ПрАТ "ВНЗ "МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ"

Інститут безпеки

МАУП

Кафедра національної безпеки

Затверджую:
Директор Інституту безпеки
_____
Сергій ЛИСЕНКО
"08" серпня 2025 р.

Схвалено на засіданні кафедри
Національної безпеки
Протокол № 1 від 08 08 2025 р.
Заст. зав. кафедри
_____
Іван СЕРВЕЦЬКИЙ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«БЕЗПЕКА КРИТИЧНОЇ ТА ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ»

Спеціальності: **К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)**

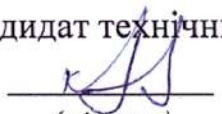
Освітнього рівня: **перший (бакалаврський) рівень**

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

Київ МАУП 2025

Розробник силабусу навчальної дисципліни:

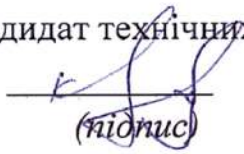
Юрченко Костянтин Миколайович - кандидат технічних наук



(підпис)

Викладач:

Юрченко Костянтин Миколайович - кандидат технічних наук



(підпис)

Силабус розглянуто на засіданні кафедри національної безпеки
Протокол № 1 від «04» серпня 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 кредитів/150 год** Лекції : **24** Семінарські заняття:**36** Самостійна робота студентів: **90**
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.

Юрченко Костянтин Миколайович	
Науковий ступінь	Кандидат технічних наук
Вчене звання	Доцент
Посада	Доцент кафедри інформаційної та фінансової безпеки
Дисципліни, які викладає НПП	Безпека критичної та енергетичної інфраструктури
Напрями наукових досліджень	Цивільна безпека
Посилання на реєстри ідентифікаторів для науковців	ORCID: https://orcid.org/0000-0003-2054-4307 Google Scholar: https://scholar.google.com.ua/citations?user=ECeGQGUAAAAJ&hl=uk
Контактна інформація викладача:	
E-mail:	victor.rovnuy.ta@gmail.com
Контактний тел.	+380507417375
Телефон кафедри	
Портфоліо викладача на сайті кафедри/Інституту/Академії	https://maup.com.ua/ua/pro-akademiyu/instituti/institut-bezpeki-prat-vnz-maup/yurchenko.html

Анотація курсу. Курс «Безпека критичної та енергетичної інфраструктури» спрямований на формування у здобувачів вищої освіти системного уявлення про сутність завдання та принципи захисту критичної інфраструктури зокрема енергетичної її роль у забезпеченні національної безпеки та стабільності держави У межах дисципліни розглядаються організаційно правові та методологічні засади функціонування критичної інфраструктури класифікація об'єктів і загроз механізми управління ризиками а також питання взаємодії державних органів операторів критичної інфраструктури та міжнародних партнерів Особлива увага приділяється проблемам захисту енергетичного сектору від фізичних кібер та гібридних загроз забезпеченню його стійкості в умовах криз і воєнних дій а також впровадженню міжнародних стандартів і практик у сфері критичної інфраструктури

Предмет вивчення дисципліни є закономірності організації функціонування та розвитку системи безпеки критичної та енергетичної інфраструктури її інституційно правове організаційне й технічне забезпечення методи оцінювання та управління ризиками механізми забезпечення стійкості та відновлення у разі кризових подій

Метою курсу «Безпека критичної та енергетичної інфраструктури» є формування у здобувачів вищої освіти базових знань про сутність принципи та напрями захисту критичної інфраструктури розвиток умінь аналізувати сучасні загрози і ризики оцінювати вразливості енергетичних систем а також набуття навичок планування і реалізації заходів із забезпечення стійкості й безпеки

Завдання навчальної дисципліни «Безпека критичної та енергетичної інфраструктури» полягають у тому щоб ознайомити студентів із законодавчою базою та міжнародними стандартами захисту критичної інфраструктури сформувати розуміння її ролі в системі національної безпеки розвинути вміння ідентифікувати й класифікувати ризики навчити застосовувати управлінські та технічні механізми захисту об'єктів розвинути здатність оцінювати ефективність заходів безпеки та застосовувати отримані знання у практичній діяльності підготувати основу для засвоєння спеціалізованих дисциплін у сфері кіберзахисту енергетики й управління ризиками

Пререквізити навчальної дисципліни. Вивчення навчальної дисципліни «Безпека критичної та енергетичної інфраструктури не пов'язане з іншими дисциплінами.

