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
«ІНФОРМАЦІЙНА БЕЗПЕКА ТА ГІБРИДНІ ЗАГРОЗИ»

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 «Інформаційна безпека та гібридні загрози» 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 «Інженерія програмного забезпечення та аналітика гібридних загроз»</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="15">Тижневих годин для денної форми здобуття освіти: аудиторних – 3 год.; самостійної роботи – 5,6 год.</td><td rowspan="15">Рівень вищої освіти
<u>другий (магістерський)</u></td><td>28 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>2 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>-</td><td>контрольна робота – 21 год. у складі самостійної роботи</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td colspan="2">Екзамен</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 «Інформаційна безпека та гібридні загрози» є формування у здобувачів здатності системно забезпечувати інформаційну безпеку програмних та інформаційних систем в умовах гібридних загроз: визначати активи й критичні функції,

виявляти та класифікувати загрози, оцінювати ризики, формувати вимоги до захисту, проєктувати й перевіряти комплекс організаційних і технічних контролів, а також приймати обґрунтовані рішення щодо реагування, ресурсів, безперервності та адаптації за невизначеності.

Основні завдання дисципліни «Інформаційна безпека та гібридні загрози» – засвоєння принципів конфіденційності, цілісності, доступності, автентичності та підзвітності; інвентаризація інформаційних активів, потоків даних, довірчих меж і залежностей; моделювання кібернетичних та інформаційних складників гібридних загроз; оцінювання вразливостей і ризиків; формування, класифікація та трасування вимог безпеки; застосування законодавства, стандартів і професійних рекомендацій; проєктування багаторівневого захисту, керування доступом, мережевої сегментації, моніторингу та захисту ланцюга постачання; аналіз інформаційних впливів і соціальної інженерії; планування ресурсів, реагування на інциденти, безперервності й відновлення; перевірка контролів та вдосконалення захисту.

Міждисциплінарні зв'язки

Паралельно вивчають: «Ділова іноземна мова», «Методологія та організація наукових досліджень», «Гібридні загрози та комплексна безпека», «Інноваційні технології Big Data та інформаційної безпеки в управлінні транспортними системами», «Моделі управління IT-інфраструктурою», «Проєктування систем з розподіленими базами даних», «Хмарні технології».

Послідовно: «Проєктування програмного забезпечення інтелектуальних систем», науково-дослідницька та передкваліфікаційна практики, виконання і публічний захист кваліфікаційної роботи магістра.

Згідно з вимогами освітньої програми вивчення дисципліни «Інформаційна безпека та гібридні загрози» 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
ОК5	+				+	+				+	+	+			+

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК05. Здатність генерувати нові ідеї (креативність).

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

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

ФК06. Здатність ефективно керувати фінансовими, людськими, технічними та іншими проєктними ресурсами у 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.

ФКС10. Здатність адаптувати робочі процеси та особистий простір до складних та непередбачуваних ситуацій, спричинених гібридними загрозами, з урахуванням аспектів соціальної відповідальності.

Нормативний зміст підготовки здобувачів вищої освіти 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
ОК5												+						+	+

ПР12. Приймати ефективні організаційно-управлінські рішення в умовах невизначеності та зміни вимог, порівнювати альтернативи, оцінювати ризики.
ПРС18. Розуміти комплексну природу, складність, логіку і закономірності гібридних загроз.
ПРС19. Виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Модуль 1. Управління інформаційною безпекою в умовах гібридних загроз

Тема 1. Інформаційна безпека програмних і транспортних систем.

Інформація та дані як активи. Конфіденційність, цілісність, доступність, автентичність, підзвітність і неспростовність. Критичні функції, власники активів, користувачі, постачальники та інші зацікавлені сторони. Інвентаризація активів, класифікація даних, карти потоків, довірчі межі й залежності. Особливості інформаційних систем транспортної галузі та критичної інфраструктури.

Система управління інформаційною безпекою: контекст, політики, ролі, відповідальність, процеси та контрольні показники. Джерела кібернетичних, інформаційних, інсайдерських, фізичних і ланцюгових загроз. Поєднання кібероперацій, витоків даних, соціальної інженерії, дезінформації та впливу на доступність сервісів у гібридній кампанії. Поверхня атаки, каскадні наслідки та соціальна відповідальність.

