

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Захист об'єктів критичної інфраструктури»

Освітня програма	<i>Кіберзахист інформаційних ресурсів</i>
Рівень вищої освіти	<i>перший (бакалаврський)</i>
Форма навчання	<i>денна</i>
Статус навчальної дисципліни	<i>обов'язкова</i>
Мова викладання	<i>українська</i>

КИЇВ – 2024

N 409 по мс. 417

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри технічного захисту інформації від 18.09.2024 року, протокол № 12.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	3
Семестр	5
Обсяг (кредити ЄКТС/години)	4 / 120
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	30
семінарські заняття (СЗ)	16
практичні заняття (ПЗ)	14
самостійна робота (СР)	60
форма підсумкового контролю (семестр)	Екзамен

Передумовами для вивчення та успішного засвоєння навчальної дисципліни «Захист об'єктів критичної інфраструктури» є: «Фізичні основи захисту інформації», «Національна безпека», «Програмні засоби захисту інформації».

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: навчання здобувачів принципам визначення загальних вимог до кіберзахисту об'єктів критичної інфраструктури, встановлення переліку базових заходів з кіберзахисту, які повинні бути впроваджені на об'єкті критичної інфраструктури, на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації, визначення порядку та критеріїв віднесення об'єктів до об'єктів критичної інфраструктури.

Завдання: надання здобувачам вищої освіти знань здатності забезпечувати захист інформації, що обробляється в автоматизованих системах з метою реалізації встановленої політики інформаційної та кібербезпеки; здатності здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Захист об'єктів критичної інфраструктури» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної / освітньо-наукової програми «Кіберзахист інформаційних ресурсів» (від 11.09.2024 № 29/3/1/3-1277 81), а саме:

ПРН-06. Використання знань з основних методів наукового пошуку; вміння узагальнювати отримані результати, обробки та аналізу інформації з різних джерел, оформлення та презентування результатів наукової діяльності, здатності використовувати статистичні методи в професійній діяльності.

ПРН-09. Вміти здійснювати комплексний аналіз загроз національній безпеці, розробляти та реалізовувати ефективні стратегії їх нейтралізації, застосовуючи знання з основ теорії національної безпеки та синтезуючи різнопланову інформацію.

ПРН-11. Вміти читати й розуміти фахову іншомовну літературу, використовуючи її у соціальній і професійній сферах, а також демонструвати культуру мислення та виявляти навички щодо організації культурного діалогу з іноземними партнерами на рівні, необхідному для професійної діяльності.

ПРН-12. Планувати та організовувати особисту діяльність в умовах протиборства в інформаційній сфері та кіберпросторі для забезпечення інформаційної безпеки та кібербезпеки держави та організації.

ПРН-21. Вирішувати завдання захисту інформації, що обробляється на об'єктах інформаційної інфраструктури та кіберінфраструктури, з використанням методів, засобів і механізмів криптографічного захисту інформації, а також володіти методами сучасних систем цифрової криміналістики і застосовувати їх в дослідницькій та прикладній діяльності.

