МІЖНАРОДНИЙ ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут «Європейська школа бізнесу»
Кафедра інформаційних технологій

ЗАТВЕРДЖЕНО
Директор ННІ
«Європейська школа бізнесу»
_____Юлія РЕМИГА
від «11»09 2023 р.
М.П.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Рівень вищої освіти перший (бакалаврський)

Спеціальність 121 «Інженерія програмного забезпечення»

Освітня програма «Інженерія програмного забезпечення»

Київ – 2023

Робоча програма навчальної дисципліни «Безпека програм та даних» складена на основі освітньо-професійної програми 121 «Інженерія програмного забезпечення» для першого (бакалаврського) рівня спеціальності 121 «Інженерія програмного забезпечення», затвердженої Вченою радою Університету «30» травня 2023 року, протокол № 4.

Укладач: Нестеренко Олександр Васильович, доктор технічних наук, доцент

Рецензент: Фаловський Олександр Олександович, к.т.н.

Гарант освітньої програми:  Олександр НЕСТЕРЕНКО, доктор технічних наук, доцент

Робочу програму навчальної дисципліни розглянуто та схвалено кафедрою інформаційних технологій, протокол від 31.08.2023 р. № 1.

ВСТУП

Програма вивчення навчальної дисципліни «Безпека програм та даних» складена відповідно до Стандарту вищої освіти України (далі – Стандарт) галузі знань 12 «Інформаційні технології» спеціальності 121 «Інженерія програмного забезпечення».

Опис навчальної дисципліни (анотація). Дана навчальна дисципліна належить до обов'язкових компонентів освітньої програми «Інженерія програмного забезпечення» підготовки майбутніх розробників програмного забезпечення.

Таблиця 1

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній рівень</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>Галузь знань,
12 «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»</td><td colspan="2">Нормативна</td></tr>
<tr><td>Розділів – 2</td><td rowspan="8">Спеціальність:
121 «ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових розділів – 4</td><td>4</td><td>4</td></tr>
<tr><td rowspan="6">Індивідуальне науково-дослідне завдання:
стартап</td><td colspan="2">Семестр</td></tr>
<tr><td>7</td><td>7</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>22</td><td>4</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32</td><td>8</td></tr>
<tr><td rowspan="6">Тижневе навантаження:
аудиторних – 4
самостійної роботи студента – 6</td><td rowspan="6">Освітній рівень:
бакалавр</td><td colspan="2">Самостійна робота</td></tr>
<tr><td>96</td><td>138</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td>екзамен</td></tr>
</table>

Предметом вивчення навчальної дисципліни є комп'ютерні мережі.

Міждисциплінарні зв'язки: програма упорядкована відповідно до анотації освітньо-професійної програми підготовки бакалаврів, базується на вивченні дисциплін «Фізика (вибрані розділи)», «Методи та засоби інформаційних технологій», «Архітектура та проектування програмного забезпечення», «Архітектура комп'ютера», передує вивченню нормативних дисциплін «Конструювання програмного забезпечення», «Емпіричні методи програмної інженерії» .

Знання, отримані здобувачами вищої освіти під час вивчення дисципліни «Безпека програм та даних» можуть бути застосовані під час проходження виробничої практики, підготовки кваліфікаційних робіт за спеціальністю.

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1.1. **Метою** вивчення дисципліни «Безпека програм та даних» є опанування здобувачами вищої освіти принципів захисту програмного забезпечення упродовж всього його життєвого циклу, знань щодо сучасних стандартів, підходів, методів та засобів захисту програм та даних, дослідження та використання сучасних процедур забезпечення основних послуг безпеки інформації в кіберпросторі, що засновані на використанні алгоритмів криптографії, електронному цифровому підписі та протоколах інфраструктури відкритих ключів.

1.2. Основними **завданнями** вивчення дисципліни «Безпека програм та даних» є:

- опанування основних відомостей про потенційні загрози та типи атак, про проблеми захисту програм та даних;
- вивчення та використання основних методів кодування та шифрування даних, знання та використання різних криптографічних методів та систем захисту даних
- формування вміння класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп'ютерних вірусів, захищати інформацію персонального комп'ютера та розроблене програмне забезпечення, розробляти індивідуальні системи управління доступом і захистом інформації.

