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

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
_____
"____" _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК 31 «Технології захисту інформації»

Рівень вищої освіти	**перший (бакалаврський)**
Галузь знань	**12 – Інформаційні технології**
Спеціальність	**122 - Комп'ютерні науки**
Освітньо-професійна програма	**Комп'ютерні науки**

ОНУ
Одеса
2023

Робоча програма навчальної дисципліни «Технології захисту інформації». – Одеса: ОНУ, 2023. – 20с.

Розробник: Стукалов Сергій Анатолійович, старший викладач кафедри комп'ютерних систем та технологій

Робоча програма затверджена на засіданні кафедри комп'ютерних систем та технологій ФМФІТ

Протокол № 1 від. "30 " серпня 2023 р.

Завідувач кафедри _____ (Юрій ГУНЧЕНКО)

Погоджено із гарантом ОПП «Комп'ютерні науки»

_____(Алла КАМЄНЄВА)

Схвалено навчально-методичною комісією (НМК) ФМФІТ

Протокол № 1 від " 31" серпня 2023 р.

Голова НМК _____ (Алла РАЧИНСЬКА)

Переглянуто та затверджено на засіданні кафедри комп'ютерних систем та технологій

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____ (_____)

Переглянуто та затверджено на засіданні кафедри комп'ютерних систем та технологій

Протокол № ___ від. "____"_____20__ р.

Завідувач кафедри _____ (_____)

1. **Опис навчальної дисципліни**

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, Спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Очна (денна) форма навчання</td></tr>
<tr><td rowspan="9">Загальна кількість
кредитів – 4
годин – 120
змістових модулів - 2</td><td rowspan="9">Галузь знань
12 – науки інформаційні технології

Спеціальність:
122 – Комп’ютерні науки

Рівень вищої освіти:
<u>Перший (бакалаврський)</u></td><td>Обов’язкова дисципліна</td></tr>
<tr><td>Рік підготовки:
4-й</td></tr>
<tr><td>Семестр
7-й</td></tr>
<tr><td>Лекції
26 год.</td></tr>
<tr><td>Практичні, семінарські
0 год.</td></tr>
<tr><td>Лабораторні
34 год.</td></tr>
<tr><td>Самостійна робота
60 год.</td></tr>
<tr><td>Форма підсумкового контролю:
екзамен</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою викладання дисципліни є – формування теоретичних знань щодо можливих небезпек, загроз і ступеня ризику втрат інформації, а також практичних навичок щодо забезпечення захисту інформації та програмного забезпечення. Ознайомлення із сучасними підходами до збереження та захисту інформації, зі складом і змістом технологічних процедур, протоколів і операцій криптографії, криптоаналізу, стеганографії, що використовуються для вирішення проблем політики безпеки та захисту інформаційних ресурсів.

Завдання:

- вивчення і поглиблення на основі сучасних інформаційних технологій теоретичних знань та практичних навиків у галузі інформаційної безпеки та криптографічних методів захисту інформації;
- сформувати вміння з розробки та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності, контролю передачі інформації;
- оволодіння методами ідентифікації, аутентифікації, криптографії;
- набуття практичного досвіду з політики та менеджменту в галузі технологій захисту та безпеки інформації.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей.**

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.

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

ЗК11. Здатність приймати обґрунтовані рішення.

ЗК14. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні..

Спеціальні (фахові) компетентності:

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури

В результаті вивчення навчальної дисципліни здобувач вищої освіти повинен **знати**:

- об'єкти програмного забезпечення, на які можливі атаки та методи здійснення несанкціонованого доступу до інформації;
- принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх взлому;

- принципи функціонування систем захисту, призначення привілеїв, зберігання паролів та автентифікації користувачів в операційних системах WINDOWS та LINUX, методи з несанкціонованого проникнення до інформації, привласнення привілеїв адміністратора тощо;
- методи несанкціонованого зйому та навмисного пошкодження інформації та засоби протидії цім спробам;
- методи побудови захисту окремих програмних продуктів;
- основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання, методи захисту від дизасемблювання.

Вміти:
- виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконувати адміністрування прав доступу до комп'ютерної системи з метою перешкоди призначення невиправданих привілеїв;
- виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації;
- використовувати основні прийоми та програмні засоби для перевірки надійності захисту інформації та стійкості його щодо хакерських атак.

