ПрАТ "ВНЗ "МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ"

Навчально-науковий інститут права та безпеки імені князя Володимира Великого

МАУП

Кафедра національної безпеки

Затверджую:
Директор інституту безпеки
_____
Сергій ЛИСЕНКО
"___" _____ 2025 р.

Схвалено на засіданні кафедри
Національної безпеки
Протокол №1 від 07.04 2025 р.
Заст. зав. кафедри
_____
Іван СЕРВЕЦЬКИЙ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«БЕЗПЕКА КРИТИЧНОЇ ТА ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ»

Спеціальності: **256 Національна безпека (за окремими сферами забезпечення і видами діяльності)**

Освітнього рівня: **перший (бакалаврський) рівень**

Освітньої програми: **«Національна безпека (за окремими сферами забезпечення і видами діяльності)»**

Спеціалізація: _____

Київ МАУП 2025

Розробник силабусу навчальної дисципліни:

Кривошликов Сергій Федорович - кандидат технічних наук, доцент кафедри національної безпеки.

(підпис)

Викладач:

Кривошликов Сергій Федорович - кандидат технічних наук, доцент кафедри національної безпеки.

(підпис)

Силабус розглянуто на засіданні кафедри національної безпеки

Протокол № 1 від «07» 08 2025р.

Загальна інформація про навчальну дисципліну

Назва навчальної дисципліни	**Безпека критичної та енергетичної інфраструктури**
Шифр та назва спеціальності	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Рівень вищої освіти	перший (бакалаврський) рівень
Статус дисципліни	обов'язкова
Кількість кредитів і годин	**5 кредита/150 год** Лекції : **34** Семінарські заняття:**34** Самостійна робота студентів: **82**
Терміни вивчення дисципліни	IV семестр
Мова викладання	українська
Вид підсумкового контролю	**екзамен**
Сторінка дисципліни на сайті	https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-b/vstup-do-specialnosti-nacionalna-bezpeka.pdf

Загальна інформація про викладача. Контактна інформація.

Кривошликов Сергій Федорович	
Науковий ступінь	кандидат технічних наук
Вчене звання	професор
Посада	Доцент кафедри національної безпеки.
Дисципліни, які викладає НПП	Безпека критичної та енергетичної інфраструктури
Напрями наукових досліджень	Національна безпека
Посилання на реєстри ідентифікаторів для науковців	ORCID: https://orcid.org/0009-0008-5494-8880
Контактна інформація викладача:	
E-mail:	
Контактний тел.	+380507417375
Телефон кафедри	
Портфоліо викладача на сайті кафедри/Інституту/Академії	https://maup.com.ua/ua/pro-akademiyu/instituti/institut-prava/nacionalna-bezpeka/krivoshlikov.html

1.1 Анотація курсу.

Курс «Безпека критичної та енергетичної інфраструктури» є обов'язковою дисципліною для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності). Курс вивчається протягом 4 семестру обсягом 5 кредитів ECTS (лекції – 34 год., семінарські заняття – 34 год., самостійна робота студентів – 82 години) та дає можливість зрозуміти значення критичної інфраструктури для функціонування держави і суспільства, засвоїти базові підходи до її захисту та принципи забезпечення безперервності життєво важливих функцій.

1.2 Предмет вивчення курсу.

Предметом вивчення навчальної дисципліни є сукупність теоретичних положень, підходів та механізмів державного управління, спрямованих на захист об'єктів критичної та енергетичної інфраструктури, запобігання загрозам, реагування та відновлення їх функціонування.

1.3 Метою викладання «Безпека критичної та енергетичної інфраструктури» є формування у здобувачів здатності визначати об'єкти критичної інфраструктури, аналізувати загрози та вразливості, а також усвідомлювати роль держави й операторів у забезпеченні стійкості, захисту та відновлення.

1.4 Завдання: поглиблене засвоєння понятійно-категоріального апарату у сфері захисту критичної інфраструктури; забезпечення знань про сутність, принципи та завдання державної політики щодо забезпечення безперервності надання критично важливих послуг; розкриття ролі й повноважень суб'єктів забезпечення безпеки об'єктів енергетики та інфраструктури; формування уявлення про сучасні загрози, ризики та фактори дестабілізації функціонування інфраструктурних мереж; набуття навичок аналізу вразливостей, ранжирування загроз та вибору першочергових заходів реагування і відновлення під час кризових ситуацій.

1.5 Пререквізити і постреквізити навчальної дисципліни:

Пререквізити:

«Вступ до спеціальності "Національна безпека"». Зазначена дисципліна створює необхідну концептуальну основу для розуміння структури національної безпеки, її об'єктів та суб'єктів, а також логіки функціонування безпекових інститутів. Опанування базового понятійно-категоріального апарату дозволяє здобувачам вищої освіти коректно розуміти значення критичної інфраструктури для функціонування держави та суспільства, а також принципи забезпечення безперервності надання послуг.

«Логіка». Зв'язок зумовлений необхідністю формування здатності до абстрактного мислення, пошуку, аналізу та синтезу інформації. Ці навички є критично важливими для здійснення класифікації загроз об'єктам безпеки, а також для аналізу та ранжирування джерел загроз і вразливостей критичної та енергетичної інфраструктури.

Постреквізити:

1.6 Програмні компетентності (загальні (ЗК); спеціальні (СК)):

К3. Знання та розуміння предметної області та розуміння професійної діяльності. Забезпечено дисципліною через формування фундаментальних знань про критичну та енергетичну інфраструктуру як основу життєзабезпечення держави та суспільства. Курс закладає системне розуміння професійної діяльності фахівця з національної безпеки у

контексті ідентифікації, категоризації та захисту життєво важливих об'єктів від спектра сучасних загроз.

СК1. Здатність осмислювати та застосовувати знання у сфері національної безпеки, її концепції, цінностей та досягнень. Забезпечено дисципліною шляхом вивчення ролі критичної інфраструктури у загальній системі національної безпеки держави. Здобувачі набувають здатності застосовувати базові безпекові концепції для розробки стратегій захисту енергетичного сектору та забезпечення стійкості держави під час кризових ситуацій.

СК3. Здатність демонструвати та використовувати знання з теорії національної безпеки, виявляти та аналізувати загрози економічній, політичній, інформаційній, воєнній, соціальній та іншим напрямкам життєдіяльності держави. Забезпечено дисципліною завдяки опануванню методології ідентифікації та аналізу специфічних загроз об’єктам критичної та енергетичної інфраструктури. Курс вчить аналізувати комплексний вплив фізичних, кібернетичних та гібридних загроз на функціонування енергосистеми та суміжних галузей.

СК4. Здатність визначати та використовувати знання щодо місця, ролі та функцій суб’єктів національної безпеки та безпекових інститутів України. Забезпечено опрацюванням нормативно-правових та організаційних засад функціонування державної системи захисту критичної інфраструктури. Здобувачі вивчають механізми взаємодії уповноважених державних органів, операторів об’єктів критичної інфраструктури та сектору безпеки і оборони.

СК5. Здатність оцінювати стан безпеки особистості, суспільства та держави в окремих сферах забезпечення національної безпеки або видах діяльності на основі положень теорії безпеки щодо окремих сфер забезпечення національної безпеки та виду діяльності. Забезпечено через формування навичок проведення оцінки вразливостей та ризиків для об’єктів енергетичного сектору. Курс надає інструментарій для оцінювання рівня захищеності критичних послуг та їхнього впливу на загальний стан суспільної безпеки.

СК6. Здатність описувати і оцінювати безпекові процеси і явища в регіональному та національному середовищі, систематизувати оперативно-тактичну інформацію щодо сфер системи національної безпеки. Реалізується через вивчення впливу регіональних та глобальних дестабілізуючих факторів на безперервність роботи критичної інфраструктури. Здобувачі вчаться систематизувати інформацію про інциденти та формувати оперативну картину стану безпеки енергетичних об'єктів.

