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

«ГІБРИДНІ ЗАГРОЗИ ТА КОМПЛЕКСНА БЕЗПЕКА»

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 «Гібридні загрози та комплексна безпека» 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="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>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 rowspan="2">-</td><td rowspan="2">контрольна робота – 21 год. у складі самостійної роботи</td></tr>
<tr></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 «Гібридні загрози та комплексна безпека» є формування у здобувачів системного розуміння комплексної природи, логіки та закономірностей гібридних загроз; здатності виявляти, ідентифікувати, класифікувати й моделювати їх у

взаємопов'язаних кібернетичному, інформаційному, політичному, економічному, соціальному, правовому та фізичному вимірах; розробляти вимоги до програмних і організаційних засобів комплексної безпеки та обґрунтовувати узгоджені міжгалузеві заходи реагування, стійкості й адаптації з урахуванням якості, невизначеності та соціальної відповідальності.

Основні завдання дисципліни «Гібридні загрози та комплексна безпека» – засвоєння понятійного апарату та моделей гібридних загроз; визначення активів, суб'єктів, цілей, вразливостей, залежностей, індикаторів і наслідків гібридних кампаній; критичне оцінювання джерел та доказів; побудова сценаріїв, дерев загроз і карт міжсекторальних зв'язків; застосування чинних національних, європейських і міжнародних стандартів та нормативно-правових документів; формування, класифікація і трасування вимог до програмного забезпечення комплексної безпеки; проєктування багаторівневої системи захисту; оцінювання ризику й якості заходів; планування міжгалузевої взаємодії, кризових комунікацій, безперервності та відновлення; розроблення адаптивних робочих процедур і перевірка їх результативності за сценаріями.

Міждисциплінарні зв'язки

Паралельно вивчають: «Ділова іноземна мова», «Методологія та організація наукових досліджень», «Інноваційні технології Big Data та інформаційної безпеки в управлінні транспортними системами», «Інформаційна безпека та гібридні загрози», «Моделі управління ІТ-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 «Гібридні загрози та комплексна безпека» 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
ОК3	+	+			+	+				+		+		+	+

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

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

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.

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.

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
ОК3	+																	+	+

ПР01. Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення

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. Концептуальні, аналітичні та нормативні засади гібридних загроз

Тема 1. Гібридні загрози як комплексне соціотехнічне явище.

Поняття гібридної загрози, гібридної кампанії та комплексної безпеки. Суб'єкти, наміри, цілі, об'єкти впливу та поєднання військових і невійськових засобів. Кібернетичний, інформаційний, політичний, економічний, соціальний, правовий і фізичний виміри. Синхронізація впливів, неоднозначність, прихованість, заперечуваність та каскадні наслідки.

Системні межі, активи, критичні функції, зацікавлені сторони, міжсекторальні залежності і вразливості. Життєвий цикл гібридної кампанії: підготовка середовища, формування вразливостей, комбінований вплив, ескалація та закріплення наслідків. Особливості транспортних систем і критичної інфраструктури. Соціальна відповідальність та етичні межі аналізу загроз.

Тема 2. Виявлення, ідентифікація, класифікація та моделювання гібридних загроз.

Джерела даних і свідчень, індикатори, аномалії, ознаки координації та часові зв'язки. Критична оцінка надійності джерел, повноти, актуальності, упередженості й суперечностей. Відмінність помилкової інформації, дезінформації та іноземного інформаційного втручання. Обмеження атрибуції та прийняття рішень за неповних даних.

Таксономії загроз за суб'єктом, ціллю, доменом, інструментом, етапом, масштабом і наслідком. Сценарний аналіз, дерева загроз, причинно-наслідкові моделі, карти залежностей та матриці індикаторів. Оцінювання ймовірності, впливу, швидкості розвитку і рівня впевненості. Вимоги до даних, програмних засобів моніторингу та підтримки рішень; критерії якості й перевірюваності моделей.

Тема 3. Нормативні засади та архітектура комплексної безпеки.

