НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПОЖЕЖНОЇ ТА ТЕХНОГЕННОЇ БЕЗПЕКИ

КАФЕДРА ДЕРЖАВНОГО НАГЛЯДУ У СФЕРІ ПОЖЕЖНОЇ ТА ТЕХНОГЕННОЇ БЕЗПЕКИ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Системи інженерного захисту об'єктів критичної інфраструктури

вибіркової

за освітньо-професійною програмою

Цивільний захист, Охорона праці

підготовки бакалавра

у галузі знань 26 «Цивільна безпека»

за спеціальністю 263 «Цивільна безпека»

Рекомендовано кафедрою
Державного нагляду у сфері
пожежної та техногенної безпеки
на 2025-2026 навчальний рік
Протокол від
« 25 » серпня 2025 року № 01

Силабус розроблений відповідно до Робочої програми навчальної дисципліни «Системи інженерного захисту об'єктів критичної інфраструктури»

2025 рік

Загальна інформація про дисципліну

Анотація дисципліни

Навчальна дисципліна «Системи інженерного захисту об’єктів критичної інфраструктури» є дисципліною циклу вибіркової підготовки, за першим (бакалаврським) рівнем вищої освіти у галузі знань 26 «Цивільна безпека» за спеціальністю 263 «Цивільна безпека», за освітньо-професійною програмою Цивільний захист, Охорона праці.

Дисципліна «Системи інженерного захисту об'єктів критичної інфраструктури» охоплює принципи захисту життєво важливих об'єктів (енергетика, охорона здоров'я, транспорт, IT) від різноманітних загроз шляхом застосування інженерних рішень.

Знання отримані під час вивчення навчальної дисципліни «Системи інженерного захисту об’єктів критичної інфраструктури» передбачають підготовку здобувачів вищої освіти, що володіють спеціальною термінологією, розуміють закономірності інженерного захисту об’єктів критичної інфраструктури, принципи категорування об’єктів критичної інфраструктури, визначення ступеню їх захисту і можуть самостійно пропонувати заходи щодо його підвищення.

Дисципліна «Системи інженерного захисту об’єктів критичної інфраструктури» викладається протягом п’ятого семестру, складається з лекційних та семінарських занять та входить у вибіркову частину професійної підготовки навчального плану підготовки бакалаврів. У відповідності до навчального плану закінчується диференційним заліком.

У курсі лекцій викладаються загальні відомості про теоретико-правові засади формування політики інфраструктурної безпеки як складової національної безпеки, а також практичні питання забезпечення безпеки та стійкості критичної інфраструктури щодо надання життєво важливих функцій та послуг.

Семінарське заняття – форма навчального заняття, за якої викладач організує детальний розгляд здобувачами окремих теоретичних положень навчальної дисципліни та формує вміння і навички їх практичного застосування через індивідуальне виконання відповідно до сформульованих завдань.

Основними функціями семінарського заняття є: розширення, поглиблення й деталізація знань, отриманих на лекціях та в процесі самостійної роботи і спрямованих на підвищення рівня засвоєння навчального матеріалу, закріплення знань, умінь і навичок, розвиток критичного мислення та усного мовлення здобувачів.

Інформація про науково-педагогічного(них) працівника(ів)

Загальна інформація	Рудешко Ірина Вікторівна старший викладач кафедри Державного нагляду у сфері пожежної та техногенної безпеки
Контактна інформація	18034 м. Черкаси, вул. Онопрієнка, 8, кабінети № 127
E-mail	rudeshko1603@ukr.net
Наукові інтереси	вогнестійкість будівельних конструкції із врахуванням спільної роботи будівельних конструкцій будівель каркасного типу.
Професійні здібності	Володіння різними методиками визначення та перевірки класів вогнестійкості будівельних конструкцій, у тому числі із використанням спеціальних програмних комплексів CFD.
Наукова діяльність	Проведення досліджень за допомогою спеціальних програмних комплексів CFD щодо визначення меж вогнестійкості та перевірки на відповідність класам вогнестійкості будівельних конструкцій з різними рівнями механічних навантажень, а також з використанням вогнезахисту. Системи інженерного захисту критичної інфраструктури

Час та місце проведення занять з дисципліни

Аудиторні заняття з навчальної дисципліни проводяться згідно затвердженого розкладу, дистанційно. Електронний варіант розкладу розміщується на сайті Університету. Консультації з навчальної дисципліни проводяться протягом семестру щовівторка з 15.00 до 16.00 у режимі «online». У разі додаткової потреби здобувача в консультації час погоджується з викладачем.

Метою викладання дисципліни «Системи інженерного захисту об’єктів критичної інфраструктури» є поглиблення компетентностей, у т.ч. у секторальному вимірі, здобувачів першого (бакалаврського рівня) вищої освіти щодо: захисту об'єктів критичної інфраструктури та попередження порушень у сфері життєзабезпечення населення; забезпечення безпеки та стійкості критичної інфраструктури у контексті національної безпеки.

Набуття нових професійних та загальних компетентностей необхідних для забезпечення безпеки та стійкості критичної інфраструктури: організація захисту, забезпечення функціональності, цілісності і стійкості критичної інфраструктури, ефективного зниження та контролю за ризиками безпеки, можливості функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз.

Предметом навчальної дисципліни «Системи інженерного захисту об’єктів критичної інфраструктури» є: теоретичні засади та практичні механізми забезпечення інженерних, організаційно-правових, інформаційних, експлуатаційних, наукових та інших заходів, спрямованих на забезпечення інфраструктурної безпеки як складової національної безпеки.