Постреквізити навчальної дисципліни. Знання та уміння, отримані студентами в процесі вивчення навчальної дисципліни «Безпека критичної та енергетичної інфраструктури, сприяють успішному вивченню здобувачами вищої освіти цілої низки інших навчальних дисциплін, спрямованих на формування професійних знань і умінь.

Програмні компетентності

Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані та професійні завдання та вирішувати практичні проблеми в галузі національної безпеки, що передбачає здійснення кваліфікованого аналізу, пояснення та прогнозування безпекових явищ і характеризується комплексністю та невизначеністю умов.
Загальні компетентності (ЗК)	ЗК3. Знання та розуміння предметної області та розуміння професії. ЗК7. Здатність застосовувати знання у практичних ситуаціях, постійно самовдосконалюватися, здобувати нові фахові знання з використанням різних джерел інформації
Спеціальні (фахові) компетентності (СК)	СК1. Здатність критично та на межі предметних галузей осмислювати понятійно-категоріальний апарат загальної теорії національної безпеки. СК2. Здатність аналізувати основні напрями забезпечення національної безпеки в державі. СК6. Здатність до активної діяльності в умовах протиборства в окремих сферах забезпечення національної безпеки і видах діяльності.

	СК8. Здатність визначати основні положення щодо методів та заходів забезпечення безпеки держави у різноманітних сферах життєдіяльності.
Програмні результати навчання (ПРН)	ПРН9. Характеризувати систему забезпечення національної безпеки, включаючи повноваження і функції суб'єктів забезпечення національної безпеки, контроль за здійсненням заходів забезпечення національної безпеки, основні завдання суб'єктів забезпечення національної безпеки, а також недержавній системі забезпечення національної безпеки. ПРН14. Характеризувати систему забезпечення безпеки за окремою сферою забезпечення національної безпеки і видом діяльності, включаючи повноваження і функції суб'єктів забезпечення безпеки, контроль за здійсненням заходів забезпечення безпеки, основні завдання суб'єктів національної системи забезпечення безпеки України за окремою сферою забезпечення національної безпеки і видом діяльності.

Зміст навчальної дисципліни

№	Назва теми	К-сть годин, з них:			
		Лекції	**Семінарські зан.**	**Самостійна робота**	**Методи навчання/методи оцінювання**
1 семестр **Модуль 1. Теоретико методологічні засади безпеки критичної інфраструктури**					**Методи навчання:** словесні (навчальна лекція; бесіда; навчальна дискусія); індуктивний метод; дедуктивний метод; традуктивний метод; аналітичний; синтетичний; практичний (робота з фабулами юридичних справ); пояснювально-ілюстративний; репродуктивний; метод проблемного викладу; частково-пошуковий; дослідницький; інтерактивні методи (аналіз ситуацій; дискусії, дебати, полеміки; діалог, синтез думок; мозковий штурм; відпрацювання навичок; ситуативне моделювання, опрацювання дискусійних питань); моделювання професійної діяльності; інноваційні методи навчання (компетентнісний; проєктно-дослідницький); кейс-метод.
Тема 1.	Поняття та структура критичної інфраструктури	1	1	3	
Тема 2.	Роль критичної інфраструктури в системі національної безпеки	1	1	3	
Тема 3.	Принципи та завдання забезпечення безпеки критичної інфраструктури	1	1	3	
Тема 4.	Класифікація загроз та ризиків для критичної інфраструктури	1	1	3	
Тема 5.	Методологічні підходи до управління ризиками та стійкістю систем	1	1	3	
Модуль 2. Нормативно правові та інституційні основи безпеки критичної інфраструктури					
Тема 6.	Законодавство України у сфері критичної та енергетичної інфраструктури	1	1	3	
Тема 7.	Міжнародні стандарти та практика ЄС і НАТО у сфері захисту критичної інфраструктури	1	1	3	

