НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра комп'ютерних та інформаційних технологій і систем

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Богдан КОРОБКО
«__» _____ 2026 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЄВРОПЕЙСЬКИЙ ДОСВІД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ МАСШТАБНИХ КІБЕРАТАК»

(назва навчальної дисципліни)

Підготовки — Доктор філософії
(назва ступеня вищої освіти)

Освітньої програми — Комп'ютерні науки
(назва освітньої програми)

Спеціальності — 122/F3 Комп'ютерні науки
(код і назва спеціальності)

Полтава
2026 рік

Робоча програма навчальної дисципліни «Європейський досвід інформаційної безпеки та систем захисту інформації в сучасних умовах масштабних кібератак» для здобувачів вищої освіти спеціальності 122/F3 Комп'ютерні науки, третього (освітньо-наукового) рівня вищої освіти.

Розробник: Вергал К.Ю., кандидат економічних наук, доцент кафедри комп'ютерних та інформаційних технологій і систем

Погоджено:

Гарант освітньої програми _____ Олена ДВІРНА

Робоча програма затверджена на засіданні кафедри комп'ютерних та інформаційних технологій і систем

Протокол від «26» серпня 2026 року № 1

Завідувач кафедри комп'ютерних та інформаційних технологій і систем
_____ Олена ДВІРНА

«26» серпня 2026 року

Схвалено навчально-методичною комісією навчально-наукового інституту інформаційних технологій та робототехніки

Протокол від «27» серпня 2026 року № 1

Голова навчально-методичної комісії навчально-наукового інституту інформаційних технологій та робототехніки _____ Олександр ШЕФЕР

« 27 » серпня 2026 року

© Вергал К.Ю., 2026 рік
© Національний університет
імені Юрія Кондратюка, 2026 рік

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="3">Найменування показників</td><td rowspan="3">Галузь знань, спеціальність, ступінь вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">Форма здобуття освіти</td></tr>
<tr><td>денна</td><td>заочна</td></tr>
<tr><td>Кількість кредитів – 3</td><td rowspan="2">Галузь знань

F Інформаційні технології</td><td colspan="2" rowspan="2">вибіркова</td></tr>
<tr><td>Загальна кількість годин – 90</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="5">Спеціальність

F3 Комп’ютерні науки</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й/3-й</td></tr>
<tr><td rowspan="3">Змістових модулів – 2</td><td colspan="2">Семестр</td></tr>
<tr><td colspan="2">4/5/6</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Індивідуальне завдання – не передбачено</td><td rowspan="9">Ступінь вищої освіти: третій (освітньо-науковий)
Доктор філософії</td><td>16 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>14 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>60 год.</td><td>80 год.</td></tr>
<tr><td colspan="2">Індивідуальна робота
0 год.</td></tr>
<tr><td colspan="2">Вид контролю:
диференційований залік</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми здобуття освіти – 30/60
для заочної форми здобуття освіти – 10/80

2. Мета навчальної дисципліни

Метою навчальної дисципліни є поглиблення концептуальних і методологічних знань здобувачів третього (освітньо-наукового) рівня щодо європейських підходів до врядування інформаційною та кібербезпекою, дослідження масштабних кібератак, моделювання кіберризиків і каскадних наслідків, проєктування та експериментального оцінювання систем захисту інформації. Особлива увага приділяється критичному порівнянню регуляторних і технологічних рішень ЄС, перевірці наукових гіпотез, кількісному оцінюванню кіберстійкості, відтворюваності досліджень та обґрунтуванню можливостей адаптації європейського досвіду в Україні.

Дисципліна «Європейський досвід інформаційної безпеки та систем захисту інформації в сучасних умовах масштабних кібератак» є вибірковою складовою професійної підготовки здобувачів третього (освітньо-наукового) рівня вищої освіти за спеціальністю F3 «Комп’ютерні науки».

У результаті вивчення дисципліни очікується формування таких компетентностей:

– Здатність продукувати нові ідеї, розв’язувати комплексні проблеми у сфері комп’ютерних наук, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

– Здатність до абстрактного мислення, аналізу та синтезу.

– Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

– Здатність розв'язувати комплексні проблеми комп'ютерних наук на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.

– Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у комп’ютерних науках та дотичних до них міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з комп'ютерних наук та суміжних галузей.

