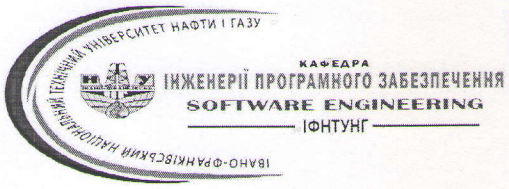
Міністерство освіти і науки України
Івано-Франківський національний технічний університет нафти і газу
Інститут інформаційних технологій
назва інституту випускової кафедри



ЗАТВЕРДЖУЮ
Директор ІІТ
(назва інституту)
Володимир ПІХ
(підпис) (Ім'я ПРІЗВИЩЕ)
«30» 08 2024 р.

РОБОЧА ПРОГРАМА

Безпека програм та даних
(назва навчальної дисципліни)

Освітній рівень перший (бакалаврський)
(назва освітнього рівня)

Галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

Спеціальність 121 Інженерія програмного забезпечення
(код і назва спеціальності)

Спеціалізація _____
(назва спеціалізації за наявності)

Освітня програма Інженерія програмного забезпечення
(назва ОП)

Статус дисциплін обов'язкова
(обов'язкова/вибіркова)

Мова викладання українська

2024 р.

Розробник(и):

доцент, к-ра ІПЗ, к.т.н., доцент _____ Михайло КРИХІВСЬКИЙ
(посада, назва кафедри, науковий ступінь, вчене звання) (підпис) (Ім'я ПРІЗВИЩЕ)
mykhailo.krykhivskyi@nung.edu.ua

Схвалено на засіданні _____кафедри Інженерії програмного забезпечення_____
(назва кафедри)

Протокол від «_30_» _серпня_ 20_24_ року № _9/24_.

Завідувач кафедри _Інженерії програмного забезпечення_ _____ Вікторія БАНДУРА
(назва кафедри) (підпис) (Ім'я ПРІЗВИЩЕ)

Узгоджено:

Гарант ОП _Інженерії програмного забезпечення_ _____ Вікторія БАНДУРА_____
(назва програми) (підпис) (Ім'я ПРІЗВИЩЕ)

1 ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ

Мета і завдання дисципліни	***Метою дисципліни*** *«Безпека програм та даних» є оволодіння студентами комплексом знань у галузі захисту інформації, засобів та методів визначення захищеності програмних продуктів та їх складових, набуття на основі цих знань практичних навичок з розроблення програмного забезпечення певного рівня надійності та захищеності даних.* ***Завдання дисципліни*** *«Безпека програм та даних» полягає в отриманні теоретичних знань щодо принципів побудови та стандартів захисту програмних продуктів, безпеки програмного забезпечення та даних, вивченні сучасних технологій захисту інформації в комп'ютерних мережах, принципи криптографічного захисту, опанування практичних методів захисту програм та даних.*
Посилання на розміщення дисципліни на навчальній платформі	*https://dn.nung.edu.ua/course/view.php?id=1791*
Попередні вимоги для вивчення дисципліни / пререквізити	*Дискретна математика* *Основи програмної інженерії*
Постреквізити	*Якість програмного забезпечення та тестування* *Моделі створення інноваційного ПЗ*
Результати навчання	*ПР01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.* *ПР07. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструменталь-них і обчислювальних засобів інженерії програмного забезпечення.* *ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.*
Компетентності	*ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.* *ЗК2. Здатність застосовувати знання у практичних ситуаціях.* *ЗК5. Здатність вчитися і оволодівати сучасними знаннями.* *ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.* *ЗК7. Здатність працювати в команді.* *ФК6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).* *ФК7. Володіння знаннями про інформаційні моделі даних, здатність створюва* *ти програмне забезпечення для зберігання, видобування та опрацювання даних.* *ФК12. Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності*

	програмного забезпечення.
Підсумковий контроль, форма	*Екзамен*
Перелік соціальних, «м'яких» навичок (softskills)	***Самостійність:*** *Здобувачі навчаються самостійно виконувати завдання, приймати власні рішення без необхідності постійної спрямованості з боку інших учасників.* ***Організаційні навички:*** *Кожен здобувач має вміти організовувати своє робоче середовище, керувати своїми ресурсами та засобами, дотримуватися графіків та виконувати завдання вчасно. Це розвиває вміння планувати та організовувати свою роботу.* ***Критичне мислення:*** *Здобувачі навчаються аналізувати проблеми, шукати ефективні рішення, оцінювати та вдосконалювати свою роботу.* ***Комунікація****: В процесі навчання студенти обмінюються інформацією, консультують, підтримують один одного, обговорюють результати.* ***Креативність****: Безпека програм та даних може спонукати студентів до творчого мислення та знаходження нових, ефективних рішень в інженерії програмного забезпечення.* ***Аналітичні навички****: Застосування засобів безпеки програм та даних вимагає аналізу завдання, розбору його компонентів та визначення оптимального шляху реалізації, що сприяє розвитку аналітичних здібностей.* ***Терпимість до помилок:*** *Оволодіння принципами безпеки програм та даних допомагає здобувачам ступеня бакалавра розвивати терпимість і наполегливість до пошуку та виправлення помилок.*