Тема 8.	Суб'єкти системи захисту критичної інфраструктури їхні функції та повноваження	1	0	3	**Методи оцінювання:** усний контроль (усне опитування, оцінювання участі у дискусіях, інших інтерактивних методах навчання); письмовий контроль (контрольні, самостійні роботи, реферати); тестовий контроль (тести закритої форми: тест-альтернатива, тест-відповідність); метод самоконтролю та самооцінки; оцінювання кейс-завдань.
Тема 9.	Політика державного управління у сфері енергетичної безпеки	1	1	4	
Тема 10.	Взаємодія держави бізнесу та громадянського суспільства у сфері захисту критичної інфраструктури	1	1	4	
Модуль 3. Загрози безпеці критичної та енергетичної інфраструктури					
Тема 11.	Фізичні загрози та захист об'єктів критичної інфраструктури	1	1	4	
Тема 12.	Кіберзагрози та їх вплив на енергетичну інфраструктуру	1	1	4	
Тема 13.	Терористичні та гібридні загрози для енергетичної системи	1	0	4	
Тема 14.	Вплив воєнних дій на безпеку критичної інфраструктури	1	1	4	
Тема 15.	Екологічні та техногенні ризики для об'єктів критичної інфраструктури	1	1	4	
Модуль 4. Стратегії та перспективи забезпечення безпеки критичної та енергетичної інфраструктури					
Тема 16.	Державна стратегія захисту критичної інфраструктури	1	1	4	
Тема 17.	Планування безперервності та стійкості функціонування енергетичних об'єктів	2	1	4	
Тема 18.	Системи моніторингу прогнозування та реагування на загрози	2	1	6	
Тема 19.	Інноваційні технології та цифрові рішення у сфері енергетичної безпеки	2	1	6	
Тема 20.	Перспективи розвитку безпеки критичної інфраструктури в умовах глобалізації та євроінтеграції	2	1	6	
Модульна контрольна робота					
Всього:		**24**	**18**	**78**	
Форма контролю: екзамен					

Зміст самостійної роботи здобувача освіти з навчальної дисципліни «Безпека критичної та енергетичної інфраструктури передбачає підготовку до аудиторних занять шляхом

опанування матеріалів лекції, вивчення базової і додаткової літератури, періодичних видань, Інтернет-джерел та судової практики, виконання практичних завдань (написання рефератів, аналіз проблемних ситуацій, підготовка результатів власних досліджень до виступу на конференціях, участь в конкурсах наукових робіт, підготовці та публікації наукових статей, тез тощо) протягом семестру; самостійне опрацювання окремих тем навчальної дисципліни; підготовку доповідей та презентацій за тематикою практичних занять; переклад іноземних текстів установлених обсягів; виконання індивідуальних завдань; підготовку до усіх видів контролю, у тому числі модульних контрольних робіт і підсумкової атестації; підготовку юридичних документів, інші види діяльності, що використовуються в Академії, Інституті і кафедрі.

Зміст самостійної роботи здобувача освіти визначається робочою програмою навчальної дисципліни конкретної навчальної дисципліни, методичними рекомендаціями для завданнями та рекомендаціями викладача.

Технічне обладнання та/або програмне забезпечення. В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проектор та комп'ютер для проведення лекційних та семінарських занять з елементам презентації. Вивчення окремих тем і виконання практичних завдань потребує доступу до інформації зі всесвітньої мережі Інтернет, який забезпечується безкоштовною мережею Wi-Fi.

Форми методи контролю.

Контроль успішності здобувачів освіти поділяється на поточний і підсумковий (семестровий).

Поточний контроль здійснюють під час проведення практичних, лабораторних і семінарських занять, метою якого є систематична перевірка розуміння та засвоєння теоретичного навчального матеріалу, уміння використовувати теоретичні знання під час виконання практичних завдань тощо. Можливості поточного контролю є надзвичайно широкими: мотивація навчання, стимулювання навчально-пізнавальної діяльності, диференційований підхід до навчання, індивідуалізація навчання тощо.

Форми участі студентів у навчальному процесі, які підлягають поточному контролю:

-виступ з основного питання;

-усна доповідь;

- доповнення, запитання до того, хто відповідає;

- систематичність роботи на семінарських заняттях, активність під час обговорення питань;

- участь у дискусіях, інтерактивних формах організації заняття;

- аналіз законодавства та монографічної літератури;

- письмові завдання (тестові, контрольні, творчі роботи, реферати тощо);

- підготовка тез, конспектів навчальних або наукових текстів;

- самостійне опрацювання тем;

Контроль успішності здобувачів освіти поділяється на поточний і підсумковий .

Методи поточного контролю: усний контроль (опитування, бесіда, доповідь, повідомлення тощо); письмовий контроль (контрольна робота, реферат, виклад матеріалу на задану тему в письмовій формі тощо); комбінований контроль; презентація самостійної роботи; спостереження як метод контролю; тестовий контроль; проблемні ситуації.

Система оцінювання та вимоги.