Основні завдання вивчення дисципліни «Системи інженерного захисту об’єктів критичної інфраструктури»:

- сформулювати понятійні та науково-теоретичні засади розуміння сутності інфраструктурної безпеки;
- .вивчити об’єкти критичної інфраструктури, та включення підприємств, установ, організацій до переліку об’єктів критичної інфраструктури;
- поглиблення знань щодо категоризації об'єктів критичної інфраструктури, секторів критичної інфраструктури;
- вивчити загрози щодо об’єктів критичної інфраструктури, включаючи загрози, пов’язані із воєнним станом;
- знати принципи проектування та функціонування інженерних систем захисту критичної інфраструктури;
- освоєння навичок формування та реалізації політики безпеки та стійкості національної критичної інфраструктури щодо всього спектра загроз і ризиків, як одного із пріоритетних напрямів безпекової політики;
- набуття знань і навичок застосування міжнародних практик щодо впровадження державної системи захисту критичної інфраструктури, а також її адміністративно-правового регулювання;
- формування навичок виявлення, запобігання і зниження ризику реалізації ідентифікованих та прогнозованих ризиків у сфері інфраструктурної безпеки;
- надання знань щодо методів паспортизації об'єктів критичної інфраструктури (ОКІ), інструментів розробки стратегій захисту об'єктів критичної інфраструктури від зовнішніх та внутрішніх загроз, політик інформаційної безпеки на об’єктах критичної інфраструктури;
- формування умінь застосовувати комплексні й інклюзивні економічні, юридичні, медико-санітарні, освітні, екологічні та адміністративні заходи, що запобігають і знижують схильність до впливу небезпечних факторів і вразливість до катастроф, підвищують готовність до реагування і відновлення;
- задання знань і навичок щодо залучення громадськості та бізнесу до підвищення безпеки та стабільності функціонування критичної інфраструктури;
- формування системного підходу до реалізації політики інфраструктурної

безпеки в практиках управління сектору безпеки і оборони України;

- визначення інфраструктурної безпеки в умовах війни: проблеми та шляхи вирішення.

У результаті вивчення дисципліни «Системи інженерного захисту об’єктів критичної інфраструктури» здобувач вищої освіти повинен отримати:

знання:

- системи нормативної документації у сфері захисту критичної інфраструктури;;
- поняття та термінологію;
- методики вирішення загальних питань щодо належності об’єкта до критичної інфраструктури;
- методу категоризації ОКІ;
- методики оцінювання стану захищеності ОКІ;
- загроз і небезпек для ОКІ;
- загальних принципів проектування інженерного захисту КІ;
- основних елементів інженерних систем захисту;
- міжнародних практик щодо впровадження державної системи захисту критичної інфраструктури, а також її адміністративно-правового регулювання;
- системного підходу до реалізації політики інфраструктурної безпеки в практиках управління сектору безпеки і оборони України;
- механізмів державного управління захистом об'єктів критичної інфраструктури;
- світового досвіду створення національних систем забезпечення безпеки та стійкості критичної інфраструктури;
- адміністративно-правового регулювання інфраструктурної безпеки у контексті формування нової безпекової програмиУкраїни;
- систем захисту критичної інфраструктури;
- інфраструктурної безпеки на регіональному, місцевому та об’єктовому рівнях

уміння/навички:

- аналізувати дані щодо призначення будівель та споруд і режиму їх експлуатації, кількості людей; визначати ступені стійкості будівель та споруд; оцінювати інженерно-технічні рішення на відповідність встановленим вимогам безпеки; розробляти та оформляти експертні висновки, протоколи узгодження для застосування заходів щодо усунення порушень;
- аналізувати і визначати критичність об’єктів інфраструктури;
- визначати категорію критичності об’єктів інфраструктури;
- визначати ступінь захищеності об’єктів інфраструктури;
- складати необхідні документи щодо причетності об’єктів до критичної інфраструктури;
- розробляти заходи щодо підвищення ступеня захищеності об’єкту;
- проводити паспортизацію об’єктів критичної інфраструктури;
- розробляти плани захисту за кожною із проектних загроз національного, секторального та об’єктового рівня
- приймати обґрунтовані рішення з питань забезпечення національної безпеки держави;
- формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності);
- управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів;
- розробляти методики побудови системи управління інформаційною безпекою на об’єктах критичною інфраструктурою;
- проводити моніторинг рівня безпеки об’єктів критичної інфраструктури;
- використовувати систему аудиту інформаційної безпеки на об’єктах критичної інфраструктури.
- визначати критичні елементи об’єкта критичної інфраструктури; вибирати

необхідний ефективний рівень інженерного захисту для критичних елементів об’єкта критичної інфраструктури;

- проводити класифікацію споруд інженерного захисту критичного елементу об’єкту критичної інфраструктури,
- визначити недоліки у інженерному захисті та надавати рекомендації щодо їх усунення;
- проводити розрахунки та складати аркуш оцінювання стану та обсягів виконання робіт з інженерного захисту об’єктів критичної інфраструктури.

відповідальність та автономія:

- проводити обстеження технічного стану будівельних конструкцій і будівель у цілому;
- оформлювати і надавати оцінку за результатами обстежень будівель і споруд;
- вибирати і пропонувати методи відновлення і посилення будівельних конструкцій;
- оцінювати характеристики пожежної безпеки будівельних матеріалів та конструкцій, будівель і споруд та контролю додержання вимог пожежної безпеки під час проведення будівельних робіт;
- проводити розрахунки щодо визначення несучої здатності конструкцій нових і із врахуванням зносу;
- аналізувати дані щодо призначення будівель та споруд і режиму їх експлуатації, відповідність об`ємно-планувальних, конструктивних рішень, зокрема евакуаційних шляхів та виходів; інженерно- технічних рішень в будівлях та спорудах вимогам пожежної безпеки.