СК7. Здатність визначати основні властивості об’єктів безпеки в окремих сферах забезпечення національної безпеки і видах діяльності. Забезпечено детальним розглядом критеріїв віднесення об’єктів до критичної інфраструктури, процесу їх категоризації та паспортизації. Дисципліна формує вміння виокремлювати критичні елементи інфраструктури та визначати їхні ключові системні властивості.

СК11. Здатність користуватися інформаційно-аналітичними системами, засобами зв’язку для ефективної комунікації, обміну та захисту інформації. Формується через вивчення принципів функціонування сучасних інформаційних та

кібернетичних систем управління промисловими об'єктами, а також механізмів їх захисту. Здобувачі усвідомлюють важливість захищеного обміну інформацією щодо інцидентів безпеки на об'єктах критичної інфраструктури.

1.7 Очікувані результати навчання (ПРН)

ПРН11. Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності. Забезпечено дисципліною через практичне застосування методик оцінювання рівня захищеності об’єктів критичної інфраструктури. Здобувачі вчаться ідентифікувати вразливості та визначати потенційний вплив інцидентів на безперервність надання життєво важливих послуг населенню та державі.

ПРН12. Планувати та організовувати професійну діяльність в окремих сферах забезпечення національної безпеки та видах діяльності для забезпечення безпеки окремої сфери і виду діяльності держави та організації. Реалізується шляхом набуття навичок розроблення планів забезпечення безперервності діяльності та відновлення функціонування об’єктів критичної інфраструктури після кризових інцидентів, а також планування превентивних безпекових заходів.

ПРН13. Аналізувати та упорядковувати основні властивості об’єктів безпеки окремих сфер забезпечення національної безпеки і видів діяльності та здійснювати класифікацію загроз об’єктам безпеки, класифікацію та ранжирування джерел загроз і вразливостей безпеки. Забезпечено через системний аналіз категорій критичної інфраструктури та ранжирування ризиків за ступенем їхнього впливу. Дисципліна навчає класифікувати джерела загроз енергетичному сектору та розробляти матриці ризиків для пріоритезації заходів захисту.

ПРН15. Характеризувати складові системи забезпечення безпеки за окремою сферою забезпечення національної безпеки і видом діяльності, включаючи повноваження і функції суб’єктів, їх основні завдання, контроль за здійсненням ними заходів забезпечення національної безпеки. Забезпечується детальним вивченням інституційної архітектури національної системи захисту критичної інфраструктури. Здобувачі опановують знання щодо розмежування повноважень між регуляторами, уповноваженими органами державної влади та безпосередніми операторами об'єктів.

ПРН22. Вміти аналізувати та оцінювати детермінанти тінізації економіки як загрози національній безпеці держави, застосовувати сучасні методи та інструменти детінізації економіки України, синтезувати спектр заходів та підходів реалізації політики детінізації під час здійснення професійної діяльності. Формується через аналіз впливу тіньових схем та корупційних ризиків в енергетичному секторі на загальний рівень національної безпеки та стійкість інфраструктури. Дисципліна закладає розуміння економічних передумов вразливості критичних підприємств.

ПРН23. Сприяти захисту економічних інтересів держави в межах своєї компетенції шляхом ідентифікації потенційних загроз, уразливостей та дестабілізаційних чинників економічній безпеці держави, моніторингу підозрілих фінансових операцій, а також розроблення обґрунтованих пропозицій щодо їх нейтралізації та вдосконалення механізмів забезпечення економічної безпеки. Забезпечено шляхом вивчення механізмів виявлення фінансових, організаційних та

управлінських вразливостей операторів критичної інфраструктури. Курс підводить до розуміння необхідності протидії економічним диверсіям та дестабілізаційним впливам на стратегічні підприємства держави.

2. Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ЗАГАЛЬНІ ЗАСАДИ ФУНКЦІОНУВАННЯ ТА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Тема 1. Поняття та архітектура критичної інфраструктури держави

Тема спрямована на формування у здобувачів вищої освіти цілісного уявлення про сутність критичної інфраструктури, її життєво важливі функції та значення для забезпечення національної безпеки, суверенітету і територіальної цілісності України.

У процесі опанування теми здобувачі засвоюють базові підходи до визначення критичних секторів, розуміють взаємозалежність інфраструктурних систем та їхній вплив на стійкість суспільства і держави в умовах сучасних викликів.

Тема 2. Правові та інституційні основи захисту критичної інфраструктури в Україні

Вивчення цієї теми покликане забезпечити здобувачів знаннями про актуальну нормативно-правову базу, що регулює суспільні відносини у сфері захисту критичної інфраструктури, принципи державної політики та стратегічні орієнтири.

Тема формує здатність аналізувати законодавчі акти, розуміти правові механізми легітимації безпекових заходів та усвідомлювати відповідальність за забезпечення функціонування стратегічно важливих об'єктів.

Тема 3. Суб’єкти національної системи захисту: повноваження, координація та взаємодія

Тема спрямована на засвоєння здобувачами інституційної архітектури системи захисту критичної інфраструктури, функцій уповноважених органів державної влади, регуляторів, сектору безпеки і оборони та операторів об’єктів.

Опанування теми розвиває здатність аналізувати організаційні моделі міжвідомчої координації, розподіл зон відповідальності та механізми інформаційної взаємодії суб’єктів у нормальних умовах функціонування та під час кризових ситуацій.

Тема 4. Категоризація та паспортизація об’єктів критичної інфраструктури

Тема дає можливість засвоїти методологію ідентифікації об’єктів критичної інфраструктури, критерії визначення рівня їхньої значущості та порядок внесення до державних реєстрів.

Вивчення теми спрямоване на набуття практичних навичок аналізу властивостей об’єктів, розуміння процедур складання паспортів безпеки та встановлення вимог до забезпечення їхньої стійкості залежно від присвоєної категорії критичності.

Тема 5. Міжнародний та європейський досвід захисту критичної інфраструктури

Тема формує у здобувачів розуміння глобальних тенденцій у сфері безпеки інфраструктури, стандартів Європейського Союзу та підходів НАТО до забезпечення національної стійкості.

Вивчення теми забезпечує здатність оцінювати перспективи імплементації кращих міжнародних практик у національне законодавство та адаптації вітчизняних механізмів управління безпекою до вимог євроатлантичної інтеграції.

ЗМІСТОВИЙ МОДУЛЬ 2. ЕНЕРГЕТИЧНА БЕЗПЕКА ЯК БАЗОВА СКЛАДОВА НАЦІОНАЛЬНОЇ СТІЙКОСТІ

Тема 6. Енергетична безпека держави: сутність, критерії та сучасні загрози

Тема спрямована на формування уявлення про енергетичну безпеку як фундаментальну основу економічної та національної безпеки, її ключові індикатори, дестабілізаційні чинники та гібридні загрози.

Опанування теми дає здобувачам можливість зрозуміти вплив енергетичної стійкості на соціально-політичну стабільність, а також ідентифікувати геополітичні, економічні та технологічні ризики для енергетичного сектору.

Тема 7. Паливно-енергетичний комплекс України як об'єкт критичної інфраструктури

Тема розкриває структуру паливно-енергетичного комплексу, особливості функціонування систем генерації, передачі та розподілу енергоресурсів, а також їхню вразливість перед фізичними впливами.

Вивчення теми формує здатність визначати критичні вузли енергосистеми, аналізувати наслідки їх пошкодження для суміжних секторів економіки та життєдіяльності населення.

Тема 8. Фізичний захист та антитерористична захищеність енергетичних об'єктів

Тема спрямована на засвоєння здобувачами базових знань про інженерно-технічні засоби охорони, режимні заходи та організацію фізичного захисту об'єктів енергетики від диверсійно-терористичних актів і воєнних загроз.

Вивчення теми формує уявлення про комплексний підхід до охорони периметру, контролю доступу та взаємодію підрозділів охорони з правоохоронними органами у разі виникнення нештатних ситуацій.

Тема 9. Кібербезпека в енергетичному секторі: захист технологічних систем управління

Тема дає можливість зрозуміти специфіку кібернетичних загроз для промислових систем управління, приховані вразливості автоматизованих систем та наслідки несанкціонованого втручання в їхню роботу.