– Здатність застосовувати сучасні методології, методи та інструменти експериментальних і теоретичних досліджень у сфері комп'ютерних наук, сучасні цифрові технології, бази даних та інші електронні ресурси у науковій та освітній діяльності.

– Здатність виявляти, ставити та вирішувати дослідницькі науково-прикладні задачі та/або проблеми в сфері комп'ютерних наук, оцінювати та забезпечувати якість виконуваних досліджень.

– Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку комп'ютерних наук та інформаційних технологій.

3. Передумови для вивчення дисципліни

Передумовою вивчення навчальної дисципліни є дисципліни, що формують основу підготовки здобувачів вищої освіти другого (магістерського) рівня.

4. Очікувані результати навчання з дисципліни

– Мати передові концептуальні та методологічні знання з комп’ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.

– Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.

– Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у комп'ютерних науках та дотичних міждисциплінарних напрямах.

– Планувати і виконувати експериментальні та/або теоретичні дослідження з комп'ютерних наук та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.

– Розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв’язувати значущі наукові та технологічні проблеми комп’ютерної науки з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.

– Відшуковувати, оцінювати та критично аналізувати інформацію щодо поточного стану та трендів розвитку, інструментів та методів досліджень, наукових та інноваційних проєктів з комп'ютерних наук.

5. Критерії оцінювання результатів навчання

Критерієм успішного проходження здобувачем вищої освіти підсумкового оцінювання є досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом вивчення навчальної дисципліни.

Мінімальний пороговий рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати в мінімальну позитивну оцінку числової (рейтингової) шкали.

Сума балів	ЄКТС значення	Оцінка за національною шкалою	Критерій оцінювання	Рівень компетентності
90 – 100	**A**	**Відмінно**	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Власні пропозиції здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін.	**Високий**, що повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.
82 – 89	**B**	**Добре**	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.	**Достатній**, що забезпечує здобувачу самостійне вирішення основних практичних задач.
74 - 81	**C**	**Добре**	Здобувач загалом добре володіє матеріалом, знає основні положення матеріалу, що відповідають робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та використовує для рішення характерних/типових практичних завдань на професійному рівні. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають ускладнення.	**Достатній**, конкретний рівень, за вивченим матеріалом робочої програми дисципліни.
64 - 73	**D**	**Задовільно**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній**, що забезпечує достатньо надійний рівень відтворення основних положень дисципліни.

60 – 63	**E**	**Достатньо**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постановку стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень і володіє основними положеннями на рівні, який визначається як мінімально допустимий. Правила вирішення практичних завдань з використанням основних теоретичних положень пояснюються з труднощами. Виконання практичних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній,** що є мінімально допустимим у всіх складових навчальної дисципліни.
35 - 59	**FX**	**Незадовільно** з можливістю повторного складання диференційованого заліку	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є неправильними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький**, не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни.
0 – 34	**F**	**Незадовільно** з обов'язковим повторним вивченням дисципліни	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі диференційованого заліку.	**Незадовільний**, здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.

6. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання є:
Поточний контроль:

- виконання практичних робіт
- виконання завдань самостійної роботи (тестування)

Модульний контроль:

- тестування

Підсумковий контроль:

- диференційований залік

7. Програма навчальної дисципліни

Змістовий модуль 1. Європейські засади врядування кібербезпекою, моделювання загроз і ризиків

Тема 1. Європейська архітектура управління кібербезпекою та цифровою стійкістю.

Наукові засади порівняльного дослідження європейської архітектури кібербезпеки та механізмів цифрової стійкості.

Європейська багаторівнева система управління кібербезпекою: компетенції ENISA, CERT-EU, мережі CSIRT та EU-CyCLONe. Порівняння сфери дії та механізмів виконання NIS2, DORA, GDPR і Cyber Resilience Act; розмежування чинних вимог та перехідних положень. Управління безпекою критичних і важливих суб'єктів, стійкість цифрових послуг і захист персональних даних. Науково-методологічні підходи до зіставлення європейських інституційних і правових моделей із практиками України; індикатори результативності та обмеження порівняльного аналізу.

Практичне заняття № 1.

Тема 2. Наукові підходи до моделювання масштабних кібератак та їхніх каскадних наслідків.