.

1.3. **Компетентності та результати навчання,** формуванню яких сприяє дисципліна (взаємозв'язок з нормативним змістом підготовки здобувачів вищої освіти, сформульованим у термінах результатів навчання у Стандарті).

Згідно з вимогами стандарту дисципліна забезпечує набуття студентами ***компетентностей*** (Таблиця 2):

Таблиця 2

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані завдання або практичні проблеми інженерії програмного забезпечення, що характеризуються комплексністю та невизначеністю умов, із застосуванням теорій та методів інформаційних технологій.
Спеціальні (фахові, предметні) компетентності	СК6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

Інтегративні кінцеві програмні результати навчання, формуванню яких сприяє навчальна дисципліна:

Програмні результати навчання	ПР02. Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти інженерії програмного забезпечення і дотримуватись їх в професійній діяльності.

	ПР14. Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проєктування, тестування, візуалізації, вимірювань та документування програмного забезпечення. ПР16. Мати навички командної розробки, погодження, оформлення і випуску всіх видів програмної документації. ПР23. Вміти документувати та презентувати результати розробки програмного забезпечення.

Після опанування дисципліни студент повинен

знати:

- основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки даних; основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки;
- моделі порушника, основні види атак, принципи лінійного та диференційного криптоаналізу;
- механізми та протоколи керування ключами в інформаційній системі;

уміти:

- застосовувати сучасні блочні симетричні шифри і режими шифрування;
- аналізувати крипостійкість простих симетричних шифрів;
- досліджувати сучасні асиметричні криптосистеми шифрування;
- аналізувати безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти PGP;
- проводити статистичні дослідження генераторів випадкових і псевдовипадкових послідовностей за методикою NIST.

2. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

РОЗДІЛ 1

ЗМІСТОВИЙ РОЗДІЛ 1
БЕЗПЕКА І ЗАХИСТ ПРОГРАМ І ДАНИХ

Тема 1.1. Основні поняття безпеки програм та даних.
Тема 1.2. Основні принципи захисту програмного забезпечення.
Тема 1.3. Ідентифікація та автентифікація користувачів.
Тема 1.4. Системи аналізу захищеності мережі.

ЗМІСТОВИЙ РОЗДІЛ 2
ОСНОВИ ПОБУДОВИ СИСТЕМ ЗАХИСТУ ПРОГРАМ І ДАНИХ

Тема 2.1. Методи та засоби обмеження доступу до програм та даних.
Тема 2.2. Захист програм від несанкціонованого дослідження.
Тема 2.3. Криптографічний захист інформації.

Тема 2.4. Віртуальні приватні мережі.

РОЗДІЛ 2

ЗМІСТОВНИЙ РОЗДІЛ 3
КРИПТОГРАФІЧНИЙ ЗАХИСТ ПРОГРАМ І ДАНИХ

Тема 3.1. Механізми шифрування. Симетричні та несиметричні криптосистеми.
Тема 3.2. Основи технології відкритих ключів (PKI).
Тема 3.3. Основи цифрової стеганографії.
Тема 3.4. Основи криптоаналізу.

ЗМІСТОВНИЙ РОЗДІЛ 4
БЕЗПЕКА В ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ

Тема 4.1. Основні принципи захисту програмного забезпечення.
Тема 4.2. Захист програмного забезпеченні в Інтернет-технологіях.
Тема 4.3. Захист персональних даних.
Тема 4.4. Комплексні системи захисту інформації.