Таблиця розподілу балів, які отримують здобувачі вищої освіти*

1-й семестр

	Поточний контроль знань										Модульна контрольна робота	екзамен **	Загальна кількість балів
Теми	Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Тема 7	Тема 8	Тема 9	Тема 10			
Робота на семінарському занятті	10		10		5	10		5	10		20	20**	100
Самостійна робота	3	3	3	3	3	3	3	3	3	3			

*Таблиця містити інформацію про максимальні бали за кожен вид навчальної роботи здобувача вищої освіти.

Під час оцінювання засвоєння кожної теми за поточну навчальну діяльність здобувачу освіти виставляють оцінки з урахуванням затверджених критеріїв оцінювання для відповідної дисципліни.

Критерії оцінювання результатів навчання здобувачів освіти та розподіл балів, які вони отримують, регламентуються Положенням про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП».

Модульний контроль. Модульна контрольна робота з навчальної дисципліни «Безпека критичної та енергетичної інфраструктури» проводиться на останньому занятті модуля у письмовій формі, у вигляді тестування, а саме, тести закритої форми: тест-альтернатива, тест-відповідність на основі аналізу фабул юридичних справ.

Критерії оцінювання модульної контрольної роботи з навчальної дисципліни «Безпека критичної та енергетичної інфраструктури»:

при оцінюванні модульної контрольної роботи враховується обсяг і правильність виконаних завдань:

- оцінка «відмінно» (A) ставиться за правильне виконання всіх завдань (або більше 90% усіх завдань);

- оцінка «добре» (B) ставиться за виконання 80% усіх завдань;

- оцінка «добре» (C) ставиться за виконання 70% усіх завдань;

- оцінка «задовільно» (D) ставиться, якщо правильно виконано 60% запропонованих завдань;

- оцінка «задовільно» (E) ставиться, якщо правильно виконано більше 50% запропонованих завдань;

- оцінка «незадовільно» (FX) ставиться, якщо завдань виконано менше від 50 %.

Неявка на модульну контрольну роботу – 0 балів.

Вище наведені оцінки трансформуються в рейтингові бали у такий спосіб:

«A» – 18-20 балів;

«B» – 16-17 балів;

«C» – 14-15 балів;

«D» – 12-13 балів.

«E» – 10-11 балів;

«FX» – менше 10 балів.

Підсумковий семестровий контроль з навчальної дисципліни «Безпека критичної та енергетичної інфраструктури є обов'язковою формою оцінювання результатів навчання здобувача вищої освіти. Він проводиться в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеного програмою навчальної дисципліни.

Підсумковий контроль проводиться у формі **екзамену** (письмово). Студента допускають до семестрового контролю за умови виконання ним усіх видів робіт.

Семестровий контроль у формі екзамену передбачає, що підсумкова оцінка з дисципліни визначається як сума (проста або зважена) балів за змістовими модулями. екзамен виставляється за результатами роботи здобувача освіти впродовж усього семестру. Рейтингова оцінка здобувача освіти складається з балів, отриманих здобувачем за результатами заходів поточного контролю, заохочувальних балів.

Здобувачі освіти, які виконали всі умови допуску до екзамену та мають рейтингову оцінку 60 і більше балів, отримують відповідну до набраного рейтингу оцінку без додаткових випробувань.

******Зі здобувачами, які виконали всі умови допуску до екзамену та мають рейтингову оцінку менше 60 балів, а також з тими здобувачами, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі викладач проводить підсумковий семестровий контроль у вигляді екзамену.

Оцінювання додаткових (індивідуальних) видів навчальної діяльності. 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 екзаменово-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.

Підсумкова кількість балів, набрана здобувачами освіти за виконання завдань з самостійної роботи, є однією з складових поточної успішності з навчальної дисципліни. Самостійна робота з кожної теми за робочою програмою навчальної дисципліни оцінюється в

діапазоні від 0 до 3 балів з використанням стандартизованих узагальнених критеріїв оцінювання знань.

Шкала оцінювання виконання самостійної роботи (індивідуальних завдань)

Можлива максимальна оцінка виконання самостійної роботи (індивідуальних завдань)	Рівень виконання			
	Відмінний	Добрий	Задовільний	Незадовільний
3	3	2	1	0

Для оцінювання результатів навчання здобувача вищої освіти впродовж семестру застосовується 100-бальна, національна та шкала ЄКТС оцінювання

Шкала підсумкового оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECT8	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для екзамену
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

Політика курсу.

