Прим. № ____

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
ТА СТРАТЕГІЧНИХ КОМУНІКАЦІЙ
ЦЕНТР КІБЕРБЕЗПЕКИ
КАФЕДРА КІБЕРБЕЗПЕКИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Кіберзахист об’єктів критичної інфраструктури»

освітня програма	Кіберзахист у сфері інформаційних технологій та кіберпросторі
рівень вищої освіти	другий (магістерський)
форма навчання	заочна
статус навчальної дисципліни	обов’язкова
мова викладання	українська

КИЇВ – 2024

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри кібербезпеки від «02» 09 2024 року, протокол №15

Робочу програму навчальної дисципліни погоджено з гарантом освітньої програми

Завідувач кафедри кібербезпеки
ЦКБ ННІ ІБ СК НА СБ України
д.т.н., професор
«02» 09 2024 р.

Анастасія ВАВІЛЕНКОВА

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	2
Семестр	3
Обсяг *(кредити ЄКТС/години)*	6 / 180
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	10
семінарські заняття (СЗ)	-
практичні заняття (ПЗ)	14
лабораторні заняття (ЛЗ)	-
індивідуальні завдання (ІЗ)	курсова робота (30)
самостійна робота (СР)	156
форма підсумкового контролю *(семестр)*	екзамен (2) курсова (2)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: отримання студентами знань та навичок щодо застосування та впровадження організаційних та технологічних заходів, пов'язаних з кіберзахистом об'єктів критичної інфраструктури, здобуття практичних навичок щодо здійснення технологічних операцій з кіберзахисту, які впроваджуються на об'єктах критичної інформаційної інфраструктури.

Завдання:

- вивчення основних організаційно-методологічних та технічних заходів з кіберзахисту, які впроваджуються на об'єкті критичної інфраструктури;
- визначення заходів з кіберзахисту на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури;
- оволодіння теоретичними та практичними знаннями, що необхідні для використання та застосування технологічних операцій з кіберзахисту об'єкта критичної інформаційної інфраструктури.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Кіберзахист об'єктів критичної інфраструктури» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» *(від 11.09.2024 № 29/3/1/1-1276/ві)*, а саме:

ПРН 1	Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.
ПРН 2	Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.
ПРН 7	Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.
ПРН 12	Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки.
ПРН 19	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення
ПРН 22	Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації
ПРН 26	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Семестр 3						
Змістовий модуль 1. «Кіберзахист об'єктів критичної інфраструктури»						
Тема 1.1 Вимоги до кіберзахисту об'єктів критичної інфраструктури	**4**					**4**
Самостійна робота 1. Нормативні документи, що визначають вимоги до кіберзахисту об'єктів критичної інфраструктури.						4
Тема 1.2. Політика інформаційної безпеки на об'єктах критичної інфраструктури	**12**	**2**		**2**		**8**
Лекція 1. Політика управління ризиками інформаційної безпеки		2				
Самостійна робота 2. Основні розділи політики інформаційної безпеки на об'єкті критичної інфраструктури.						4
Практичне заняття 1. Визначення прав користувачів програмними засобами об'єкта критичної інфраструктури				2		
Самостійна робота 3. Особливості створення груп та призначення паролів користувачам в операційній						4

системі Windows						
Тема 1.3. Доступ користувачів до об'єктів критичної інфраструктури	**12**	**2**		**2**		**8**
Лекція 2. Управління доступом користувачів до об'єктів критичної інфраструктури. Багатофакторна автентифікація користувачів та обладнання об'єкта критичної інфраструктури		2				
Самостійна робота 4. Дослідження політик управління доступом						4
Практичне заняття 2. Налаштування централізованого доступу користувачів до об'єктів критичної інфраструктури за допомогою групових політик домену операційної системи Windows				2		
Самостійна робота 5. Методика налаштування ролів адміністративного доступу до маршрутизатору мережі критичної інфраструктури						4
Тема 1.4. Ідентифікація та автентифікація користувачів об'єкта критичної інфраструктури	**14**			**2**		**12**
Самостійна робота 7. Характеристика методів аутентифікації, що застосовуються на об'єктах критичної інформаційної інфраструктури						4
Практичне заняття 3. Ідентифікація об'єкта критичної інфраструктури за допомогою IP та MAC адреси.				2		
Самостійна робота 8. Технологічні прийоми захисту MAC адреси засобами операційної системи Windows.						4
Самостійна робота 9. Перелік системних користувачів та груп в операційної системі Linux, призначення та перевірки атрибутів папок і файлів						4
Тема 1.5. Реєстрація подій та аудит об'єкта критичної інфраструктури	**12**	**2**		**2**		**8**
Лекція 3.Технологія реєстрації подій та аудиту об'єкта критичної інфраструктури. Організаційні та технологічні вимоги щодо мережевого захисту об'єктів критичної інформаційної інфраструктури		2				
Самостійна робота 10. Етапи виконання робіт з аудиту безпеки на об'єктах критичної інфраструктури.						4
Практичне заняття 4. Використання засобів аудиту безпеки для підвищення захисту операційної системи Windows та Linux				2		
Самостійна робота 11. Виконання операції з аудиту						4