Що забезпечують наступні **програмні результати навчання:**

ПР2. Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об'єктів інформатизації.

ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних..

3. Зміст навчальної дисципліни
ЗМІСТОВИЙ МОДУЛЬ 1.
ОСНОВИ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Тема 1. Захист інформації та його основні завдання. Класифікація загроз для інформації та їх джерел. Задачі системи комп'ютерної безпеки. Класифікація засобів протидії загрозам безпеки. Інформація з обмеженим доступом. Структура політики безпеки та її основні частини. Структура і зміст профілю захисту.

Тема 2. Поняття інформаційної безпеки. Основні складові інформаційної безпеки. Важливість і складність проблеми інформаційної безпеки. Причини існування комп'ютерних злодіїв. Законодавчий, адміністративний і

процедурний рівні. Класифікація методів та засобів захисту програмного забезпечення.

Тема 3. Механізми і політики розмежування прав доступу. Стандарти у галузі оцінки захищеності комп'ютерних систем. Функціональні вимоги безпеки. Вимоги довіри (гарантія безпеки). Рівні оцінки довіри "Загальних критеріїв". Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу.

Тема 4. Основні програмно-технічні заходи інформаційної безпеки. Основні поняття програмно-технічного рівня інформаційної безпеки. Особливості сучасних інформаційних систем, які є важливими з точки зору безпеки. Архітектурна безпека. Сервіси безпеки.

Тема 5. Методи та пристрої забезпечення захисту і безпеки. Основні принципи захисту інформації при підключені до мережі Інтернет. Захист інформації на мережному рівні. Протоколи забезпечення цілісності та автентичності даних.

Тема 6. Моделі захисту інформації. Аналіз умов функціонування та загроз інформації в комп'ютерних системах та мережах. Моделі загроз у сучасних комп'ютерних мережах та системах. Побудова моделі порушника у сучасних комп'ютерних мережах та системах. Організація та засоби захисту пам'яті в ЕОМ.

Тема 7. Паролі і механізми контролю за доступом. Формальні моделі доступу. Дискреційний та мандатний доступ до інформації. Аналіз захищеності операційних систем.

ЗМІСТОВИЙ МОДУЛЬ 2.
КРИПТОГРАФІЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Тема 8. Шифрування даних. Симетричні, асиметричні та комбіновані криптосистеми. Основні вимоги та класифікація сучасних криптосистем. Сітка Х.Фейстеля, її переваги та недоліки. Математичні основи асиметричної криптографії.

Тема 9. Алгоритми з секретним ключем. DES (Data Encryption Standard) – стандарт шифрування даних. Основні модифікації DES. Блокові шифри. Сучасні потокові шифри, їх переваги та недоліки.

Тема 10. Алгоритми з відкритим ключем. Алгоритм SSA. Алгоритм Ель-Гамаля. Криптостійкість та швидкість роботи алгоритмів.

Тема 11. Протоколи аутентифікації. Хешувальні алгоритми, їх призначення, вимоги до них. Колізійно-стійкі функції хешування. Алгоритми сімейства MD 204.

Тема 12. Цифрові підписи. Поняття про цифровий підпис (на прикладі RSA). Вимоги до цифрового підпису. Стандарти цифрового підпису. Алгоритм ЕЦП ДСТУ 4145 270.

Тема 13. Основні види атак, принципи криптоаналізу. Класифікація атак на криптоалгоритми. Диференціальний криптоаналіз. Лінійний криптоаналіз.

Тема 14. Напрями розвитку сучасної криптографії. Асиметричні алгоритми на основі еліптичних кривих. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри. Алгоритми на генераторах випадкових та псевдовипадкових послідовностей. Криптографічно стійкі генератори псевдовипадкових послідовностей.

Тема 15. Механізми та протоколи керування ключами інформаційної системи. Життєвий цикл криптографічного ключа Безпека керування ключами. Компоненти і сервіси інфраструктури відкритих ключів. Стандарти і специфікації PKI. Управління сертифікатами.