2 ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1) щодо відвідування занять і поведінки на них

Згідно «Положення про організацію освітнього процесу в Івано-Франківському національному технічному університеті нафти і газу» (від 31.03.2022 р., наказ № 68) відвідування здобувачами вищої освіти всіх аудиторних занять за чинним протягом семестру розкладом є обов'язковим. Відвідування та запізнення не мають прямого впливу на систему нарахування балів, однак у разі систематичних пропусків занять та невиконання передбачених оцінюваних активностей (тестування, лабораторних робіт), викладач залишає за собою право доповісти про даний випадок в дирекцію інституту в письмовій формі.

Під час лекційних занять дозволяється використання мобільних телефонів, ноутбуків та планшетів для перегляду презентаційних та текстових складових лекційних матеріалів. Під час лабораторних занять дозволяється використовувати телефони та планшети для перегляду презентаційних матеріалів, а також власні ноутбуки для виконання лабораторних робіт та демонстрації результатів роботи під час захисту.

Вітається активність студента на лекціях та уміння ставити запитання за темою лекції до викладача.

У разі проведення заняття з використанням засобів дистанційного навчання, доступ до відео-конференції здійснюється виключно з корпоративного облікового запису електронної пошти з метою ідентифікації здобувача вищої освіти. У разі, якщо захисти лабораторних робіт проходять з використанням засобів дистанційного навчання, студент на час захисту роботи зобов'язаний увімкнути відеозв'язок.

2) щодо дотримання принципів академічної доброчесності

Здобувачі освіти зобов'язані неухильно виконувати «Положення про академічні доброчесність працівників та здобувачів вищої освіти Івано-Франківського національного технічного університету нафти і газу» (від 05.04.2022р., наказ №73). Зокрема, самостійно виконувати аудиторні завдання, контрольні роботи, не фальсифікувати свої результати навчання; уникати списування, не користуватися підказками інших осіб під час проведення заходів поточного контролю знань; дотримуватися коректності в посиланнях на джерела інформації у разі запозичення відомостей, тверджень та ідей.

Під час виконання лабораторних робіт допускається використання фрагментів вихідного коду програми з відкритих джерел (форумів, генераторів коду на основі штучного інтелекту, тощо). Вихідний код програми не є об'єктом перевірки на плагіат, хоча оригінальність та нетривіальність рішення може позитивно вплинути на оцінку.

3) щодо оцінювання

За умови виконання всіх лабораторних робіт (оцінка за звіт складає не більше ніж 50% загальної максимальної оцінки за лабораторну роботу і є обов'язковою умовою для зарахування лабораторної роботи як виконаної), складання колоквіуму за результатами лекційного курсу та підтвердження опанування на мінімальному рівні результатів навчання (за семестр отримано не менше 35 балів за шкалою ЄКТС) здобувач вищої освіти допускається до семестрового контролю з дисципліни. Форма семестрового контролю – екзамен.

Заохочувальні бали виставляються за підготовку оглядів наукових праць, презентацій по одній із тем СРС дисципліни, виконання додаткових завдань, тощо. Кількість заохочуваних балів не більше 10.

У разі застосування дистанційної технології навчання поточний та семестровий контролі здійснюються згідно «Положення щодо організації поточного, семестрового контролю та атестації здобувачів вищої освіти із застосуванням дистанційних технологій» від 22.10.2022р. (наказ №262).

4) щодо кінцевих термінів (дедлайнів) та перескладання

Виконана лабораторна робота повинна бути захищена на початку наступного лабораторного

заняття. За кожний тиждень запізнення з поданням звіту з лабораторної роботи нараховується штрафний (–1) бал, але в сумі не більше –2 за одну лабораторну роботу

Умови допуску до перескладання модульного та підсумкового контролів, графік і форми перескладання регламентовані Положення про організацію освітнього процесу в ІФНТУНГ, зазначеному в пункті 1) цього розділу.

