МОН УКРАЇНИ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ

Навчально-науковий Київський інститут залізничного транспорту

Кафедра інформаційних технологій та штучного інтелекту

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Олег НІКОНОВ
«27» серпня 2026 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«BIG DATA ТА ІНФОРМАЦІЙНА БЕЗПЕКА В УПРАВЛІННІ ТРАНСПОРТНИМИ СИСТЕМАМИ»

Рівень вищої освіти **другий (магістерський)**

Галузь знань **F Інформаційні технології**

Спеціальність **F2 Інженерія програмного забезпечення**

Освітня програма **«Інженерія програмного забезпечення та аналітика гібридних загроз»**

Тип дисципліни **обов'язкова**

Мова викладання **українська**

Київ
НТУ 2026

Робоча програма дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» для здобувачів другого рівня вищої освіти за спеціальністю F2 Інженерія програмного забезпечення освітньої програми «Інженерія програмного забезпечення та аналітика гібридних загроз».

Обговорено та рекомендовано до затвердження на засіданнях:

кафедри інформаційних технологій та штучного інтелекту,
протокол № 1 від 26 серпня 2026 року,

науково-методичної комісії спеціальності F2 Інженерія програмного забезпечення,
протокол № 1 від 26 серпня 2026 року,

Вченої ради ННКІЗТ НТУ,
протокол № 1 від 27 серпня 2026 року.

Робочу програму схвалено на засіданні Вченої ради ННКІЗТ НТУ

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, освітня програма, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма здобуття вищої освіти</td><td>заочна форма здобуття вищої освіти</td></tr>
<tr><td rowspan="2">Кількість кредитів – 4 ECTS</td><td>Галузь знань
<u>F Інформаційні технології</u></td><td colspan="2" rowspan="2"><u>обов’язкова</u></td></tr>
<tr><td>Спеціальність
<u>F2 Інженерія програмного забезпечення</u></td></tr>
<tr><td rowspan="2">Модулів – 2</td><td rowspan="5">Освітня програма
<u>«Інженерія програмного забезпечення та аналітика гібридних загроз»</u></td><td colspan="2">Рік підготовки</td></tr>
<tr><td>1-й</td><td>1-й</td></tr>
<tr><td>Індивідуальне завдання – контрольна робота для заочної форми</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120 год.</td><td>1-й</td><td>1-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="16">Тижневих годин для денної форми здобуття освіти: аудиторних – 3 год.; самостійної роботи – 5,6 год.</td><td rowspan="16">Рівень вищої освіти
<u>другий (магістерський)</u></td><td>14 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>28 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>78 год.</td><td>114 год.</td></tr>
<tr><td colspan="2">Індивідуальне завдання</td></tr>
<tr><td rowspan="2">-</td><td rowspan="2">контрольна робота – 21 год. у складі самостійної роботи</td></tr>
<tr><td></td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td colspan="2">Залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):

для денної форми навчання – 35/65 %

для заочної форми навчання – 5/95 %

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Головною метою дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» є формування у здобувачів системного розуміння технологій збирання, зберігання, потокового і пакетного оброблення великих обсягів транспортних

даних, а також здатності проєктувати захищені програмні рішення, виявляти інформаційні потреби, класифікувати дані, оцінювати ризики інформаційної безпеки та здійснювати реінжиніринг інформаційних систем відповідно до вимог замовника.

Основні завдання дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» – вивчення джерел і характеристик Big Data у транспортних системах; формування вимог і класифікація даних; порівняння пакетних та потокових архітектур; проєктування конвеєрів даних; забезпечення якості, метаданих і простежуваності; моделювання загроз і визначення заходів захисту; практичне застосування стандартів і рекомендацій з інформаційної безпеки; побудова захищених сервісів оброблення даних; планування міграції та реінжинірингу транспортних інформаційних систем; обґрунтування технічних рішень українською й англійською мовами.

Міждисциплінарні зв'язки

Паралельно вивчають: «Ділова іноземна мова», «Методологія та організація наукових досліджень», «Гібридні загрози та комплексна безпека», «Моделі управління IT-інфраструктурою», «Проєктування систем з розподіленими базами даних», «Хмарні технології».

Послідовно: «Проєктування програмного забезпечення інтелектуальних систем», дослідницька практика, підготовка та публічний захист кваліфікаційної роботи магістра.