Методологія дослідження DDoS, ransomware, атак на ланцюг постачання програмного забезпечення, APT і атак на хмарну та критичну інфраструктуру. Таксономії загроз, MITRE ATT&CK, етапи атаки та побудова графів атак. Визначення активів, залежностей, поверхні атаки, наслідків порушення доступності й цілісності. Моделювання каскадних збоїв і комбінованих сценаріїв. Формулювання дослідницьких гіпотез, відбір показників і меж застосовності моделей; робота з відкритими даними й відтворюваність.

Практичне заняття № 2.

Тема 3. Ризик-орієнтоване проєктування та верифікація систем захисту інформації.

Європейські підходи до управління кіберризиками та до оцінювання пропорційності захисних заходів. ISO/IEC 27001:2022 та ISO/IEC 27005:2022; порівняння з NIST CSF 2.0 як неєвропейським методологічним орієнтиром. Формалізація загроз, вразливостей, ймовірності та наслідків із урахуванням невизначеності. Принципи Zero Trust, контролю доступу, криптографічного захисту, сегментації, захисту персональних даних та безпеки ланцюгів постачання. Побудова альтернативних архітектур захисту; кількісне і якісне порівняння залишкового ризику та експериментальна верифікація.

Практичне заняття № 3.

Змістовий модуль 2. Інтелектуальна протидія кібератакам, реагування та дослідження кіберстійкості

Тема 4. Інтелектуальний аналіз кіберзагроз і виявлення складних атак.

Методологія побудови моніторингу та кореляції подій на основі SIEM, SOAR, IDS/IPS і EDR/XDR. Джерела мережевої телеметрії, журнали подій, контекст загроз і дослідницькі набори даних. Зіставлення сигнатурного, поведінкового та інтелектуального виявлення атак; методи класифікації, аномалій та графової аналітики. Дисбаланс класів, витік даних, перенавчання, дрейф, хибні спрацювання й adversarial ML. Обґрунтування метрик precision, recall, F1 та пропускної здатності аналізу; пояснюваність і відтворюваність експериментів.

Практичне заняття № 4.

Тема 5. Координоване реагування на інциденти та оцінювання кіберстійкості.

Координація реагування на транскордонні масштабні інциденти в ЄС: мережа CSIRT, EU-CyCLONe, CERT-EU та обмін кіберрозвідданими. Стандартизація обміну відомостями про загрози за допомогою STIX/TAXII, аналіз достовірності й умов конфіденційності. Планування реагування, цифрова криміналістика, відновлення, резервування та безперервність діяльності. Сценарне дослідження каскадних інцидентів і tabletop exercises. Відмінності та обмеження MTTD, MTTR, RTO і RPO; критерії перевірки кіберстійкості та оцінювання ефективності відновлення.

Практичне заняття № 5.

Тема 6. Наукове обґрунтування та порівняльне дослідження європейських моделей кіберзахисту.

Проєктування науково-прикладної моделі багаторівневого кіберзахисту для розподіленої, хмарної або критичної інформаційної системи. Вибір і обґрунтування дослідницьких критеріїв: імовірність успішної атаки, залишковий ризик, час виявлення й відновлення, ресурсоємність та доступність. Порівняльна перевірка архітектур відповідно до обраних вимог ЄС і умов їх адаптації в Україні. Планування відтворюваних експериментів, аналіз чутливості, невизначеності та компромісів. Обґрунтування наукової новизни, обмежень і практичного значення; представлення результатів у науковій публікації або дисертації.

Практичне заняття № 6.

Практичне заняття № 7.

8. Структура навчальної дисципліни

для денної форми здобуття освіти

Назви змістовних модулів і тем	**Кількість годин**					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Змістовий модуль 1. Європейські засади врядування кібербезпекою, моделювання загроз і ризиків						

Тема 1. Європейська архітектура управління кібербезпекою та цифровою стійкістю	14	4	2			8
Тема 2. Наукові підходи до моделювання масштабних кібератак та їхніх каскадних наслідків	14	2	2			10
Тема 3. Ризик-орієнтоване проєктування та верифікація систем захисту інформації	14	2	2			10
Разом за змістовим модулем 1	42	8	6			28
Змістовий модуль 2. Інтелектуальна протидія кібератакам, реагування та дослідження кіберстійкості						
Тема 4. Інтелектуальний аналіз кіберзагроз і виявлення складних атак	16	4	2			10
Тема 5. Координоване реагування на інциденти та оцінювання кіберстійкості	16	2	2			12
Тема 6. Наукове обґрунтування та порівняльне дослідження європейських моделей кіберзахисту	16	2	4			10
Разом за змістовим модулем 2	48	8	8			32
Усього годин	**90**	**16**	**14**			**60**