IP та MAC адрес обчислювальних засобів об'єкту критичної інфраструктури, перевірка номерів програмних портів та порядок їх захисту.						
Тема 2.1. Мережевий захист об'єктів критичної інформаційної інфраструктури	**14**			**2**		**12**
Самостійна робота 13. Доменна модель управління мережевими ресурсами, переваги та недоліки.						4
Практичне заняття 5. Формування сегментації мережі об'єктів критичної інфраструктури. Аналіз моніторингу трафіка на маршрутизаторі Cisco				2		
Самостійна робота 14. Порядок визначення кількості вузлів підмережі (зон безпеки) об'єкту критичної інфраструктури						4
Самостійна робота 15. Способи аналізу мережевого трафіку комп'ютерної мережі об'єкту критичної інфраструктури.						
Самостійна робота 16. Класифікація та коротка характеристика програмного забезпечення щодо моніторингу трафіку комп'ютерної мережі об'єкта критичної інформаційної інфраструктури						4
Тема 2.2. Апаратні та програмні засоби мережевого захисту об'єкта критичної інформаційної інфраструктури	**16**	**2**		**2**		**12**
Лекція 4. Характеристика та особливості застосування апаратного та програмного забезпечення щодо захисту об'єкта критичної інформаційної інфраструктури		2				
Самостійна робота 17. Існуючі технологічні підходи щодо застосуванню апаратних та програмних засобів на об'єктах критичної інфраструктури.						4
Самостійна робота 18. Основні команди маршрутизатору Cisco щодо створення на налаштування VLAN.						4
Практичне заняття 6. Налаштування системи запобігання атакам та вторгненням на маршрутизатор Cisco				2		
Самостійна робота 19. Команди налаштування статичної маршрутизації, їх застосування на маршрутизаторі Cisco						4
Тема 2.3. Аналіз захищеності мережевих об'єктів критичної інфраструктури	**14**	**2**				**12**
Лекція 5. Характеристика систем захисту інформації на об'єктах критичної інфраструктури. Виявлення та запобігання атакам та вторгненням на програмні		2				

компоненти об’єкта критичної інфраструктури. Використання технології віртуальних захищених мереж на об’єктах критичної інфраструктури						
Самостійна робота 20. Основні компоненти захисту ОС Windows						4
Самостійна робота 21. Основні команди програми Nmap щодо ідентифікації мережі, перевірки відкритих портів та запущених служб						4
Самостійна робота 22. Класифікація систем виявлення атак.						4
Тема 2.4. Використання бездротових мереж на об’єктах критичної інфраструктури	**8**					**8**
Самостійна робота 23. Технології реалізації віртуальних захищених мереж на об’єктах критичної інфраструктури.						4
Самостійна робота 22. Технологія захисту інформації на об’єкті критичної інфраструктури з застосуванням VPN						4
Тема 3.1. Забезпечення відмовостійкості об’єктів критичної інфраструктури	**18**			**2**		**16**
Самостійна робота 25. Дослідження технологій збереження інформаційних ресурсів об’єктів критичної інфраструктури						8
Практичне заняття 7. Технологія резервування інформаційних ресурсів об’єктів критичної інфраструктури				2		
Самостійна робота 26. Програмні сервіси та технології для відновлення даних на об’єктах критичної інфраструктури						8
Тема 3.2. Організаційні та технологічні питання підтримки працездатності інформаційних ресурсів об’єктів критичної інфраструктури	**26**					**26**
Самостійна робота 27. Особливості відновлення інформації, що використовується на об’єктах критичної інфраструктури						4
Самостійна робота 28. Аналіз переваг та недоліків програмних засобів для вдосконалення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури						4
Самостійна робота 29. Підготовка до модульної контрольної роботи						8
Самостійна робота 30. Модульна контрольна робота						10

Всього годин за перший модуль	**150**	**10**		**14**		**126**
Змістовний модуль 2. «Курсова робота»						
Виконання та захист курсової роботи	**30**					**30**
Всього годин за четвертий модуль	**30**					**30**
Всього годин за навчальну дисципліну	**180**	**10**		**14**		**156**
Підсумковий контроль (*екзамен***)**						

Організаційно-методичні вказівки до проведення навчальних занять та контрольних заходів*: при проведенні в режимі офлайн планувати проведення практичних занять в центрі кібербезпеки.*

4. Основні методи навчання

Під час викладання навчальної дисципліни передбачено застосування наступних форм.

Лекція – логічно вивершений, науково обґрунтований та систематизований виклад певного наукового або науково-педагогічного питання, ілюстрований засобами наочності та демонстрацією результатів досліджень.