5) щодо визнання результатів навчання у неформальній освіті

Результати неформального навчання можуть бути визнані та перезараховані як частина оцінюваних активностей, ПОЛОЖЕННЯ про порядок визнання результатів отриманих у неформальній та інформальній освіті в ІФНТУНГ (https://griml.com/Ew5zh) у разі пред'явлення сертифікату про успішне завершення курсу (з вказаною оцінкою) та у випадку якщо теми онлайн-курсу, тренінгу, курсу відповідають навчальним елементам дисципліни.

6) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до Положення про звернення здобувачів вищої освіти з питань, пов'язаних з освітнім процесом, затвердженого наказом ректора університету № 43 від 24.02.2020 року. Ознайомитись з документом можна за покликанням https://griml.com/L3VUV.

7) щодо конфліктних ситуацій

Спілкування учасників освітнього процесу (викладачі, здобувачі) відбувається на засадах партнерських стосунків, взаємопідтримки, взаємоповаги, толерантності та поваги до особистості кожного, спрямованості на здобуття істинного знання. Вирішення конфліктних ситуацій здійснюється відповідно до Положення про вирішення конфліктних ситуацій в ІФНТУНГ, затвердженого наказом ректора університету № 44 від 24.02.2020 року. Ознайомитись з документом можна за покликанням https://griml.com/i42PI.

8) щодо опитування здобувачів

Після завершення курсу здобувачу надається можливість пройти опитування стосовно якості викладання дисципліни за покликанням https://nung.edu.ua/department/yakist-osviti/04-anketuvannya

9) щодо політики використання інструментів генеративного штучного інтелекту в навчальному процесі

Всі учасники освітнього процесу повинні дотримуватися базових принципів використання інструментів генеративного штучного інтелекту відповідно до Положення про загальні політики використання інструментів генеративного штучного інтелекту в навчальному процесі ІФНТУНГ, затвердженого наказом ректора університету від 15.03.2024 року № 82. Ознайомитись з документом можна за покликанням https://salo.li/1E36Aae.

3 ПРОГРАМА ТА СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

3.1. Обсяг навчальної дисципліни

Ресурс годин на вивчення дисципліни «Безпека програм та даних» згідно зчинним НП, розподіл по семестрах і видах навчальної роботи для різних форм навчання характеризує таблиця 1.

Таблиця 1 – Розподіл годин, виділених на вивчення дисципліни

Найменування показників	Усього	Розподіл по семестрах	
		Семестр _5___	Семестр_____
Кількість кредитів ECTS	6	6	
Загальний обсяг часу, год.	180	180	
Аудиторні заняття, год., у т.ч.:	72	72	
– лекційні заняття	36	36	
– практичні/семінарські заняття	-	-	
– лабораторні заняття	36	36	
Самостійна робота, год	108	108	
Форма семестрового контролю (іспит, залік, захист КР, захист КП)	Іспит	Іспит	

3.2. Лекційні заняття

Тематичний план лекційних занять дисципліни характеризує таблиця 2.

Таблиця 2 – Тематичний план лекційних занять

	Назви модулів (М), змістових модулів (ЗМ), тем (Т)та їх зміст	Кількість годин	Література
М1	**Безпека програм та даних**	36	
ЗМ1	**Основні поняття та принципи безпеки програм та даних**	6	
Т1.1	Конфіденційність, цілісність та доступність даних.	2	1,2
Т1.2	Класифікація загроз. Сервіси та механізми захисту.	2	1,2
Т1.3	Безпека зберігання даних в ОС Microsoft. Центр безпеки.	2	1,2
ЗМ2	**Аналіз захисту, атаки**	6	
Т2.1	Концепція проникнення. Методи та техніки розвідки. Методики сканування.	2	1,2
Т2.2	Атаки введення в оману. Омани ARP, маршрутизації, DNS.	2	1,2
Т2.3	Атака типу «відмова в обслуговуванні». Зловживання фрагментацією пакетів. Розподілені DoS атаки.	2	1,2

