

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**

ЗАТВЕРДЖУЮ

Директор ННІ

_____ Віктор КАПЛУН

" ____ " _____ 2026 р.

СХВАЛЕНО

на засіданні кафедри

Інженерії енергосистем

Протокол № ____ від " ____ " _____ 2026 р.

Завідувач кафедри

_____ Євген АНТИПОВ

РОЗГЛЯНУТО

Гарант ОП «Цифрова інженерія та автоматизація електроенергетичних систем (Digital engineering and automation of electric power systems)»

_____ Павленко Володимир Миколайович

**РОБОЧА ПРОГРАМА
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

ЕНЕРГЕТИЧНА БЕЗПЕКА

Галузь знань G Інженерія, виробництво та будівництво

Спеціальність G3 Електрична інженерія

Освітня програма Цифрова інженерія та автоматизація електроенергетичних систем (Digital engineering and automation of electric power systems)

ННІ енергетики, автоматики і енергозбереження

Розробник: Макаревич С.С., к.т.н., доцент, доцент кафедри Інженерії енергосистем

Київ - 2026 р.

Опис навчальної дисципліни

Дисципліна «Енергетична безпека» є обов'язковим компонентом освітньої програми «Цифрова інженерія та автоматизація електроенергетичних систем» для студентів магістерського рівня спеціальності G3 Електрична інженерія, яка спрямована на формування системного розуміння сучасних викликів та ризиків у галузі енергетичної безпеки. В рамках курсу вивчаються основи енергетичної безпеки, її концептуальні засади, сучасні виклики та загрози, а також засоби їх аналізу та управління, включаючи питання кібербезпеки, ризик-менеджменту та забезпечення стабільності електроенергетичних систем. Особлива увага приділяється розробці та впровадженню заходів із підвищення надійності, ефективності та безпеки електроенергетичних об'єктів і систем, а також оцінці ризиків у кризових ситуаціях і в умовах відновлення інфраструктури. Вивчення дисципліни має прикладну спрямованість і сприяє формуванню компетентностей, необхідних для забезпечення безпеки та стабільності сучасних електроенергетичних систем у контексті цифровізації та автоматизації.

Галузь знань, спеціальність, освітня програма, освітній ступінь

Освітній ступінь	Другого (магістерського) ОП
Галузь знань	G Інженерія, виробництво та будівництво
Спеціальність	G3 Електрична інженерія
Освітня програма	Цифрова інженерія та автоматизація електроенергетичних систем (Digital engineering and automation of electric power systems)
Факультет/ННІ	ННІ енергетики, автоматики і енергозбереження

Характеристика навчальної дисципліни

Вид	Обов'язкова
Загальна кількість годин	150
Кількість кредитів ECTS	5
Кількість змістових модулів	3
Курсовий проект (робота) (за наявності)	-
Форма контролю	Екзамен

Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти (повний термін навчання)

	Форма здобуття вищої освіти	
	денна	заочна
Курс (рік підготовки)	1	-
Семестр	1	-
Лекційні заняття	15 год.	-
Лабораторні роботи	-	-
Практичні, семінарські заняття	30 год.	-
Самостійна робота	105 год.	-
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	3 год.	-
Форма контролю	Екзамен	-

Мета, компетентності та програмні результати навчальної дисципліни

Мета: Мета дисципліни полягає у формуванні у студентів системних знань щодо сучасних підходів та технологій забезпечення енергетичної безпеки електроенергетичних систем, здобутті навичок аналізу ризиків і прийняття обґрунтованих управлінських рішень у сфері енергетичної безпеки з урахуванням сучасних викликів та загроз, а також ознайомленні з методами оцінки та підвищення надійності й безпеки електроенергетичної інфраструктури.

Перелік навчальних дисциплін, які передують вивченню «Енергетична безпека » (за їх наявності)

Набуття компетентностей

ЗК1 — Здатність до абстрактного мислення, аналізу та синтезу, пошуку і оброблення інформації з різних джерел.

ЗК2 — Здатність генерувати нові ідеї (креативність) та проводити наукові і прикладні дослідження на відповідному рівні.

ЗК6 — Здатність приймати обґрунтовані рішення, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності, у тому числі виявляти та оцінювати ризики в умовах невизначеності.