Назви розділів і тем	Кількість годин			
	Всього	у тому числі		
		Лекції	Лабораторні	СРС
Розділ 1.				
Змістовний розділ 1. БЕЗПЕКА І ЗАХИСТ ПРОГРАМ І ДАНИХ				
Тема 1.1. Основні поняття безпеки програм та даних	5	1		4
Тема 1.2. Основні принципи захисту програмного забезпечення	5	1		4
Тема 1.3. Ідентифікація та автентифікація користувачів	11	1	4	6
Тема 1.4. Системи аналізу захищеності мережі	11	1	4	6
Разом за змістовним розділом 1	32	4	8	20
Змістовний розділ 2. ОСНОВИ ПОБУДОВИ СИСТЕМ ЗАХИСТУ ПРОГРАМ І ДАНИХ				
Тема 2.1. Методи та засоби обмеження доступу до програм та даних	7	1		6
Тема 2.2. Захист програм від несанкціонованого дослідження	11	1	4	6
Тема 2.3. Криптографічний захист інформації	9	1	2	6
Тема 2.4. Віртуальні приватні мережі	9	1	2	6
Разом за змістовним розділом 2	36	4	8	24
Разом за розділом 1	68	8	16	44

Розділ 2.				
Змістовний розділ 3. КРИПТОГРАФІЧНИЙ ЗАХИСТ ПРОГРАМ І ДАНИХ				
Тема 3.1. Механізми шифрування. Симетричні та несиметричні криптосистеми	11	2	2	7
Тема 3.2. Основи технології відкритих ключів (PKI)	11	2	2	7
Тема 3.3. Основи цифрової стеганографії	11	2	2	7
Тема 3.4. Основи криптоаналізу	11	2	2	7
4	44	8	8	28
Змістовний розділ 4. ВІДНОВЛЕННЯ ТА РЕЗЕРВНЕ КОПІЮВАННЯ ДАНИХ				
Тема 4.1. Основні принципи захисту програмного забезпечення	7	1		6
Тема 4.2. Захист програмного забезпеченні в Інтернет-технологіях	11	1	4	6
Тема 4.3. Захист персональних даних	10	2	2	6
Тема 4.4. Комплексні системи захисту інформації	10	2	2	6
Разом за змістовним розділом 4	38	6	8	24
Разом за розділом 2	82	14	16	52
Всього	150	22	32	96

4. ТЕМИ ЛЕКЦІЙ

№ лекції	Назва теми лекції та перелік основних питань
1	Тема 1.1. ОСНОВНІ ПОНЯТТЯ БЕЗПЕКИ ПРОГРАМ ТА ДАНИХ. Предмет і задачі захисту програм і даних. Вразливість комп'ютерних систем. Політика безпеки в комп'ютерних системах. Оцінка та механізми захисту програм та даних. Стандарти захисту даних. Тема 1.2. ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. Технологія тіньового копіювання даних, обмеження тіньового копіювання томів, установка і використання технології тіньового копіювання томів, архівація даних, робота з програмою архівації backup, стратегії архівації, створення відмовостійких томів для зберігання даних, робота з дзеркальними.
2	Тема 1.3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ. Ідентифікація користувачів. Автентифікація користувачів. Перевірка автентичності користувачів. Протоколи ідентифікації. Тема 1.4. СИСТЕМИ АНАЛІЗУ ЗАХИЩЕНОСТІ МЕРЕЖІ. Принципи роботи систем аналізу захищеності. Microsoft Baseline Security Analyzer. Опис перевірок, виконуваних MBSA. Сканер безпеки XSpider.
3	Тема 2.1. МЕТОДИ ТА ЗАСОБИ ОБМЕЖЕННЯ ДОСТУПУ ДО ПРОГРАМ ТА ДАНИХ. Вразливість комп'ютерних систем. Способи проникнення до комп'ютерних систем. Спостереження за користувачами КС. Особливості обмеження доступу до програм та даних. Тема 2.2. ЗАХИСТ ПРОГРАМ ВІД НЕСАНКЦІОНОВАНОГО ДОСЛІДЖЕННЯ. Методи дослідження програмного коду. Засоби дослідження програмного коду. Принципи та підходи щодо захисту програмного коду від несанкціонованого дослідження.