Опис навчальної дисципліни

Найменування показників	Форма здобуття освіти
	очна (денна)
Статус дисципліни *(обов’язкова загальна або обов’язкова професійна або вибіркова)*	вибіркова
Рік підготовки	3
Семестр	5
Обсяг дисципліни:	
- в кредитах ЄКТС	4
- кількість змістовних модулів	1
- загальна кількість годин	120
- лекції (годин)	22
- практичні заняття (годин)	
- семінарські заняття (годин)	20
- лабораторні заняття (годин)	
– курсовий проект (робота) (годин)	
- інші види занять (годин)	
- самостійна робота (годин)	76
- індивідуальні завдання (науково-дослідне) (годин)	- -
- підсумковий контроль (диференційний залік, екзамен)	2

Передумови для вивчення дисципліни:

математика, фізика, матеріалознавство, хімія.

Результати навчання та компетентності з дисципліни

Відповідно до освітньої програми «Цивільний захист» Охорона праці

назва

вивчення навчальної дисципліни повинно забезпечити:

- досягнення здобувачами вищої освіти таких результатів навчання:

Програмні результати навчання	ПРН
- Використовувати у професійній діяльності сучасні інформаційні технології, системи управління базами даних та стандартні пакети прикладних програм.	ПРН09
- Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог	ПРН03
- Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.	ПРН14
- Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності).	ПРН10.
-. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.	ПРН15.
- Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.	ПРН17
Дисциплінарні результати навчання	
- Здатність здійснювати керівництво особовим складом під час виконання функціональних обов'язків;	
- Здатність контролювати дотримання підлеглими норм та правил з охорони праці, пожежної безпеки та виробничої санітарії;	
- Здатність організовувати та проводити заняття, навчання з особовим складом підрозділу.	

- формування у здобувачів вищої освіти наступних компетентностей:

Програмні компетентності (загальні та професійні)	ЗК, СК
- Здатність до абстрактного мислення, аналізу та синтезу.	ЗК03
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	ЗК06
- Навики здійснення безпечної діяльності.	ЗК09
- Прагнення до збереження навколишнього середовища	ЗК10
Очікувані компетентності з дисципліни	абревіатура
- Здатність оперувати термінами та визначеннями понять у сфері цивільного захисту, охорони праці; основними положеннями, вимог та правил стосовно проведення моніторингу, організовування та впровадження заходів щодо запобігання, ліквідування надзвичайних ситуацій.	СК12
- Здатність оперувати фізичними та хімічними термінами, розуміти сутність математичних, фізичних та хімічних понять та законів, які необхідні для здійснення професійної діяльності	СК14
- Здатність організовувати нагляд (контроль) за додержанням вимог законодавства у сфері цивільного захисту, техногенної, промислової безпеки та охорони праці.	СК15

- Здатність до оцінювання ризиків виникнення та впливу надзвичайних ситуацій на об’єктах суб’єкта господарювання та ризиків у сфері безпеки праці.	СК16
- Здатність до аналізу й оцінювання потенційної небезпеки об’єктів, технологічних процесів та виробничого устаткування для людини й навколишнього середовища.	СК18

Програма навчальної дисципліни

Теми навчальної дисципліни:

Модуль 1. Комплексний інженерний захист та безпека об'єктів критичної інфраструктури

Тема 1. Об’єкти критичної інфраструктури. Загальні відомості. Нормативне забезпечення

Понятійні й науково-теоретичні засади розуміння сутності інфраструктурної безпеки Об’єкти критичної інфраструктури. Включення підприємств, установ, організацій до переліку об’єктів критичної інфраструктури Складові національної інфраструктури. Дефініція «критична інфраструктура» у контексті національної безпеки Категорізація об’єктів критичної інфраструктури. Поняття національної системи стійкості та її формування в Україні у контексті захисту критичної інфраструктури. Інфраструктурний потенціал та інфраструктурна могутність держави. Характеристика критичної інфраструктури як об’єкта державного управління.

Нормативне забезпечення інженерного захисту об’єктів критичної інфраструктури.

Тема 2. Види небезпек та загроз об’єктів критичної інфраструктури

Природні загрози щодо об’єктів критичної інфраструктури. Техногенні загрози щодо об’єктів критичної інфраструктури. Загрози соціально-політичного характеру. Загрози об’єктам критичної інфраструктури України в умовах воєнного стану.

Механізми державного управління захистом об'єктів критичної інфраструктури. Інфраструктурна безпека в умовах війни: проблеми та шляхи вирішення.

Аналіз загроз для об’єктів критичної інфраструктури. Класифікація посягань на об'єкти критичної інфраструктури. Координація та взаємодія систем: фізичного захисту, запобігання терористичним актам, цивільного захисту. Залучення громадськості та бізнесу до підвищення безпеки та стабільності функціонування критичної інфраструктури.

Тема 3.. Принципи проектування та функціонування інженерних систем захисту критичної інфраструктуриє

Загальні принципи проєктування інженерного захисту критичної інфраструктури. Основні елементи інженерних систем захисту критичної інфраструктури. Функціонування інженерних систем захисту критичної інфраструктури.

Завдання законодавства щодо захисту критичної інфраструктури. Наднаціональні нормативні правові акти, стандарти та керівництва в галузі регулювання критичної інфраструктури та протидії гібридним загрозам.

Системоутворюючі (базові) нормативно-правові акти України у сфері інфраструктурної безпеки. Правова природа щорічних послань Президента України.

Законодавство у сфері попередження терористичних актів щодо об'єктів критичної інфраструктури.

Тема 4. Методика оцінки стану захищеності об’єктів критичної інфраструктури.