ЗМ3	**Криптографічні методи захисту інформації**	6	
Т3.1	Моделі безкоштовного, умовно безкоштовного, комерційного програмного забезпечення. Хмарні моделі.	2	3,4
Т3.2	Алгоритми симетричного шифрування, шифрування з відкритим ключем, хешування.	2	3,4
Т3.3	Цифровий підпис, розподіл ключів шифрування, інфраструктура відкритого ключа. Технологія Blockchain.	2	3,4
ЗМ4	**Системи аутентифікації, управління доступом**	6	
Т4.1	Класифікація методів аутентифікації, словники паролів. Захист пароля, системи з одноразовим паролем.	2	1,2
Т4.2	Матриця доступу, мітки чутливості, інші моделі захисту. Функціонування управління доступом, приховані канали.	2	1,2
Т4.3	Методи дослідження програмного коду. Засоби дослідження програмного коду. Принципи та підходи щодо захисту програмного коду від несанкціонованого дослідження.	2	1,2
ЗМ5	**Захищені мережеві протоколи, брандмауери виявлення вторгнень**	8	
Т5.1	Протоколи IPSec, L2TP, PPTP, SSL та TLS	2	
Т5.2	Фільтрація пакетів, трансляція мережних адрес (NAT). Проксі сервери, етапи побудови брандмауерів.	2	1,2
Т5.3	Поняття про віртуальні захищені (приватні) мережі (VPN). Види віртуальних приватних мереж. Сервіси VPN.	2	1,2
Т5.4	Способи утворення захищених тунелів. Рівні реалізації VPN. Протоколи: SSL, SOCKS, IPSec, PPTP, L2F, L2TF.	2	1,2
ЗМ6	**Політика безпеки, безпека електронної пошти**	4	1,2
Т6.1	Задачі підрозділу безпеки, реалізації політик безпеки.	2	1,2
Т6.2	Властивості безпечної поштової системи. Загрози безпеці систем відправлення пошти. Поштові протоколи і безпека	2	1,2
	Усього годин	36	

3.3. Практичні (семінарські) заняття
Практичні (семінарські) заняття не передбачені.

3.4. Лабораторні заняття

Теми лабораторних занять (перелік лабораторних робіт) дисципліни наведено у таблиці 4.

Таблиця 4 – Теми лабораторних занять

Шифр	Назви модулів (М), змістових модулів (ЗМ), тем лабораторних занять (Л) та їх зміст	Кількість годин	Література
М1	**Безпека програм та даних**	**36**	
ЗМ1	**Основні поняття та принципи безпеки програм та даних**	**2**	
Л1.1	Альтернативні потоки даних.	2	5
ЗМ2	**Аналіз захисту, атаки**	**2**	
Л2.1	Керування доступом MS Windows.	2	5
ЗМ3	**Криптографічні методи захисту інформації**	**26**	
Л3.1	Стеганографія з *.jpeg.	2	5
Л3.2	Криптографічні хеш-функції. Алгоритм MD5.	4	5
Л3.3	Криптографічні хеш-функції. Сімейство алгоритмів SHA.	4	5
Л3.4	Криптографічні хеш-функції. Сімейство алгоритмів RIPEMD.	4	5
Л3.5	Генерація криптографічно-безпечної псевдовипадкової послідовності. Алгоритми FIPS–186, ANSI X9.17.	4	5
Л3.6	Генерація криптографічно-безпечної псевдовипадкової послідовності. Алгоритми BBS (Blum-Blum-Shub), RSA (Шамира), Yarrow–160.	4	5
Л3.7	Статистичні тести.	4	5
ЗМ4	**Системи автентифікації, управління доступом**	**2**	
Л4.1	Створення програми генерації випадкових паролей.	2	5
ЗМ5	**Захищені мережеві протоколи, брандмауери виявлення вторгнень**	**2**	
Л5.1	Захист від копіювання. Прив’язка до апаратного забезпечення. Використання реєстру.	2	5
ЗМ6	**Політика безпеки, безпека електронної пошти**	**2**	
Л6.1	Рольове управління доступом. Розроблення захищених додатків.	2	5
	Усього годин	**36**	

3.5. Завдання для самостійної роботи здобувача

Види самостійної роботи в межах даного курсу наводяться у таблиці 5.

Таблиця 5 – Види самостійної роботи

Найменування видів самостійної роботи	Кількість годин
Опрацювання матеріалу, викладеного на лекціях	18
Опрацювання матеріалу, винесеного на самостійне вивчення	30
Підготування до контрольних заходів	6
Підготування до лабораторних робіт	24
Підготовка до іспиту	30
Усього годин	108

Перелік матеріалу, який виноситься на самостійне вивчення, наведено у таблиці 6.