4	Тема 2.3. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. Основні поняття та визначання криптографічного захисту інформації. Симетричне та асиметричне шифрування. Цифрові підписи. Хеш-функції. Цифрові сертифікати. Технологія Blockchain
	Тема 2.4. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ. Поняття про віртуальні захищені (приватні) мережі (VPN). Види віртуальних приватних мереж. Сервіси VPN. Способи утворення захищених тунелів. Рівні реалізації VPN. Протоколи: SSL, SOCKS, IPSec, PPTP, L2F, L2TF
5	Тема 3.1. МЕХАНІЗМИ ШИФРУВАННЯ. СИМЕТРИЧНІ ТА АСИМЕТРИЧНІ КРИПТОСИСТЕМИ. Основні класи симетричних криптосистем (транзитивні, регулярні та мінімальні криптосистеми). Визначення і математичні моделі шифрів простої заміни та перестановки. Методика дешифрування простої заміни та перестановки. Основні класи симетричних криптосистем. Математична модель і принципи побудови потокових шифрів. Принципи побудови і критерії стійкості шифрів гамування. Загальні принципи побудови і використання асиметричних криптографічних систем. Основні класи задач, що вирішуються з використанням асиметричних криптографічних систем. Система відкритого шифрування RSA. Схема цифрового підпису RSA. Розв'язання задач зашифрування, розшифрування і цифрового підпису повідомлень з використанням криптосистеми RSA
6	Тема 3.2. ОСНОВИ ТЕХНОЛОГІЇ ВІДКРИТИХ КЛЮЧІВ (PKI). Основні компоненти і сервіси інфраструктури відкритих ключів. Архітектура та топологія PKI. Сертифікати відкритих ключів X.509.
7	Тема 3.3. ОСНОВИ ЦИФРОВОЇ СТЕГАНОГРАФІЇ. Основні принципи приховування повідомлення на основі методів стеганографії. Класифікація і принципи приховування алгоритмів цифрової стеганографії
8	Тема 3.4. ОСНОВИ КРИПТОАНАЛІЗУ. Історія криптоаналізу та загальні відомості. Задачі криптоаналізу. Криптографічна стійкість. Теоретична та практична стійкість шифру. Абсолютна стійкість. Принцип Кірхгофа. Методи криптоаналізу. Частотний криптоаналіз, метод повного перебору. Криптоаналіз шифрів простої заміни. Програмна реалізація криптоаналізу шифрів зсуву (шифр Цезаря)
9	Тема 4.1. ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. Основні алгоритми захисту програмного забезпечення. Показники застосовності та критерії оцінювання. Основні вимоги до розробки систем захисту програмного забезпечення. Локальне і віддалене резервне копіювання. Тема 4.2. ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННІ В ІНТЕРНЕТ-ТЕХНОЛОГІЯХ. Основні принципи захисту інформації під час підключення до мережі Інтернет. Використання паролів і механізмів контролю.
10	Тема 4.3. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ. Основні принципи захисту персональних даних на основі програмного коду. Моделі захисту персональних даних.
11	Тема 4.4. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ. Поняття комплексності захисту інформації. Загальні положення про комплексні системи захисту інформації. Сутність та задачі КСЗІ. Суб'єкти та об'єкти захисту КСЗІ. Атестація системи захисту інформації

5. ТЕМИ ЛАБОРАТОРНО-ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1.	Логування дій користувачів у програмних системах	4
2.	Розробка програми розмежування повноважень користувачів на основі парольного аутентифікації	4
3.	Захист веб-ресурсів від ботів та спаму за допомогою механізму CAPTCHA.	4
4.	Формування вмінь і навиків реалізації Blockchain.	2
5.	Інструменти створення віртуальних приватних мереж	2
6.	Використання хеш-функцій (на прикладі MD5), оцінка стійкості паролю до зламу	2
7	Електронний цифровий підпис на прикладі GnuPG для захисту документів та електронної пошти	2
8	Методи приховування інформації в потоках даних	2
9	Алгоритми та методи шифрування в комп’ютерних системах	2
10	Інструментальні засоби захисту програм та даних	4
11	Розробка політики конфіденційності IT-компанії відповідно до вимог GDPR	2
12	Створення DMZ (demilitarized zone) для IT-компанії з урахуванням питань безпеки даних	2
Разом:		32