Вивчення теми спрямоване на розвиток здатності визначати пріоритетні напрями захисту інформаційно-телекомунікаційних систем енергетичних підприємств та застосовувати організаційні підходи до управління кіберризиками.

Тема 10. Економічні детермінанти та детінізація енергетичної сфери

Тема формує цілісне бачення економічних ризиків функціонування енергетичної інфраструктури, зокрема впливу корупційних схем, монополізації та тіньового сектору на зниження рівня безпеки держави.

Опанування теми дозволяє здобувачам засвоїти методи ідентифікації економічних вразливостей операторів критичної інфраструктури та розробляти обґрунтовані пропозиції щодо нейтралізації фінансових ризиків.

ЗМІСТОВИЙ МОДУЛЬ 3. УПРАВЛІННЯ РИЗИКАМИ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ФУНКЦІОНУВАННЯ

Тема 11. Методологія виявлення, аналізу та оцінювання ризиків для критичної інфраструктури

Тема допомагає сформувати у здобувачів теоретичні знання та практичні навички щодо проведення аудитів безпеки, побудови матриць ризиків та визначення ймовірності реалізації загроз і масштабу їхніх наслідків.

Вивчення теми спрямоване на розвиток аналітичного мислення, необхідного для ранжирування вразливостей та застосування ризик-орієнтованого підходу під час планування заходів захисту.

Тема 12. Забезпечення безперервності надання життєво важливих послуг

Тема дає можливість засвоїти принципи управління безперервністю бізнес-процесів операторів критичної інфраструктури, планування резервних потужностей та забезпечення функціональної стійкості систем.

Вивчення теми спрямоване на розуміння алгоритмів розробки планів забезпечення безперервності та механізмів мінімізації негативного впливу інцидентів на споживачів послуг.

Тема 13. Кризове управління та реагування на інциденти безпеки

Тема спрямована на формування уявлення про організацію кризового управління, алгоритми дій оперативного персоналу та керівництва у разі виникнення надзвичайних ситуацій, диверсій або масштабних аварій.

Вивчення теми дозволяє здобувачам усвідомити роль швидкого реагування, локалізації загрози та ефективної кризової комунікації з органами державної влади і суспільством.

Тема 14. Відновлення інфраструктури: організаційні, правові та ресурсні механізми

Тема розкриває логіку планування відновлювальних робіт, визначення пріоритетів відбудови пошкоджених об'єктів та залучення необхідних матеріально-технічних і фінансових ресурсів.

Вивчення теми забезпечує розуміння того, як процес швидкого відновлення критичних функцій впливає на загальну національну стійкість і обороноздатність держави в умовах дії правового режиму воєнного стану.

Тема 15. Публічно-приватне партнерство у сфері захисту критичної інфраструктури

Тема спрямована на систематизацію знань щодо взаємодії державних інституцій та приватних власників об'єктів критичної інфраструктури, розподілу фінансового тягаря на забезпечення безпеки та формування взаємної довіри.

Вивчення теми допомагає здобувачам зрозуміти межі відповідальності сторін, проблеми стимулювання приватного сектору до інвестицій у безпеку та перспективи спільного протистояння загрозам.

3. Технічне й програмне забезпечення/обладнання

В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проектор та комп'ютер для проведення аудиторних занять з елементам презентацій Microsoft PowerPoint. Вивчення окремих тем і виконання практичних завдань потребує доступу до інформації зі всесвітньої мережі Інтернет, який забезпечується безкоштовною мережею Wi-Fi.

4. Форми і методи навчання

Основними формами занять із навчальної дисципліни «Безпека критичної та енергетичної інфраструктури є практичні заняття та самостійна робота здобувачів вищої освіти.

При проведенні практичних занять передбачено поєднання таких форм і методів навчання, як-то: робота у малих групах, рольові ігри, дискусія, публічні виступи, групові проєкти та кейс-завдання.

Здобувачі освіти опрацьовують інформацію з наукових, навчальних та лекційних джерел, в тому числі за допомогою всесвітньої мережі Інтернет і бібліотек, під час занять виконують усні та письмові завдання, виступають із доповідями та презентаціями, що можуть бути підготовленими як у групі, так і індивідуально.

Програмою курсу також передбачено **індивідуальні завдання.**

5. Система оцінювання та вимоги (критерії оцінювання результатів навчання здобувачів освіти та розподіл балів, які вони отримують)

Оцінювання знань здійснюється відповідно до:

1. Положення про організацію освітнього процесу в ПрАТ «ВНЗ «МАУП» https://surl.li/bpxlbj
2. Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП» http://surl.li/fkfyye

4-й семестр.

№ тем	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Заг.сума балів**
Робота на сем.занятті	4	4	4	4	4	4	4	4	4	36
Сам.робота	1	1	1	1	1	1	1	1	1	9
Всього										**45**

Підсумкове оцінювання	Сума балів за семінари	Сума балів за самостійні роботи	Модульна контрольна робота	Сума балів за екзамен	Загальна сума
	36	9	15	40	100

5.1 Відвідування та робота на семінарських (практичних) заняттях та критерії їх оцінювання

Під час вивчення курсу виконується *робота на семінарських (практичних) заняттях по кожній з тем*.

Критерії оцінювання:

правильність відповідей та розрахунків – від 0 до 3 балів;
відповідність оформлення практичних робіт вимогам – 1 бал.
(враховуються лише за умови нарахування балів за правильність відповідей).

Робота на семінарському занятті оцінюється у **4 бали**.

Максимальна кількість балів за семінарські (практичні) заняття по курсу – **36 балів.**

Зміст практичних занять

№ з/п	**Назва теми**
1	**Тема 1. Поняття та архітектура критичної інфраструктури держави** **Завдання:** Проаналізувати базові підходи до визначення критичної інфраструктури та пояснити її значення для забезпечення життєдіяльності суспільства. Скласти схему взаємозв'язку ключових секторів критичної інфраструктури на прикладі каскадного ефекту при виведенні з ладу одного з них. Розглянути приклади впливу сучасних загроз на функціонування критичних систем управління державою.

	Результат: Здобувачі зможуть систематизувати уявлення про сутність критичної інфраструктури та її архітектуру. Вміння розмежовувати об’єкти за секторальною належністю та інтерпретувати потенційні ризики. Формування навичок узагальнення теоретичних знань щодо стійкості інфраструктурних систем. **Дискусія:** Обговорити межу між звичайним важливим об’єктом економіки та об’єктом критичної інфраструктури. Порівняти підходи до визначення критичності у мирний час та в умовах правового режиму воєнного стану. Розглянути ситуації перехресної залежності секторів та шляхи мінімізації каскадних аварій. **Тема 2. Правові та інституційні основи захисту критичної інфраструктури в Україні** **Завдання:** Визначити ключові нормативно-правові акти, що регулюють захист критичної інфраструктури, та проаналізувати їхні основні положення. Скласти порівняльну характеристику обов'язків держави та приватних операторів відповідно до чинного законодавства. Розглянути кейс застосування правових санкцій за порушення вимог безпеки на стратегічному підприємстві. **Результат:** Здобувачі зможуть орієнтуватися в законодавчому полі сфери захисту критичної інфраструктури. Вміння застосовувати правові норми для вирішення модельних управлінських ситуацій. Формування здатності до правового аналізу відповідальності суб'єктів забезпечення безпеки. **Дискусія:** Обговорити достатність існуючої нормативної бази для протидії гібридним загрозам. Порівняти адміністративну та кримінальну відповідальність операторів за допущені інциденти. Розглянути проблему балансу між режимом секретності та необхідністю публічного контролю. **Тема 3. Суб’єкти національної системи захисту: повноваження, координація та взаємодія** **Завдання:** Проаналізувати інституційну побудову системи захисту та розмежувати повноваження уповноважених органів державної влади. Скласти схему міжвідомчої взаємодії у випадку виникнення надзвичайної ситуації на об'єкті інфраструктури. Розглянути приклад координації дій правоохоронних органів та спеціальних служб під час нейтралізації загрози. **Результат:** Здобувачі зможуть пояснювати роль і функції ключових інституцій у системі