Згідно з вимогами освітньої програми вивчення дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» забезпечує формування таких загальних і фахових компетентностей:

	Загальні компетентності					Спеціальні (фахові) компетентності									
	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ФК01	ФК02	ФК03	ФК04	ФК05	ФК06	ФК07	ФК08	ФК09	ФКС10
ОК4	+	+		+		+		+		+		+		+	

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність спілкуватися іноземною мовою як усно, так і письмово.

ЗК04. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами інших галузей знань/видів економічної діяльності).

ФК01. Здатність аналізувати предметні області, формувати, класифікувати вимоги до програмного забезпечення.

ФК03. Здатність проєктувати архітектуру програмного забезпечення, моделювати процеси функціонування окремих підсистем і модулів.

ФК05. Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення.

ФК07. Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах.

ФК09. Здатність забезпечувати якість програмного забезпечення.

Нормативний зміст підготовки здобувачів другого (магістерського) рівня, сформульований у програмних результатах навчання:

	ПР01	ПР02	ПР03	ПР04	ПР05	ПР06	ПР07	ПР08	ПР09	ПР10	ПР11	ПР12	ПР13	ПР14	ПР15	ПР16	ПР17	ПРС18	ПРС19
ОК4		+		+											+				

ПР02. Оцінювати і вибирати ефективні методи і моделі розроблення, впровадження, супроводу програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу.

ПР04. Виявляти інформаційні потреби і класифікувати дані для проєктування програмного забезпечення.

ПР15. Здійснювати реінжиніринг програмного забезпечення відповідно до вимог замовника.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Модуль 1. Транспортні дані, архітектури Big Data та інформаційна безпека

Тема 1. Інформаційні потреби, класифікація та якість транспортних даних.

Учасники та процеси транспортної системи. Джерела даних: телематика, навігація, датчики інфраструктури, квиткові системи, логістика, експлуатаційні журнали та відкриті дані. Приклади наборів даних АТ «Укрзалізниця». Характеристики Big Data. Виявлення інформаційних потреб зацікавлених сторін.

Структуровані, напівструктуровані й потокові дані. Класифікація та чутливість даних. Метадані, походження даних, повнота, точність, узгодженість, своєчасність та унікальність. Профілювання, очищення і валідація даних.

Тема 2. Архітектури та конвеєри Big Data у транспортних системах.

Пакетне і потокове оброблення. Надходження, буферизація, зберігання, перетворення, аналітика та надання даних. Подієво-орієнтовані рішення. Розподілене зберігання й оброблення великих масивів даних на прикладах транспортних та залізничних інформаційних систем.

Архітектурні подання, інтерфейси та атрибути якості. Масштабованість, відмовостійкість, затримка, пропускна здатність і вартість. Критерії оцінювання та вибору технологічної моделі.

Тема 3. Інформаційна безпека та приватність транспортних даних.

Активи, загрози, вразливості, межі довіри й поверхня атаки в інформаційних системах залізничного транспорту. Конфіденційність, цілісність, доступність і простежуваність. Керування доступом, мінімізація та псевдонімізація даних, журналювання й моніторинг. Secure by Design. Застосування NIST CSF 2.0, NIST IR 8576, ENISA Transport Threat Landscape та OWASP ASVS.

Модуль 2. Захищене впровадження, аналітика та реінжиніринг транспортних систем

Тема 4. Захищені потокові сервіси та аналітика транспортних даних.

Захищена подієво-орієнтована взаємодія. Ідентифікація, автентифікація та авторизація компонентів. Захист даних під час передавання і зберігання. Аудит, резервне копіювання, відновлення та спостережуваність.

Показники ефективності й безпеки транспортних процесів. Агрегування, часові ряди, виявлення аномалій і оцінювання ризиків. Інтерпретація якості та обмежень даних. Застосування потокової аналітики для даних залізничного транспорту на прикладі АТ «Укрзалізниця».

Контейнеризоване розгортання навчального потокового стенда. Візуалізація результатів і підготовка рекомендацій для керівників та технічних фахівців. Відповідальне використання даних.

Тема 5. Реінжиніринг транспортних інформаційних систем і міграція даних.