для заочної форми здобуття освіти

Назви змістовних модулів і тем	**Кількість годин**					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Змістовий модуль 1. Європейські засади врядування кібербезпекою, моделювання загроз і ризиків						
Тема 1. Європейська архітектура управління кібербезпекою та цифровою стійкістю	14	—	—	—	—	14
Тема 2. Наукові підходи до моделювання масштабних кібератак та їхніх каскадних наслідків	14	2	2	—	—	10
Тема 3. Ризик-орієнтоване проєктування та верифікація систем захисту інформації	14	—	—	—	—	14
Разом за змістовим модулем 1	42	2	2	—	—	38
Змістовий модуль 2. Інтелектуальна протидія кібератакам, реагування та дослідження кіберстійкості						
Тема 4. Інтелектуальний аналіз кіберзагроз і виявлення складних атак	16	2	2	—	—	12
Тема 5. Координоване реагування на інциденти та оцінювання кіберстійкості	16	2	—	—	—	14

Тема 6. Наукове обґрунтування та порівняльне дослідження європейських моделей кіберзахисту	16	—	—	—	—	16
Разом за змістовим модулем 2	48	4	2	—	—	42
Усього годин	90	6	4	—	—	80

9. Перелік питань для семінарських занять

Тема заняття та перелік питань	**Кількість годин**	
	для денної форми	для заочної форми
Семінарські заняття не передбачені		

10. Перелік питань для практичних занять

Тема заняття та перелік питань	Кількість годин	
	для денної форми	для заоч-ної форми
Практичне заняття 1. Порівняльний аналіз інституційних та нормативних моделей кібербезпеки ЄС. 1. Розмежування ролей ENISA, CERT-EU, мережі CSIRT та EU-CyCLONe. 2. Порівняння сфери дії NIS2, DORA, GDPR і Cyber Resilience Act та строків запровадження вимог. 3. Формування критеріїв порівняння із практиками забезпечення кібербезпеки в Україні.	2	—
Практичне заняття 2. Побудова відтворюваного сценарію масштабної кібератаки. 1. Ідентифікація активів, векторів атак і критичних залежностей. 2. Побудова графа атаки з використанням таксономії MITRE ATT&CK. 3. Обґрунтування дослідницьких гіпотез, можливих каскадних наслідків і метрик.	2	2
Практичне заняття 3. Моделювання ризик-орієнтованої архітектури кіберзахисту. 1. Формалізація ризику та відбір контрзаходів за ISO/IEC 27005. 2. Проєктування альтернативних архітектур контролю доступу, сегментації та захисту даних. 3. Порівняльне оцінювання залишкового ризику, витрат і критеріїв верифікації.	2	—

Практичне заняття 4. Дослідницьке оцінювання методів виявлення кібератак. 1. Порівняння базового сигнатурного й альтернативного інтелектуального підходів. 2. Обґрунтування вибірки та метрик виявлення з урахуванням дисбалансу класів. 3. Аналіз хибних спрацювань, ризику витоку даних та обмежень моделей.	2	2
Практичне заняття 5. Сценарне моделювання реагування на транскордонний кіберінцидент. 1. Побудова схеми обміну кіберрозвідданими та координації CSIRT. 2. Дослідження етапів реагування, відновлення й резервування. 3. Інтерпретація MTTD, MTTR, RTO, RPO та оцінювання результативності сценарію.	2	—
Практичне заняття 6. Проєктування дослідницької моделі багаторівневого кіберзахисту. 1. Вибір об’єкта, дослідницьких критеріїв і європейських вимог до захисту. 2. Зіставлення альтернативних наборів контрзаходів і оцінювання компромісів. 3. Обґрунтування протоколу перевірки залишкового ризику й стійкості.	2	—
Практичне заняття 7. Верифікація та представлення результатів порівняльного дослідження кіберзахисту. 1. Підготовка відтворюваного протоколу експерименту та вихідних даних. 2. Аналіз чутливості, невизначеності й меж застосовності рекомендацій. 3. Аргументація наукової новизни та умов адаптації європейського досвіду в Україні.	2	—
Усього	14	4