Методика оцінки стану захищеності об’єктів критичної інфраструктури. Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури.

Порядок проведення моніторингу рівня безпеки об’єктів критичної інфраструктури.

Критерії і показники оцінки стану захищеності об’єктів критичної інфраструктури.

Тема 5. Оцінки стану кіберзахисту ОКІ

Порядок оцінювання кіберзахисту. Види та частота здійснення оцінювання. Вимоги до оцінювачів/об'єктів оцінювання. Порядок здійснення Державного контролю за додержанням вимог законодавства у сфері кіберзахисту ОКІ. Державний контроль за додержанням вимог законодавства у сфері кіберзахисту ОКІ. Критерії і показники оцінки стану захищеності об'єктів критичної інфраструктури.

Принципи адміністративно-правового забезпечення стійкості критичної інформаційної інфраструктури України. Категоріювання об'єктів критичної інформаційної інфраструктури. Державний реєстр об'єктів критичної інформаційної інфраструктури.

Система аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Тема 6. Нормативна база техногенної безпеки об'єктів критичної інфраструктури України

Техногенна безпека як невід'ємна складова національної безпеки України. Нормативно-правове забезпечення техногенної безпеки в Україні.

Національний класифікатор ДК 019:2010 «Класифікатор надзвичайних ситуацій», (наказ Держспоживстандарту України 11.10.2010 № 457).

- Порядок класифікації НС за їх рівнями (ПКМУ від 24.03.2004 № 368)
- Правила техногенної безпеки (наказ МВС України від 05.11.2018 № 879)
- ІНСТРУКЦІЯ з організації роботи щодо ідентифікації об'єктів підви-щеної небезпеки (Наказ ДСНС від 04.09.2025 № 1102)
- ПОРЯДОК ідентифікації ОПН та їх обліку (ПКМУ від 13.09.2022 р. № 1030)
- Порядок розроблення звіту про заходи безпеки на об'єкті підвищеної небезпеки наказ МВС України від 21.02.2023 № 114
- Порядок розроблення політики запобігання аваріям на об'єкті підви-щеної небезпеки (наказ МВС України від 21.02.2023 № 115)
- ПОРЯДОК функціонування та ведення Державного електронного реєстру об'єктів підвищеної небезпеки (ПКМУ від 07.07.2023 № 690)
- МЕТОДИЧНІ РЕКОМЕНДАЦІЇ щодо розроблення планів локалізації і ліквідації аварій та їх наслідків (Наказ ДСНС 17.05.2022 N 253).

Тема 7. Системи інженерного захисту АЕС

Загальна характеристика технологічного процесу отримання електроенергії на АЕС. Особливості пожежно небезпеки машинних залів АЕС. Особливості роботи реакторів типу ВВЕР-1000. Загрози для інфраструктурної безпеки АЕС в умовах воєнного стану.

Тема 8. Системи безпеки регламентної роботи АЕС

Системи захисту. Системи локалізації. Системи забезпечення. Системи керування. Технічне водопостачання. Спеціальне водоочищення. Радіактивні відходи.

Тема 9. Системи інженерного захисту об'єктів нафтопереробної промисловості

Безпека об'єктів критичної інфраструктури в секторі нафтопереробної промисловості. Об'єкти критичної інфраструктури у сфері нафтопереробної промисловості та суб'єкти їх охорони. Система об'єктів критичної інфраструктури у виробничій галузі. Загрози для інфраструктурної безпеки нафтопереробної промисловості в умовах воєнного стану..

Тема 10. Формування та реалізація державної політики захисту критичної інфраструктури у сфері соціального захисту та систем життєзабезпечення

Інфраструктурна безпека у сфері комунальних послуг. Складові безпеки у секторі критичної інфраструктури «Транспорт і пошта». Об'єкти критичної інфраструктури у сфері охорони здоров'я.. ОКІ у соціально-економічних аспектах життєдіяльності громад.

Тема 11. Управління ризиками об'єктів критичної інфраструктури в умовах сучасних викликів і загроз.

Ризик-орієнтовані підходи до управління безпекою на об’єктах критичної інфраструктури. Оцінка загроз та ризиків критичній інфраструктурі у відповідних сферах. Адміністративно-правові основи скринінгу іноземних інвестицій в стратегічно важливі державні об’єкти. Методика побудови системи управління інформаційною безпекою на об’єктах критичною інфраструктурою. Моніторинг рівня безпеки об’єктів критичної інфраструктури.

Розподіл дисципліни у годинах за формами організації освітнього процесу та видами навчальних занять очна (денна) форма навчання:

Назви змістових модулів і тем	Кількість годин						
	очна (денна) форма						
	усього	у тому числі					
		лекції	семінарські заняття	практичні заняття	лабораторні заняття	самостійна робота.	поточний контроль
1	2	3	4	5	6	7	8
Модуль 1							
Змістовий модуль 1. Комплексний інженерний захист та безпека об'єктів критичної інфраструктури							
Тема 1. Об’єкти критичної інфраструктури. Загальні відомості. Нормативне забезпечення	11	2	2			7	тести, реферати, доповіді
Тема 2. Види небезпек та загроз об’єктів критичної інфраструктури	11	2	2			7	тести, реферати, доповіді
Тема 3. Принципи проектування та функціонування інженерних систем захисту критичної інфраструктуриє	11	2	2			7	тести, реферати, доповіді
Тема 4. Методика оцінки стану захищеності об’єктів критичної інфраструктури.	11	2	2			7	тести, реферати, доповіді
Тема 5. Оцінки стану кіберзахисту ОКІ	11	2	2			7	тести, реферати, доповіді
Тема 6. Нормативна база техногенної безпеки об’єктів критичної інфраструктури України	11	2	2			7	тести, реферати, доповіді
Тема 7 Системи інженерного захисту АЕС	11	2	2			7	тести, реферати, доповіді