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>1</i>	2	3	4	5	6	7
Семестр 5						
Змістовий модуль 1. Стратегії та принципи побудови систем безпеки критичної інфраструктури.						
Тема 1. Наукові підходи дослідження СЗ ОКІ	10	4	2			4
Лекція 1. Загально визнані підходи до побудови СБ ОКІ.		2				
Лекція 2. Фундаментальні умови (висновки) щодо побудови систем безпеки критичної інфраструктури.		2				
Семінарське заняття 1. Фундаментальні умови (висновки) щодо побудови систем безпеки критичної інфраструктури.			2			
Самостійна робота 1. Наукові підходи дослідження СЗ ОКІ.						4
Тема 2. Матрична модель системи захисту об'єктів критичної інфраструктури.	8	2		2		4
Лекція 3. Матрична модель системи захисту об'єктів критичної інфраструктури.		2				
Практичне заняття 1. Матрична модель системи захисту об'єктів критичної інфраструктури.				2		
Самостійна робота 2. Матрична модель системи захисту об'єктів критичної інфраструктури.						4
Тема 3. Державна система захисту об'єктів критичної інфраструктури.	8	2		2		4
Лекція 4. Державна система захисту об'єктів критичної інфраструктури.		2				
Практичне заняття 2. Державна система захисту об'єктів критичної інфраструктури.				2		
Самостійна робота 3. Державна система захисту об'єктів критичної інфраструктури.						4
Тема 4. Нормативно-правове забезпечення СЗ ОКІ	8	4	2			2
Лекція 5. Нормативно-правове забезпечення СЗ ОКІ		2				
Лекція 6. Забезпечення безпеки критичної інфраструктури у системі забезпечення національної безпеки розвинутих країн.		2				
Семінарське заняття 2. Забезпечення безпеки критичної інфраструктури у системі забезпечення національної безпеки розвинутих країн.			2			
Самостійна робота 4. Нормативно-правове забезпечення СЗ ОКІ.						2
Тема 5. Структура органів (суб'єктів) державної СЗ ОКІ	8	2	2			4

Лекція 7. Структура органів (суб'єктів) державної СЗ ОКІ		2				
Семінарське заняття 3. Ментальна модель системи безпеки об'єктів критичної інфраструктури.			2			
Самостійна робота 5. Структура органів (суб'єктів) державної СЗ ОКІ						4
Тема 6. Організаційно-технічні заходи державної системи захисту ОКІ.	10	2		2		6
Лекція 8. Організаційно-технічні заходи державної системи захисту ОКІ.		2				
Практичне заняття 3. Організаційно-технічні заходи державної системи захисту ОКІ.				2		
Самостійна робота 6. За тематикою лекції 6						6
Тема 7. Об'єкти критичної інфраструктури.	12	2	2	2		6
Лекція 9. Об'єкти критичної інфраструктури.		2				
Семінарське заняття 4. Об'єкти критичної інфраструктури.			2			
Самостійна робота 7. Об'єкти критичної інфраструктури.						6
Практичне заняття 4. Модульна контрольна робота 1.				2		
Всього годин за змістовий модуль 1	64	18	8	8		30
Змістовий модуль 2. Всебічна система захисту критичної інфраструктури (КІ) у контексті національної безпеки розвинених країн						
Тема 8. Загрози ОКІ	8	2	2			4
Лекція 10. Загрози ОКІ		2				
Семінарське заняття 5. Загрози ОКІ			2			
Самостійна робота 8. Загрози ОКІ.						4
Тема 9. Кіберзахист об'єктів критичної інфраструктури	10	2		2		6
Лекція 11. Кіберзахист об'єктів критичної інфраструктури		2				
Практичне заняття 5. Кіберзахист об'єктів критичної інфраструктури				2		
Самостійна робота 9. Кіберзахист об'єктів критичної інфраструктури						6
Тема 10. Безпека ІКС ОКІ	8	2	2			4
Лекція 12. Безпека ІКС ОКІ		2				
Семінарське заняття 6. Безпека ІКС ОКІ			2			
Самостійна робота 10. Безпека ІКС ОКІ						4
Тема 11. Технічний захист інформації на ОКІ	10	2		2		6
Лекція 13. Технічний захист інформації на ОКІ		2				
Практичне заняття 6. Технічний захист інформації на ОКІ				2		
Самостійна робота 11. Технічний захист інформації на ОКІ						6
Тема 12. Безпека АСУ та об'єктів критичної інфраструктури	8	2	2			4
Лекція 14. Безпека АСУ та об'єктів критичної інфраструктури		2				
Семінарське заняття 7. Безпека АСУ та об'єктів критичної інфраструктури.			2			
Самостійна робота 12. Безпека АСУ та об'єктів критичної інфраструктури.						4
Тема 13. Система інженерного та фізичного захисту ОКІ	12	2	2	2		6
Лекція 15. Система інженерного та фізичного захисту ОКІ		2				
Семінарське заняття 8. Система інженерного та фізичного захисту ОКІ.			2			
Самостійна робота 13. Система інженерного та фізичного захисту ОКІ.						6
Практичне заняття 7. Модульна контрольна робота 2				2		
Всього годин за змістовий модуль 2	56	12	8	6		30
Підсумковий контроль (Екзамен)						
Всього годин за навчальну дисципліну	120	30	16	14		60