Для успішного засвоєння курсу «Безпека критичної та енергетичної інфраструктури» здобувач освіти має:

- регулярно відвідувати лекційні та практичні заняття;
- систематично, системно й активно працювати на лекційних і практичних заняттях;
- відпрацьовувати пропущені заняття або незадовільні оцінки, отримані на заняттях;
- виконувати у повному обсязі завдання, які вимагає підготувати викладач, належна їх якість;
- виконувати контрольні та інші самостійні роботи;
- дотримуватися норм академічної поведінки та етики.

Курс «Безпека критичної та енергетичної інфраструктури» передбачає засвоєння та дотримання принципів етики та академічної доброчесності, 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 заняттях, виконання завдань для самостійної роботи, а також виконання завдань, які здатні розвинути практичні уміння та навички за які можуть бути, за рішенням викладача, нараховані додаткові (бонусні) бали (участь у круглих столах, наукових конференціях, олімпіадах та наукових конкурсах серед студентів).

Рекомендовані джерела

Основна література

1. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. – Соціально-правові студії, 2021, № 3 (13), с. 142–148.

2. Гора І. В., Батюк О. В. Окремі питання захисту об’єктів критичної інфраструктури: зарубіжний досвід. – Соціально-правові студії, 2021, № 1 (11), с. 132–139.

3. Бірюков Д. С., Кондратов С. І. Стратегія захисту критичної інфраструктури в системі національної безпеки держави. – Стратегічні пріоритети, 2012, вип. 3, с. 107–113.

4. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: монографія. – Дніпро: ДДУВС, 2018, 180 с.

5. Суходоля О. М., Бірюков Д. С., Кондратов С. І. (упор.) Зелена книга з питань захисту критичної інфраструктури в Україні: зб. міжнар. експерт. нарад. – Київ: НІСД, 2016, 176 с.

6. Каніщев Г., Тур І. Критична інфраструктура тимчасово окупованих територій України в українському законодавстві. – Соціально-правові студії, 2024, с. 18–25.

7. Уряднікова І. В., Заплатинський В. М. Наукові підходи до визначення терміну «критична інфраструктура». – Вісті Донецького гірничого інституту, 2020, № 2 (47), с. 184–193.

8. Теленик С. С. Критична інфраструктура як об’єкт адміністративно-правового регулювання. – Юридичний часопис Нац. академії внутрішніх справ, 2018, № 1 (15).

9. Батюк О. В. Криміналістичне забезпечення протидії злочинам на об’єктах критичної інфраструктури: монографія. – Луцьк: Волиньполіграф, 2021, 455 с.

10. Герасименко О. М. Загрози об’єктам критичної інфраструктури України в умовах воєнного стану. – Науковий вісник УжНУ. Серія «Право», 2024, № 84 (3).

11. Іваницька О., Возненко О. Управління ризиками об’єктів критичної інфраструктури. – Фінанси України, 2024, № 6, с. 93–107.

12. Плахотнюк Р. В. Забезпечення стійкості критичної інфраструктури в Україні в умовах сучасних викликів. – Economic-prostir, 2025, с. 47–54.

13. Мельник Д. С. Створення моделі загроз національній критичній інфраструктурі України як основи забезпечення її безпеки та стійкості. – Вісник ХНУВС, 2024, № 104 (1(1)), с. 237–250.

14. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. – Державне управління: удосконалення та розвиток, 2022, № 1.

15. Тарасенко Ю. С., Клим В. Ю. Безпека об’єктів критичної інфраструктури з позицій зниження ризиків. – Системні технології, 2022, № 4 (141).

16. Братель С. Г. Досвід зарубіжних країн у сфері забезпечення безпеки об’єктів критичної інфраструктури. – Південноукраїнський правничий часопис, 2023, № 3, с. 261–265.

17. Арсенович Л. А. Система управління інформаційною безпекою як інструмент підвищення захисту об’єктів критичної інфраструктури. – Міжнародний науковий журнал інженерії та сільського господарства, 2023, № 2 (6), с. 12–22.

18. Азаренко О. та ін. Шляхи підвищення ефективності системи фізичного захисту об’єктів критичної інфраструктури держави. – Соціальний розвиток і безпека, 2021, № 11, с. 200–213.

19. Коціюруба В. І., Білик А. С. Захист об’єктів критичної інфраструктури України від прямих влучань ракет за допомогою підземного розташування. – Ядерна та радіаційна безпека, 2023, № 2 (98), с. 69–79.

20. Volkov A. та ін. The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. – Machinery & Energetics, 2023, 14(4), s. 23–32.