Лекція є одним із основних видів і, водночас, методів проведення навчальних занять, призначених для засвоєння теоретичного матеріалу. Вона закладає основи наукових знань, визначаючи напрям, основний зміст та характер усіх видів навчальних занять, а також, головним чином, самостійної роботи здобувачів вищої освіти.

Практичне заняття – форма навчального заняття, на якому у здобувача вищої освіти під керівництвом викладача формуються вміння та навички практичного застосування теоретичних положень навчальної дисципліни шляхом виконання здобувачем вищої освіти відповідно сформульованих завдань.

Практичні заняття проводяться в аудиторії, оснащеною комп’ютерною технікою та технічними засобами навчання.

Практичне заняття включає в себе: проведення викладачем контролю знань, вмінь та навичок здобувачів вищої освіти, постановку загальної проблеми (завдання) та її обговорення за участю здобувачів вищої освіти, розв’язування завдань та їх обговорення, виконання контрольних завдань, їх перевірку та оцінювання викладачем.

Консультація – форма навчального заняття, на якому здобувач вищої освіти отримує від викладача відповіді на конкретні запитання або пояснення окремих теоретичних положень та їх використання на практиці.

Самостійна робота забезпечується навчально-методичними засобами, передбаченими для вивчення навчальної дисципліни: підручниками, навчально-методичними посібниками, конспектами лекцій, практикумами, електронно-обчислювальною технікою тощо.

Самостійна робота над засвоєнням навчального матеріалу може виконуватися в бібліотеці, комп'ютерному класі.

Форми самостійної роботи здобувачів вищої освіти:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем або питань, передбачених для самостійного опрацювання;
- виконання різних за формою і змістом завдань;
- підготовка до практичних занять;
- підготовка до поточного, модульного та підсумкового контролю знань;
- пошук та огляд літературних джерел за проблематикою навчальної дисципліни;
- виконання індивідуальних завдань (написання курсової роботи);
- аналітичний розгляд наукової публікації тощо.

Під час вивчення начальної дисципліни «Кіберзахист об'єктів критичної інфраструктури» використовуються такі методи навчання:

– під час проведення лекційних занять – лекція-діалог, бесіда, а також наочних методів навчання, зокрема використання мультимедійних презентацій. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії;

– під час проведення практичних занять – використання роздаткового матеріалу, нормативно-правові акти.

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)	5
Робота на практичних заняттях	50

Виконання завдань для самостійної роботи	5
Виконання індивідуальних завдань (курсова робота)	100
Виконання модульної контрольної роботи	10
Екзамен	20

Мінімальна кількість балів для допуску до підсумкового контролю 48 балів.

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	*Відмінно – відмінне виконання лише з незначною кількістю помилок.* Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить 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	*Дуже добре – вище середнього рівня, але з кількома помилками.* 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	*Добре – загалом правильна робота, але з певною кількістю помилок.* 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	*Задовільно – непогано, але зі значною кількістю недоліків.* 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	*Достатньо – виконання задовольняє мінімальні вимоги.* Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	*Незадовільно – потрібна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	*Незадовільно – потрібна значна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Рекомендовані джерела інформації

Основна література:

1. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. : іл.

2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с. : іл

3. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. З-38 Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с. : іл

4. Гайворонський М. В. Безпека інформаційно-комунікаційних систем/ М. В. Гайворонський, О. М. Новіков. — К. : Видавнича група BHV, 2009. — 608 с.

5. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с. : іл

Допоміжна література:

1. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. : іл

2. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструк-

тури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с. : іл

3. Богуш В.М.,Кривуца В.Г.,Кудін А.М.Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Г. Київ:ООО Д.В.К., 2004 . - 508 с.

Інформаційні ресурси:

1. Національна бібліотека ім. В.І.Вернадського / [Електронний ресурс]. – Режим доступу: http:www.nbuv.gov.ua/

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України”: Указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015.

3. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року “Про Концепцію розвитку сектору безпеки і оборони України”: Указ Президента України від 14.03.2016 р.№ 92/2016. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/92/2016.

4. Рада національної безпеки та оборони розгляне Концепцію реформування Служби безпеки України – Офіційне інтернет-представництво Президента України. [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/news/rada-nacionalnoyi-bezpeki-taoboroni-rozglyane-koncepciyu-re-40542.

5. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І Кондратов; за заг. ред. О.М. Суходолі. – К. НІСД, 2016. – 176 с. – [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2213.

6. Наказ Адміністрації Держспецзв′язку від 15 січня 2021 року № 23 «Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури». - [Електронний ресурс].- Режим доступу: https://cip.gov.ua/ua/news/nakaz.

Адреса розміщення робочої програми навчальної дисципліни:

_____ https://moodle.nasbu.edu.ua/ _____

(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.			
3.			
4.			
5.