	захисту. Вміння аналізувати механізми координації, відповідальності та підзвітності різних відомств. Формування навичок моделювання управлінських рішень у багатосуб'єктному середовищі. **Дискусія:** Обговорити ефективність централізованої моделі управління безпекою критичної інфраструктури. Порівняти роль регуляторів та силових структур у превентивній діяльності. Розглянути типові управлінські конфлікти при перетині повноважень відомств. **Тема 4. Категоризація та паспортизація об'єктів критичної інфраструктури** **Завдання:** Визначити критерії та алгоритм віднесення об'єктів до відповідних категорій критичності. Скласти структуру паспорта безпеки об'єкта критичної інфраструктури та заповнити модельний зразок. Проаналізувати умовний об'єкт та обґрунтувати присвоєння йому певної категорії значущості. **Результат:** Здобувачі зможуть застосовувати методологію категоризації на практиці. Вміння розробляти документальне забезпечення процесів захисту інфраструктурних об'єктів. Формування навичок оцінювання масштабів можливих наслідків від руйнування об'єкта. **Дискусія:** Обговорити, які критерії категоризації є найбільш вагомими: економічні, соціальні чи екологічні. Порівняти ризики заниження та завищення категорії критичності для підприємства. Розглянути проблематику захисту даних, що містяться у державних реєстрах критичної інфраструктури. **Тема 5. Міжнародний та європейський досвід захисту критичної інфраструктури** **Завдання:** Проаналізувати директиви Європейського Союзу щодо стійкості критичних суб'єктів та визначити їхні ключові вимоги. Скласти таблицю порівняння вітчизняного законодавства зі стандартами НАТО у сфері національної стійкості. Розглянути успішний кейс іноземної держави щодо захисту інфраструктури та запропонувати шляхи його імплементації в Україні. **Результат:** Здобувачі зможуть оперувати міжнародними стандартами у сфері безпеки інфраструктури. Вміння оцінювати рівень адаптації національного законодавства до європейських норм. Формування навичок компаративного аналізу безпекових політик різних держав. **Дискусія:**

	Обговорити виклики, що стоять перед Україною на шляху впровадження європейських директив. Порівняти американську та європейську моделі управління критичною інфраструктурою. Розглянути роль міжнародної технічної допомоги у зміцненні національної стійкості. **Тема 6. Енергетична безпека держави: сутність, критерії та сучасні загрози** **Завдання:** Визначити основні індикатори стану енергетичної безпеки та пояснити їхній вплив на суверенітет держави. Скласти схему гібридних загроз для енергетичного сектору із зазначенням потенційних наслідків. Проаналізувати кейс енергетичного шантажу на міжнародній арені та окреслити заходи протидії. **Результат:** Здобувачі зможуть класифікувати загрози енергетичній сфері та розуміти їхню природу. Вміння визначати пріоритетні напрями державної політики для забезпечення енергонезалежності. Формування навичок макроекономічного аналізу безпеки енергетичних ринків. **Дискусія:** Обговорити співвідношення енергетичної незалежності та інтеграції у глобальні ринки. Порівняти вплив традиційної та відновлюваної енергетики на загальний рівень безпеки. Розглянути проблему диверсифікації джерел постачання енергоресурсів в умовах криз. **Тема 7. Паливно-енергетичний комплекс України як об'єкт критичної інфраструктури** **Завдання:** Охарактеризувати структуру паливно-енергетичного комплексу та виокремити його найбільш критичні вузли. Скласти модель взаємозалежності систем генерації, передачі та розподілу електричної енергії. Розглянути приклад системної аварії в енергомережі та проаналізувати її каскадні наслідки для інших галузей. **Результат:** Здобувачі зможуть пояснювати технологічну логіку функціонування енергетичних об'єктів. Вміння ідентифікувати слабкі місця в інфраструктурі постачання життєво важливих ресурсів. Формування навичок системного бачення єдиної енергетичної системи держави. **Дискусія:** Обговорити вразливості централізованої енергосистеми порівняно з розподіленою генерацією. Порівняти рівень критичності об'єктів атомної та теплової енергетики. Розглянути вплив зношеності основних фондів на рівень стійкості комплексу.

	Тема 8. Фізичний захист та антитерористична захищеність енергетичних об'єктів **Завдання:** Визначити базові вимоги до інженерно-технічного облаштування та охорони периметру стратегічного об'єкта. Скласти план організації контрольно-пропускного режиму та протидії несанкціонованому проникненню. Проаналізувати навчальний сценарій спроби диверсії та запропонувати алгоритм дій підрозділу охорони. **Результат:** Здобувачі зможуть розробляти організаційні заходи фізичного захисту підприємств. Вміння оцінювати ефективність існуючих систем безпеки на конкретних об'єктах. Формування навичок тактичного планування охорони в умовах підвищеного ризику. **Дискусія:** Обговорити баланс між необхідним рівнем безпеки та економічною доцільністю витрат на охорону. Порівняти ефективність фізичних бар'єрів та сучасних електронних систем виявлення. Розглянути проблему використання безпілотних літальних апаратів як інструменту диверсій. **Тема 9. Кібербезпека в енергетичному секторі: захист технологічних систем управління** **Завдання:** Визначити специфічні вектори кібератак на автоматизовані системи управління технологічними процесами. Скласти алгоритм первинного реагування на виявлення шкідливого програмного забезпечення в мережі підприємства. Проаналізувати відомий кейс кібератаки на енергетичну компанію та визначити допущені помилки в захисті. **Результат:** Здобувачі зможуть ідентифікувати кібернетичні вразливості промислових систем. Вміння застосовувати базові підходи до забезпечення кіберстійкості технологічних процесів. Формування навичок інтеграції заходів кібербезпеки у загальну систему захисту об'єкта. **Дискусія:** Обговорити необхідність повної фізичної ізоляції технологічних мереж від корпоративних. Порівняти наслідки витоку інформації та порушення цілісності команд управління обладнанням. Розглянути роль персоналу у формуванні вразливостей через недотримання цифрової гігієни. **Тема 10. Економічні детермінанти та детінізація енергетичної сфери** **Завдання:**

	Визначити типові корупційні ризики та тіньові схеми, що послаблюють економічну стійкість енергетичних підприємств. Скласти схему впливу монополізації ринку на зниження загального рівня енергетичної безпеки. Розглянути кейс фінансових зловживань у сфері закупівель та запропонувати інструменти контролю. **Результат:** Здобувачі зможуть аналізувати економічні передумови вразливості критичної інфраструктури. Вміння визначати маркери підозрілих фінансових операцій та неефективного управління. Формування навичок розробки пропозицій щодо детінізації та підвищення прозорості компаній. **Дискусія:** Обговорити, як корупція безпосередньо впливає на фізичну захищеність об'єктів. Порівняти ефективність державного регулювання та ринкових механізмів у забезпеченні прозорості. Розглянути роль корпоративного управління у мінімізації внутрішніх економічних загроз. **Тема 11. Методологія виявлення, аналізу та оцінювання ризиків для критичної інфраструктури** **Завдання:** Провести ідентифікацію потенційних загроз для умовного об'єкта та скласти реєстр ризиків. Розробити матрицю оцінювання ризиків за критеріями ймовірності настання та тяжкості наслідків. Проаналізувати результати оцінки та визначити першочергові заходи щодо їх мінімізації. **Результат:** Здобувачі зможуть застосовувати ризик-орієнтований підхід у професійній діяльності. Вміння аргументовано визначати пріоритети фінансування заходів безпеки на основі аналізу. Формування навичок структурування аналітичної інформації у вигляді формалізованих звітів. **Дискусія:** Обговорити проблему суб'єктивності експертних оцінок під час аналізу ризиків. Порівняти кількісні та якісні методи оцінювання вразливостей. Розглянути ситуації, коли усунення одного ризику призводить до виникнення нових загроз. **Тема 12. Забезпечення безперервності надання життєво важливих послуг** **Завдання:** Визначити критичні бізнес-процеси підприємства, порушення яких є неприпустимим. Скласти базову структуру плану забезпечення безперервності діяльності для оператора послуг. Проаналізувати сценарій втрати основного джерела живлення та розробити