ЗК7 — Здатність діяти, неухильно дотримуючись цінностей, принципів і правил академічної доброчесності в освітньому процесі та науковій (творчій) діяльності.

СК2 — Здатність розробляти та впроваджувати заходи з підвищення надійності, ефективності та безпеки при проектуванні й експлуатації обладнання та об'єктів електроенергетичних систем (G3).

СК5 — Здатність забезпечувати інформаційну безпеку та оцінювати ризики електроенергетичної інфраструктури в умовах кризових ситуацій та повоєнного відновлення (G3 + G7).

Програмні результати навчання

ПРН6 — Здійснювати кіберзахист, забезпечувати інформаційну безпеку та оцінювати ризики критичної електроенергетичної інфраструктури для забезпечення енергостійкості в умовах кризових ситуацій та повоєнного відновлення (G3 + G7).

ПРН8 — Оцінювати показники надійності, електромагнітної сумісності та якості електричної енергії, розробляти заходи з підвищення безпеки експлуатації обладнання ЕЕС (G3).

Програма та структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин (денна форма)						Кількість годин (заочна форма)					
	л	лаб	сем	п	с.р.	усього	л	лаб	сем	п	с.р.	усього
Модуль 1. ЗМІСТОВИЙ МОДУЛЬ 1. Концептуальні основи енергетичної безпеки												
Тема 1. Енергетична безпека як складова національної безпеки. Критерії та індикатори енергетичної стійкості держави	2	-	-	4	14	20	-	-	-	-	-	-
Тема 2. Вразливість енергетичної інфраструктури. Фізичні, техногенні та кліматичні загрози. Резервування та диверсифікація джерел енергопостачання	2	-	-	6	9	17	-	-	-	-	-	-
Тема 3. Екологічна безпека експлуатації енергооб'єктів. Мінімізація впливу на довкілля	2	-	-	-	13	15	-	-	-	-	-	-
Разом за модулем 1	6	0	0	10	36	52	-	-	-	-	-	-
Модуль 2. ЗМІСТОВИЙ МОДУЛЬ 2. Кіберзахист промислових систем керування (OT/ICS)												
Тема 1. Специфіка кіберзагроз для електроенергетики. Вразливості протоколів АСУ ТП, SCADA-систем та пристроїв Інтернету Речей (IoT).	2	-	-	4	10	16	-	-	-	-	-	-

Назви змістових модулів і тем	Кількість годин (денна форма)						Кількість годин (заочна форма)					
	л	лаб	сем	п	с.р.	усього	л	лаб	сем	п	с.р.	усього
Тема 2. Вектори кібератак на цифрові підстанції (IEC 61850). Підміна даних вимірювань (False Data Injection) та атаки типу Denial of Service (DoS) на контролери.	2	-	-	-	13	15	-	-	-	-	-	-
Тема 3. Стратегії кіберзахисту. Міжнародні стандарти та фреймворки (NIST, ISO/IEC 27001). Мережеві екрани (Firewalls), сегментація мереж, шифрування трафіку в системах автоматики.	2	-	-	6	12	20	-	-	-	-	-	-
Разом за модулем 2	6	0	0	10	35	51	-	-	-	-	-	-
Модуль 3. ЗМІСТОВИЙ МОДУЛЬ 3. Безпека експлуатації та Охорона праці в сучасній енергетиці												
Тема 1. Правові та організаційні засади охорони праці в галузі. Оцінка професійних ризиків при обслуговуванні електроустановок	2	-	-	4	18	24	-	-	-	-	-	-
Тема 2. Безпека експлуатації сучасних кіберфізичних систем. Ергономіка роботи оперативного (диспетчерського) персоналу із засобами людино-машинного інтерфейсу	1	-	-	6	16	23	-	-	-	-	-	-
Разом за модулем 3	3	0	0	10	34	47	-	-	-	-	-	-
Курсовий проект (робота)	-	-	-	-	-	-	-	-	-	-	-	-
Усього годин	15	0	0	30	105	150	-	-	-	-	-	-

Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Тема 1. Енергетична безпека як складова національної безпеки. Критерії та індикатори енергетичної стійкості держави	2
2	Тема 2. Вразливість енергетичної інфраструктури. Фізичні, техногенні та кліматичні загрози. Резервування та диверсифікація джерел енергопостачання	2
3	Тема 3. Екологічна безпека експлуатації енергооб'єктів. Мінімізація впливу на довкілля	2