Таблиця 6 – Матеріал, що виноситься на самостійне вивчення

Шифр	Назви модулів (М), змістових модулів (ЗМ),питання, що виноситься на самостійне вивчення	Кількість годин	Література
			Порядковий номер
М1	Аналіз тенденцій розвитку безпеки програм та даних	30	
ЗМ1	**Основні поняття та принципи безпеки програм та даних**	5	
Т1.1	Засоби здійснення шифрування інформації	5	1,2
ЗМ2	**Аналіз захисту, атаки**	5	
Т2.1	Атака на геш-функцію на базі «Парадокса днів народження»		3,4
ЗМ3	**Криптографічні методи захисту інформації**	10	
Т3.1	Алгоритм підпису ЕльГамаля	5	3,4
Т3.2	Протокол ECKEP	5	3,4
ЗМ4	**Системи автентифікації, управління доступом**	10	
Т4.1	Американський стандарт цифрового підпису ECDSA	5	3,4
Т4.2	Німецький стандарт цифрового підпису EC-GDSA	5	3,4
	Усього годин	30	

4 НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

4.1. Основна література

1. Крихівський М. В., Саманів Л. В. Безпека програм і даних : конспект лекцій. – Івано-Франківськ : ІФНТУНГ, 2024. – 95 с.
2. Горбенко В. І., Лісняк А. О. Безпека програм та даних : навчальний посібник. Запоріжжя: ЗНУ, 2022. – 72 с.
3. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. Інформаційна безпека: навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
4. Щур Н. О., Покотило О. А. Основи криптології : навчальний посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. – 120 с.
5. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навчальний посібник. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
6. Дем'яненко В. А., Кузнецова Ю. А. Безпека програм та даних [Електронний ресурс] : навч. посіб. до лаб. практикуму. – Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського, 2021. – 95 с.

4.2. Додаткова література

7. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.
8. Тарнавський Ю. А. Технології захисту інформації : підручник. – К.: КПІ ім. Ігоря Сікорського, 2018.– 162 с.
9. Kravchenko O. Cybersecurity in the face of information warfare and cyberattacks / O. Kravchenko, V. Veklych, M. Krykhivskyi T. Madryga // Multidisciplinary Science Journal №6(2024) e2024ss0219.
10. Крихівський М. В., Бандура В. В., Ваврик Т. О. Математичні моделі інформаційної безпеки / Прикладні питання математичного моделювання, Том 7 № 1 (2024). – С. 147-154.

4.3. Інформаційні ресурси в Інтернеті

11. The CrypTool Portal [Електронний ресурс]. — Режим доступу : https://www.cryptool.org/en
12. The GNU Privacy Guard [Електронний ресурс]. – Режим доступу : https://gnupg.org/
13. http://esu.com.ua/search_articles.php?id=1576
14. https://archive.org/details/literaturoznavchat1/page/n532/mode/1up?view=theater

5 ФОРМИ ТА МЕТОДИ НАВЧАННЯ Й ОЦІНЮВАННЯ

Форми та методи навчання й оцінювання в межах даного курсу наводяться в таблиці 7.

Таблиця 7 – Забезпечення програмних результатів навчання відповідними формами та методами

Результати навчання	Методи навчання	Форми оцінювання
ПР1, ПР7, ПР21	МН 1.1 – лекція МН 1.3 – бесіда МН 2.4 – комп'ютерні і мультимедійні методи МН 3.2 – лабораторні роботи МН 10 – узагальнення МН 20.3 - мозковий штурм	МФО 1 – іспит МФО 4 – поточний контроль МФО 7 – лабораторно-практичний контроль МФО 8 – тестовий контроль

6. МЕТОДИ КОНТРОЛЮ ТА СХЕМА НАРАХУВАННЯ БАЛІВ

Розподіл балів, які здобувачі освіти можуть отримати за результатами кожного виду поточного та підсумкового контролів, наведено в таблиці 8.

Таблиця 8 – Розподіл балів оцінювання

Види робіт, що контролюються	Максимальна кількість балів
Контроль засвоєння теоретичних знань змістових модулів (комп'ютерне тестування)	40
Виконання 12 лабораторних робіт (по 5 балів за роботу)	60
Максимальна кількість набраних балів	100

Для визначення ступеня оволодіння навчальним матеріалом з подальшим його оцінюванням застосовуються рівні навчальних досягнень здобувачів вищої освіти, наведені в таблиці 9.