	алгоритм переходу на резерви. **Результат:** Здобувачі зможуть застосовувати логіку управління безперервністю у кризових умовах. Вміння визначати необхідний мінімум ресурсів для підтримки функціональності об'єкта. Формування навичок завчасного планування резервних спроможностей. **Дискусія:** Обговорити, хто має фінансувати створення резервних потужностей: держава чи приватний власник. Порівняти стратегії повного відновлення роботи та підтримання мінімального рівня послуг. Розглянути критерії визначення допустимого часу простою критичних систем. **Тема 13. Кризове управління та реагування на інциденти безпеки** **Завдання:** Визначити функції кризового штабу підприємства та алгоритм його розгортання при інциденті. Скласти план невідкладних дій оперативного персоналу при виявленні ознак диверсії. Розглянути ситуацію інформаційної атаки на фоні аварії та розробити стратегію антикризової комунікації. **Результат:** Здобувачі зможуть пояснювати механізми переходу від штатного режиму до кризового управління. Вміння організовувати первинне реагування та взаємодію з державними службами порятунку. Формування навичок управління інформаційним фоном навколо кризової події. **Дискусія:** Обговорити важливість наявності чітких протоколів реагування порівняно з імпровізацією керівництва. Порівняти пріоритети рятування життя людей та збереження критичного обладнання. Розглянути типові помилки комунікації з громадськістю під час масштабних збоїв у наданні послуг. **Тема 14. Відновлення інфраструктури: організаційні, правові та ресурсні механізми** **Завдання:** Проаналізувати етапи відновлювальних робіт після масштабних руйнувань об'єктів. Скласти схему залучення підрядних організацій, матеріалів та фінансування для оперативної відбудови. Розглянути кейс відновлення інфраструктури в умовах дефіциту часу та запропонувати оптимізацію процесів. **Результат:** Здобувачі зможуть розуміти логіку циклу відновлення та його організаційне забезпечення. Вміння визначати пріоритетність робіт та раціонально розподіляти наявні ресурси.

	Формування навичок оцінювання ефективності вжитих заходів щодо повернення до нормального функціонування. **Дискусія:** Обговорити дилему: швидке тимчасове відновлення чи тривала капітальна модернізація. Порівняти складнощі відновлення об'єктів у мирний час та в умовах постійних загроз. Розглянути механізми міжнародної допомоги в контексті відбудови енергетичного сектору. **Тема 15. Публічно-приватне партнерство у сфері захисту критичної інфраструктури** **Завдання:** Визначити переваги та ризики взаємодії держави та приватного бізнесу в питаннях безпеки. Скласти модель розподілу відповідальності за захист об'єкта між державними органами та приватним оператором. Проаналізувати ситуацію відмови приватного власника інвестувати в безпеку та запропонувати механізми державного впливу. **Результат:** Здобувачі зможуть аргументувати необхідність кооперації різних секторів для досягнення стійкості. Вміння розробляти формати взаємовигідного співробітництва у сфері захисту інфраструктури. Формування навичок вирішення конфліктів інтересів між вимогами безпеки та комерційною вигодою. **Дискусія:** Обговорити межі втручання держави у господарську діяльність приватних операторів заради безпеки. Порівняти дієвість заохочувальних стимулів та жорстких санкцій у державному регулюванні. Розглянути проблему обміну чутливою безпековою інформацією між державним та приватним секторами.
Усього за навчальною дисципліною	

5.2 Завдання для самостійної роботи та критерії її оцінювання.

Під час вивчення курсу виконуються завдання для самостійних робіт до 19 тем.

Критерії оцінювання:

Змістовність, відповідність темі та вимогам оформлення – 1 бал.

Максимальна кількість балів за одиницю самостійної роботи – 1 бал.

Максимальна кількість балів за самостійну роботу по курсу – 19 балів.

Зміст завдань для самостійної роботи здобувача (СРЗ)

№ п/п	Зміст самостійної роботи здобувача вищої освіти	Форми контролю СРЗ
1	**Тема 1. Поняття та архітектура критичної**	Презентація

	інфраструктури держави Завдання для самостійної роботи: Проаналізувати еволюцію підходів до визначення критичної інфраструктури в національному та міжнародному вимірах. Скласти структурну схему секторів і підсекторів критичної інфраструктури України із зазначенням їхніх життєво важливих функцій.	результатів
2	**Тема 2. Правові та інституційні основи захисту критичної інфраструктури в Україні** Завдання для самостійної роботи: Опрацювати базові положення Закону України «Про критичну інфраструктуру» та скласти аналітичну довідку щодо прав і обов’язків операторів об’єктів. Підготувати короткий огляд існуючих законодавчих прогалин у сфері регулювання захисту інфраструктурних об'єктів.	Презентація результатів
3	**Тема 3. Суб’єкти національної системи захисту: повноваження, координація та взаємодія** Завдання для самостійної роботи: Скласти матрицю розподілу повноважень між секторальними органами, суб'єктами сектору безпеки і оборони та національним органом управління безпекою критичної інфраструктури. Описати модельний сценарій міжвідомчої взаємодії під час ліквідації наслідків надзвичайної ситуації.	Презентація результатів
4	**Тема 4. Категоризація та паспортизація об’єктів критичної інфраструктури** Завдання для самостійної роботи: Дослідити методику віднесення об'єктів до категорій критичності та підготувати таблицю з описом рівнів значущості. Розробити макет паспорта безпеки для умовного підприємства водопостачання або енергетики із зазначенням обов'язкових розділів.	Презентація результатів
5	**Тема 5. Міжнародний та європейський досвід захисту критичної інфраструктури** Завдання для самостійної роботи: Проаналізувати ключові директиви Європейського Союзу у сфері стійкості критичних суб'єктів та мережевої безпеки. Підготувати порівняльний аналіз американської та європейської моделей управління захистом інфраструктури.	Презентація результатів

6	**Тема 6. Енергетична безпека держави: сутність, критерії та сучасні загрози** Завдання для самостійної роботи: Скласти класифікацію глобальних та регіональних загроз енергетичній безпеці України. Підготувати аналітичний огляд впливу геополітичних чинників на диверсифікацію джерел постачання енергоресурсів.	Презентація результатів
7	**Тема 7. Паливно-енергетичний комплекс України як об'єкт критичної інфраструктури** Завдання для самостійної роботи: Описати структуру паливно-енергетичного комплексу держави та виокремити його найбільш вразливі технологічні ланки. Скласти схему каскадного впливу системної аварії в електромережі на функціонування транспортного та телекомунікаційного секторів.	Презентація результатів
8	**Тема 8. Фізичний захист та антитерористична захищеність енергетичних об'єктів** Завдання для самостійної роботи: Опрацювати нормативні вимоги щодо інженерно-технічного облаштування стратегічних об'єктів. Розробити базовий план заходів з посилення фізичного захисту та пропускного режиму умовного об'єкта генерації енергії в умовах підвищеної загрози.	Презентація результатів
9	**Тема 9. Кібербезпека в енергетичному секторі: захист технологічних систем управління** Завдання для самостійної роботи: Дослідити специфіку кібератак на автоматизовані системи управління технологічними процесами та скласти класифікатор таких загроз. Підготувати опис відомого кіберінциденту в енергетичному секторі з аналізом його наслідків та винесених уроків.	Презентація результатів
10	**Тема 10. Економічні детермінанти та детінізація енергетичної сфери** Завдання для самостійної роботи: Проаналізувати вплив монополізації та корупційних ризиків на зниження загального рівня енергетичної безпеки. Підготувати обґрунтовані пропозиції щодо впровадження інструментів комплаєнсу та антикорупційного контролю на підприємствах критичної інфраструктури.	Презентація результатів