4. Структура навчальної дисципліни «Технології захисту інформації»

Назва тем	Кількість годин				
	Очна (денна) форма				
	Усього	у тому числі			
		Лек.	Пр.	Лаб.	СР
1	**2**	**3**	**4**	**5**	**6**
Змістовий модуль 1. Основи технології захисту інформації					
Тема 1. Захист інформації та його основні завдання.	4	2			2
Тема 2. Поняття інформаційної безпеки.	4	2			2
Тема 3. Механізми і політики розмежування прав доступу.	8	2		4	2
Тема 4. Основні програмно-технічні заходи інформаційної безпеки.	8	2		4	2
Тема 5. Методи та пристрої забезпечення захисту і безпеки.	10	4		4	2
Тема 6. Моделі захисту інформації.	4	2			2
Тема 7. Паролі і механізми контролю за доступом.	8	2		4	2
Разом за змістовим модулем 1	**46**	**16**		**16**	**14**
Змістовий модуль 2. Криптографічні основи захисту інформації					
Тема 8. Шифрування даних.	6	2			4
Тема 9. Алгоритми з секретним ключем.	12	2		6	4
Тема 10. Алгоритми з відкритим ключем.	5	1			4

Тема 11. Протоколи аутентифікації.	5	1			4
Тема 12. Цифрові підписи.	7	1		4	2
Тема 13. Основні види атак, принципи криптоаналізу.	7	1		4	2
Тема 14. Напрями розвитку сучасної криптографії.	3	1			2
Тема 15. Механізми та протоколи керування ключами інформаційної системи.	9	1		4	4
Разом за змістовим модулем 2	**54**	**10**		**18**	**26**
ІНДЗ	20				20
Усього годин	**120**	**26**		**34**	**60**

5. Теми семінарських занять

Семінарські заняття не передбачені навчальним планом.

6. Теми практичних занять

Практичні заняття не передбачені навчальним планом.

7. Теми лабораторних робіт

№	Назва теми	Кількість годин
1.	**Захист інформації в операційних системах Windows та Linux.** Установка парольного захисту BIOS. Парольний захист операційної системи. Налаштування брандмауера. Налагодження безпеки стека протоколів TCP/IP. Локальна політика безпеки. Аудит керування обліковими записами. Аудит подій входу в систему. Аудит доступу до служби каталогів. Аудит використання привілеїв. Аудит відстеження процесів. Аудит системних подій.	4
2.	**Захист інформації у мережах Microsoft Windows.** Засвоїти принципи і технологію захисту інформації у операційній системі Microsoft Windows. Надання прав різним категоріям користувачів, доступу до дисків, каталогів, файлів, використання загальних ресурсів в локальній мережі та контроль за їх використанням. Пошук інформації про порушення безпеки інформації. Визначення способів злому. Напрацювання методів та засобів захисту інформації.	4
3.	**Захист інформації в операційній системі Windows.** Засвоїти принципи й елементи технології кібербезпеки в	4

	операційній системі Windows. Ознайомитись з рівнями захисту комп'ютера, можливістю надання прав різним категоріям користувачів, встановлення, зміна, зберігання паролів, встановлення їх параметрів, блокуванням приймання інформації та роботи програм приховування файлів та каталогів. Резервне копіювання даних	
4.	**Створення і зберігання надійних паролів.** Визначити загальні вимоги до надійного паролю. Зберігання паролів. Політика створення надійного паролю. Онлайн інструменти створення паролів.	4
5.	**Шифрування за допомогою алгоритмів з секретним та відкритим ключем.** Отримання теоретичних та практичних навичок роботи з програмними засобами шифрування даних. Комп'ютерна програма Pretty Good Privacy). Генерації й розподіл ключів. Ключі для шифрування й, пов'язані з ними, ключі для дешифрування.	6
6.	**Електронний цифровий підпис.** Електронно-цифровий підпис на основі алгоритму RSA. Використанням криптопровайдерів .Net для створення і перевірки цифрового підпису.	4
7.	**Організація атак на архіви з парольним захистом методом «грубої сили».** Методи зламу пароля. Атаки на систему парольного захисту zip архівів.	4
8.	**Дослідження якості ключових файлів.** Критерії стохастичної якості ключових файлів. Підрахування інформаційної ентропії та перевірка файлу на відповідність критеріям стохастичної якості (згідно до варіанту).	4
	Разом	**34**

