Затверджено Вченою Радою ОНУ
імені І.І. Мечникова
від "20" грудня 2016 р. № 4

Одеський національний університет імені І.І. Мечникова
Кафедра математичного забезпечення комп'ютерних систем

"ЗАТВЕРДЖУЮ"

Проректор

"_____ 20___ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК 25 «Технології захисту інформації»
(назва навчальної дисципліни)

Рівень вищої освіти бакалавр

Спеціальність 126 – Інформаційні системи та технології
(код і назва спеціальностітей)

Факультет математики, фізики та інформаційних технологій
(назва інституту, факультету)

2021 – 2022

Робоча програма складена на основі навчальної програми з дисципліни «Технології захисту інформації».

Розробник:
Шпінарева І.М., к.ф.-м. наук, доцент кафедри МЗКС

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

Протокол № 1 від. "30" 08 2021 р.

Завідувач кафедри _____ (підпис) (Є.В. Малахов) (прізвище та ініціали)

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

Протокол № 1 від. "6" 09 2021 р.

Голова НМК _____ (підпис) (О.В.Савастру) (прізвище та ініціали)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____ (підпис) (_____) (прізвище та ініціали)

Переглянуто та затверджено на засіданні кафедри _____

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____ (підпис) (_____) (прізвище та ініціали)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="15">Загальна кількість:

кредитів – 4

годин – 120

залікових модулів – 1

змістових модулів – 3

ІНДЗ* – _____
(вид завдання)</td><td>Галузь знань
12 – Інформаційні технології
(шифр і назва)</td><td colspan="2">Нормативна</td></tr>
<tr><td rowspan="5">Спеціальність
126 – Інформаційні системи та технології
(шифр і назва)</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>3</td><td></td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>2 (6)</td><td></td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Рівень вищої освіти:
бакалавр</td><td>36 год.</td><td></td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>36 год.</td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>70 год.</td><td></td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">Вид контролю: іспит</td></tr>
</table>

* – за наявності

2. Мета та завдання навчальної дисципліни

Метою вивчення дисципліни є формування комплексу знань та вмінь в галузі теорії захисту інформації, в використанні методів та засобів забезпечення інформаційної безпеки та здобуття навичок у практичному використанні криптографічних методів у створенні захищених комп'ютерних систем.

Задачі дисципліни:

- отримати знання основних аспектів проблеми забезпечення безпеки інформації;
- отримати знання методів та засобів забезпечення безпеки комп'ютерної інформації для вирішення практичних завдань в інформаційних 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**:

а) загальних (ЗК):

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

б) фахових загальних (КФЗ):

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

в) спеціальних фахових (КФС):

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводження інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

КС 14. Здатність формувати нові конкурентоспроможні ідеї й реалізовувати їх у проектах (стартапах).

Програмні результати навчання:

ПРН 4. Проводити системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях.

ПРН 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.

ПРН 7. Обґрунтовувати вибір технічної структури та розробляти відповідне програмне забезпечення, що входить до складу інформаційних систем та технологій.

ПРН 12. Розробляти та застосовувати моделі представлення знань, стратегії логічного виведення, технологій інженерії знань, технологій і інструментальних засобів побудови інтелектуальних систем і систем штучного інтелекту

Очікувані результати навчання. У результаті вивчення навчальної дисципліни студент повинен

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

вміти:

- шифрувати інформацію симетричними і асиметричними методами;
- створювати і перевіряти ЕЦП;
- вміти працювати з криптографічними бібліотеками OpenSSL, CryptoAPI.

3. Зміст навчальної дисципліни

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

Тема 1. Основні визначення і поняття теорії захисту інформації. Методи захисту інформації. Історія розвитку. Термінологія. Види загроз, їх системна класифікація. Зловмисники та випадкова втрата даних. Поняття атаки на комп’ютерну систему.
Література: [3,5, 6,7].

Тема 2. Симетричні криптосистеми. Блочне шифрування. Структура шифру Фейстеля. Сучасні алгоритми шифрування. Стандарт шифрування даних (DES, AES). Режими шифрування.
Література: [1, 2,4,5,7].

Тема 3. Криптографія з відкритим ключем. Алгоритми криптографії з відкритим ключем. Алгоритм RSA. Обмін ключами по схемі Діффі-Хеллмана.
Література: [1, 3,4,5,7]

Тема 4. Методи забезпечення цілісності даних. Одностороння функція хешування. Колізійно-стійкі функції хешування Whirpool та SHA256, SHA-384, SHA-512.
Література: [1, 4,6]

Тема 5. Електронно-цифрові підписи. Схема створення і перевірки ЕЦП. Алгоритми ЕЦП: Ель-Гамаля, RSA. Сліпа підпис Чома.
Література: [3,4, 5, 7]

Змістовий модуль 2. Технології та методи захисту інформації.