Тема 8. Системи безпеки регламентної роботи АЕС із реактором типу ВВЕР-1000	11	2	2			7	тести реферати, доповіді
Тема 9. Системи інженерного захисту об'єктів нафтопереробної промисловості	11	2	2			7	тести реферати, доповіді
Тема 10. Формування та реалізація державної політики захисту критичної інфраструктури у сфері соціального захисту та систем життєзабезпечення	11	2	2			7	тести реферати, доповіді
Тема 11. Управління ризиками об'єктів критичної інфраструктури в умовах сучасних викликів і загроз	10	2	2			6	тести реферати, доповіді
Залік			2				
Разом за змістовим модулем	**120**	**22**	**22**			**76**	

Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1.	Тема 1.Ідентифікація та категоризація об'єкта критичної інфраструктури	2
2.	Тема 2. Методика категоризації об'єктів критичної інфраструктури.	2
3.	Тема 3. Принципи проектування інженерного захисту критичної інфраструктури	2
4.	Тема 4. Оцінювання стану захищеності об'єктів критичної інфраструктури.	2
5.	Тема 5. Визначення рівня ризику при використанні небезпечних хімічних речовин.	2
6.	Тема 6. Системи інженерного захисту технологічного процесу АЕС.	2
7.	Тема 7. Системи захисту технологічного процесу виробництва електроенергії на АЕС. Вивчення зменшення несучої здатності з/б конструкцій внаслідок корозії арматури.	2
8.	Тема 8. План захисту із забезпечення цивільного захисту, пожежної та техногенної безпеки на об'єктах критичної інфраструктури та протидії проектній загрозі національного рівня «Пожежі та вибухи».	2
9.	Тема 9. Об'єкти критичної інфраструктури у фінансовій та екологічній сферах	2
10.	МКР	2

11.	Залік	2
	Усього годин	22

Орієнтовна тематика індивідуальних завдань

Відповідно до навчального плану передбачено виконання контрольних і самостійних робіт за кожною темою.

Тематика рефератів: згідно основним темам дисципліни із погодженням із викладачем.

Оцінювання освітніх досягнень здобувачів вищої освіти

Засоби оцінювання

Засобами оцінювання та методами демонстрування результатів навчання є: диференційний залік.

Оцінювання рівня освітніх досягнень здобувачів за освітніми компонентами, здійснюється за 100-бальною шкалою, що використовується в НУЦЗ України з переведенням в оцінку за рейтинговою шкалою - ЄКТС та в 4-бальну шкалу.

Таблиця відповідності результатів оцінювання знань з навчальної дисципліни за різними шкалами

За 100-бальною шкалою, що використовується в НУЦЗ України	За рейтинговою шкалою (ЄКТС)	За 4-бальною шкалою
90–100	A	відмінно
80–89	B	добре
65–79	C	
55–64	D	задовільно
50–54	E	
35–49	FX	незадовільно
0–34	F	

Критерії оцінювання

Форми поточного та підсумкового контролю

Поточний контроль проводиться на кожному семінарському занятті. Він передбачає оцінювання теоретичної та практичної підготовки здобувачів вищої освіти із зазначеної теми (у тому числі, самостійно опрацьованого матеріалу) за набутими навичками під час вивчення теоретичного матеріалу та виконання завдань практичних робіт.

Модульна контрольна робота є складовою поточного контролю і здійснюється через проведення письмової роботи під час проведення останнього практичного заняття (для очної(денної) та дистанційної форм навчань) в межах залікового модуля. Кожний варіант модульної контрольної роботи складається з індивідуальних задач та контрольних питань.

Підсумковий контроль проводиться у формі диференційного заліку.

Розподіл та накопичення балів, які отримують здобувачі, за видами навчальних занять та контрольними заходами з дисципліни

Види навчальних занять		Кількість навчальних занять	Максимальний бал за вид навчального заняття	Сумарна максимальна кількість балів за видами навчальних занять
Змістовий модуль 1	лекції	11	-	5
	практичні заняття*	9	5	45
	за результатами виконання контрольних робіт	1	25	25
Участь у конференціях, олімпіадах				-
Виконання індивідуального завдання				25
Всього				**100**

. **Поточний контроль.**

Поточний контроль проводиться у формі тестування на кожному занятті, виконання самостійних робіт і модульної контрольної роботи.

Контрольні заходи, які здійснюються впродовж семестрових модулів з метою оцінювання рівня навчальних досягнень здобувачів. Основна мета поточного контролю – забезпечення зворотного зв'язку між викладачем та здобувачем, перевірка готовності сприйняття здобувачам навчального матеріалу дисципліни, оцінювання досягнених ними програмних результатів навчання.

Модульна контрольна робота є складовою поточного контролю і здійснюється через проведення письмової роботи під час проведення останнього семінарського заняття (для очної(денної) та дистанційної форм навчань) в межах залікового модуля. Кожний варіант модульної контрольної роботи складається з індивідуальних задач та контрольних питань.

Підсумковий контроль.

Підсумковий контроль проводиться у формі диференційного заліку.

Диференційний залік виставляється накопиченням балів за результатами поточного контролю додаванням результатів поточного та підсумкового тестування. Питання , які входять до підсумкового тестування надаються здобувачам вищої освіти на першій лекції, входять до вмісту силабусу дисципліни «Системи інженерного захисту об'эктыв критичноъ ынфраструктури» та розміщуються у відповідних гугл-класах.