8. Самостійна робота

№	Назва теми/питання для підготовки, завдання	Кількість годин
1.	**Законодавство в сфері інформаційної безпеки.** Основні положення інформаційної безпеки держави. Система нормативно-правового та організаційного управління інформаційною безпекою. Визначення об’єктів та суб’єктів інформаційної діяльності, що підлягають захисту.	2
2.	**Комп’ютерні злочини та засоби їх запобігання.** Види комп’ютерних злочинів та відповідальність за їх здіснення. Особливості розслідування комп’ютерних злочинів. Захист інформації в автоматизованих системах.	2
3.	**Основні методи криптоаналізу.** Історія криптоаналізу. Класичний криптоаналіз. Сучасні	4

	методи розкриття алгоритмів шифрування.	
4.	**Класифікація вірусів за шкідливістю, механізмом поширення та особливостями алгоритмів.** Визначення вірусу. Історичні дані про комп'ютерні віруси. Алгоритми роботи вірусів. Механізми розмноження вірусів.	2
5.	**Дескриптор вірусу.** Складові дескриптора вірусу. Декодування дескриптору.	2
6.	**Пошук вірусів за сигнатурами.** Визначення сигнатури вірусу та вимоги до них. Види сигнатур. Штами вірусів.	2
7.	**Стеганографія.** Використання графічних, звукових та текстових файлів для прихованої передачі інформації. Галузі застосування стеганографії. Практичні аспекти побудови стеганосистем.	2
8.	**Алгоритм оптимального стиснення інформації Хаффмана.** Побудова дерева кодування Хаффмана (Н-дерево). Недоліки класичного алгоритму Хаффмана. Адаптивне стиснення. Застосування методу стиснення даних методом Хаффмана.	2
9.	**Моноалфавітні і багатоалфавітні криптосистеми.** Традиційні історичні шифри. Адитивні моноалфавітні шифри підстановки (шифри Цезаря). Автоключовий шифр підстановки. Шифр підстановки Плейфера.	2
10.	**Модулярні шифри.** Асиметричні алгоритми шифрування інформаційних потоків. Підвищення швидкодії асиметричних криптосистем за допомогою операцій модулярного множення та експоненціювання.	2
11.	**Шифри Віженера.** Список Віженера. Етапи застосування шифру Віженера. Методи знаходження довжини ключів.	2
12.	**Шифри Плейфейера, Хіла, одноразового блокноту.** Біграми. Алгоритм застосування шифрів.	2
13.	**Сітка Фейстеля.** Дифузія і конфузія (розсіювання і перемішування). Алгоритм дешифрування.	2
14.	**Канальне і наскрізне шифрування даних в мережах передачі даних.** Способи передачі зашифрованих даних. Шифрування електронного листування. Стандарти наскрізного шифрування. Концепція канального шифрування. Недоліки канального шифрування. Розподіл ключів.	2
15.	**Криптосистеми, що базуються на задачі про рюкзак.** Формулювання задачі рюкзака. Підрахунок варіантів перебору. Алгоритм розв’язання задачі «суперзростаючого»	2

	рюкзака. Алгоритми шифрування «рюкзачних» криптосистем.	
16.	**Складність обчислень. Гіпотеза P=NP та стійкість криптосистем.** Визначення криптостійкості. Вимірювання криптостійкості. Основні принципи криптології. класифікація криптосистем.	2
17.	**Односторонні функції.** Гіпотеза про існування односторонніх функцій та стійкість криптосистем.	2
18.	**Псевдовипадкові генератори в системах інформаційної безпеки.** Криптографічно стійкі генератори псевдовипадкових чисел. Стандарти алгоритмів генерації послідовностей випадкових чисел. Атаки на генератори псевдовипадкових чисел.	2
19.	**Протокол, що базується на ізоморфізмі графів. Аутентифікація.** Підходи до використання теорії графів в області захисту інформації. Використання теорії графів для опису схеми інформаційних потоків в інформаційній системі. Моделювання, аналіз та застосування графів атак.	2
20.	**Керування ключами.** Життєвий цикл криптографічного ключа. Методи керування ключами. Безпека керування ключами. Протоколи забезпечення безпеки ключів. Життєвий цикл сертифікатів і ключів.	2
	Індивідуальне науково-дослідне завдання (ІНДЗ): Доповідь та мультимедійна презентація за темами: 1. Шифр підстановки (квадрат Поліція). 2. Кодування тексту в k-значному цифровому алфавіті. 3. Накладення гами (псевдовипадкові послідовності). 4. XOR – кодування. 5. Стовпчикова транспозиція. 6. Порівняння криптографічних засобів різних протоколів мобільних платежів.	20
	Разом	**60**