11. Перелік питань для лабораторних занять

Тема заняття та перелік питань	Кількість годин	
	для денної форми	для заочної форми
Лабораторні заняття не передбачені		

12. Самостійна робота

Метою самостійної роботи здобувачів третього (освітньо-наукового) рівня вищої освіти є поглиблення знань і розвиток дослідницьких компетентностей

шляхом самостійного пошуку, критичного аналізу та систематизації наукової інформації з використанням сучасних цифрових ресурсів, наукометричних баз даних та інструментів штучного інтелекту; опанування методів обробки, аналізу й візуалізації дослідницьких даних; критичного осмислення та порівняння наукових концепцій, обґрунтування дослідницьких гіпотез, формулювання аргументованих висновків і представлення результатів власних наукових досліджень із дотриманням принципів академічної доброчесності та відкритої науки.

Види самостійної роботи здобувача вищої освіти:

- опрацювання лекційного матеріалу;
- підготовка до практичних занять;
- опрацювання тем курсу, які виносяться на самостійне вивчення, за списками літератури, рекомендованими в робочій програмі навчальної дисципліни;
- підготовка до виконання модульного контролю (тестування);
- відвідування консультацій (згідно графіку консультацій кафедри);
- підготовка до складання диференційованого заліку.

Питання
для самостійного вивчення здобувачами вищої освіти

№ п/п	Перелік питань	Кількість годин	
		для денної форми	для заочної форми
Змістовий модуль 1. Європейські засади врядування кібербезпекою, моделювання загроз і ризиків			
Тема 1. Європейська архітектура управління кібербезпекою та цифровою стійкістю			
1	Критичний аналіз європейських моделей управління кібербезпекою та інституційних повноважень	4	7
2	Порівняння NIS2, DORA, GDPR і CRA: межі дії, чинність вимог та можливості адаптації	4	7
Тема 2. Наукові підходи до моделювання масштабних кібератак та їхніх каскадних наслідків			
3	Систематизація тактик масштабних атак і розроблення графів атак для дослідницьких сценаріїв	5	5
4	Моделювання каскадних наслідків, залежностей та оцінювання поверхні атаки	5	5
Тема 3. Ризик-орієнтоване проєктування та верифікація систем захисту інформації			
5	Порівняння ISO/IEC 27001, 27005 і NIST CSF 2.0 у задачах оцінювання кіберризиків	5	7

6	Обґрунтування контрзаходів Zero Trust та дослідження залишкового ризику	5	7
Змістовий модуль 2. Інтелектуальна протидія кібератакам, реагування та дослідження кіберстійкості			
Тема 4. Інтелектуальний аналіз кіберзагроз і виявлення складних атак			
7	Порівняльне оцінювання сигнатурних, поведінкових та інтелектуальних методів детектування	5	6
8	Планування відтворюваного експерименту з виявлення атак і перевірки якості даних	5	6
Тема 5. Координоване реагування на інциденти та оцінювання кіберстійкості			
9	Аналіз європейських моделей обміну кіберрозвідданими та взаємодії CSIRT	6	7
10	Обґрунтування показників реагування та відновлення в умовах масштабних інцидентів	6	7
Тема 6. Наукове обґрунтування та порівняльне дослідження європейських моделей кіберзахисту			
11	Проєктування порівнюваних архітектур кіберзахисту та набору критеріїв ефективності	5	8
12	Оформлення відтворюваних результатів, аналіз невизначеності й обмежень адаптації моделей ЄС	5	8
Разом		60	80

13. Індивідуальне завдання

Не передбачено планом.

14. Методи навчання

При викладанні дисципліни застосовуються словесні, наочні та практичні методи навчання.

Словесні та наочні методи навчання використовуються під час лекцій, індивідуальних та групових консультацій, практичні – при виконанні практичних занять.

Під час проведення лекцій та практичних робіт використовуються такі словесні методи як розповідь і пояснення.

До числа наочних методів, які застосовуються при викладанні дисципліни, належать: ілюстрація, демонстрація.