Аналіз станів AS-IS і TO-BE. Вимоги замовника, розриви та технічний борг. Стратегії модернізації, зміни схем та інтерфейсів, сумісність, перенесення й перевірка даних. Кейс модернізації інформаційної системи залізничного підприємства на прикладі АТ «Укрзалізниця». План переходу, тестування, критерії приймання, моніторинг і повернення до попередньої версії.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	Усього	у тому числі				Усього	у тому числі			
		Лекції	Практичні або семінарські	Самостійна робота	Інд. завд.		Лекції	Практичні або семінарські	Самостійна робота	Інд. завд.
Модуль 1.										
Тема 1. Інформаційні потреби, класифікація та якість транспортних даних	14	2	4	8	-	13	-	-	13	-
Тема 2. Архітектури та конвеєри Big Data у транспортних системах	17	2	4	11	-	14	1	1	12	-
Тема 3. Інформаційна безпека та приватність транспортних даних	17	4	4	9	-	14	-	1	13	-
Підготовка до модульного контролю	2	-	-	2	-	-	-	-	-	-
Проведення модульного контролю	2	-	2	-	-	-	-	-	-	-
Разом за модулем 1	52	8	14	30	-	41	1	2	38	-
Модуль 2.										
Тема 4. Захищені потокові сервіси та аналітика транспортних даних	30	2	6	22	-	24	-	-	24	-
Тема 5. Реінжиніринг транспортних інформаційних систем і міграція даних	32	4	6	22	-	30	1	2	27	-
Підготовка до модульного контролю	2	-	-	2	-	-	-	-	-	-
Проведення модульного контролю	2	-	2	-	-	-	-	-	-	-
Разом за модулем 2	66	6	14	46	-	54	1	2	51	-
Виконання контрольної роботи	-	-	-	-	-	21	-	-	21	-
Підготовка до підсумкового контролю (заліку)	2	-	-	2	-	4	-	-	4	-
РАЗОМ ГОДИН	**120**	**14**	**28**	**78**	-	**120**	**2**	**4**	**114**	-

5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ

Виконання семінарських занять при вивченні дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» не передбачено.

6. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з.ч	Найменування тем	Кількість годин	
		Денна	**Заочна**
Модуль 1.			
1	Інвентаризація джерел транспортних даних: інформаційні потреби, класифікація, паспорт і профіль якості набору даних	4	-
2	Моделювання пакетної та потокової архітектур транспортної системи; порівняння варіантів і технічне резюме англійською мовою	4	1
3	Моделювання загроз конвеєра транспортних даних: активи, межі довіри, ризики, вимоги й заходи захисту	4	1
4	Модульний контроль	2	
Модуль 2.			

4	Побудова захищеного потокового стенда Apache Kafka і PostgreSQL у Docker Compose; аналіз даних і тестування захисту	6	-
5	Реінжиніринг транспортної інформаційної системи: AS-IS/TO-BE, міграція, перевірка даних, критерії приймання та план повернення	6	2
6	Модульний контроль	2	
	Разом	***28***	***4***

7. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

Виконання лабораторних занять при вивченні дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» не передбачено.

8. САМОСТІЙНА РОБОТА

Форми організації освітнього процесу	Кількість годин	
	Денна форма	Заочна форма
ПА – опрацювання теоретичного матеріалу, підготовка до практичних занять і оформлення результатів	**72**	**89**
ПМК – підготовка до модульного контролю	**4**	**-**
ППК – підготовка до підсумкового контролю (заліку)	**2**	**4**
Виконання контрольної роботи для заочної форми здобуття освіти	-	**21**
Усього годин	**78**	**114**

9. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Для денної форми окремі індивідуальні завдання не передбачено. Для заочної форми передбачено контрольну роботу на матеріалах транспортного кейсу; завдання та вимоги до оформлення надає викладач у Google Classroom.

10. МЕТОДИ НАВЧАННЯ

У процесі викладання дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» застосовуються словесні, наочні та практичні методи; проблемні лекції; аналіз транспортних кейсів та інцидентів; моделювання архітектур і загроз; порівняння технічних альтернатив; практико-орієнтоване навчання, взаємне рецензування та захист обґрунтованих рішень.

Основними методами навчання є лекційні та практичні заняття, презентації у LibreOffice Impress або Google Slides, робота з даними у Google Colab і PostgreSQL, моделювання у diagrams.net, навчальне потокове оброблення в Apache Kafka, контейнеризоване розгортання з Docker Compose, тестування API та засобів захисту, дискусії й самостійне опрацювання актуальної літератури та офіційних інформаційних ресурсів.