Критерії оцінювання виконання самостійної роботи

1. Структура – короткі повідомлення оформлюються на папері (2-3 сторінки) або у вигляді короткої презентації із використанням застосунків для створення презентацій. Друкований текст –14 кегль, інтервал 1,5, Times New Roman. Вимогою до презентації є яскравість, інформативність, презентабельність (5-7 слайдів для короткого повідомлення). *Усі матеріали мають супроводжуватись переліком використаних інформаційних джерел.*
2. Критерії для оцінювання:

– своєчасність виконання;
– доброчесність та коректність у представлені текстів, презентацій та посилань (у разі доведеного плагіату бали за роботу анулюються);
– повнота, грамотність і коректність розкриття основних положень;
– творчий підхід до постановки і реалізації завдання;
– відповідність формальним критеріям (структура, послідовність, логічність, мовна грамотність, якість оформлення тощо).
– вміння застосовувати теоретичні знання для рішення практичних завдань.

3. Критерії щодо виконання та оцінювання ІНДЗ. Оформлене ІНДЗ розміщується в будь-якому «хмарному середовищі» із доступом викладача (адреса погоджується з викладачем). Критерії щодо оформлення та оцінювання співпадають із критеріями оцінювання самостійної роботи.

Тема індивідуального науково-дослідного завдання та терміни його подання узгоджуються з викладачем. Захист завдання відбувається не пізніше початку екзаменаційної сесії.

9. Методи навчання

1. Методи організації та здійснення навчально-пізнавальної діяльності:

а) за джерелом інформації – словесні (пояснення, розповідь, бесіда), наочні (спостереження, демонстрація), практичні (моделювання).

б) за логікою передачі і сприймання навчальної інформації (індуктивні, дедуктивні, аналітичні, синтетичні);

в) за ступенем самостійності мислення (репродуктивні, пошукові, дослідницькі);

г) за ступенем керування навчальною діяльністю (під керівництвом викладача, самостійна робота студентів).

2. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності: навчальні дискусії, створення ситуації пізнавальної новизни, інтерактивні вправи та завдання.

Під час вивчення навчальної дисципліни використовують такі форми роботи – лекція, лабораторна робота, самостійна робота, індивідуальне науково-дослідне завдання.

Під час проведення лекцій використовуються наступні методи навчання: пояснювально-ілюстративний метод, інформаційно-рецептивний; репродуктивний метод (репродукція - відтворення); метод проблемного викладу; частково-пошуковий метод.

Під час лабораторних занять використовуються наступні методи навчання частково-пошуковий, або евристичний метод; дослідницький, при захисті лабораторних робіт та індивідуальних завдань використовується дискусійний метод.

10. Форми контролю та методи оцінювання

Поточний контроль здійснюється за результатами виконання 2 контрольних робіт за змістовими модулями, захисту індивідуального завдання.

Оцінюється також активність студента в процесі занять: усне опитування на лекції, написання звітів до лабораторних робіт, їх захист, розв'язання практичних задач. Підсумковий контроль - екзамен.
При оцінюванні в балах рівня засвоєння матеріалу використовуються загальні критерії оцінювання навчальних досягнень здобувачів вищої освіти:

Критерії оцінювання виконання самостійної роботи

Результати індивідуального завдання представляються на папері (2-3 сторінки) або у вигляді доповіді (7-10 хв), що супроводжується презентацією (5-7 слайдів).
Критеріями оцінювання є: повнота представленого матеріалу, якість доповіді та презентації, відповідей на запитання викладача та однокурсників.

Критерії оцінювання виконання лабораторних робіт

Студент повинен виконати всі лабораторні роботи. За виконання розрахунків та оформлення роботи згідно вимог методичних вказівок до лабораторних робіт нараховується 7 балів за кожну роботу. При захисті роботи, за кожну правильну відповідь на запитання додається 1 бал. За неправильну відповідь, або її відсутність бали не додаються. Максимальна кількість балів за лабораторну роботу не повинна перевищувати 10 балів. При виставленні підсумкової оцінки береться середня арифметична оцінка за всіма лабораторними роботами.