11	**Тема 11. Методологія виявлення, аналізу та оцінювання ризиків для критичної інфраструктури** Завдання для самостійної роботи: Опанувати методологію проведення ризик-асесменту та розробити матрицю оцінювання ризиків (ймовірність/наслідки) для обраного об'єкта інфраструктури. Підготувати короткий висновок щодо пріоритетності впровадження захисних заходів.	Презентація результатів
12	**Тема 12. Забезпечення безперервності надання життєво важливих послуг** Завдання для самостійної роботи: Дослідити стандарти управління безперервністю діяльності та скласти алгоритм розробки відповідного плану для оператора критичних послуг. Описати механізми формування резервів матеріально-технічних ресурсів на випадок тривалих відключень живлення.	Презентація результатів
13	**Тема 13. Кризове управління та реагування на інциденти безпеки** Завдання для самостійної роботи: Скласти схему організації роботи кризового штабу підприємства під час настання надзвичайної події. Розробити проєкт стратегії антикризової комунікації для інформування населення щодо тимчасового припинення надання критичних послуг.	Презентація результатів
14	**Тема 14. Відновлення інфраструктури: організаційні, правові та ресурсні механізми** Завдання для самостійної роботи: Проаналізувати алгоритм планування та проведення невідкладних відновлювальних робіт на зруйнованих об'єктах інфраструктури. Підготувати аналітичний огляд механізмів залучення міжнародної фінансової та технічної допомоги для відбудови енергетичного сектору.	Презентація результатів
15	**Тема 15. Публічно-приватне партнерство у сфері захисту критичної інфраструктури** Завдання для самостійної роботи: Оцінити переваги та ризики реалізації проєктів публічно-приватного партнерства в контексті забезпечення безпеки. Запропонувати дієві моделі обміну чутливою інформацією щодо загроз між	Презентація результатів

	державними органами та приватними операторами інфраструктури.	

Реферат є формою самостійної роботи здобувача, метою якої є поглиблення та засвоєння знань з дисципліни «Безпека критичної та енергетичної інфраструктури».

Тему реферату здобувач визначає за першою буквою за списком групи.

В окремих випадках здобувач може самостійно запропонувати та розробити тему реферату, попередньо обговоривши її з викладачем.

Структура, зміст і тема рефератів визначаються програмою курсу, що зумовлює таку послідовність роботи:

вибір теми;

розробка плану;

ознайомлення з рекомендованою літературою;

написання та оформлення роботи.

При написанні реферату та його оформленні варто керуватися такими критеріями:

обґрунтування вибраної теми;

опрацювання відповідної літератури;

наявність авторського розділу;

наявність списку використаних джерел.

Цитати та статистичні матеріали слід обов'язково супроводжувати посиланнями на джерела інформації, які мають бути відображені у списку використаних джерел. Посилання на інформаційні джерела необхідно подавати по тексту у квадратних дужках, наприклад [15, с. 74], 15 – це порядковий номер джерела у списку літератури, а 74 – сторінка із вказаного джерела.

Реферат має складатися із вступу (актуальність теми, предмет, об'єкт, мета, завдання), основної частини (визначення проблеми та послідовне її розкриття), висновків та списку використаних літературних джерел.

Загальний обсяг реферату – до 20 машинописних сторінки формату А4 з 14 шрифтом та інтервалом 1,5, із полями (верхнє/нижнє – 2 см, ліве – 3 см, праве –

1 см.).

Слід мати на увазі, що головною вимогою до реферату є розкриття суті питань, а не кількість сторінок.

Теми рефератів

Теми рефератів:

1 Поняття та ознаки критичної інфраструктури в системі національної безпеки України.
2 Нормативно-правове забезпечення захисту критичної інфраструктури: стан та перспективи розвитку.
3 Роль уповноважених органів державної влади у формуванні політики захисту критичної інфраструктури.
4 Механізми міжвідомчої взаємодії суб'єктів національної системи захисту критичної інфраструктури.
5 Категоризація об'єктів критичної інфраструктури: критерії та методичні підходи.
6 Паспортизація об'єктів критичної інфраструктури як інструмент державного контролю.

7 Міжнародний досвід забезпечення стійкості критичної інфраструктури на прикладі країн Північної Америки.
8 Європейські стандарти захисту мережевих та інформаційних систем критичних суб'єктів.
9 Адаптація національного законодавства у сфері захисту критичної інфраструктури до стандартів євроатлантичної безпеки.
10 Секторальний підхід до визначення об’єктів критичної інфраструктури в Україні.
11 Вразливість взаємозалежних секторів критичної інфраструктури до каскадних аварій.
12 Роль операторів об’єктів критичної інфраструктури у забезпеченні національної стійкості.
13 Відповідальність суб’єктів господарювання за порушення вимог безпеки критичної інфраструктури.
14 Правовий режим функціонування критичної інфраструктури в умовах воєнного стану.
15 Інформаційна взаємодія у системі захисту критичної інфраструктури: виклики та управлінські рішення.
16 Енергетична безпека як фундаментальна складова економічної та національної безпеки.
17 Геополітичні фактори впливу на енергетичну безпеку європейського регіону.
18 Гібридні загрози паливно-енергетичному комплексу України: сутність та наслідки.
19 Вразливість об'єктів об'єднаної енергетичної системи України до фізичних впливів.
20 Організація фізичного захисту та охорони об’єктів атомної енергетики.
21 Інженерно-технічне облаштування периметрів стратегічних об'єктів критичної інфраструктури.
22 Антитерористичний захист стратегічних підприємств енергетичного сектору.
23 Кібернетичні загрози для автоматизованих систем управління технологічними процесами.
24 Забезпечення кіберстійкості операторів систем розподілу електричної енергії.
25 Вплив тіньової економіки на фінансову стійкість підприємств енергетичної сфери.
26 Монополізація енергетичних ринків як загроза національній безпеці держави.
27 Корупційні ризики у сфері державних закупівель для потреб енергетичного сектору.
28 Механізми детінізації економічних відносин у паливно-енергетичному комплексі.
29 Роль комплаєнс-контролю у забезпеченні фінансової прозорості операторів критичної інфраструктури.
30 Диверсифікація джерел постачання енергоресурсів як стратегія підвищення національної стійкості.
31 Розвиток розподіленої генерації енергії як фактор зменшення вразливості інфраструктури.
32 Екологічні ризики та загрози при експлуатації об'єктів критичної енергетичної інфраструктури.
33 Методологія оцінювання ризиків для об’єктів критичної інфраструктури.
34 Ризик-орієнтований підхід у плануванні заходів безпеки стратегічних підприємств.
35 Розробка планів забезпечення безперервності діяльності операторів критичних послуг.
36 Стратегії створення резервних потужностей для критичних систем життєзабезпечення населених пунктів.
37 Організація роботи кризових штабів на підприємствах критичної інфраструктури.
38 Алгоритми реагування на масштабні інциденти безпеки та диверсійні акти.
39 Антикризова комунікація операторів критичної інфраструктури з населенням та органами державної влади.

40 Планування та організація невідкладних відновлювальних робіт на зруйнованих інфраструктурних об'єктах.
41 Ресурсне забезпечення процесів швидкого відновлення надання критичних послуг.
42 Міжнародна фінансова та технічна допомога у відбудові енергетичної інфраструктури держави.
43 Публічно-приватне партнерство як інструмент залучення інвестицій у безпеку інфраструктури.
44 Межі відповідальності держави та приватного бізнесу за захист стратегічних інфраструктурних активів.
45 Економічне стимулювання операторів до підвищення рівня захищеності об'єктів.
46 Вплив людського фактору на виникнення інцидентів безпеки на об'єктах критичної інфраструктури.
47 Організація внутрішніх аудитів безпеки на підприємствах критичної інфраструктури.
48 Сценарне планування як інструмент підготовки до кризових ситуацій в енергетичному секторі.
49 Захист ланцюгів постачання критично важливих матеріалів та обладнання для енергетики.
50 Інтеграція підсистем фізичної, інформаційної та кадрової безпеки на стратегічних підприємствах держави.