Законодавство України про критичну інфраструктуру, стратегії кібербезпеки та державної безпеки. Стратегічний компас ЄС, NIS2, CER, підходи НАТО і Hybrid CoE. NIST CSF 2.0, ISO/IEC 27001:2022, ISO/IEC 27005:2022 та ISO 22361:2022. Формування, класифікація і трасування вимог до програмного забезпечення. Архітектура комплексної безпеки: управління, персонал, фізичний та інформаційний захист, кібербезпека, ланцюги постачання, безперервність сервісів, багаторівневий захист і контроль якості.

Модуль 2. Міжгалузева протидія, стійкість та адаптивний захист

Тема 4. Міжгалузеве реагування, кризове управління та стійкість.

Принципи комплексного реагування: спільна ситуаційна обізнаність, розподіл повноважень, координація державних органів, бізнесу, операторів критичної інфраструктури, громад і міжнародних партнерів. Виявлення, верифікація, ескалація та пріоритизація подій. Міжвідомчий обмін інформацією з урахуванням конфіденційності, цілісності та довіри.

Кризове лідерство і командні структури, ролі та відповідальність, матриця RACI, операційні процедури, журнали рішень і кризові комунікації. Вибір заходів за невизначеності, ризику ескалації, обмежених ресурсів та суперечливих даних. Плани реагування на інциденти, безперервності діяльності та відновлення; резервні канали й мінімально допустимі рівні сервісу.

Показники стійкості, готовності, часу виявлення, реагування й відновлення. Сценарні та настільні навчання, перевірка припущень, контроль виконання, післяопераційний аналіз і коригувальні дії. Оцінювання результативності, простежуваності та якості взаємодії.

Тема 5. Адаптивний захист програмних систем і транспортної інфраструктури.

Принципи secure by design, defense in depth і zero trust. Захист ланцюга постачання, керування доступом, сегментація, резервування, журналювання, моніторинг та перевірка захисних контролів. Узгодження організаційних, інформаційних, кібернетичних і фізичних заходів для транспортних систем. Адаптація робочих процесів та особистого простору до складних і непередбачуваних ситуацій; безпечні комунікації, психологічна стійкість і соціальна відповідальність. Цільовий профіль захисту, план реагування, дорожня карта підвищення стійкості, тестування, валідація та безперервне вдосконалення.

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. Гібридні загрози як комплексне соціотехнічне явище	16	6	2	8	-	16	1	-	15	-
Тема 2. Виявлення, ідентифікація, класифікація та моделювання гібридних загроз	18	6	2	10	-	17	1	-	16	-
Тема 3. Нормативні засади та архітектура комплексної 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. Міжгалузеве реагування, кризове управління та стійкість	27	4	2	21	-	20	1	-	19	-
Тема 5. Адаптивний захист програмних систем і транспортної інфраструктури	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 «Гібридні загрози та комплексна безпека» не передбачено.

6. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з.ч	*Найменування тем*	*Кількість годин*	
		Денна	***Заочна***
Модуль 1.			
1	Картування сценарію гібридної загрози для транспортної організації: активи, критичні функції, суб'єкти, цілі, залежності, вразливості, індикатори та можливі каскадні наслідки	2	-
2	Виявлення та класифікація гібридної кампанії за набором свідчень: перевірка джерел, дерево загроз, матриця індикаторів, оцінка невизначеності та стислий англомовний термінологічний огляд	2	-
3	Розроблення профілю комплексної безпеки на основі законодавства України, NIS2, CER, NIST CSF 2.0 та ISO: специфікація і трасування вимог, багаторівнева архітектура захисту, критерії якості; модульний контроль	4	1
Модуль 2.			
4	Розроблення міжгалузевого плану реагування і безперервності: ролі та RACI, порядок верифікації й ескалації, матриця рішень, обмін інформацією, кризові комунікації та показники стійкості	2	-
5	Настільне навчання за комплексним сценарієм для транспортної системи: адаптивний профіль захисту, перевірка контролів, журнал рішень, післяопераційний звіт і дорожня карта підвищення стійкості; модульний контроль	4	1
	Разом	***14***	***2***

7. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

Виконання лабораторних занять при вивченні дисципліни «Гібридні загрози та комплексна безпека» 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: комплексний аналіз сценарію гібридної загрози для транспортної організації та розроблення узгодженого плану реагування і підвищення стійкості. Завдання, вимоги до структури, оформлення та захисту розміщуються у Google Classroom.