Тема 2. Оцінювання ризиків і формування вимог інформаційної безпеки.

Виявлення, ідентифікація та класифікація загроз, вразливостей і несприятливих подій. Моделі порушника, сценарії зловживання, дерева атак, причинно-наслідкові зв’язки та матриці загроз. Якісне й кількісне оцінювання ймовірності, впливу та рівня ризику. Невизначеність, достовірність даних, припустимий ризик і критерії пріоритизації.

Вимоги законодавства України, NIS2 і CER. NIST CSF 2.0, ISO/IEC 27001:2022, ISO/IEC 27002:2022 та ISO/IEC 27005:2022. Формування, класифікація, пріоритизація і трасування функціональних та нефункціональних вимог безпеки. Вибір варіантів оброблення ризику, обґрунтування ресурсів, критерії приймання і перевірюваність вимог.

Тема 3. Архітектура, технічні контролі та моніторинг інформаційної безпеки.

Принципи secure by design, defense in depth, least privilege і zero trust. Керування ідентичностями та доступом, багатофакторна автентифікація, криптографічний захист, сегментація мережі, захищене конфігурування, резервування та журналювання. Безпечний життєвий цикл програмного забезпечення, керування вразливостями, оновленнями й ланцюгом постачання. Збирання та кореляція подій, аналіз мережевого трафіку, індикатори компрометації, контроль базового стану, тестування і перевірка результативності захисних контролів.

Модуль 2. Інформаційні впливи, реагування та адаптивний захист

Тема 4. Інформаційні впливи, соціальна інженерія та перевірка інформації.

Помилкова інформація, дезінформація, пропаганда та іноземне інформаційне маніпулювання і втручання. Цілі, аудиторії, канали, наративи, методи посилення і координації. Соціальна інженерія: фішинг, претекстинг, маніпулювання довірою та компрометація облікових даних. Взаємодія інформаційного й кібернетичного складників гібридних загроз.

Збирання й верифікація відкритих даних, оцінювання походження, надійності, актуальності, повноти, узгодженості та упередженості джерел. Виявлення аномалій, повторюваних шаблонів, координованої поведінки та часових зв’язків. Обмеження атрибуції, захист персональних даних, етичні межі аналізу та документування рівня впевненості.

Захист інформаційної цілісності: політики комунікації, перевірка повідомлень, навчання персоналу, резервні канали, протидія фішингу та управління кризовими повідомленнями.

Індикатори інформаційного впливу, процедури ескалації та узгодження технічних, організаційних і комунікаційних заходів.

Тема 5. Реагування на інциденти, безперервність та адаптація захисту.

Життєвий цикл реагування: підготовка, виявлення, аналіз, локалізація, усунення, відновлення та післяінцидентне вдосконалення. Класифікація й пріоритизація інцидентів, ролі, матриця RACI, плани реагування, журнали рішень, збереження доказів та обмін інформацією. Планування людських, технічних і фінансових ресурсів. Безперервність критичних функцій, резервування, RTO і RPO. Сценарні та настільні навчання, показники готовності, часу виявлення, реагування й відновлення. Адаптація робочих процесів та особистого простору, коригувальні дії і дорожня карта вдосконалення захисту.