5.3 Форми проведення модульного контролю та критерії оцінювання

Проведення модульного контролю з дисципліни «Безпека критичної та енергетичної інфраструктури».

здійснюється у формі тестового завдання.

Тестові завдання стосуються термінології, функцій, принципів та особливостей адміністративного судочинства.

Запитання формулюються з урахуванням принципів:

Лаконічність: чіткі та стислі формулювання.

Завершеність: відповіді охоплюють всі аспекти запитання.

Гомогенність: правильні та неправильні варіанти відповіді логічно та граматично подібні.

Вибірковість: питання стосуються суттєвих аспектів вивченого матеріалу.

Завдання передбачають вибір одного правильного варіанта з трьох запропонованих.

Кожне тестове завдання оцінюється в **1 бал**. (**1 бал** – відповідь правильна; **0** балів – відповідь неправильна).

Загальна максимальна можлива кількість балів за модульну контрольну роботу - 15 балів.

Час на виконання.

На виконання всього контрольного завдання відводиться **30 хвилин.**

Мінімальний поріг.

Для успішного складання модульного контролю здобувач повинен набрати не менше 10 балів (60% від максимальної кількості).

Загальні критерії оцінювання тестових завдань:

Бали	Процент виконання	Результат
14-15	-100%	Зараховано
13	83-90%	
12	76-82%	
11	60-75%	
10	60-67%	
0-9	< 60%	Не зараховано

5.4 Індивідуальні завдання та критерії їх оцінювання

До додаткових (індивідуальних) видів навчальної діяльності відносять участь здобувачів у роботі наукових конференцій, наукових гуртків здобувачів і проблемних груп, підготовці публікацій, участь у Всеукраїнських олімпіадах і конкурсах та Міжнародних конкурсах тощо понад обсяги завдань, які встановлені відповідною робочою програмою навчальної дисципліни.

За рішенням кафедри здобувачам освіти, які брали участь у науково-дослідній роботі та виконували певні види додаткових (індивідуальних) видів навчальної діяльності, можуть присуджуватися заохочувальні (бонусні) бали за визначену освітню компоненту.

Також, заохочувальні бали можуть нараховуватися, якщо здобувач освіти, наприклад, виконав і захистив певні види робіт, відвідував всі лекції, семінарські й практичні заняття, має власний рукописний конспект лекцій та опрацьований додатковий навчальний матеріал, немає пропусків занять без поважних причин, відвідував додаткові консультації за участі лектора тощо.

Сума заохочувальних балів враховується при виставленні підсумкових балів в заліково-екзаменаційну відомість (але не більше **89 балів** в загальному підсумку) і може бути автоматично зарахована при виставленні підсумкової семестрової оцінки з відповідної освітньої компоненти.

Заохочувальні бали не є нормативними і не входять до таблиці розподілу балів, які отримують здобувачі вищої освіти та основної шкали системи оцінювання.

Один захід може бути підставою для виставлення заохочувальних балів лише за однією найбільш релевантною освітньою компонентою.

5.5 Форми проведення семестрового контролю та критерії оцінювання

Екзамен. Відбувається згідно з «Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ ВНЗ МАУП» https://maup.com.ua/assets/files/yakist/studcentr/polozhennya-pro-sistemu-ocinyuvannya-rezultativ-navchannya-zdobuvachiv-vishhoi-osviti.pdf

Орієнтовний перелік питань для комплексного контролю:

1 Розкрийте сутність поняття критичної інфраструктури та її роль у забезпеченні національної безпеки держави.
2 Охарактеризуйте основні життєво важливі функції, які забезпечуються об'єктами критичної інфраструктури.
3 Поясніть концепцію каскадного ефекту при порушенні функціонування об'єктів критичної інфраструктури.
4 Назвіть ключові сектори та підсектори критичної інфраструктури держави.
5 Обґрунтуйте взаємозалежність різних секторів критичної інфраструктури.
6 Охарактеризуйте вплив сучасних загроз на стійкість критичних систем управління державою.
7 Проаналізуйте базові положення законодавства України про критичну інфраструктуру.
8 Охарактеризуйте правові механізми легітимації безпекових заходів на об'єктах критичної інфраструктури.
9 Розкрийте обов'язки операторів об'єктів критичної інфраструктури відповідно до чинного законодавства.
10 Поясніть правовий режим функціонування критичної інфраструктури в умовах воєнного стану.
11 Охарактеризуйте систему юридичної відповідальності за порушення вимог безпеки критичної інфраструктури.
12 Визначте основні напрями вдосконалення нормативно-правової бази у сфері захисту критичної інфраструктури.
13 Охарактеризуйте інституційну архітектуру національної системи захисту критичної інфраструктури.
14 Розкрийте повноваження національного органу управління безпекою критичної інфраструктури.
15 Поясніть роль секторальних органів у системі захисту об'єктів критичної інфраструктури.
16 Охарактеризуйте функції суб'єктів сектору безпеки і оборони щодо захисту критичної інфраструктури.
17 Розкрийте механізми міжвідомчої координації при ліквідації наслідків надзвичайних ситуацій на об'єктах інфраструктури.
18 Поясніть проблеми фрагментації повноважень державних органів у сфері безпеки інфраструктури.
19 Розкрийте методологію категоризації об'єктів критичної інфраструктури.
20 Охарактеризуйте критерії віднесення об'єктів до відповідних категорій критичності.
21 Поясніть процедуру складання та затвердження паспорта безпеки об'єкта критичної інфраструктури.
22 Визначте призначення та порядок ведення державних реєстрів об'єктів критичної інфраструктури.
23 Обґрунтуйте диференціацію вимог щодо захисту об'єктів залежно від їхньої категорії критичності.
24 Охарактеризуйте проблематику захисту інформації, що міститься у реєстрах та паспортах безпеки.
25 Проаналізуйте міжнародні підходи до визначення та захисту критичної інфраструктури.
26 Охарактеризуйте стандарти Європейського Союзу у сфері стійкості критичних суб'єктів.

27 Розкрийте особливості північноамериканської моделі управління безпекою критичної інфраструктури.
28 Поясніть підходи Організації Північноатлантичного договору до забезпечення національної стійкості держав.
29 Визначте перспективи імплементації міжнародного досвіду в національне законодавство України.
30 Охарактеризуйте механізми залучення міжнародної технічної допомоги для захисту критичної інфраструктури.
31 Розкрийте сутність енергетичної безпеки як складової національної стійкості.
32 Охарактеризуйте ключові індикатори оцінки стану енергетичної безпеки держави.
33 Визначте глобальні та регіональні геополітичні фактори впливу на енергетичну безпеку.
34 Поясніть природу гібридних загроз для енергетичного сектору України.
35 Обґрунтуйте стратегію диверсифікації джерел постачання енергоресурсів.
36 Охарактеризуйте вплив енергетичної незалежності на економічну та політичну стабільність держави.
37 Охарактеризуйте структуру паливно-енергетичного комплексу України як об'єкта критичної інфраструктури.
38 Розкрийте технологічні особливості функціонування систем генерації електричної енергії.
39 Поясніть роль систем передачі та розподілу енергоресурсів у забезпеченні життєдіяльності держави.
40 Визначте найбільш вразливі технологічні ланки об'єднаної енергетичної системи України.
41 Проаналізуйте наслідки пошкодження об'єктів атомної енергетики для національної безпеки.
42 Обґрунтуйте значення розвитку розподіленої генерації для підвищення стійкості енергосистеми.
43 Розкрийте принципи організації фізичного захисту об'єктів енергетичної інфраструктури.
44 Охарактеризуйте базові вимоги до інженерно-технічного облаштування периметрів стратегічних підприємств.
45 Поясніть порядок організації контрольно-пропускного режиму на об'єктах критичної інфраструктури.
46 Визначте заходи антитерористичної захищеності підприємств енергетичного сектору.
47 Охарактеризуйте механізми протидії несанкціонованому проникненню та диверсіям на об'єктах енергетики.
48 Обґрунтуйте алгоритми взаємодії підрозділів охорони об'єктів із правоохоронними органами.
49 Розкрийте специфіку кібернетичних загроз для автоматизованих систем управління технологічними процесами.
50 Охарактеризуйте вразливості промислових інформаційно-телекомунікаційних систем в енергетиці.
51 Поясніть наслідки несанкціонованого втручання в роботу диспетчерських систем управління енергомережами.
52 Визначте організаційні підходи до забезпечення кіберстійкості операторів критичної інфраструктури.