Критерії оцінювання підсумкового контролю

Підсумковий семестровий контроль (екзамен) проводиться в усній формі. Екзаменаційний білет містить два теоретичних питання, кожне з яких оцінюється окремо за 20 бальною шкалою.
Критерії оцінювання теоретичного питання:
– повна розгорнута відповідь – 20 балів;
– повна, але не розгорнута відповідь – 17 балів;
– повна, але не розгорнута відповідь, яка містить незначну помилку чи суперечність – 15 балів, за кожну наступну незначну помилку чи суперечність знімається 1 бал;
– неповна відповідь, яка не містить критичних помилок чи суперечностей – 10 балів,
за кожну наступну незначну помилку чи суперечність знімається 1 бал;
– відповідь, що містить критичну помилку чи неточність, або відсутність відповіді оцінюється в 0 балів.
Кількість балів, що здобувач отримав на іспиті, є сумою балів, що були отримані за кожне завдання з екзаменаційного білету.
Кінцева оцінка виставляється за сумою балів поточного та підсумкового контролю за шкалою, що наведена нижче (п.12).

11. Питання для підготовки для поточного та підсумкового контролю.

1. Політика безпеки. Основні поняття та принципи.
2. Структура політики безпеки та її основні частини.

3. Життєвий цикл розробки систем безпеки.
4. Система безпеки. Основні поняття про інформацію.
5. Поняття про інформацію з обмеженим доступом.
6. Основні поняття щодо системи безпеки відповідно до "Оранжевої книги".
7. Критерії європейського стандарту у галузі оцінки захищеності комп'ютерних систем.
8. Основні поняття українського стандарту у галузі оцінки захищеності комп'ютерних систем – НД ТЗІ 2.5-004-99 України.
9. Механізми безпеки інформаційних систем.
10. Основні принципи захисту інформації при підключенні до мережі Інтернет.
11. Захист інформації в інформаційних системах за допомогою міжмережевих екранів.
12. Основні режими використання мережних протоколів.
13. Забезпечення конфіденційності, цілісності та автентичності даних в IP-мережах.
14. Забезпечення безпеки даних в інформаційних системах за допомогою Log-сервера.
15. Забезпечення безпеки даних в інформаційних системах за допомогою Proxy-сервера.
16. Забезпечення електронної пошти за допомогою антивірусних програм.
17. Основні вимоги, які висуваються до обчислювальних мереж та інформаційних систем.
18. Модель реалізації загроз інформаційних ресурсів в інформаційних системах.
19. Моделі порушника в сучасних глобальних (локальних) мережах та інформаційних системах.
20. Організація захисту пам'яті в сучасних ПК.
21. Моделі безпеки, що застосовуються при побудові захисту в СУБД.
22. Формальні моделі доступу до інформації. Дискреційний та мандатний доступ до даних в інформаційних системах.
23. Основи захищеності сучасних операційних систем.
24. Підсистема захисту в ОС Windows. Основні послуги та механізми захисту.
25. Підсистема захисту в ОС Linux. Основні переваги і недоліки.
26. Класифікація сучасних криптосистем та основні вимоги до них.
27. Комбіновані криптосистеми. Їх переваги та недоліки.
28. Основні математичні операції щодо побудови криптосистем.
29. Математична модель секретної системи. Основні вимоги щодо забезпечення криптостійкості інформаційних систем.
30. Основні вимоги щодо криптостійкості секретного (особистого) ключа у симетричних та асиметричних криптосистемах.