№ з/п	Назва теми	Кількість годин
4	Тема 4. Специфіка кіберзагроз для електроенергетики. Вразливості протоколів АСУ ТП, SCADA-систем та пристроїв Інтернету Речей (IoT).	2
5	Тема 5. Вектори кібератак на цифрові підстанції (IEC 61850). Підміна даних вимірювань (False Data Injection) та атаки типу Denial of Service (DoS) на контролери.	2
6	Тема 6. Стратегії кіберзахисту. Міжнародні стандарти та фреймворки (NIST, ISO/IEC 27001). Мережеві екрани (Firewalls), сегментація мереж, шифрування трафіку в системах автоматизації.	2
7	Тема 7. Правові та організаційні засади охорони праці в галузі. Оцінка професійних ризиків при обслуговуванні електроустановок	2
8	Тема 8. Безпека експлуатації сучасних кіберфізичних систем. Ергономіка роботи оперативного (диспетчерського) персоналу із засобами людино-машинного інтерфейсу	1
Всього годин		15

Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Комплексна оцінка вразливостей критичної інфраструктури та аналіз сценаріїв Blackout у регіональній енергосистемі	4
2	Розробка стратегічного плану дій з резервування, диверсифікації джерел та мінімізації екологічних ризиків при відновленні живлення критичних споживачів громади (включає розрахунки потреб та вибір резервних потужностей).	6
3	Аналіз реальних кейсів кібератак на енергетичну інфраструктуру та побудова моделі загроз.	4
4	Проектування базової архітектури кіберзахисту енергооб'єкта та розробка політики безпеки.	6
5	Оцінка професійних ризиків та аудит ергономіки робочого місця оперативного (диспетчерського) персоналу при роботі з людино-машинними інтерфейсами (HMI) кіберфізичних систем.	4
6	Розробка комплексного регламенту з безпечної експлуатації та охорони праці при технічному обслуговуванні цифрових електроустановок (на прикладі комірки цифрової підстанції).	6
Всього годин		30

Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Опрацювання лекційного матеріалу (Тем 1-3)	3
2	Підготовка до комплексних практичних робіт №1 та №2	10
3	Підготовка та складання Модульної контрольної роботи №1 (в eLearn): 15 год	15
4	Роль мікромереж (Microgrid) та розподіленої генерації у забезпеченні автономності під час системних аварій (Blackout).	4
5	Дослідження міжнародного досвіду диверсифікації джерел енергопостачання та європейського «Зеленого курсу» (Green Deal)	4
6	Опрацювання лекційного матеріалу (Тем 4-6)	3
7	Підготовка до комплексних практичних робіт №3 та №4	10
8	Підготовка та складання Модульної контрольної роботи №2 (в eLearn)	15
9	Аналіз історичних кейсів кібератак на енергетичну інфраструктуру (наприклад, атаки на Прикарпаттяобленерго у 2015 р. або вірус Stuxnet).	4
10	Опрацювання міжнародних стандартів інформаційної безпеки NIST та ISO/IEC 27001 в контексті промислових мереж.	3
11	Опрацювання лекційного матеріалу (Тем 7-8):	2
12	Підготовка до комплексних практичних робіт №5 та №6	10
13	Підготовка та складання Модульної контрольної роботи №3 (в eLearn)	15
14	Вивчення сучасних європейських директив щодо безпеки праці при експлуатації високовольтних цифрових електроустановок.	4
15	Дослідження новітніх вимог до ергономіки та психофізіологічної безпеки диспетчерського персоналу при тривалій роботі з людино-машинними інтерфейсами (НМІ).	3
Всього годин		105

Методи навчання

Методи та засоби діагностики результатів навчання:

- Усне опитування для перевірки теоретичних знань та розуміння концепцій енергетичної безпеки
- Тестування для оцінки засвоєння ключових понять, термінів та основних аспектів курсу