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. Інформаційна безпека програмних і транспортних систем	16	6	2	8	-	16	1	-	15	-
Тема 2. Оцінювання ризиків і формування вимог інформаційної безпеки	18	6	2	10	-	17	1	-	16	-
Тема 3. Архітектура, технічні контролі та моніторинг інформаційної безпеки	18	6	2	10	-	16	-	-	16	-
Підготовка до модульного контролю	2	-	-	2	-	-	-	-	-	-
Проведення модульного контролю	2	-	2	-	-	1	-	1	-	-
Разом за модулем 1	56	18	8	30	-	50	2	1	47	-
Модуль 2.										
Тема 4. Інформаційні впливи, соціальна інженерія та перевірка інформації	27	4	2	21	-	20	1	-	19	-
Тема 5. Реагування на інциденти, безперервність та адаптація захисту	31	6	2	23	-	24	1	-	23	-
Підготовка до модульного контролю	2	-	-	2	-	-	-	-	-	-
Проведення модульного контролю	2	-	2	-	-	1	-	1	-	-
Разом за модулем 2	62	10	6	46	-	45	2	1	42	-
Виконання контрольної роботи	-	-	-	-	-	21	-	-	21	-
Підготовка до підсумкового контролю (екзамену)	2	-	-	2	-	4	-	-	4	-
РАЗОМ ГОДИН	**120**	**28**	**14**	**78**	-	**120**	**4**	**2**	**114**	-

5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ

Виконання семінарських занять при вивченні дисципліни «Інформаційна безпека та гібридні загрози» не передбачено.

6. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з.ч	*Найменування тем*	*Кількість годин*	
		Денна	***Заочна***
Модуль 1.			
1	Інвентаризація інформаційних активів транспортної організації: класифікація даних, критичні функції, власники, потоки даних, довірчі межі, залежності та комбінований сценарій гібридної загрози	2	-
2	Оцінювання ризиків інформаційної безпеки: модель порушника, дерево атаки, вразливості, ймовірність і вплив, рівень невизначеності, варіанти оброблення ризику та специфікація вимог до захисту	2	-
3	Проєктування і перевірка багаторівневого захисту: сегментація мережі, керування доступом, аналіз навчального трафіку, виявлення вебвразливостей, моніторинг і критерії результативності контролів; модульний контроль	4	1
Модуль 2.			
4	Аналіз інформаційного впливу і соціальної інженерії: верифікація джерел, матриця індикаторів, оцінювання рівня впевненості, сценарій фішингу та заходи захисту інформаційної цілісності	2	-
5	Настільне навчання з реагування на комплексний інцидент: класифікація і пріоритизація, RACI, ресурсний план, локалізація, відновлення, адаптація робочих процесів, післяінцидентний звіт і дорожня карта вдосконалення; модульний контроль	4	1
	Разом	***14***	***2***

7. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

Виконання лабораторних занять при вивченні дисципліни «Інформаційна безпека та гібридні загрози» 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 (екзамену)	**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 обсягом 21 година у складі самостійної роботи: оцінювання ризиків інформаційної безпеки транспортної організації, формування вимог до захисту та розроблення ресурсно обґрунтованого плану реагування на комплексний інцидент. Завдання, вимоги до структури, оформлення та захисту розміщуються у Google Classroom.

10. МЕТОДИ НАВЧАННЯ

У процесі викладання дисципліни «Інформаційна безпека та гібридні загрози» застосовуються словесні, наочні та практичні методи; проблемні лекції; системний і ризик-орієнтований аналіз; моделювання загроз, атак і довірчих меж; аналіз нормативних вимог; дослідження мережевого трафіку та вебвразливостей у навчальному середовищі; перевірка інформації; розбір інцидентів; сценарні й настільні навчання; командне прийняття рішень, взаємне рецензування та захист рішень.

Основними методами навчання є лекційні та практичні заняття, побудова моделей активів, потоків даних, довірчих меж і дерев атак у diagrams.net / draw.io, оцінювання ризиків та аналіз індикаторів у Google Sheets, підготовка звітів і презентацій, координація завдань у Jira, аналіз мережевого трафіку у Wireshark, моделювання захищених мереж у Cisco Packet Tracer, дослідження вебвразливостей з OWASP ZAP та OWASP Juice Shop, а також самостійне опрацювання сучасної літератури й офіційних документів.

11. МЕТОДИ КОНТРОЛЮ

У процесі вивчення дисципліни «Інформаційна безпека та гібридні загрози» 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 моделей активів і загроз, реєстрів ризиків, специфікацій вимог, результатів аналізу мережевого трафіку, перевірки вебвразливостей та інформаційних впливів, планів реагування і захист практичних робіт. Модульний контроль містить теоретичні та ситуаційні завдання за комплексним інцидентом. Для заочної форми додатково оцінюються виконання та захист контрольної роботи.