31. Основні операції шифрування у DES (DataEncryptionStandard) – стандарті шифрування даних США.
32. Основні модифікації шифру DES (3DES, DESX). Переваги та недоліки.
33. Основні режими роботи блоково-симетричних шифрів на основі використання алгоритму DES.
34. Сучасні потокові шифри, їх переваги та недоліки.
35. Алгоритм асиметричного шифрування даних RSA, його криптостійкість та швидкість роботи.
36. Основні операції алгоритму Ель-Гамаля, його безпека та криптостійкість.
37. Протоколи забезпечення автентичності даних за допомогою алгоритмів RSA.
38. Основні вимоги щодо криптостійкості асиметричних криптосистем.
39. Спеціальні механізми безпеки на основі використання асиметричних алгоритмів шифрування даних в інформаційних системах.
40. Поняття про хешувальні алгоритми, їх призначення, вимоги до них.
41. Алгоритми формування кодів-хешування за допомогою безключових хеш-функцій.
42. Коди цілісності даних (MDC-коди). Способи використання у сучасних інформаційних системах.
43. Коди автентичності даних (MAC-коди). Способи їх побудови.
44. Основні поняття універсальних класів хешування даних. Побудова каскадних схем хешування на основі використання хеш-функцій на універсальних класах.
45. Поняття цифрового підпису, вимоги до нього.
46. Класифікація схем цифрового підпису. Основні алгоритми (стандарти) ЕЦП.
47. Операції схеми цифрового підпису на основі алгоритму Ель-Гамаля (стандарт DSA).
48. Протоколи колективного підпису на основі протоколу ECPR.
49. Основні поняття теорії криптоаналізу.
50. Класифікація атак на криптоалгоритми.
51. Основні поняття диференціального криптоаналізу.
52. Основні поняття лінійного криптоаналізу.
53. Сутність атаки дешифрування ітераціями.
54. Сутність атаки на спільний модуль.
55. Сутність атаки на електронний підпис.
56. Сутність атаки на основі обраного тексту (chosen-text attack).
57. Сутність атаки на основі обраного шифротексту (chosenciphertext attack).
58. Нові асиметричні алгоритми на основі еліптичних кривих. Основні переваги та недоліки.
59. Математичні моделі нелінійних вузлів замін (S-box). Основні математичні операції при їх побудові.

60. Генерування випадкових та псевдовипадкових послідовностей щодо використання в механізмах безпеки інформаційних систем.
61. Сучасні алгоритми побудови каскадних хеш-функцій на універсальних класах.
62. Основні положення керування ключами. Життєвий цикл криптографічного ключа.
63. Безпека керування ключами. Протоколи забезпечення безпеки ключів.

12. Розподіл балів, які отримують здобувачі

Поточний та періодичний контроль																		**Індивідуальне самостійне завдання**	**Підсумковий контроль (екзамен)**	**Сума балів**
Змістовий модуль 1									**Змістовий модуль 2**											
Т1	Т2	Т3	Т4	Т5	Т6	Т7	КР	ЛР	Т8	Т9	Т10	Т11	Т12	Т13	Т14	Т15	КР	ЛР			
1	1	1	1	1	1	1	7	10	1	1	1	1	1	1	1	1	8	10	10	40	100

Т1…Т15 – теми, КР – контрольна робота, ЛР – лабораторні роботи

Контрольна робота за змістовим модулем здійснюється у формі письмових тестових завдань після вивчення матеріалу кожного змістового модуля. Тестові письмові завдання для модульних контрольних робіт складаються з 7 (Змістовий модуль 1) або 8 (Змістовий модуль 2) тестових завдань і відповідають змісту навчального матеріалу модуля. За кожну правильну відповідь на одне тестове завдання студент отримує 1 бал.

Розподіл балів за видами навчальної роботи

Види навчальної роботи	Бали за одне заняття (завдання)	Кількість занять	Сумарна кількість балів
Змістовий модуль 1			
Поточний контроль на лекціях	1	7	7
Виконання і захист лабораторних робіт	10	4	10 (середня)
Контрольна робота	7	1	7
Усього за змістовим модулем 1			**0 - 24**
Змістовий модуль 2			
Поточний контроль на лекціях	1	8	8
Виконання і захист лабораторних робіт	10	4	10 (середня)
Контрольна робота	8	1	8
Усього за змістовим модулем 2			**0 - 26**

Виконання та захист ІНДЗ			0 - 10
Підсумковий контроль (екзамен)			0 - 40
Підсумкова сума балів			**0 - 100**

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності		**Оцінка за національною шкалою**	
	Оцінка ЄКТС	для екзамену, курсового проекту (роботу), 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	не зараховано
1-34	F		