Підсумкове тестування є обов'язковим для всіх здобувачів вищої освіти не зважаючи на результат поточного контролю. Всі форми обов'язкового контролю повинні відпрацьовані до початку тестування. Отримані здобувачем бали за накопичувальною 100-бальною шкалою оцінювання знань переводиться у національну шкалу та в рейтингову шкалу ЄКТС згідно з таблицею.

Таблиця відповідності результатів контролю знань за різними шкалами з начальної дисципліни

За 100-бальною шкалою, що використовується в НУЦЗ України	За рейтинговою шкалою (ЄКТС)	За 4-бальною шкалою
90–100	A	відмінно
80–89	B	добре
65–79	C	
55–64	D	задовільно
50–54	E	

35–49	FX	незадовільно
0–34	F	

Питання для підготовки до модульного контролю, заліку.

1.Критерій, за яким визначається ступінь загрози вчинення терористичного акту щодо об'єкта критичної інфраструктури та можливі негативні наслідки від терористичного акту?

2. Документ, що визначає мету, основні принципи і механізми забезпечення здатності держави і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики національній безпеці, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після виникнення загроз або настання надзвичайних та кризових ситуацій усіх видів, включаючи загрози гібридного типу ?

3. Комплекс цілеспрямованих дій, методів та механізмів взаємодії органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, інститутів громадянського суспільства, які гарантують збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після настання кризової ситуації?

4. Здатність системи пристосовуватися до кризових умов і нових обставин, які виникли під впливом загрози або кризової ситуації, забезпечувати виживання, а також застосовувати інноваційні рішення?

5. Оцінка ризику виникнення на промислових об'єктах надзвичайних ситуацій з урахуванням визначення джерел загроз, умов розвитку і можливих наслідків надзвичайних ситуацій це:

6. Яким шляхом здійснюється взаємодія між державними системами захисту у разі загрози виникнення або виникнення протиправних дій, диверсій, надзвичайних ситуацій на інфраструктурних об’єктах?

7. Які об’єкти мають загальнодержавне значення, розгалужені зв’язки та значний вплив на іншу інфраструктуру?

8. Об’єкти, порушення функціонування яких призведе до кризової ситуації регіонального значення, це

9. На якому рівні забезпечується розроблення та здійснення інженерно-технічних заходів цивільного захисту під час будівництва та експлуатації об’єктів критичної інфраструктури із забезпеченням їх стійкого функціонування у різних режимах?

10. На якому рівні забезпечується розроблення та передбачення здійснення інженерно-технічних заходів цивільного захисту у містобудівній документації стосовно розміщення, проектування та експлуатації об’єктів критичної інфраструктури?

«Теоретико-методологічні та історичні засади публічного управління». Запитання тесту корегуються з питаннями, що були розглянуті під час лекційних та практичних занять та віднесених до самостійного вивчення. Модульна контрольна робота 1 полягає у заповненні тесту в Google-формі.

Приклад типових тестових завдань, які входять до модульної контрольної роботи 1:З якими системами захисту у сфері національної безпеки взаємодіє національна система захисту критичної інфраструктури:з єдиною державною системою цивільного захисту;із системою захисту персональних данихз правоохоронними органами у сфері протидії злочинності, а також з контррозвідувальними та розвідувальними органами у сфері забезпечення державної безпеки;з системою стратегічної екологічної оцінки ризиків

Які суб’єкти спільно з операторами критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури:секторальні органи у сфері захисту критичної інфраструктури місцеві органи виконавчої влади та військово-цивільні адміністрації функціональні органи у сфері захисту критичної інфраструктури уповноважений орган у сфері захисту критичної інфраструктури України У якому режимі національної системи захисту критичної інфраструктури здійснюється функціонування інфраструктури з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи:штатний режим режим готовності та запобігання реалізації загрозрежим реагування на виникнення кризової ситуаціїрежим відновлення штатного функціонування

1.На якому рівні забезпечується збір, аналіз та узагальнення даних щодо об’єктів критичної інфраструктури, постійний моніторинг стану безпеки об’єктів критичної інфраструктури?

2. На якому рівні забезпечується організація взаємодії суб’єктів державної системи захисту критичної інфраструктури, створення мережі ситуаційних центрів?

3. Державна система захисту критичної інфраструктури забезпечує ефективне функціонування критичної інфраструктури в таких режимах:

4. У якому режим функціонування Державної системи захисту критичної інфраструктури здійснюється проведення оцінки можливих загроз та аналіз

5. Сукупність об’єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв, це:

6. До об’єктів виробничо-економічної інфраструктури належать:

7. Сукупність взаємозалежних і взаємодіючих елементів, що створюють комплекс матеріального виробництва, життєдіяльності населення регіону або розв’язання нагальних потреб суспільства це:

8. Об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам, це:

9. На період дії воєнного стану уповноваженим органом у сфері захисту критичної інфраструктури в Україні є:

10. На якому рівні управління ДСЗКІ розробляються програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій?

«Теоретико-методологічні та історичні засади публічного управління». Запитання тесту корегуються з питаннями, що були розглянуті під час лекційних та практичних занять та віднесених до самостійного вивчення. Модульна контрольна робота 1 полягає у заповненні тесту в Google-формі.