- Комп'ютерне тестування з використанням спеціалізованих програм для перевірки навичок аналізу ризиків та застосування цифрових інструментів
- Поточне оцінювання (заліки, короткі контрольні роботи) для моніторингу прогресу студентів у процесі навчання
- Модульний контроль для оцінки знань за кожен модуль або блок тем, що дозволяє систематизувати знання та визначити рівень засвоєння матеріалу
- Підсумковий екзамен для комплексної оцінки знань та навичок, отриманих під час курсу

Методи навчання:

- Лекційний метод з використанням сучасних презентацій та мультимедійних засобів для викладення теоретичних аспектів дисципліни
- Кейс-стаді для аналізу реальних ситуацій та розвитку навичок прийняття рішень
- Дискусії та дебати для формування критичного мислення та обговорення сучасних викликів у енергетичній безпеці
- Проєктне навчання для розробки та впровадження заходів з підвищення безпеки та стабільності систем
- Моделювання та симуляції для практичного засвоєння аналізу ризиків та управління кризовими ситуаціями
- Самостійна робота з аналізу наукових джерел та підготовки презентацій
- Групова робота над розробкою стратегій забезпечення енергетичної безпеки

Оцінювання результатів навчання

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України»

Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Модуль 1. ЗМІСТОВИЙ МОДУЛЬ 1. Концептуальні основи енергетичної безпеки		
Практична робота. Виконання та захист Практичної роботи 1 (Комплексна оцінка вразливостей критичної інфраструктури).	ПРН 6, ПРН 8. Модуль спрямований на формування системного розуміння концепцій енергетичної безпеки, включаючи питання кіберзахисту, оцінки ризиків критичної інфраструктури, надійності та якості електроенергії. Студенти здобудуть знання щодо сучасних підходів до забезпечення енергетичної безпеки, вивчать інструменти аналізу ризиків, а також ознайомляться з міжнародним досвідом та стандартами у цій сфері.	25
Практична робота. Виконання та захист Практичної роботи 2 (Розробка стратегічного плану дій з резервування та відновлення живлення).		30
Самостійна робота. Виконання завдань самостійної роботи (опрацювання додаткової літератури у вигляді підготовки есе/презентації).		15
Модульна контрольна. Модульна контрольна робота №1 (тестування та вирішення ситуаційної задачі в системі eLearn).		30
Всього за модулем 1		100
Модуль 2. ЗМІСТОВИЙ МОДУЛЬ 2. Кіберзахист промислових систем керування (OT/ICS)		
Практична робота. Виконання та захист Практичної роботи 3 (Аналіз реальних кейсів кібератак та побудова моделі загроз).	ПРН 6, ПРН 8. Модуль присвячений засвоєнню сучасних підходів до кіберзахисту та інформаційної безпеки в енергетичних системах. Студенти навчаться аналізувати історичні кейси кібератак, опрацьовувати міжнародні стандарти NIST та ISO/IEC 27001, а також оцінювати ризики та розробляти заходи для підвищення безпеки промислових систем.	25

Вид навчальної діяльності	Результати навчання	Оцінювання
Практична робота. Виконання та захист Практичної роботи 4 (Проектування базової архітектури кіберзахисту енергооб'єкта та політики безпеки).		30
Самостійна робота. Виконання завдань самостійної роботи (опрацювання міжнародних стандартів NIST, ISO/IEC 27001).		15
Модульна контрольна. Модульна контрольна робота №2 (тестування в системі eLearn).		30
Всього за модулем 2		100
Модуль 3. ЗМІСТОВИЙ МОДУЛЬ 3. Безпека експлуатації та Охорона праці в сучасній енергетиці		
Практична робота. Виконання та захист Практичної роботи 5 (Оцінка професійних ризиків та аудит ергономіки робочого місця оперативного персоналу).	ПРН 6, ПРН 8. Модуль орієнтований на формування знань та навичок щодо безпечної експлуатації електроустановок, сучасних директив та вимог до ергономіки і психофізіологічної безпеки диспетчерського персоналу. Студенти здобудуть компетенції у застосуванні європейських стандартів та аналізі сучасних вимог до безпеки праці.	25
Практична робота. Виконання та захист Практичної роботи 6 (Розробка комплексного регламенту з безпечної експлуатації цифрових електроустановок).		30
Самостійна робота. Виконання завдань самостійної роботи (вивчення європейських директив щодо безпеки праці).		15