11. МЕТОДИ КОНТРОЛЮ

У процесі вивчення дисципліни «Big Data та інформаційна безпека в управлінні транспортними системами» використовуються такі засоби оцінювання та методи демонстрування результатів навчання:

Оцінювання навчальних досягнень здобувачів за усіма видами навчальних робіт проводиться за поточним та підсумковим контролем.

Поточний контроль: усне та письмове опитування, короткі тести, перевірка й захист практичних робіт, аналіз архітектурних схем, паспортів даних, моделей загроз і результатів аналітики, презентація рішень українською та англійською мовами. Модульний контроль охоплює тестові, аналітичні та ситуаційні завдання. Для заочної форми додатково оцінюється контрольна робота.

Підсумковий контроль досягнутих результатів навчання – залік у формі комплексного транспортного кейсу з класифікації даних, вибору архітектури Big Data, оцінювання ризиків інформаційної безпеки та обґрунтування реінжинірингу.

12. РОЗПОДІЛ МАКСИМАЛЬНОЇ КІЛЬКОСТІ БАЛІВ, ЯКІ ОТРИМУЮТЬ ЗДОБУВАЧІ ВИЩОЇ ОСВІТИ

<table>
<tr><td colspan="6">Контроль протягом семестру</td><td rowspan="3">Підсумковий контроль (залік)</td><td rowspan="3">Сума балів</td></tr>
<tr><td colspan="5">Модуль 1 | Модуль 2</td><td rowspan="2">Модуль 3 (ІЗ)</td></tr>
<tr><td>Тема 1</td><td>Тема 2</td><td>Тема 3</td><td>Тема 4</td><td>Тема 5</td></tr>
<tr><td colspan="6">Для денної форми: активність і короткі завдання за темами – 10 балів; підготовка та захист практичних робіт – 30 балів; дві модульні контрольні роботи – 20 балів.</td><td>Не передбачено навчальним планом</td><td rowspan="2">40</td><td rowspan="2">100</td></tr>
<tr><td colspan="6">Для заочної форми: виконання та захист практичних завдань – 40 балів.</td><td>Контрольна робота – 20 балів</td></tr>
<tr><td colspan="6"></td><td></td><td></td></tr>
</table>

Бали від 1 до 60 за роботу протягом семестру розподіляються між двома модулями; підсумковий контроль оцінюється у 40 балів.

Контрольна робота для заочної форми оцінюється у 20 балів і враховується у семестровому контролі.

Здобувач вищої освіти отримує допуск до підсумкового семестрового контролю, якщо за результатами роботи протягом семестру він набрав не менше 30 балів.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності за формами організації освітнього процесу	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проєкту (роботи), циклу РГР / РР / ГР	для заліку, контрольної роботи
90–100	**A**	відмінно	зараховано
82–89	**B**	добре	
74–81	**C**		
64–73	**D**	задовільно	
60–63	**E**		
35–59	**FX**	незадовільно (з можливістю повторного складання)	не зараховано (з можливістю повторного складання)

1–34	**F**	незадовільно (з обов'язковим повторним вивченням дисципліни)	не зараховано (з обов'язковим повторним вивченням дисципліни)

Критерії оцінювання:

«відмінно» – здобувач вищої освіти демонструє повні і глибокі знання навчального матеріалу, достовірний рівень розвитку умінь та навичок, правильне й обґрунтоване формулювання практичних висновків, уміння приймати необхідні рішення в нестандартних ситуаціях, вільне володіння науковими термінами, аналізує причинно-наслідкові зв'язки;

«добре» – здобувач вищої освіти демонструє повні знання навчального матеріалу, але допускає незначні пропуски фактичного матеріалу, вміє застосувати його щодо конкретно поставлених завдань, у деяких випадках нечітко формулює загалом правильні відповіді, допускає окремі несуттєві помилки та неточності;

«задовільно» – здобувач вищої освіти володіє більшою частиною фактичного матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, не завжди вміє інтегровано застосувати набуті знання для аналізу конкретних ситуацій, нечітко, а інколи й неправильно формулює основні теоретичні положення та причинно-наслідкові зв'язки;

«незадовільно» – здобувач вищої освіти не володіє достатнім рівнем необхідних знань, умінь, навичок, науковими термінами.

13. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Методичне забезпечення:

1 Робоча програма навчальної дисципліни та силабус.

2 Курс лекцій і презентаційні матеріали за темами дисципліни.