Приклад типових тестових завдань, які входять до модульної контрольної роботи 1:З якими системами захисту у сфері національної безпеки взаємодіє національна система захисту критичної інфраструктури:з єдиною державною системою цивільного захисту;із системою захисту персональних данихз правоохоронними органами у сфері протидії злочинності, а також з контррозвідувальними та розвідувальними органами у сфері забезпечення державної безпеки;з системою стратегічної екологічної оцінки ризиків

Які суб’єкти спільно з операторами критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури:секторальні органи у сфері захисту критичної інфраструктури місцеві органи виконавчої влади та військово-цивільні адміністрації функціональні органи у сфері захисту критичної інфраструктури уповноважений орган у сфері захисту критичної інфраструктури України У якому режимі національної системи захисту критичної інфраструктури здійснюється функціонування інфраструктури з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи:штатний режим режим готовності та запобігання реалізації загрозрежим реагування на виникнення кризової ситуаціїрежим відновлення штатного функціонування

Модульна контрольна робота складається з 25 тестових завдань, що охоплюють усі теми семестрового модулю «Прикладний та науковий виміри публічного управління в Україні в умовах системних змін». Запитання тесту корегуються з питаннями, що були розглянуті під час лекційних та практичних занять та віднесених до самостійного вивчення. Модульна контрольна робота полягає у заповненні тесту в Google-формі.

8. Засоби провадження освітньої діяльності

Дисципліна викладається дистанційно при використанні імплементованих нормативних документів Євросоюзу, гармонізованих із сучасними нормативними документами

України та із застосуванням програмного комплексу ANSYS WB TRAINING VERSION. А також дистанційно.

9. Рекомендовані джерела інформації

Література

Базова

1. Азаров С. І., Сидоренко В. Л., Єременко С. А., Пруський А. В., Демків А. М. Захист критичної інфраструктури в умовах надзвичайних ситуацій: монографія; за заг. ред. П. Б. Волянського. Київ, 2021. 375 с.
2. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. за заг. ред. О. М. Суходолі. К.: НІСД, 2019. 224 с.
3. Богдан Б. В. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні. Проблеми сучасних трансформацій. Серія : право, публічне управління та адміністрування. 2022. № 6. URL: https://doi.org/10.54929/2786-5746-2022-6-01-09
4. Богуцький П. П. Концептуальні засади права національної безпеки України: монографія. Київ – Одеса: Фенікс, 2020. 376 с.
5. Бойко О.В., Пушак Я.Я., Трушкіна Н.В. Формування сучасної парадигми інформаційної безпеки національної економіки: теоретичні засади. Вісник післядипломної освіти. Сер.: Соціальні та поведінкові науки. 2022. Вип. 22 (51). С. 139-160. URL: https://doi.org/10.32405/2522-9931-2022-22(51)-139-160.
6. Братель, С. Досвід зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури. Південноукраїнський правничий часопис. № 3. 2023. С. 261 265. https://dspace.oduvs.edu.ua/handle/123456789/6423
7. Глушко А.Д. Оптимізація заборгованості підприємства критичної інфраструктури в аспекті зміцнення фінансово-економічної безпеки. Вісник Хмельницького національного університету. 2023. № 1 (314). С. 47-54. DOI: https://doi.org/10.31891/2307-5740-2023-314-1-6
8. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналітична доповідь За ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с. URL: https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-...
9. Дикий А. П. Симптоми проблеми гарантування економічної безпеки держави в контексті запобігання та протидії економічній злочинності. Бізнес Інформ. 2022. № 12.- С. 6-16. URL: http://nbuv.gov.ua/UJRN/binf_2022_12_2
10. Домарацький М. Б. Забезпечення безпеки та підвищення ефективності захисту критично важливих об'єктів на державному рівні. Публічне управління і адміністрування в Україні. 2019. Вип. 14. С. 82–85.
11. Домарацький М. Б. Методика державного категорування критично важливих об’єктів / М. Б. Домарацький. Держава та регіони. 2019. № 4(68). С. 278 – 281.
12. Домарацький М. Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка. Вісник Національного університету цивільного захисту України. 2020. Вип. 1(12). С. 470–475.
13. Домарацький М. Б. Особливості категоріювання об’єктів критичної інформаційної інфраструктури. Фінансова система та економічна безпека: стан, проблеми, ефективність: збірник тез наукових робіт учасників міжнародної науково-практичної конференції для студентів, аспірантів та молодих учених. -К.: Аналітичний центр «Нова Економіка», 2019. Ч. 2. – С. 91–92.
14. Домарацький М. Б. Особливості формування та функціонування державної системи моніторингу стану об’єктів критичної інфраструктури. Право та державне управління. 2019. № 4. С. 170– 174.
15. Домбровська С., Помаза-Пономаренко А., Порока С., Урбанек А. Безпекова політика України в умовах євроінтеграції : монографія. Харків: НУЦЗУ, 2023. 252 с.

16. Єремчук О. Паспорт безпеки об’єкта критичної інфраструктури як обов’язковий елемент системи захисту критичної інфраструктури. In: Jurnalul juridic national: teorie şi practică, 2019, nr. 3(37), pp. 53-58. ISSN 2345-1130.

17. Захист критичної інфраструктури в умовах надзвичайних ситуацій / за заг. ред. П. Б. Волянського. Київ : НІСД, 2021. 375 с.Зубко Г. Ю. Система суб’єктів реалізації державної інфраструктурної політики України. Правові новели. 2020. № 11. С. 166–178. URL:http://legalnovels.in.ua/journal/11_2020/11_2020.pdf

18. Кваша Т. К. Світові наукові та технологічні тренди у сфер і забезпечення національної безпеки / Т. К. Кваш а. Київ: УкрІН ТЕІ, 2019 . 107 с.

19. Коцюруба В. І., Білик А. С., Веретнов А. О. та ін. Методика розрахунків та обґрунтування вимог до інженерного захисту об’єктів критичної інфраструктури від БпЛА типу баражуючий боєприпас. Опір матеріалів і теорія споруд. 2022. № 109. С. 164-183.

