. Симетричні криптосистеми. Блочне шифрування. Сучасні структури симетричних криптосистемю Сучасні алгоритми шифрування. Режими шифрування.
Література: [2, 3, 4, 5, 8].

Тема 3. Криптографія з відкритим ключем. Алгоритми криптографії з відкритим ключем. Алгоритм RSA, DSA. Обмін ключами по схемі Діффі-Хеллмана.
Література: [1 , 2, 3, 4, 5]

Тема 4. Методи забезпечення цілісності даних. Одностороння функція хешування. Колізійно-стійкі функції хешування Whirpool та SHA256, SHA-384, SHA-512.
Література: [1 , 2, 3, 4, 5]

Тема 5. Електронно-цифрові підписи. Схема створення і перевірки ЕЦП. Алгоритми ЕЦП: Ель-Гамаля, RSA. Сліпа підпис Чома.
Література: [1 , 2, 3, 4]

Змістовий модуль 2. **Методи захисту в комп'ютерних системах**

Тема 6. Аутентифікація повідомлень (MAC). Методи аутентифікації повідомлень: MAC-CBC, HMAC.
Література: [1, 2, 3, 4]

Тема 7. Поняття ідентифікації, автентифікації. Способи автентифікації. Біометричні засоби автентифікації та контролю. Парольні системи. Основні компоненти та загрози безпеки парольних систем.
Література: [4, 1, 7].

Тема 8. Інфраструктура відкритих ключів (PKI). Функції PKI.Сертифікат X509. Сертифікат PGP. Система Kerberos.

Література: [1, 2, 3]

Змістовий модуль 3. **Механізми і політики розмежування прав доступу**

Тема 9. Формальні моделі доступу. Дискреційна модель доступу.
Література: [1, 4, 6]

Тема 10. Мандатна та роліва модель доступу.
Література: [1, 4, 6]

Тема 11. Підсистеми захисту в ОС Windows та в ОС Linux. Порівняння архітектури Windows та Linux
Література: [3, 4, 6,]

Тема 12. Нормативні документи системи ЗІ .TCSEC ("Оранжева книга") – перший стандарт у галузі оцінки захищеності комп'ютерних систем. Common Criteria ("Загальні критерії") – європейський стандарт у галузі оцінки захищеності комп'ютерних систем. Нормативні документи системи ЗІ в Україні. Державний стандарт України із захисту інформації.
Література: [4, 6, 8] .

4. Структура навчальної дисципліни

Назви тем	Кількість годин									
	Денна форма					Заочна форма				
	Усього	у тому числі				Усього	у тому числі			
		л	п/с	лаб	ср		л	п/с	лаб	ср
1	2	3	4	5	6	7	8	9	10	11
Змістовий модуль 1. Основні положення теорії інформаційної безпеки та захисту інформації. Сучасні алгоритми криптографії										
Тема 1. Основи теорії захисту інформації.	7	2			5	7				7
Тема 2. Симетричні криптосистеми.	12	4		2	6	9	1		1	7
Тема 3. Криптографія з відкритим ключем.	12	4		2	6	9	1		1	7
Тема 4. Методи забезпечення цілісності даних.	12	4		2	6	9	1		1	7
Тема 5. Електронно-цифрові підписи.	13	4		3	6	10	1		1	8
Разом за змістовим модулем 1	**56**	**18**		**9**	**29**	**44**	**4**		**4**	**36**
Змістовий модуль 2. Методи захисту в комп'ютерних системах.										