Організаційно-методичні вказівки до проведення навчальних занять та контрольних заходів:

1. *Лекції проводять у лекційних залах, обладнаних засобами мультимедіа (мультимедійними проекторами, персональними комп'ютерами (ноутбуками), аудіосистемами).*
2. *Практичні заняття проводяться у кабінетах, обладнаних засобами мультимедіа (мультимедійними проекторами, аудіосистемами, веб-камерами) та інтерактивними дошками.*
3. *Для підготовки здобувачів до виконання модульних контрольних робіт та іспиту має бути 2-3 робочі дні, в яких не проводяться заняття з дисципліни «Захист об'єктів критичної інфраструктури».*

4. Основні методи навчання

На практичних заняттях широко використовуються традиційні та інноваційні методи навчання.

Традиційні методи навчання:

- словесні методи: розповідь (монологічний виклад навчального матеріалу), бесіда (діалогічний метод), синтезуючі або закріплюючі і контрольні-коректуючі;
- наочні методи (демонстрація);
- практичні методи: вправи (їх виконання сприяє набуттю навичок та вмінь, що є дуже важливим в навчанні іноземної мови). Усні вправи сприяють оволодінню технікою читання, розповіді, логічного викладу знань тощо. Письмові вправи включають опис, диктанти, твори та інші;
- робота з книгою є одним з найважливіших методів навчання тому, що здобувач має можливість багаторазово обробити навчальну інформацію в доступному для нього темпі та в зручний час. Навчання роботі з книгою передбачає формування у здобувачів навичок самоконтролю;
- відео метод, який базується на наочному сприйманні інформації, яка будучи доступною, легше і швидше засвоюється;
- індуктивний метод, який вчить здобувачів виявляти причинно-наслідкові залежності, висувати проблеми і долати суперечності, що сприяє розвитку їхнього творчого мислення;
- дедуктивний метод забезпечує систематичний і стрункий виклад навчального матеріалу, уміння виводити одні знання з інших, зв'язувати їх;
- репродуктивний метод (відтворення готових зразків) забезпечує можливість передачі значного обсягу знань, умінь за короткий час і з невеликими витратами зусиль;
- частково-пошуковий (евристичний) метод, коли частину знань повідомляє викладач, а частину самостійно здобувають здобувачі, відповідаючи на поставлені питання чи вирішуючи проблемні завдання;
- самостійна робота здобувачів – метод, який передбачає виконання усних та письмових вправ, творів, підготовку доповідей. Організація самостійної роботи курсантів над засвоєнням англійської мови здійснюється у формі роботи з підручником, аудіо- та відеозаписами;
- спеціальні методи – використання ситуативних та рольових ігор за темами модулів;
- метод інсценізації – завчасно підготовлений діалог, відтворення подій, генерація ідей – “мозкова атака”.

Інноваційні методи навчання спрямовані на розвиток і самовдосконалення особистості, на розкриття її резервних можливостей і творчого потенціалу. Основними принципами сучасних методів є: рух від цілого до окремого, орієнтація занять на здобувачів (*learner-centered lessons*), цілеспрямованість та змістовність занять.

Інтерактивна діяльність включає організацію спрямовану на взаєморозуміння, взаємодію, вирішення проблем. В системі інтерактивного навчання на практичних заняттях виділяються такі основні принципи методики співробітництва:

- 1) *позитивна взаємозалежність – група досягає успіху за умови гарного виконання завдань кожним здобувачем;*
- 2) *індивідуальна відповідальність – працюючи в групі, кожен здобувач виконує своє завдання, відмінне від інших;*
- 3) *однакова участь – кожному здобувачеві надається однаковий за обсягом час для ведення бесіди або завершення завдання;*
- 4) *одночасна взаємодія – коли всі здобувачі залучені до роботи.*

5. Оцінювання результатів навчання

5.1. Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	0,6
Підсумковий контроль (ПК)	0,4

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: ПСО=К+ПК

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

Види навчальної діяльності	Кількість балів (максимальна)
Робота на лекціях (ведення конспекту лекцій або інше)	15
Робота на практичних заняттях	20
Виконання завдань для самостійної роботи	15
Виконання модульної контрольної роботи	50

Мінімальна кількість балів для допуску до підсумкового контролю 40.