3 Методичні вказівки до практичних занять і контрольної роботи.

4 Навчальні набори транспортних даних, шаблони паспорта даних, архітектурних схем і моделей загроз.

5 Матеріали у Google Classroom. Програмне забезпечення та сервіси: Google Workspace, Google Colab, Visual Studio Code, Git і GitHub, diagrams.net / draw.io, PostgreSQL, Apache Kafka, Docker, Postman, OWASP ZAP, Wireshark, Zotero.

14. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова (основна):

1. Reis J., Housley M. Fundamentals of Data Engineering. O'Reilly Media, 2022. 450 p. ISBN 978-1-098-10830-4.

2. Kohnfelder L. Designing Secure Software: A Guide for Developers. No Starch Press, 2021. 312 p. ISBN 978-1-71850-192-8.

3. Jarmul K. Practical Data Privacy: Enhancing Privacy and Security in Data. O'Reilly Media, 2023. 346 p. ISBN 978-1-098-12945-3.

4. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. 2024. 32 p.

5. National Institute of Standards and Technology. Transit Cybersecurity Framework Community Profile. NIST IR 8576. 2026.

6. European Union Agency for Cybersecurity. ENISA Transport Threat Landscape. 2023.

7. Dehghani Z. Data Mesh: Delivering Data-Driven Value at Scale. O'Reilly Media, 2022. 384 p. ISBN 978-1-492-09239-1.

8. OWASP Foundation. OWASP Application Security Verification Standard 5.0.0. 2025.
9. National Institute of Standards and Technology. Secure Software Development Framework (SSDF) Version 1.1. NIST SP 800-218. 2022.
10. National Institute of Standards and Technology. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. NIST SP 800-207A. 2023.
11. International Organization for Standardization. ISO/IEC 27001:2022. Information security management systems – Requirements. 2022.
12. International Organization for Standardization. ISO/IEC 27002:2022. Information security controls. 2022.
13. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks. 2021.
14. OWASP Foundation. OWASP API Security Top 10. 2023.

Додаткова:

1. Apache Kafka Documentation. URL: https://kafka.apache.org/documentation/
2. PostgreSQL Documentation. URL: https://www.postgresql.org/docs/
3. Docker Documentation. URL: https://docs.docker.com/
4. NIST Cybersecurity Framework 2.0. URL: https://www.nist.gov/cyberframework
5. NCCoE Transit Cybersecurity Framework Community Profile. URL: https://www.nccoe.nist.gov/projects/transit-cybersecurity-framework-csf-community-profile
6. ENISA Transport Threat Landscape. URL: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape
7. OWASP Application Security Verification Standard. URL: https://owasp.org/www-project-application-security-verification-standard/

15. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Apache Kafka Documentation. URL: https://kafka.apache.org/documentation/
2. PostgreSQL Documentation. URL: https://www.postgresql.org/docs/
3. NIST Cybersecurity Framework 2.0. URL: https://www.nist.gov/cyberframework
4. NCCoE Transit Cybersecurity Framework Community Profile. URL: https://www.nccoe.nist.gov/projects/transit-cybersecurity-framework-csf-community-profile
5. OWASP Application Security Verification Standard. URL: https://owasp.org/www-project-application-security-verification-standard/

ДОДАТОК А

К Р И Т Е Р І Ї
оцінювання досягнутих результатів навчання здобувачів вищої освіти Національного транспортного університету

А.1 Загальні положення

Досягнуті результати навчання з кожної навчальної дисципліни за семестр оцінюють балами від 1 до 100: результати роботи здобувачів вищої освіти протягом семестру – балами від 1 до 60, відповіді на екзамені або заліку – від 1 до 40. Розподіл балів для оцінювання результатів роботи здобувачів вищої освіти протягом семестру за кожною дисципліною встановлюють розробники робочих програм.

Індивідуальне завдання у вигляді курсової роботи / проєкту, циклу розрахунково-графічних / графічних / розрахункових робіт та практику оцінюють окремо балами від 1 до 100.

Загальна семестрова оцінка з дисципліни є сумою балів, отриманих під час контролю протягом семестру, та балів, отриманих під час підсумкового контролю (на екзамені або заліку).

Здобувач вищої освіти може бути допущений до підсумкового контролю (екзамену або заліку) тільки після зарахування модульних контрольних робіт, а також виконання індивідуального завдання, яке передбачене освітньою програмою та навчальним планом.