Тема 6. Аутентифікація повідомлень. Методи аутентифікації повідомлень. Код аутентичності повідомлення.
Література: [1, 2,3,4,5]

Тема 7. Поняття ідентифікації, автентифікації та різновиди способів автентифікації. Біометричні засоби автентифікації та контролю. Парольні системи. Основні компоненти та загрози безпеки парольних систем. Оцінка стійкості парольної системи.
Література: [3, 4,5,6,7,8].

Тема 8. Інфраструктура відкритих ключів (PKI). Функції PKI. Сертифікат X509. Сертифікат PGP. Система Kerberos.
Література: [1, 3,5,7,8]

Тема 9. Комп'ютерні віруси та їх властивості. Класифікація вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.
Література: [3, 5,6,7].

Тема 10. Захист інформації за допомогою міжмережних екранів.
Література: [3, 5,7].

Тема 11. Протоколи AAA.
Література: [3, 5,7].

Змістовий модуль 3. Механізми і політики розмежування прав доступу в ОС.

Тема 12. Формальні моделі доступу. Дискреційна модель доступу.
Література: [3,7,8]

Тема 13. Мандатна модель доступу. Рольова модель доступу.
Література: [3,7,8]

Тема 14. Підсистема захисту в ОС Windows. Підсистема захисту в ОС Linux. Порівняння архітектури Windows та Linux
Література: [3,7]

Тема 15. 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 ТЗІ в Україні.
Література: [3,7].

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
	Форма контролю	Усього	у тому числі			
			л	п	лаб	ср
1	2	3	4	5	6	7
Змістовий модуль 1. Основні положення теорії інформаційної безпеки та захисту інформації.						
Тема 1.	КО		2			
Тема 2.			2		4	6
Тема 3.			4		4	6
Тема 4.			4		4	6
Тема 5.			4		4	6
Змістовий модуль 2. Технології та методи захисту інформації.						
Тема 6.	КО		2		4	6
Тема 7.	КО		2		2	6
Тема 8.	КО		2		4	6
Тема 9.			2			6
Тема 10.			2		4	6
Тема 11.			2		4	6
Змістовий модуль 3. Механізми і політики розмежування прав доступу в ОС.						
Тема 12.	КО		2			6
Тема 13.	КМ		2			6
Тема 14.	КО		2		2	6
Тема 15.			2			4
Всього годин		**120**	**36**		**36**	**70**

* – за наявності

Форма контролю: **КО** –контрольне опитування (поточне)
ІЗ –індивідуальне завдання (домашнє)
КР – контрольна робота
КМ – контроль модуля за тестовою системою

5. Теми семінарських занять

Немає

6. Теми практичних занять

Немає

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.	2
3	Шифрування файла асиметричними алгоритмами в OpenSSL	2
4	Створення і розподіл криптографічних ключів в OpenSSL.	2
5	Забезпечення авторства та цілісності інформації за допомогою алгоритмів ЕЦП в OpenSSL.	2
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.	7
10	Програмування ЕЦП за допомоги CryptoAPI.	7
11	Програмування МАС за допомоги CryptoAPI.	7
	Разом	36

8. Самостійна робота

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

10	Стандарти у галузі оцінки захищеності комп'ютерних систем	6
11	Захист інформації за допомогою міжмережних екранів.	6
12	Протокол ААА	4
	Разом	**70**

До самостійної роботи відноситься:

[1] – підготовка до лекцій, практичних, семінарських, лабораторних занять;

9. Індивідуальне навчально-дослідне завдання

Немає

10. Методи навчання

Лекції з використанням мультимедійного презентаційного матеріалу.

11. Методи контролю

Під час **підсумкового контролю** студент повинен відповісти на 2 запитання екзаменатора з переліку, наведеному у п. 12.

Критерії оцінювання на підсумковому модульному контролі:

1. Відповідь повинна бути повною і короткою. Вона не повинна мати в собі матеріал, що не відноситься до суті 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.

11.1 Питання для підсумкового контролю

1. Поясніть загальні поняття захисту інформації. Чотири рівня захисту інформації.
2. Описати атаки на комп'ютерні системи.
3. Поясніть основні поняття криптографічного захисту інформації.
4. Поясніть класифікацію методів шифрування інформації. Шифри заміни. Шифри перестановки.
5. Дайте визначення симетричного шифрування.