Підсумковий контроль досягнутих результатів навчання – екзамен у формі відповідей на теоретичні питання та розв’язання ситуаційного завдання з ідентифікації гібридної загрози, оцінювання ризику, формування вимог інформаційної безпеки, порівняння варіантів захисту і розроблення ресурсно обґрунтованого плану реагування.

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

<table>
<tr><td colspan="6">Контроль протягом семестру</td><td rowspan="3">Підсумковий контроль (екзамен)</td><td rowspan="3">Сума балів</td></tr>
<tr><td colspan="5">Модуль 1 | Модуль 2</td><td rowspan="2">Контрольна робота</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 двох комплексних практичних завдань, включно з модульним контролем, – 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, якими оцінюють результати роботи здобувачів вищої освіти протягом семестру, охоплюють практичні роботи, поточні завдання та два модульні контролі; підсумковий екзамен оцінюється у 40 балів.

Для заочної форми контрольна робота оцінюється у 20 балів і враховується у 60 балах поточного семестрового контролю.

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, модульного контролю та контрольної роботи.

4 Шаблони реєстру активів, карти потоків даних і довірчих меж, моделі загроз, реєстру ризиків, специфікації вимог безпеки, плану реагування та післяінцидентного звіту.

5 Матеріали у Google Classroom. Програмне забезпечення та сервіси: Ubuntu Desktop LTS, Google Workspace, diagrams.net / draw.io, Jira, Wireshark, Cisco Packet Tracer, OWASP ZAP, OWASP Juice Shop, Zotero.

14. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова (основна):

1. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024.
2. International Organization for Standardization. ISO/IEC 27001:2022. Information security management systems – Requirements. 2022.
3. International Organization for Standardization. ISO/IEC 27002:2022. Information security controls. 2022.
4. International Organization for Standardization. ISO/IEC 27005:2022. Guidance on managing information security risks. 2022.
5. Ross R. et al. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160 Vol. 2 Rev. 1, 2021.
6. Chandramouli R., Butcher Z. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. NIST SP 800-207A, 2023.
7. Souppaya M., Scarfone K., Dodson D. Secure Software Development Framework (SSDF) Version 1.1. NIST SP 800-218, 2022.
8. Boyens J. et al. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST SP 800-161 Rev. 1 Update 1, 2024.
9. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. NIST SP 800-61 Rev. 3, 2025.
10. European Union Agency for Cybersecurity. ENISA Threat Landscape 2025. ENISA, 2025.
11. European Union Agency for Cybersecurity. ENISA Threat Landscape: Transport Sector. ENISA, 2023.
12. Giannopoulos G., Smith H., Theocharidou M. The Landscape of Hybrid Threats: A Conceptual Model. Publications Office of the European Union, 2021.
13. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX.
14. Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021.

Додаткова:

1. European Union. Directive (EU) 2022/2555 (NIS 2 Directive). Official Journal of the European Union, 2022.
2. European Union. Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). 2022.
3. Cybersecurity and Infrastructure Security Agency. Cross-Sector Cybersecurity Performance Goals. Version 1.0.1, 2023.
4. European Union Agency for Cybersecurity. ENISA Threat Landscape for Supply Chain Attacks. ENISA, 2021.
5. European Union Agency for Cybersecurity. ENISA NIS360 2024. ENISA, 2025.
6. European External Action Service. 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. 2024.

7. OECD. Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity. OECD Publishing, 2024.

15. ІНФОРМАЦІЙНІ РЕСУРСИ

1. NIST Cybersecurity Framework 2.0. URL: https://www.nist.gov/cyberframework (дата звернення: 10.08.2026).
2. ENISA Threat Landscape: Transport Sector. URL: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (дата звернення: 10.08.2026).
3. CISA Cross-Sector Cybersecurity Performance Goals. URL: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (дата звернення: 10.08.2026).
4. OWASP Top 10. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 10.08.2026).
5. Hybrid CoE Publications. URL: https://www.hybridcoe.fi/publications/ (дата звернення: 10.08.2026).

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 %.