20. Кудінов С. С. Міжнародний досвід протидії тероризму та його значення для України. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Юридичні науки. 2019. Т. 30(69), № 1. С. 117-123. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2019_30%2869%29_1_22

21. Курсеітов Т.Л., Мурасов Р.К., Мельник Я.В Імовірнісний метод прогнозування надзвичайних подій на потенційно-небезпечних об’єктах критичної інфраструктури.https://doi.org/10.33099/2311-7249/2022-44-2-60-63.–122.

22. Кучерина С. Є., Олєйніков Д. О. Сучасний стан кримінально-правової охорони об’єктів критичної інфраструктури. Інформація і право. 2021. №1(36) . С. 90 – 98

23. Кучерина С.Є., Павлов Д.М., Євтушенко І.В. Напрями підвищення ефективності організаційно-правового забезпечення захисту критичної інфраструктури. Честь і Закон. 2022. №80, т.1. С.51-57.

24. Музиченко М. В. Стратегічна роль розвитку газотранспортної інфраструктури у забезпеченні енергетичної безпеки ЄС. Вісник Маріупольського державного університету. Серія : Економіка. 2020. Вип. 19. С. 84-92. URL: http://nbuv.gov.ua/UJRN/Vmdu_ek_2020_19_11

25. Онишко С. В. Становлення та рівень розвитку інституційної інфраструктури фінансової безпеки України. Молодий вчений. 2022. № 9. С. 144-149. URL: http://nbuv.gov.ua/UJRN/molv_2022_9_33

26. Підюков П.П., Калиновський О.В. Система державного захисту критичної інфраструктури України: генеза, сучасний стан і перспективи оптимізування в умовах подальшого забезпечення національної безпеки країни. Часопис Київського університету права, № 2020/4, С. 355-359. DOI: 10.36695/2219-5521.4.2020.63.

27. Сокіран М. В., Система принципів адміністративно-правового забезпечення стійкості критичної інформаційної інфраструктури України. Наукові записки. Серія: Право. 2020. Випуск 8. Спецвипуск С.73-77. URL: https://cusu.edu.ua/images/nauk_zapiski/pravo/8_spec_2020/73-77.pdf

28. Стратегічні орієнтири розвитку партнерства держави, бізнесу та науки в контексті повоєнного відновлення України: моногр. /за ред. д.е.н., проф., академіка НАПН України І. М. Грищенка, д.е.н., проф. А. О. Касич, д.е.н., проф. І. О. Тарасенко. Київ: КНУТД, 2023. 267 с.

29. Страхніцький Я. О. Структурно-функціональна характеристика державної політики у сфері захисту критичної інфраструктури в Україні. Публічне управління та митне адміністрування. № 4 (35), 2022 С.112-117 URL: http://212.1.86.13/jspui/bitstream/123456789/5360/1/17.pdf

30. Суходоля О.М. Проблеми захисту енергетичної інфраструктури в умовах гібридної війни: аналіт. зап. URL: http://www.niss.gov.ua/articles/1891.

31. Тарасенко Ю. С. Ризик-орієнтовані процеси забезпечення безпеки об’єктів критичної інфраструктури. Системи та технології. № 1 (65), 2023. С. 67-76.

32. Управління соціально-економічними системами на основі підвищення ефективності маркетингових послуг в умовах діджиталізації: колективна монографія / за ред. д.е.н., проф. В. І. Чобіток; Українська інженерно-педагогічна академія. Харків: Видавництво Іванченка І. С., 2023. 363 с.

33. Шевченко А. М. Комплексна модель системних досліджень проблем безпеки об`єктів критичної інфраструктури. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2022. № 77. С. 145-160. URL: http://nbuv.gov.ua/UJRN/Znpviknu_2022_77_15

34. Яременко О. І., Страхніцький Я. О. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. Публічне управління та митне адміністрування. 2022. № 1 (32). С. 76-82.

35. Яременко О. І., Страхніцький, Я. О. Виявлення та управління загрозами в структурі державної політики захисту критичної інфраструктури. Університетські наукові записки. 2022. № 3. С. 73-82.

Допоміжна

1.Закон України «Про критичну інфраструктуру»;

2. Закон України «Про національну безпеку України».

3. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України»;

4. Постанова Кабінету Міністрів України від 13 липня 2022 року № 563 «Про затвердження Порядку ідентифікації об'єктів критичної інфраструктури»

5. ДБН В.2.5-76:2014 «Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення».

6. Постанова Кабінету Міністрів України від 30 вересня 2015 р. № 775 «Про затвердження Порядку створення та використання матеріальних резервів (крім державних) для запобігання виникненню надзвичайних ситуацій і ліквідації їх наслідків»;

7. ДБН В.2.5-74:2013 «Водопостачання. Зовнішні мережі та споруди. Основні положення проектування».

Електронний ресурс.

1.Офіційне інтернет-представництво Президента України http://www.president.gov.ua/.

2. Верховна Рада України http://www.rada.kiev.ua .

3. Кабінет Міністрів України http://www.kmu.gov.ua/.

4. Міністерство освіти і науки, молоді та спорту України http://www.mon.gov.ua, www.osvita.com.

5. Міністерство екології та природних ресурсів України http://www.menr.gov.ua/.

6. Міністерство України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи http://www.mns.gov.ua/.

7. Рада національної безпеки і оборони України http://www.rainbow.gov.ua/.

8. Постійне представництво України при ООН http://www.uamission.org/.

9. Український інститут досліджень навколишнього середовища і ресурсів при Раді національної безпеки і оборони України http://www.erriu.ukrtel.net/index.htm.

10. http://www.dnop.kiev.ua - Офіційний сайт Державного комітету України з промислової безпеки охорони праці та гірничого нагляду (Держгірпромнагляду).

Розробник:
старший викладач кафедри
державного нагляду у сфері пожежної
та техногенної безпеки Ірина РУДЕШКО