Методи навчання, які дозволяють формувати soft skills: порівняльний аналіз європейських кейсів і командне обговорення стратегій реагування; наукове взаємне рецензування моделей загроз; дослідницькі групи з перевірки гіпотез; дискусії щодо балансу безпеки, приватності й регуляторної відповідальності; сценарні tabletop exercises та захист аргументованих рішень.

У межах вивчення навчальної дисципліни передбачена можливість використання результатів неформальної освіти, зокрема проходження онлайн-

курсів Cisco Networking Academy «Network Defense» та «Endpoint Security». Їхні матеріали можуть використовуватися для поглибленого критичного аналізу засобів моніторингу, реагування, захисту мереж і кінцевих пристроїв. Результати неформальної освіти можуть бути визнані за умови відповідності результатам навчання цієї дисципліни та згідно з установленим в університеті порядком; проходження курсу саме по собі не означає автоматичного зарахування балів.

15. Методи контролю

Поточний контроль успішності засвоєння здобувачами вищої освіти навчального матеріалу здійснюється шляхом оцінювання знань здобувачів вищої освіти під час практичних занять, оцінювання виконання здобувачами вищої освіти самостійної роботи, або в ході індивідуальних співбесід зі здобувачами вищої освіти під час консультацій. Вибір конкретних форм і методів поточного контролю знань здобувачів вищої освіти залежить від викладача і доводиться до їхнього відома на першій практичній роботі.

Модульний контроль є частиною поточного контролю і має на меті перевірку засвоєння здобувачем вищої освіти певної сукупності знань та вмінь, що формують відповідний модуль. Він реалізується шляхом проведення тестування, проводиться наприкінці кожного змістового модулю за рахунок аудиторних занять, під час групових консультацій або ж за рахунок часу, відведеного на самостійну роботу здобувачів вищої освіти. На підставі результатів модульного контролю здійснюється міжсесійний контроль (атестація).

Підсумковий контроль здійснюється у формі диференційованого заліку.

16. Розподіл балів, які отримують здобувачі вищої освіти

Схема нарахування балів для денної форми здобуття освіти з навчальної дисципліни
«Європейський досвід інформаційної безпеки та систем захисту інформації в сучасних умовах масштабних кібератак» за видами робіт

Види робіт / контролю	Практичне 1	Практичне 2	Практичне 3	Практичне 4	Практичне 5	Практичне 6	Практичне 7
Навчальна тема	Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	
Виконання практичної роботи	5	5	5	5	5	5	5
Самостійна робота (тестування)	3	3	3	3	3	3	
Модульний контроль	—	—	8,5	—	—	—	8,5
Всього за темами	8	8	16,5	8	8	21,5	

Диференційований залік	30
Всього за результатами вивчення навчальної дисципліни	100

Схема нарахування балів для заочної форми здобуття освіти з навчальної дисципліни
«Європейський досвід інформаційної безпеки та систем захисту інформації в сучасних умовах масштабних кібератак» за видами робіт

Види робіт / контролю		***Перелік тем***				
	Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6
		Практичне заняття				
	—	№ 1	—	№ 2	—	—
Виконання практичної роботи	—	5	—	5	—	—
Самостійна робота (тестування)	7	7	7	7	7	7
Модульний контроль	—	—	9	—	—	9
Всього за темами	7	12	16	12	7	16
Диференційований залік	30					
Всього за результатами вивчення навчальної дисципліни	100					

Шкала та критерії оцінювання виконання практичних завдань

Бали		Критерії оцінювання
для денної форми здобуття освіти	для заочної форми здобуття освіти	
5	5	Виконано завдання практичної роботи в повному обсязі, належним чином оформлено висновки, в яких відображено здатність до практичного застосування отриманих знань.
2,5	2,5	Виконано завдання практичної роботи із несуттєвими помилками або не в повному обсязі, оформлено висновки, які частково розкривають практичне завдання.
0	0	Не виконано практичну роботу або виконано із суттєвими помилками.

Шкала та критерії оцінювання самостійної роботи (тестування)

Бали за формами здобуття освіти	Критерії оцінювання
Денна: 0–3	Тестування: 6 запитань, кожна правильна відповідь — 0,5 бала (0,5 × 6 = 3 бали). Перевірка відповідно до ключа тестів.
Заочна: 0–7	Тестування за кожною темою: 14 запитань, кожна правильна відповідь — 0,5 бала (14 × 0,5 = 7 балів). Перевірка відповідно до ключа тестів.