Вид навчальної діяльності	Результати навчання	Оцінювання
Модульна контрольна. Модульна контрольна робота №3 (тестування в системі eLearn).		30
Всього за модулем 3		100
Успішне проходження сертифікованих профільних онлайн-курсів неформальної освіти (Coursera, Prometheus тощо) за темами енергетичної безпеки або енергоменеджменту		від +5 до +15 балів (або повне перезарахування відповідних практичних занять / змістового модуля)
Навчальна робота (разом за семестр)		70
Підсумковий екзамен		30
Разом за курс		100

Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамен/залік)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

Політика оцінювання

Політика щодо дедлайнів та перескладання:	Практичні, самостійні та модульні роботи необхідно здавати у заплановані терміни. Перескладання модульних робіт допускається за наявності поважних причин у визначені кафедрою строки.
Політика щодо академічної доброчесності:	Списування, використання сторонніх матеріалів і несанкціонованих пристроїв під час виконання контрольних робіт, заліку або екзамену заборонено.
Політика щодо відвідування:	Відвідування занять є обов'язковим. Пропуски відпрацьовуються згідно з індивідуальним графіком та правилами кафедри.

Навчально-методичне забезпечення

-електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - в процесі створення);

Рекомендовані джерела інформації

1. 1. Суходоля О. М., Харазішвілі Ю. М., Рябцев Г. Л. Енергетична безпека України: перспективна модель управління ризиками : монографія / за ред. О. М. Суходолі. Київ : НІСД, 2023. 228 с. Монографія НІСД (Національного інституту стратегічних досліджень), відкритий доступ: <https://scholar.google.com/citations?user=vw6MZyUAAAAJ>
2. Бондаренко Є. А. Охорона праці в електроенергетиці : електронний навчальний посібник / Бондаренко Є. А. Вінниця : ВНТУ, 2022. 138 с. Відкритий доступ (PDF): https://pdf.lib.vntu.edu.ua/books/2023/Bondarenko_2022_138.pdf
3. Маслова О. В., Гончарова І. П. Ризикоорієнтовані підходи в охороні праці : електронний навчальний курс. Біла Церква : БІНПО ДЗВО «УМО» НАПН України, 2023. 76 с. Відкритий доступ (PDF): <https://binpo.com.ua/wp-content/uploads/2023/04/ЕНК.pdf>
4. Ackerman P. Industrial Cybersecurity: Efficiently Monitor the Cybersecurity Posture of Your ICS Environment. 2nd ed. Birmingham : Packt Publishing, 2021. 800 p. ISBN 978-1-80020-209-2. Детальний опис видання: <https://www.oreilly.com/library/view/industrial-cybersecurity/9781800202092/>
5. Stouffer K., Lightman S., Pillitteri V. et al. Guide to Operational Technology (OT) Security : NIST Special Publication 800-82 Rev. 3. Gaithersburg : NIST, 2023. 335 p. DOI: 10.6028/NIST.SP.800-82r3. Відкритий доступ (PDF): <https://csrc.nist.gov/pubs/sp/800/82/r3/final>
6. Микитишин А. Г., Митник М. М., Голотенко О. С., Карташов В. В. Комплексна безпека інформаційних мережевих систем : навч. посіб. для студентів спеціальності 174. Тернопіль : ФОП Паляниця В. А., 2023. 324 с. ISBN 978-617-7875-63-4. Відкритий доступ (PDF, репозитарій ТНТУ): <http://elartu.tntu.edu.ua/handle/lib/42625>
7. Сокол Є. І., Гриб О. Г., Карпалюк І. Т. та ін. Кібербезпека енергетичних систем : підручник. Харків : Панов А. М., 2019. 389 с. Бібліографічний запис у каталозі ХОУНБ: <http://webirbis.korolenko.kharkov.com>
8. ДСТУ ІЕС TS 62351-100-6:2024 (ІЕС TS 62351-100-6:2022, IDT). Керування енергетичними системами та пов'язаний із ним інформаційний обмін. Безпека даних та комунікацій. Частина 100-6. Тестування на відповідність стандартам із кібербезпеки. ІЕС 61850-8-1 та ІЕС 61850-9-2. Київ : ДП «УкрНДНЦ», 2024. Опис стандарту: <https://uas.gov.ua/national-fund-of-regulatory-documents/780>