Таблиця 9 – Рівні навчальних досягнень

Рівні навчальних досягнень	**Відсоток балу за виконання завдань**	**Критерії оцінювання навчальних досягнень**	
		Теоретична підготовка	**Практична підготовка**
		Здобувач вищої освіти	
Відмінний	*90…100*	вільно володіє навчальним матеріалом, висловлює свої думки, робить аргументовані висновки, рецензує відповіді інших студентів, творчо виконує індивідуальні та колективні завдання; самостійно знаходить додаткову інформацію та використовує її для реалізації поставлених перед ним завдань; вільно використовує нові інформаційні технології для поповнення власних знань	може аргументовано обрати раціональний спосіб виконання завдання й оцінити результати власної практичної діяльності; виконує завдання, не передбачені навчальною програмою; вільно використовує знання для вирішення поставлених перед ним завдань
Достатній	75…89	вільно володіє навчальним матеріалом, застосовує знання на практиці; узагальнює і систематизує навчальну інформацію, але допускає незначні недоліки у порівняннях, формулюванні висновків, застосуванні теоретичних знань на практиці	за зразком самостійно виконує практичні завдання, передбачені програмою; має стійкі навички виконання завдання
Задовіль-ний	60…74	володіє навчальним матеріалом поверхово, фрагментарно, на рівні запам’ятовування відтворює певну частину навчального матеріалу з елементами логічних зв’язків, знає основні поняття навчального матеріалу	має елементарні, нестійкі навички виконання завдання
Незадо-вільний	менше 60	має фрагментарні знання (менше половини) у незначному загальному обсязі навчального матеріалу; відсутні сформовані уміння та навички; під час відповіді допускаються суттєві помилки	планує та виконує частину завдання за допомогою викладача

Результати навчання з дисципліни оцінюються за 100-бальною шкалою (від 1 до 100) з переведенням в оцінку за традиційною шкалою («відмінно», «добре», «задовільно», «незадовільно» відповідно до шкали, наведеної в таблиці 10).

Таблиця 10 – Шкала оцінювання: національна та ECTS

Національна	Університетська (в балах)	ECTS	Визначення ECTS
Відмінно	90-100	A	**Відмінно** – відмінне виконання лише з незначною кількістю помилок
Добре	82-89	B	**Дуже добре** – вище середнього рівня з кількома помилками
	75-81	C	**Добре** – в загальному правильна робота з певною кількістю грубих помилок
Задовільно	67-74	D	**Задовільно**- непогано, але зі значною кількістю недоліків
	60-66	E	**Достатньо** – виконання задовольняє мінімальні критерії
Незадовільно	35-59	FX	**Незадовільно** – потрібно попрацювати перед тим, як отримати залік або скласти іспит
	0-34	F	**Незадовільно** – необхідна серйозна подальша робота

7 ЗАСОБИ НАВЧАННЯ

Навчальний процес відбувається в мультимедійних **лекційних** аудиторіях кафедри інженерії програмного забезпечення, оснащених: 1102 - 64,4 кв.м. (Проєктор ACER X128H.modDNX1723 введений в експлуатацію 2020 р.), А-13 - 182,6 кв.м. (Проєктор ACER X1329 WHP введений в експлуатацію 2023 р.) та екранами.

Лабораторні роботи виконуються в комп'ютерних класах (1418 – 54,7 кв.м., 1419 - 54,0 кв.м.) з сучасним програмним забезпеченням.

Комп'ютерний клас (1418): Dia West DW 1033115 AMD Ryzen 3 3200G/ Sam4/ DDR4 3200 МГц, 16 ГБ/ SSD M.2 240 GB/ Acer 23.8/ Windows 10 Pro UKR OEM x 64 - 14 шт., 2023 р.

Комп'ютерний клас (1419): ПК AMD Athlon 200GE 3200G/ DDR4 8 ГБ/ SSD 120Gb / Acer 21.5/ Windows 10 Pro UKR OEM x 64 - 14 шт., 2019 р.

Програмне забезпечення: Операційна система Widows, браузер Chrome.

Для самостійної роботи знадобиться:

- комп'ютер з достатньою продуктивністю для роботи з Інтернетом. Рекомендовані характеристики включають процесор з тактовою частотою не менше 2 ГГц, 8 ГБ оперативної пам'яті і достатньо вільного місця на жорсткому диску для встановлення необхідного програмного забезпечення.

Операційна система: Windows, macOS або Linux.

Інтернет-з'єднання: Доступ до стабільного Інтернет-з'єднання є важливим для завантаження необхідного програмного забезпечення, документації та отримання доступу до онлайн-ресурсів для навчання.

Відеокамера та мікрофон: якщо навчання відбувається в онлайн-форматі.