Шкала та критерії оцінювання модульного контролю (тестування)

Бали за формами здобуття освіти	Критерії оцінювання
Денна: 0–8,5	Модульне тестування: 17 запитань, кожна правильна відповідь — 0,5 бала (0,5 × 17 = 8,5 балів). За кожним змістовим модулем проводиться окреме тестування.
Заочна: 0–9	Модульне тестування: 18 запитань, кожна правильна відповідь — 0,5 бала (18 × 0,5 = 9 балів). За кожним змістовим модулем проводиться окреме тестування.

Шкала та критерії оцінювання знань здобувачів вищої освіти за результатами складання диференційованого заліку у формі тестування

№	Завдання	Бали	Критерії оцінювання
1	Тестування	0-30	Кожна правильна відповідь оцінюється у фіксовану кількість балів (1×30=30), правильність відповідей перевіряється відповідно до ключа тестів.

Шкала оцінювання: національна та ECTS

100-бальна рейтингова система оцінювання	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою для екзамену, диференційованого заліку, курсового проекту (роботи), практики
90 – 100	**A** – відмінно	**5** – відмінно
82 – 89	**B** – дуже добре	**4** – добре
74 – 81	**C** – добре	
64 – 73	**D** – задовільно	**3** – задовільно
60 – 63	**E** – достатньо	
35 – 59	**FX** – незадовільно з можливістю повторного складання	**2 –** незадовільно
0 – 34	**F** – незадовільно з обов'язковим повторним вивченням дисципліни	

Правила модульно-рейтингового оцінювання знань

Загальна оцінка за дисципліну — 100 балів: поточний контроль — 70 балів, диференційований залік — 30 балів.

– Для допуску до диференційованого заліку необхідно набрати щонайменше 35 балів поточного контролю.

1. Поточний контроль для денної форми — максимум 70 балів: сім практичних робіт по 5 балів (35 балів); шість тестувань самостійної роботи по 3 бали (18 балів); два модульні тестування по 8,5 балів (17 балів).

Для заочної форми: два практичні заняття (№ 1 та № 2) по 5 балів (10 балів); шість тематичних тестувань самостійної роботи по 7 балів (42 бали); два модульні тестування по 9 балів (18 балів). Разом поточний контроль: 10 + 42 + 18 = 70 балів. Модульний контроль проводиться після завершення змістових модулів 1 і 2.

Для денної форми максимальна сума балів поточного контролю: 35 + 18 + 17 = 70. Модульний контроль проводиться після завершення змістових модулів 1 і 2 (після практичних занять № 3 і № 7).

Присутність на лекціях і практичних не оцінюється в балах. Пропуски занять підлягають обов'язковому відпрацюванню в індивідуальному порядку під час консультацій. Пропущене заняття має бути відпрацьоване впродовж двох наступних тижнів. При тривалій відсутності здобувача вищої освіти на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії.

2. Підсумковий контроль — диференційований залік у формі тестування (30 запитань по 1 балу, разом 30 балів). Підсумкова оцінка становить суму балів поточного й підсумкового контролю.

17. Методичне забезпечення

Тут мають бути методичні вказівки які повністю відповідають навчальній дисципліні, а це перенести у базову

1. Онищенко С. В., Вергал К. Ю., Глушко А. Д., Янко А. С. Кібербезпека та захист інформації: досвід ЄС для України : навчальний посібник. Полтава : Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2025. 185 с. URL: https://reposit.nupp.edu.ua/item/78242

2. Електронний курс навчальної дисципліни «Європейський досвід інформаційної безпеки та систем захисту інформації в сучасних умовах масштабних кібератак» на платформі Moodle Національного університету «Полтавська політехніка імені Юрія Кондратюка». URL: https://dist.nupp.edu.ua/course/view.php?id=8071