53 Розкрийте алгоритм первинного реагування на кіберінциденти в технологічних мережах.
54 Обґрунтуйте значення ізоляції технологічних мереж від корпоративних для безпеки енергетичних об'єктів.
55 Розкрийте економічні детермінанти вразливості підприємств енергетичної сфери.
56 Охарактеризуйте вплив тіньової економіки на фінансову стійкість операторів критичної інфраструктури.
57 Поясніть корупційні ризики у сфері державних закупівель для потреб енергетичного сектору.
58 Визначте наслідки монополізації енергетичних ринків для національної безпеки.
59 Розкрийте механізми детінізації економічних відносин у паливно-енергетичному комплексі.
60 Охарактеризуйте роль комплаєнс-контролю у забезпеченні прозорості компаній-операторів.
61 Розкрийте методологію проведення оцінювання ризиків для об'єктів критичної інфраструктури.
62 Охарактеризуйте процес ідентифікації потенційних загроз та вразливостей стратегічних підприємств.
63 Поясніть принципи побудови матриці ризиків за критеріями ймовірності та тяжкості наслідків.
64 Визначте роль ризик-орієнтованого підходу у плануванні заходів безпеки інфраструктури.
65 Охарактеризуйте кількісні та якісні методи оцінювання вразливостей критичних систем.
66 Обґрунтуйте порядок ранжирування ризиків для встановлення пріоритетності фінансування безпекових заходів.
67 Розкрийте принципи управління безперервністю діяльності операторів критичної інфраструктури.
68 Охарактеризуйте структуру та зміст плану забезпечення безперервності надання критичних послуг.
69 Поясніть критерії визначення допустимого часу простою критичних систем.
70 Визначте стратегії створення резервних потужностей для підприємств життєзабезпечення.
71 Розкрийте алгоритми переходу на резервні джерела живлення в умовах системних аварій.
72 Обґрунтуйте механізми формування резервів матеріально-технічних ресурсів на випадок тривалих збоїв.
73 Розкрийте сутність кризового управління на підприємствах критичної інфраструктури.
74 Охарактеризуйте функції та алгоритм розгортання кризового штабу оператора об'єкта.
75 Поясніть порядок первинного реагування оперативного персоналу на інциденти безпеки.
76 Визначте протоколи взаємодії операторів із державними службами порятунку під час надзвичайних ситуацій.
77 Охарактеризуйте стратегію антикризової комунікації оператора критичної інфраструктури.
78 Обґрунтуйте принципи інформування населення щодо припинення надання критичних послуг.

79 Розкрийте логіку планування невідкладних відновлювальних робіт на зруйнованих об'єктах інфраструктури.
80 Охарактеризуйте етапи ліквідації наслідків масштабних аварій в енергетичному секторі.
81 Поясніть організаційні механізми залучення підрядних організацій для відбудови стратегічних об'єктів.
82 Визначте критерії пріоритезації відновлення пошкоджених елементів критичної інфраструктури.
83 Розкрийте правові аспекти забезпечення швидкого відновлення інфраструктури в умовах воєнного стану.
84 Охарактеризуйте ресурсне забезпечення процесів відновлення функціонування об'єднаної енергосистеми.
85 Розкрийте сутність та значення публічно-приватного партнерства у сфері захисту критичної інфраструктури.
86 Охарактеризуйте розподіл відповідальності за безпеку об'єктів між державою та приватним бізнесом.
87 Поясніть механізми економічного стимулювання операторів до підвищення рівня захищеності активів.
88 Визначте проблеми обміну чутливою безпековою інформацією між державним та приватним секторами.
89 Розкрийте ризики залучення іноземних інвестицій у приватні об'єкти критичної інфраструктури.
90 Обґрунтуйте моделі взаємовигідного співробітництва держави та бізнесу для досягнення національної стійкості.

Шкала відповідності оцінок

Сума балів за всі види навчальної діяльності	**Оцінка ECT8**	**Оцінка за національною шкалою**	
		для екзамену, курсового проекту (роботи),	**для заліку**
90 – 100	A	відмінно	Зараховано
82-89	B	добре	
75-81	C		
68-74	D	задовільно	
60-67	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

6. Політика курсу:

Курс Безпека критичної та енергетичної інфраструктури» передбачає засвоєння та дотримання принципів етики та академічної доброчесності згідно Кодексу академічної доброчесності МАУП та Положення про запобігання та виявлення плагіату в наукових та академічних текстах у ПрАТ ВНЗ МАУП, зокрема орієнтації на запобігання плагіату у будь-яких його проявах: всі роботи, доповіді, есе,

реферати та презентації мають бути оригінальними та авторськими, не переобтяженими цитатами, що мають супроводжуватися посиланнями на першоджерела. Порушеннями академічної доброчесності вважаються: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво, необ'єктивне оцінювання.

Оцінювання здобувача освіти орієнтовано на отримання балів за активність на семінарських (практичних) заняттях, а також виконання завдань для самостійної роботи.

Відпрацювання семінарського заняття може здійснюватися у формі опитування, тестування, виконання практичного завдання, розв'язання задачі з відповідної теми.

В кінці вивчення курсу проводиться модульна контрольна робота 1. Результат модульної контрольної роботи для здобувача, який не з'явився на контрольні заходи, є нульовим. У такому разі, здобувач має можливість повторно виконати модульну контрольну роботи.

Не допустимо: пропуск занять без поважних причин; запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття (за винятком дозволу викладача при зверненні до текстів нормативно-правових актів); списування та плагіат.

Рекомендовані джерела (література):

Основні джерела:

1 Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

2 Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19

3 Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

4 Про ринок електричної енергії : Закон України від 13 квітня 2017 року № 2019-VIII. URL: https://zakon.rada.gov.ua/laws/show/2019-19

5 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020

6 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

7 Про схвалення Стратегії енергетичної безпеки : Розпорядження Кабінету Міністрів України від 04 серпня 2021 року № 907-р. URL: https://zakon.rada.gov.ua/laws/show/907-2021-р

8 Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09 жовтня 2020 року № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п

Додаткові джерела:

1 Про схвалення Концепції розвитку системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 06 грудня 2017 року № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-p
2 Методичні рекомендації щодо категоризації об’єктів критичної інфраструктури : наказ Державної служби спеціального зв’язку та захисту інформації України від 15 січня 2021 року № 23.
3 Національна стійкість та захист критичної інфраструктури: теорія і практика : колективна монографія / за заг. ред. О. В. Литвиненка. Київ : Національний інститут стратегічних досліджень, 2023. 250 с.
4 Енергетична безпека держави в умовах сучасних загроз : навчальний посібник / за ред. В. І. Мунтяна. Київ : Інститут безпеки, 2022. 315 с.
5 Забезпечення кібербезпеки технологічних систем управління : практичний посібник / Державна служба спеціального зв’язку та захисту інформації України. Київ, 2024.

Інформаційні ресурси:

1 Національна бібліотека України імені В. І. Вернадського. URL: http://www.nbuv.gov.ua
2 Офіційний вебпортал парламенту України. URL: http://zakon.rada.gov.ua
3 Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua
4 Урядовий портал Кабінету Міністрів України. URL: http://www.kmu.gov.ua
5 Рада національної безпеки і оборони України. URL: http://www.rnbo.gov.ua
6 Міністерство енергетики України. URL: http://mev.gov.ua
7 Державна служба спеціального зв'язку та захисту інформації України. URL: http://cip.gov.ua
8 Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. URL: https://cert.gov.ua