6. САМОСТІЙНА РОБОТА

№ з/п	Назва теми	Кількість годин
1.	Історія створення і розвитку засобів захисту програм і даних.	4
2.	Інформація, міри інформації, коди.	4
3.	Технології ідентифікації та автентифікації. Біометрія	6
4.	Сканери портів, сканери, що досліджують топологію комп'ютерної мережі, мережеві хробаки, CGI-сканери	6
5.	Політики безпеки та програми безпеки. Види документів	6
6.	Сучасні технології дампингу і захисту від нього	6
7.	Асиметричні методи шифрування та їх підтримка у бібліотеках мов програмування.	6
8.	Протоколи VPN	6
9.	Використання хеш-функцій для захисту програм та даних	7
10.	Інструментальні засоби електронного цифрового підпису	7
11.	Методи приховування інформації в потоках даних на основі цифрової стеганографії	7
12.	Криптоаналіз поліалфавітних шифрів. Шифр Віженера.	7
13	Методи захисту виконуваних файлів (програм) від зламу та налагодження	6
14	Захист програм з використанням антивірусних засобів	6
15	Європейські правові стандарти захисту персональних даних	6
16	Захист інформації від витоку технічними каналами	6
Разом:		96

7. МЕТОДИ НАВЧАННЯ

При викладанні навчальної дисципліни «Безпека програм та даних» застосовуються інформаційні та практичні методи навчання: класичні лекції, лекції-дискусії та лабораторні заняття, а також консультації з виконання самостійної роботи студентів, письмові завдання при проведенні контрольних робіт.

Методи навчально-пізнавальної діяльності: пояснювально-ілюстративний метод, репродуктивний метод, метод проблемного викладу, частково-пошуковий або евристичний метод, дослідницький метод.

Методи стимулювання й мотивації навчально-пізнавальної діяльності: індуктивні і дедуктивні методи навчання, методи стимулювання і мотивації навчання.

8. МЕТОДИ КОНТРОЛЮ

Відповідно до плану вивчення дисципліни «Безпека програм та даних» передбачається проведення поточного та підсумкового контролю.

Поточний контроль – оцінювання рівня знань, умінь та навичок осіб, які навчаються, що здійснюється в ході навчального процесу шляхом проведення письмового опитування по закінченню розділів (модульний колоквіум). Модульний контроль при особливих ситуаціях може проводитись у формі мережевого комп'ютерного тесту з фіксованим часом відповіді.

9. ФОРМА ПІДСУМКОВОГО КОНТРОЛЮ УСПІШНОСТІ НАВЧАННЯ

Формою підсумкового контролю є **екзамен**, який складається очно (при особливій ситуації – у формі комп'ютерного тесту) в період призначений деканатом або за індивідуальним графіком, який затверджується навчальним планом.

10. СХЕМА НАРАХУВАННЯ ТА РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ

Накопичення балів протягом семестру

№ з/п	Вид діяльності	Кількість балів за дидактичну одиницю	Кількість	Загальна кількість балів
1	Тестування за матеріалами лекцій	2	11	22
2	Виконання лабораторних робіт	3	12	36
3	Виконання самостійних робіт	1	2	2
Екзамен		40		40
Максимальна оцінка				100

Загальна оцінка знань студентів за поточним контролем

Результати поточного контролю знань студентів в цілому оцінюються в діапазоні від **0** до **60** балів.

Студент допускається до підсумкового контролю за умови виконання вимог навчальної програми та у разі, якщо за поточну навчальну діяльність він набрав не менше **36** балів.

Підсумкове оцінювання знань студентів

Підсумкове оцінювання знань студентів проводиться у формі **екзамену**.

Критерії оцінювання знань під час іспиту

Максимальна кількість балів, яку можна отримати на екзамені складає **40** балів.

Розподіл балів оцінювання при підсумковому контролі з навчальної дисципліни

Оцінка в балах за поточне оцінювання	Оцінка в балах за підсумкове оцінювання	Оцінка за національною шкалою
54-60	36-40	Відмінно
45-53	30-35	Добре
36-44	24-29	Задовільно
менше 36	менше 24	Незадовільно

Під час оцінювання відповіді на окреме питання додатково враховуються допущені недоліки та помилки, якими вважаються:

– неохайне оформлення роботи (не загальноприйняті скорочення, незрозумілий почерк, використання олівців замість чітких чорнил) (мінус **2** бали);

– неточності в назвах окремих термінів та понять (мінус **4** бали).