18. Рекомендована література

Базова

1. Онищенко С. В., Вергал К. Ю., Глушко А. Д., Янко А. С. Кібербезпека та захист інформації: досвід ЄС для України : навч. посіб. Полтава : Національний університет «Полтавська політехніка імені Юрія Кондратюка», 2025. 185 с. URL: https://reposit.nupp.edu.ua/item/78242
2. Verhal K., Kushnirenko O., Bykonia O., Romanovskyi N., Opirskyy I. Mathematical Methods for Assessing the Level of Cybersecurity and Digital Development of Countries. *CEUR Workshop Proceedings*. 2025. Vol. 4029: Proceedings of the Workshop on Digital Economy Concepts and Technologies (DECaT 2025). P. 1–11. URL: https://ceur-ws.org/Vol-4029/paper1.pdf
3. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. 2025. DOI: https://doi.org/10.2824/1946374. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
4. European Union Agency for Cybersecurity (ENISA). *ENISA Cybersecurity Threat Landscape Methodology*. 2025. URL: https://www.enisa.europa.eu/publications/enisa-cybersecurity-threat-landscape-methodology
5. European Union Agency for Cybersecurity (ENISA). *NIS2 Technical Implementation Guidance*. 2025. URL: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
6. Aghazadeh Ardebili A., Lezzi M., Pourmadadkar M. Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. *Applied Sciences*. 2024. Vol. 14, No. 24. Article 11807. DOI: https://doi.org/10.3390/app142411807.

7. Bratsas C., Anastasiadis E. K., Angelidis A. K., Ioannidis L., Kotsakis R., Ougiaroglou S. Knowledge Graphs and Semantic Web Tools in Cyber Threat Intelligence: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*. 2024. Vol. 4, No. 3. P. 518–545. DOI: https://doi.org/10.3390/jcp4030025.
8. Abiramasundari S., Ramaswamy V. Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms. *Scientific Reports*. 2025. Vol. 15. Article 13098. DOI: https://doi.org/10.1038/s41598-024-84879-y.
9. European Union Agency for Cybersecurity (ENISA). *Best Practices for Cyber Crisis Management*. 2024. URL: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management
10. Pascoe C., Quinn S., Scarfone K. *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD : National Institute of Standards and Technology, 2024. NIST CSWP 29. DOI: https://doi.org/10.6028/NIST.CSWP.29.
11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
12. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act, DORA). *Official Journal of the European Union*. 2022. L 333. P. 1–79. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Допоміжна

1. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2025*. 2025. DOI: https://doi.org/10.2824/1946374. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
2. European Union Agency for Cybersecurity (ENISA). *2024 Report on the State of the Cybersecurity in the Union*. 2024. URL: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union
3. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. 3rd ed. Geneva : ISO, 2022. URL: https://www.iso.org/standard/27001
4. ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. 4th ed. Geneva : ISO, 2022. URL: https://www.iso.org/standard/80585.html
5. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Official Journal of the European Union*. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

7. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture*. Gaithersburg, MD : National Institute of Standards and Technology, 2020. NIST Special Publication 800-207. DOI: https://doi.org/10.6028/NIST.SP.800-207.
8. Najafimehr M., Zarifzadeh S., Mostafavi S. DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. *Engineering Reports*. 2023. Vol. 5, No. 12. Article e12697. DOI: https://doi.org/10.1002/eng2.12697.

19. Інтернет-ресурси

1. Електронний курс навчальної дисципліни «Європейський досвід інформаційної безпеки та систем захисту інформації в сучасних умовах масштабних кібератак» на платформі дистанційного навчання Moodle Національного університету «Полтавська політехніка імені Юрія Кондратюка». URL: https://dist.nupp.edu.ua/course/view.php?id=8071
2. EUR-Lex — офіційна база законодавства Європейського Союзу (NIS2, DORA, GDPR, Cyber Resilience Act). URL: https://eur-lex.europa.eu/
3. European Union Agency for Cybersecurity (ENISA) — аналітичні звіти й рекомендації з кібербезпеки та кіберстійкості. URL: https://www.enisa.europa.eu/
4. MITRE ATT&CK — база знань про тактики й техніки кібератак для моделювання загроз. URL: https://attack.mitre.org/
5. NIST Cybersecurity Framework 2.0 — методологічний ресурс для порівняльного аналізу управління ризиками. URL: https://www.nist.gov/cyberframework
6. Cisco Networking Academy. Network Defense — онлайн-курс неформальної освіти із захисту мереж, моніторингу подій безпеки та аналізу сповіщень. URL: https://www.netacad.com/courses/network-defense
7. Cisco Networking Academy. Endpoint Security — онлайн-курс неформальної освіти із захисту мереж і кінцевих пристроїв. URL: https://www.netacad.com/courses/endpoint-security