10. МЕТОДИ НАВЧАННЯ

У процесі викладання дисципліни «Гібридні загрози та комплексна безпека» застосовуються словесні, наочні та практичні методи; проблемні лекції; системний, сценарний і ризик-орієнтований аналіз; розбір міжсекторальних кейсів; моделювання загроз і залежностей; критична перевірка джерел; аналіз нормативних вимог; настільні навчання; командне прийняття рішень, взаємне рецензування та захист обґрунтованих рішень.

Основними методами навчання є лекційні та практичні заняття, побудова карт активів, залежностей, дерев загроз і схем реагування у diagrams.net / draw.io або LibreOffice Draw, аналіз індикаторів і ризиків у LibreOffice Calc або Google Sheets, підготовка звітів у LibreOffice Writer або Google Docs, координація завдань у Jira, аналіз навчального мережевого трафіку у Wireshark, моделювання мережевих сценаріїв у Cisco Packet Tracer, безпечне дослідження вебвразливостей з OWASP ZAP та OWASP Juice Shop в Ubuntu Desktop LTS, презентація результатів у LibreOffice Impress або Google Slides і самостійне опрацювання сучасної літератури та офіційних документів.

11. МЕТОДИ КОНТРОЛЮ

У процесі вивчення дисципліни «Гібридні загрози та комплексна безпека» 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 карт активів і залежностей, моделей та класифікацій загроз, матриць вимог, планів реагування, аналітичних звітів і захист практичних робіт. Модульний контроль містить теоретичні та ситуаційні завдання за комплексним кейсом гібридної кампанії. 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 виявлення, ідентифікації, класифікації й моделювання гібридної загрози, застосування нормативних вимог та обґрунтування міжгалузевих заходів реагування і стійкості.

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="5">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="5">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 карти активів і залежностей, паспорта сценарію гібридної загрози, матриці індикаторів, реєстру ризиків, специфікації вимог, плану реагування та звіту за результатами навчання.

5 Матеріали у Google Classroom. Дозволене програмне забезпечення та сервіси: Ubuntu Desktop LTS, Google Classroom, Google Drive, Google Docs, Google Sheets, Google Slides, LibreOffice Writer, LibreOffice Calc, LibreOffice Impress, LibreOffice Draw, diagrams.net / draw.io, Jira, Wireshark, Cisco Packet Tracer, OWASP ZAP, OWASP Juice Shop, Zotero.

14. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова (основна):

1. Giannopoulos G., Smith H., Theocharidou M. The Landscape of Hybrid Threats: A Conceptual Model. Publications Office of the European Union, 2021.
2. NATO. NATO 2022 Strategic Concept. Brussels: NATO, 2022.
3. Council of the European Union. A Strategic Compass for Security and Defence. 2022.
4. European Union. Directive (EU) 2022/2555 (NIS 2 Directive). Official Journal of the European Union, 2022.
5. European Union. Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). 2022.
6. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX.
7. Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021.
8. Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.2022 № 56/2022.
9. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024.
10. International Organization for Standardization. ISO/IEC 27001:2022. Information security management systems – Requirements. 2022.
11. International Organization for Standardization. ISO/IEC 27005:2022. Guidance on managing information security risks. 2022.
12. Ross R. et al. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160 Vol. 2 Rev. 1, 2021.
13. European Union Agency for Cybersecurity. ENISA Threat Landscape: Transport Sector. ENISA, 2023.
14. European Union Agency for Cybersecurity. ENISA Threat Landscape 2025. ENISA, 2025.

Додаткова:

1. European Union Agency for Cybersecurity. ENISA Threat Landscape for Supply Chain Attacks. ENISA, 2021.
2. Cybersecurity and Infrastructure Security Agency. Cross-Sector Cybersecurity Performance Goals. Version 1.0.1, 2023.
3. 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.
4. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61 Rev. 3, 2025.

5. International Organization for Standardization. ISO 22361:2022. Security and resilience – Crisis management – Guidelines. 2022.
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. Hybrid CoE Publications. URL: https://www.hybridcoe.fi/publications/ (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. NATO’s response to hybrid threats. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (дата звернення: 10.08.2026).
4. NIST Cybersecurity Framework 2.0. URL: https://www.nist.gov/cyberframework (дата звернення: 10.08.2026).
5. Законодавство України про критичну інфраструктуру. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (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 %.