Таблиця А.1 – Шкала оцінювання: національна та ECTS

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності за формами організації освітнього процесу</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проєкту (роботи), циклу РГР / РР / ГР</td><td>для заліку, контрольної роботи</td></tr>
<tr><td>90–100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82–89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74–81</td><td>C</td></tr>
<tr><td>64–73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60–63</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>1–34</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>

Критерії оцінювання:

«відмінно» – здобувач вищої освіти демонструє повні і глибокі знання навчального матеріалу, достовірний рівень розвитку умінь та навичок, правильне й обґрунтоване формулювання практичних висновків, уміння приймати необхідні рішення в нестандартних ситуаціях, вільне володіння науковими термінами, аналізує причинно-наслідкові зв'язки;

«добре» – здобувач вищої освіти демонструє повні знання навчального матеріалу, але допускає незначні пропуски фактичного матеріалу, вміє застосувати його щодо конкретно поставлених завдань, у деяких випадках нечітко формулює загалом правильні відповіді, допускає окремі несуттєві помилки та неточності;

«задовільно» – здобувач вищої освіти володіє більшою частиною фактичного матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, не завжди вміє інтегровано застосувати набуті знання для аналізу конкретних ситуацій, нечітко, а інколи й неправильно формулює основні теоретичні положення та причинно-наслідкові зв'язки;

«незадовільно» – здобувач вищої освіти не володіє достатнім рівнем необхідних знань, умінь, навичок, науковими термінами.

А.2 Критерії оцінювання досягнутих результатів навчання при проведенні підсумкового контролю (екзамену, заліку)

Екзаменаційна (залікова) оцінка (від 1 до 40 балів) складається із суми балів, виставлених екзаменатором / лектором за відповіді здобувача на кожне із запитань екзаменаційного білета / завдання або запитання для заліку.

Максимальну кількість балів, яку можна отримати на екзамені / заліку, розподіляють між запитаннями екзаменаційного білета / завданнями або запитаннями для заліку.

Кількість запитань (завдань) та розподіл балів між ними визначає розробник робочої програми.

Відповідь на запитання оцінюють таким чином *(приклад для оцінювання відповіді на одне запитання балами від 0 до 15):*

від 12 до 15 балів виставляють здобувачу, який надав повну, у логічно правильній послідовності відповідь, яка свідчить про всебічні, систематизовані та глибокі знання з поставленого запитання в обсязі програми навчальної дисципліни; демонструє здатність здобувача вільно оперувати здобутими знаннями: диференціювати та інтегрувати їх, відтворювати та аналізувати отриману інформацію, робити обґрунтовані висновки та узагальнення, виявляти й відстоювати власну позицію, переконливо висловлювати думку та чітко формулювати відповідь. Як правило, таку оцінку отримує здобувач, який відповів на запитання не менше ніж на 90 %. Відповідь оцінюють у максимальну кількість балів тільки за умови надання вичерпної відповіді на запитання;

від 8 до 11 балів виставляють здобувачу, який надав досить повну, без суттєвих неточностей, у логічно правильній послідовності відповідь, яка свідчить про ґрунтовні та систематизовані знання з поставленого запитання в обсязі програми навчальної дисципліни; демонструє здатність здобувача

впевнено оперувати здобутими знаннями: відтворювати та аналізувати отриману інформацію, пояснювати основні закономірності, робити висновки, чітко висловлювати думку та формулювати відповідь. Як правило, таку оцінку отримує здобувач, який відповів на запитання на 70–90 %;

від 4 до 7 балів виставляють здобувачу, який надав не зовсім повну, із неточностями та окремими незначними помилками, в основному у правильній послідовності відповідь, яка свідчить про задовільні знання з поставленого запитання в обсязі програми навчальної дисципліни, демонструє здатність здобувача відтворювати основний матеріал відповідно до поставленого запитання. Як правило, таку оцінку отримує здобувач, який відповів на запитання на 50–70 %;

від 0 до 3 балів виставляють здобувачу, який надав фрагментарну, із суттєвими неточностями та принциповими помилками відповідь, яка свідчить про неповноту знань з поставленого запитання в обсязі програми навчальної дисципліни, демонструє наявність у здобувача утруднень при відтворенні інформації відповідно до поставленого запитання. Як правило, таку оцінку отримує здобувач, який відповів на запитання менше ніж на 50 %.