6. Описати потокові алгоритми шифрування. шифр Цезаря.
7. Описати блочні алгоритми шифрування. Наведіть приклади блочних шифрів.
8. Описати алгоритм шифрування DES.
9. Описати алгоритм шифрування AES.
10. Описати режими шифрування.
11. Описати стандарт шифрування ГОСТ 28147-89. Поясніть загальну схема шифрування.
12. Поясніть асиметричні алгоритми шифрування .
13. Дайте визначення однобічної функції і функції-пастки.
14. Поясніть алгоритм шифрування RSA.
15. Поясніть алгоритм Діффі-Хеллмана відкритого розподілу ключів.
16. Описати комбінаційні методи шифрування.
17. Дайте визначення функції хешування та описати її властивості.
18. Дайте визначення електронно - цифровій підписі. Описати схему створення та перевірки ЕЦП.
19. Описати схему цифрового підпису RSA.
20. Описати криптографічні методи контролю цілісності.
21. Дайте визначення поняттю захищеної операційної системи. Описати стандарти захищеності операційних систем.
22. Дайте визначення поняттям ідентифікації, автентичністі, авторство.
23. Описати методи аутентифікації.
24. Описати методи підбору паролей.
25. Описати методи аутентифікації за допомогою зовнішніх носіїв ключової інформації та за допомогою біометричних характеристик користувачів.
26. Поясніть інфраструктуру відкритих ключів (PKI), функції і архітектури PKI.
27. Описати формальні моделі доступу.
28. Поясніть дискреційну модель доступу.
29. Описати мандатну модель доступу.
30. Описати роліву модель доступу
31. Описати підсистема захисту в ОС Windows.
32. Описати підсистема захисту в ОС Linux.
33. Поясніть TCSEC ("Оранжева книга").
34. Описати Common Criteria ("Загальні критерії").
35. Описати комп’ютерні віруси та їх властивості, класифікація вірусів.
36. Протокол AAA

12. Розподіл балів, які отримують студенти

Змістовий модуль №1					Змістовий модуль № 2						Змістовий модуль №3				
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т9	Т10	Т11	Т12	
6	8	8	8	6	6	6	6	6	8	8	6	6	6	6	100

Т1, Т2 ... – теми змістових модулів,
КР- курсова робота, ІНДЗ –індивідуальне навчально-дослідне завдання

Шкала оцінювання: національна та ECTS

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="6">зараховано</td></tr>
<tr><td>85-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-69</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

13. Методичне забезпечення

Шпінарева І. М. Методичний посібник з курсу «Захист інформації в комп’ютерних системах» для студентів 4 курсу спеціальності «Комп’ютерні системи і мережі» / І. М. Шпінарева, О. А. Геренко. – Одеса: Одеський нац. ун-т, [2010]. – 36 с. [Електронний ресурс] Режим доступу: http://dspace.onu.edu.ua:8080/handle/ 123456789/21227

14. Рекомендована література

14.1. Основна література

1. Niels Ferguson Bruce Schneier Practical Cryptography – Wiley Publishing, Inc., 2008. – 397p.
2. Bruce Schneier Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C, – Wiley ,2002. – 662 p.
3. William Stallings Cryptography and network security principles and practice. Seventh edition – published by Pearson Education, 2017– 767p
4. William Stallings Cryptography and Network Security Principles and Practices, Fourth Edition: – Publisher: Prentice Hall, 2005. – 592 p.
5. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
6. Bruce Schneier Security and Survival in a Hyper-connected World – W. W. Norton & Company, 2018 – 288p.

14.2. Допоміжна література

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – ДМК Прес, 2012. – 592с.
8. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах / Под ред. В. Ф. Шаньгина. –2-е изд., Перераб. і доп. – М .: Радио и связь, 2001. –376 с.
9. Н.А. Гайдамакин Теоретические основы компьютерной безопасности. Учебное пособие. Екатеринбург 2008 – 212с.

14.3. Електронні інформаційні ресурси

1. Курс Мережевої академії Cisco Cisco-Cybersecurity Essentials [Електронний ресурс] Режим доступу: www.netacad.com
2. OpenSSL [Електронний ресурс] Режим доступу:https://www.openssl.org/
3. CryptoAPI [Електронний ресурс] Режим доступу:https://docs.microsoft.com
4. Schneier on Security [Електронний ресурс] Режим доступу: https://www.schneier.com/