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
А	90-100	<i>Відмінно – відмінне виконання лише з незначною кількістю помилок. Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить</i>

		та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	<i>Дуже добре – вище середнього рівня, але з кількома помилками.</i> Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.
C	75-83	<i>Добре – загалом правильна робота, але з певною кількістю помилок.</i> Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.
D	65-74	<i>Задовільно – непогано, але зі значною кількістю недоліків.</i> Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.
E	60-64	<i>Достатньо – виконання задовольняє мінімальні вимоги.</i> Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	<i>Незадовільно – потрібна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	<i>Незадовільно – потрібна значна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Рекомендовані джерела інформації:

1. Todor Tagarev, "Bulgaria: Protecting National Critical Infrastructures with the Contribution of the Ministry of Defense," The European Journal of Critical Services and Infrastructure Protection 1, no. 1 (October 2013): 28-31. ISSN 2344 – 3790
2. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. мат-лів. Міжнар. експерт. нарад/упоряд. Д.С.Бірюков, С.І.Кондратов; за заг.ред. О.М.Суходолі.-К.: НІСДб 2015.-176 с.
3. Згуровський М.З., Панкратова Н.Д. Основи системного аналізу, Київ видавнича група ВНУ, 2007.-544 с.
4. Заславський В.А., Єрмоленко Р.В., Сахно Н.В. Програмне забезпечення для управління безпечною експлуатацією парогенераторів АЕС //

Комп'ютерні засоби, мережі та системи. Інститут кібернетики ім. В.М.Глушкова НАНУ. - 2009, №8 - С.18-27.

5. Заславський В.А., Бірюков Д.С., Євгійенко В.В., Франчук О.В. Моделювання та оцінка сценаріїв загроз для об'єктів критичної інфраструктури// Наукові записки НаУКМА. Том 99: Комп'ютерні науки.- 2009.- С. 97-107.
6. Харченко В.С., Яковлев С.В., Горбачик О.С. та ін. Забезпечення функціональної безпеки критичних інформаційно-керуючих систем : монографія/ за ред. В.С.Харченка, С.В.Яковлева. Харків: Константа,2019.-272 с.
7. Zaslavsky V., Ievgienko V. Critical infrastructure protection policy and type-variety principle in decision making Proceeding First International Workshop Critical Infrastructure safety and Security (CriSS-DESSERT'11), 11-13 May, Kirovograd, Ukraine, Vol.2, 2011.
8. Zaslavsky V., Ievgienko Y. Risk analyses and redundancy for protection of critical infrastructure Monographs of System Dependability// Editor J.Mazurkiewicz, J.Sugier, T.Walkowiak, W.Zamojski, Oficyna Wydawnicza Politechniki Wroclawskiej, Wroclaw, Poland, 2010, P.161-173.
9. Zaslavsky V., Pasichna M. (2019) System Approach Towards the Creation of Secure and Resilient Information Technologies in the Energy sector/ Information & Security, 2019, p.318-330

Матеріальні ресурси

1. Лекційні зали та аудиторії для проведення практичних занять обладнані засобами мультимедіа (мультимедійними проекторами, аудіосистемами, веб-камерами) та інтерактивними дошками.

Адреса розміщення робочої програми навчальної дисципліни

(офіційний вебсайт НА СБУ / платформа дистанційного навчання / електронний ресурс навчально-наукового інституту, кафедри, бібліотеки тощо)

7. Дані про перегляд робочої програми навчальної дисципліни

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри
1.			
2.			
...			

29/3/1/4 - 1498/61
14. 10. 2024