Тема 1. Аутентифікація повідомлень.	10	2		2	6	6.5	0.5		1	5
Тема 2. Методи ідентифікації, автентифікації.	12	4		2	6	5.5	0.5			5
Тема 3. Інфраструктура відкритих ключів (PKI).	11	2		3	6	12	1		1	10
Разом за змістовим модулем 2	**33**	**8**		**7**	**18**	**24**	**2**		**2**	**20**
Змістовий модуль 3. Механізми і політики розмежування прав доступу.										
Тема 1. Формальні моделі доступу. Дискреційна модель доступу.	13	2			5	13	1			12
Тема 2. Мандатна та роліва моделі доступу	11	2			5	12				12
Тема 3. Підсистеми захисту в ОС Windows та Linux	14	2		2	5	12				12
Тема 4. Європейський стандарт. Нормативні документи системи ЗІ в Україні.	16	2			6	15	1			14
Разом за змістовим модулем 3	**31**	**8**		**2**	**21**	**52**	**2**		**0**	**50**
Усього годин	**120**	**34**		**18**	**68**	**120**	**8**		**6**	**106**

* – за наявності

Форма контролю: **КО** –контрольне опитування (поточне)
ІЗ –індивідуальне завдання
КР – контрольна робота

5. Теми семінарських занять

Семінарські заняття не передбачені.

6. Теми практичних занять

Практичні заняття не передбачені.

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Початкові навички роботи з програмою openssl	1
2	Шифрування файла симетричними алгоритмами в OpenSSL.	1
3	Шифрування файла асиметричними алгоритмами в OpenSSL	1
4	Створення і розподіл криптографічних ключів в OpenSSL.	2
5	Забезпечення авторства та цілісності інформації за допомогою алгоритмів ЕЦП в OpenSSL.	1
6	Створення центру сертифікації та сертифікатів користувачів в OpenSSL.	2
7	Робота з протоколом захисту електронної пошти S/MIME в OpenSSL.	2
8	Створення захищеного каналу по протоколу SSL/TLS між клієнтом і сервером в OpenSSL.	2
9	Програмування симетричної криптосистеми за допомоги CryptoAPI.	2
10	Програмування ЕЦП за допомоги CryptoAPI.	2
11	Програмування МАС за допомоги CryptoAPI.	2
	Разом	18

8. Самостійна робота

№ з/п	Назва теми / види завдань	Кількість годин
1	Сучасні алгоритми симетричного шифрування. Стандарт шифрування даних AES. Режими шифрування [1].	8
2	Алгоритми криптографії з відкритим ключем. Алгоритм RSA. Обмін ключами по схемі Діффі-Хеллмана [1].	8
3	Методи забезпечення цілісності даних. Одностороння функція хешування. Колізійно-стійкі функції хешування Whirpool та SHA-512 [1].	6
4	Електронно-цифрові підписи. Схема створення і перевірки ЕЦП. Алгоритми ЕЦП: Ель-Гамаля, RSA [1].	8
5	Код аутентичності повідомлення.CBC-MAC, HMAC [1]	6
6	Інфраструктура відкритих ключів (PKI). Функції PKI.Сертифікат X509. Сертифікат PGP [1].	7
7	Система Kerberos [1].	7
8	Формальні моделі доступу. Дискреційна модель доступу. Мандатна модель доступу. Роліва модель доступу [1].	6
9	Підсистема захисту в ОС Windows. Підсистема захисту в ОС Linux [1].	6

10	Стандарти у галузі оцінки захищеності комп'ютерних систем [1].	6
	Разом	**68**

До самостійної роботи відноситься:

[1] – підготовка до лекцій, лабораторних занять.

9. Методи навчання

Лекції з використанням мультимедійного презентаційного матеріалу.

10. Методи контролю

Під час **підсумкового контролю** студент повинен відповісти на 2 запитання екзаменатора з переліку, наведеному у п. 11.

Критерії оцінювання на підсумковому модульному контролі:

1. Відповідь повинна бути повною і короткою. Вона не повинна мати в собі матеріал, що не відноситься до сутті питання.
2. Чітко формулювати твердження, вправно застосовувати необхідні формули і знання основних питань програми.
3. Відповіді, що мають помилкові твердження оцінюються виходячи з близькості відповіді до правильної.
4. Пропуски в обґрунтуванні тверджень враховуються і це призводить до зменшення кількості балів.
5. Малі недоліки, неточності при викладенні матеріалу, зменшують кількість балів.
6. Незнання і нерозуміння основної ідеї теоретичного питання або задачі призводить до зняття до 90 % балів.
7. Якщо відповідь на питання відсутня то виставляється нуль балів.