Оцінка за національною шкалою та **відсоток від максимальної кількості балів**	Теоретична підготовка	Практична підготовка
	Здобувач освіти	
відмінно (90-100% від максимальної кількості балів)	у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає під час усних виступів та письмових відповідей; глибоко та всебічно розкриває зміст теоретичних питань, використовуючи при цьому нормативну, обов'язкову та додаткову літературу; робить самостійні висновки, виявляє причинно-наслідкові зв'язки; самостійно знаходить додаткову інформацію та використовує її для реалізації поставлених перед ним завдань. Здобувач здатен виділяти суттєві ознаки вивченого за допомогою операцій синтезу, аналізу, виявляти причинно-наслідкові зв'язки, формувати висновки і узагальнення, вільно оперувати	глибоко та всебічно розкриває сутність практичних/ розрахункових завдань, використовуючи при цьому нормативну, обов'язкову та додаткову літературу; може аргументовано обрати раціональний спосіб виконання завдання й оцінити результати власної практичної діяльності; виконує творчі завдання та ініціює нові шляхи їх виконання; вільно використовує набуті теоретичні знання при аналізі практичного матеріалу; проявляє творчий підхід до виконання індивідуальних та

	фактами та відомостями.	колективних завдань при самостійній роботі.
добре (75-89% від максимальної кількості балів)	достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, використовуючи при цьому нормативну та обов'язкову літературу; при представленні деяких питань не вистачає достатньої глибини та аргументації, застосовує знання для розв'язання стандартних ситуацій; самостійно аналізує, узагальнює і систематизує навчальну інформацію, але допускаються при цьому окремі несуттєві неточності та незначні помилки.	правильно вирішив більшість розрахункових /тестових завдань за зразком; має стійкі навички виконання завдання
задовільно (60-74% від максимальної кількості балів)	володіє навчальним матеріалом на репродуктивному рівні або відтворює певну частину навчального матеріалу з елементами логічних зв'язків, знає основні поняття навчального матеріалу; має ускладнення під час виділення суттєвих ознак вивченого; під час виявлення причинно-наслідкових зв'язків і формулювання висновків.	може використовувати знання в стандартних ситуаціях, має елементарні, нестійкі навички виконання завдання. Правильно вирішив половину розрахункових/тестових завдань. Здобувач має ускладнення під час виділення суттєвих ознак вивченого; під час виявлення причинно-наслідкових зв'язків і формулювання висновків.
незадовільно з можливістю повторного складання (35-59% від максимальної кількості балів)	володіє навчальним матеріалом поверхово й фрагментарно (без аргументації та обґрунтування); безсистемно виокремлює випадкові ознаки вивченого; не вміє робити найпростіші операції аналізу і синтезу; робити узагальнення, висновки; під час відповіді допускаються суттєві помилки	недостатньо розкриває сутність практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив окремі розрахункові/тестові завдання за допомогою викладача, відсутні сформовані уміння та навички.

незадовільно з обов'язковим повторним вивченням дисципліни (0-34% від максимальної кількості балів)	не володіє навчальним матеріалом	виконує лише елементи завдання, потребує постійної допомоги викладача

13. Навчально-методичне забезпечення

Навчально-методичне забезпечення: робоча програма навчальної дисципліни; силабус, конспекти лекцій; презентації; методичні вказівки до виконання лабораторних робіт, первинний інструктаж з техніки безпеки, порядок виконання лабораторних робіт:

14. Рекомендована література

Основна

1. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.
2. Остапов С. Е Технології захисту інформації: навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків: Вид. ХНЕУ, 2013. 476 с.
3. Захист інформації в автоматизованих системах управління: навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.
4. Семенов С.Г. 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.
5. Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштінський, А. В. Бережний. – Суми: Сумський державний університет, 2011. 138 с.
6. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Харків: ХНЕУ, 2011. 510 с.

Додаткова

1. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. 53 с.
2. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. 14 с.

3. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. К.: Держстандарт України, 2003.
4. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція хешування. – Чинний з 29.12.2014 р. – ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. 228 с.
5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. 228 с.

15. Електронні інформаційні ресурси

1. https://mon.gov.ua/ – офіційний сайт Міністерства освіти і науки України;
2. http://nbuv.gov.ua/ - Сайт Національної бібліотеки України імені В. І. Вернадського;
3. http://www.dnpb.gov.ua/ - Сайт Державної науково-педагогічної бібліотеки України імені В.О. Сухомлинського;
4. http://onu.edu.ua/- Сайт бібліотеки ОНУ імені 1.1. Мечникова;
5. http://odnb.odessa.ua/ - Сайт Одеської національної наукової бібліотеки;
6. http://korolenko.kharkov.com/ - Сайт Харківської державної наукової бібліотеки імені В.Г. Короленка.