Критерії оцінювання відповіді на теоретичні питання білету:

1. Повна відповідь на питання, яка оцінюється ***«відмінно»***, повинна відповідати таким вимогам:

– розгорнутий, вичерпний виклад змісту даної у питанні проблеми;

– повний перелік необхідних для розкриття змісту питання термінів та положень;

– здатність здійснювати порівняльний аналіз різних систем та самостійно робити логічні висновки й узагальнення;

– уміння користуватись методами наукового аналізу;

– демонстрація здатності висловлення та аргументування власного ставлення до альтернативних поглядів на дане питання;

2. Відповідь на питання оцінюється ***«добре»***, якщо:

– відносно відповіді на найвищий бал не зроблено розкриття хоча б одного з пунктів, вказаних вище (якщо він явно потрібний для вичерпного розкриття питання) або, якщо:

– при розкритті змісту питання в цілому правильно за зазначеними вимогами зроблені окремі помилки під час: використання формул.

3. Відповідь на питання оцінюється ***«задовільно»***, якщо:

– відносно відповіді на найвищий бал не зроблено розкриття чотирьох чи більше пунктів, зазначених у вимогах до нього (якщо вони явно потрібні для вичерпного розкриття питання);

– одночасно присутні чотири чи більше типів недоліків, які окремо характеризують критерій оцінки питання;

– висновки, зроблені під час відповіді, не відповідають правильним чи загально визначеним при відсутності доказів супротивного аргументами, зазначеними у відповіді;

– характер відповіді дає підставу стверджувати, що особа, яка складає іспит, не зовсім правильно зрозуміла зміст питання чи не знає правильної відповіді і тому не відповіла на нього по суті, допустивши грубі помилки у змісті відповіді.

З урахуванням вищевикладеного результати іспиту оцінюються в діапазоні від **0** до **40** балів для студентів.

Загальна підсумкова оцінка з дисципліни складається з суми балів за результати поточного контролю знань та за виконання завдань, що виносяться на іспит.

Загальна підсумкова оцінка не може перевищувати **100 балів**.

Загальна підсумкова оцінка в балах, за національною шкалою та за шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
66-73	D	задовільно	
60-65	E		
30-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-29	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

11. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

– робоча навчальна програма дисципліни;

– електронний курс у MOODLE з тезами лекцій, інструкціями до лабораторних занять, тестами та матеріалами для самостійної роботи студентів;

– перелік питань до екзамену.

12. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. С. Е. Остапов, С. П. Євсеєв. О. Г. Король. Технології захисту інформації. Чернівці. Видавничий дом “Родовід”, 2014. 428 с.

2. 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.

3. Літнарович Р.М. Сучасні технології інформаційної безпеки. Навчальний посібник. МЕГУ, Рівне, 2011. 97 с.

4. О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. Захист інформації в інформаційних системах. Методи традиційної криптографії. Харків : Вид. ХНЕУ, 2010. 316 с.

5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

6. Дудатьєв А.В., Каплун В.А., Семеренко В.П. Д 81 Захист програмного забезпечення. Частина 1. Навчальний посібник. Вінниця: ВНТУ, 2005. – 140 с.

7. Хант К. TCP/IP. Сетевое администрирование / пер. с англ. СПб. : Символ-Плюс, 2004. 816 с.

8. Мельник І. В. Інформаційні комп’ютерні мережі: Навч. посібник для дист. навчання. К.: Вид. Універ. «Україна», 2006. 250 с.

9. Таненбаум Э. Компьютерные сети: Пер. с англ. 4 изд. Спб: Питер, 2006. 991с

10. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. Издательский дом «Вильямс», 2001. 672 с.

Інтернет ресурси

1. Захист інформації. Режим доступу:
https://uk.wikipedia.org/wiki/Захист_інформації.

2. Комплексні системи захисту інформації. Режим доступу:
https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi

3. Науково-технічний журнал «Зв’язок». - Режим доступу : https://con.dut.edu.ua/index.php/communication