11. Питання для підсумкового контролю

1. Поясніть загальні поняття захисту інформації. Чотири рівня захисту інформації.
2. Описати атаки на комп'ютерні системи.
3. Описати комп'ютерні віруси та їх властивості, класифікація вірусів.
4. Поясніть основні поняття криптографічного захисту інформації.
5. Дайте визначення симетричного шифрування.
6. Описати блочні алгоритми шифрування. Наведіть приклади блочних шифрів.
7. Описати алгоритм шифрування DES.
8. Описати алгоритм шифрування AES.
9. Описати режими шифрування.
10. Описати стандарт шифрування ГОСТ 28147-89. Поясніть загальну схема шифрування.
11. Поясніть асиметричні алгоритми шифрування .
12. Дайте визначення однобічної функції і функції-пастки.

13. Поясніть алгоритм шифрування RSA.
14. Поясніть алгоритм Діффі-Хеллмана відкритого розподілу ключів.
15. Описати комбінаційні методи шифрування.
16. Дайте визначення функції хешування та описати її властивості.
17. Дайте визначення електронно - цифровій підписі. Описати схему створення та перевірки ЕЦП.
18. Описати схему цифрового підпису RSA.
19. Описати криптографічні методи контролю цілісності.
20. Дайте визначення поняттю захищеної операційної системи. Описати стандарти захищеності операційних систем.
21. Дайте визначення поняттям ідентифікації, автентичністі, авторство.
22. Описати методи аутентифікації.
23. Описати методи підбору паролей
24. Описати методи аутентифікації за допомогою зовнішніх носіїв ключової інформації та за допомогою біометричних характеристик користувачів.
25. Поясніть інфраструктуру відкритих ключів (PKI), функції і архітектури PKI.
26. Описати формальні моделі доступу.
27. Поясніть дискреційну модель доступу.
28. Описати мандатну модель доступу.
29. Описати роліву модель доступу
30. Описати підсистема захисту в ОС Windows.
31. Описати підсистема захисту в ОС Linux.
32. Поясніть TCSEC ("Оранжева книга").
33. Описати Common Criteria ("Загальні критерії").

12. Розподіл балів, які отримують студенти

Поточний та періодичний контроль												Підсумковий контроль (іспит)	Сума балів
Змістовий модуль №1					Змістовий модуль № 2			Змістовий модуль №3					
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12		
5	5	5	5	5	5	5	5	5	5	5	5	40	100

Т1, Т2 ... – 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
85-89	B	добре	
75-84	C		
70-74	D	задовільно	
60-69	E		

35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

13. Навчально-методичне забезпечення

Конспект лекцій у електронному форматі; методичні вказівки для виконання лабораторних робіт; нормативні документи; презентаційні матеріали.

14. Рекомендована література

Основна

1. Захист інформації в комп'ютерних системах : підручник для студ. спец. 123 «комп'ютерна інженерія» / уклад. О. М. Гапак, С. І. Балога; рец. : М. І. Глебена. – Ужгород : ПП "АУТДОР-ШАРК, 2021. – 184 с.
2. Кібербезпека: сучасні технології захисту. Навчальні посібники /Остапов С.Е., Євсеєв С.П.,Король О.Г. – Вид.: Новий світ-2000, 2020. – 678с.
3. Захист інформації в комп'ютерних системах: підручник./ Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.
4. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с

Допоміжна

5. Quick Start Guide to Penetration Testing With NMAP, OpenVAS and Metasploit /Sagar Rahalkar [Електронний ресурс] Режим доступу: https://doi.org/10.1007/978-1-4842-4270-4
6. Bruce Schneier, Niels Ferguson Cryptography Engineering: Design Principles and Practical Applications Publisher Wiley, 2010 –384 p.
7. Технології захисту інформації. Посібник/Сергій Остапов Вид.: Родовід, 2014.– 456 с.
8. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с.

15. Електронні інформаційні ресурси

1. Cisco Networking Academy Курс Cybersecurity Essentials – Режим доступу: http://www.cisco.com/web/learning/netacad/index.html