Прим. № ____

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СТРАТЕГІЧНИХ КОМУНІКАЦІЙ
ЦЕНТР КІБЕРБЕЗПЕКИ
Кафедра технологій захисту кіберпростору

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Теорія кіберпростору, кібербезпеки та кіберзахисту»

Освітня програма	*Кіберзахист у сфері інформаційних технологій та кіберпросторі*
Рівень вищої освіти	*другий (магістерський)*
Форма навчання	*очна (денна)*
Статус навчальної дисципліни	*обов'язкова*
Мова викладання	*українська*

КИЇВ – 2024

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри ТЗК від 18.10.2024 року, протокол № 13.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	1
Семестр	1
Обсяг *(кредити ЄКТС/години)*	4/120
Кількість змістових модулів	3
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	22
семінарські заняття (СЗ)	22
самостійна робота (СР)	76
Форма підсумкового контролю *(семестр)*	*Екзамен (1)*

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: опанування навичками теоретичного обґрунтування кіберпростору, кібербезпеки та кіберзахисту.

Завдання: сприяння ефективному формуванню у студентів компетентностей, знань і умінь і навичок обґрунтування застосування засобів теоретичного обґрунтування кіберпростору, кібербезпеки та кіберзахисту.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Теорія кіберпростору, кібербезпеки та кіберзахисту» 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 - 01	Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.
ПРН - 07	Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища
ПРН - 10	Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).
ПРН - 16	Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами.
ПРН - 17	Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору, здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності.

ПРН - 25	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

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 1						
Змістовий модуль 1. Основи теорії кіберпростору						
Тема 1. Основні положення та визначення кіберпростору	**10**	**2**	**2**			**6**
Лекція 1. Основні положення і визначення кіберпростору та їх розвиток в історичному контексті		2				
Семінарське заняття 1. Створення та розвиток кіберпростору			2			
Самостійна робота 1. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						3
Тема 2. Основні напрями розвитку теорії кіберпростору	**10**	**2**	**2**			**6**
Лекція 2. Теоретичні основи кіберпростору		2				
Семінарське заняття 2. Стан та основні напрями розвитку теорії кіберпростору			2			
Самостійна робота 2. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						6
Тема 3. Основи спілкування у кіберпросторі	**10**	**2**	**2**			**6**
Лекція 3. Основні теоретичні, технологічні та технічні засади спілкування в кіберпросторі		2				
Семінарське заняття 3. Гіпертекстові технології кіберпростору			2			
Самостійна робота 3. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						6
Тема 4 Основи економіки кіберпростору	**10**	**2**	**2**			**6**
Лекція 4. Основні напрями та види економічної діяльності у кіберпросторі		2				
Семінарське заняття 4. Основні види кіберекономіки			2			
Самостійна робота 4. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						6
Тема 5. Основні напрями розвитку гуманітарних наук у кіберпросторі	**14**	**2**	**2**			**10**
Лекція 5. Соціальне, психологічне та культурне середовище кіберпростору		2				
Семінарське заняття 5. Мотивації та мотиви користувачів кіберпростору. Модульна контрольна робота 1			2			
Самостійна робота 5. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						10
Всього годин за змістовий модуль 1	**54**	**10**	**10**			**34**
Змістовий модуль 2. Основи кібербезпеки						
Тема 6. Основні напрями розвитку теорії і практики кібербезпеки у контексті забезпечення національної безпеки та безпеки держави	**10**	**2**	**2**			**6**
Лекція. 6. Теоретичні основи інформаційної безпеки та кібербезпеки на державному рівні		2				
Семінарське заняття 6. Основні напрями забезпечення інформаційної безпеки та кібербезпеки на державному рівні			2			
Самостійна робота 6. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						6
Тема 7. Основні підходи до визначення видів протиборства в інформаційній сфері та кіберпросторі	**22**	**4**	**4**			**14**

Лекція 7. Теоретичні основи протиборства в інформаційній сфері та кіберпросторі		2				
Семінарське заняття 7. Теоретичні основи протиборства в інформаційній сфері та кіберпросторі			2			
Лекція 8. Основні види протиборства в інформаційній сфері та кіберпросторі і		2				
Семінарське заняття 8. Основні характеристики видів протиборства в інформаційній сфері та кіберпросторі			2			
Самостійна робота 7. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						14
Тема 8. Війна як один із способів протиборства в інформаційній сфері та кіберпросторі	**10**	**2**	**2**			**6**
Лекція 9. Основні види та характеристики війн в інформаційній сфері та кіберпросторі		2				
Семінарське заняття 9. Інформаційні війни та кібервійни			2			
Самостійна робота 8. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						6
Тема 9. Основи теорії і практики щодо розробки технології забезпечення кібербезпеки	**10**	**2**	**2**			**6**
Лекція. 10. Технологія забезпечення кібербезпеки організації		2				
Семінарське заняття 10. Визначення технології забезпечення кібербезпеки об’єктів. Модульна контрольна робота 2.			2			
Самостійна робота 9. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						6
Всього годин за змістовий модуль 2	**52**	**10**	**10**			**32**
Модуль 3. Основи кіберзахисту						
Тема 10. Теоретичні основи щодо створення архітектури захисту кіберпростору	**14**	**2**	**2**			**10**
Лекція 11. Теоретичні основи щодо створення архітектури захисту кіберпростору		2				
Семінарське заняття 11. Основні напрями забезпечення захисту архітектури кіберпростору. Методи, заходи, засоби забезпечення кіберзахисту на основі СУІБ. Модульна контрольна робота 3.			2			
Самостійна робота 10. Відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи студентів						10
Всього годин за змістовий модуль 3	**14**	**2**	**2**			**10**
Підсумковий контроль	*(екзамен)*					
Всього годин за навчальну дисципліну	**120**	**22**	**22**			**76**

Організаційно-методичні вказівки до проведення навчальних занять та контрольних заходів: індивідуальні завдання у вигляді рефератів або есе відповідно до завдань, визначених в методичних рекомендаціях до самостійної роботи студентів. Оцінка за реферат (есе) враховується при виставлянні підсумкових оцінок за відповідні модулі.

4. Основні методи навчання

Під час викладання навчальної дисципліни використовуються такі методи навчання: індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання.

Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять.

Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання.

Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією.

Теоретична підготовка слухачів забезпечується шляхом вивчення вимог керівних документів з питань національної, інформаційної безпеки та кібербезпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки (кібербезпеки).

Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій та використанням глобальної мережі.

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)	10
Робота на семінарських заняттях	10
Виконання завдань для самостійної роботи	10
Виконання модульної контрольної роботи	30

Мінімальна кількість балів для допуску до підсумкового контролю 30.

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою	Оцінка	Значення оцінки

ЄКТС	за 100-бальною шкалою	
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. Електронний ресурс кафедри. Електронний конспект лекцій з дисципліни «Теорія кіберпростору, кібербезпеки та кіберзахисту».
2. Богуш В.М., Бровко В. Д.., Настрадін В.П. Кіберпростір: основи кібербезпеки та кіберзахисту. Навч. посіб. У 3-х част. Ч.1. Теоретичні основи кіберпростору. К.: Нац. акад. СБУ, 2020. – 232 с.
3. Богуш В.М., Бровко В. Д.., Настрадін В.П. Кіберпростір: основи кібербезпеки та кіберзахисту. Навч. посіб. У 3-х част. Ч.2. Основи кібербезпеки. К.: Нац. акад. СБУ, 2020. – 184 с.
4. Богуш В.М., Бровко В.Д., Настрадін В.П. Кіберпростір: основи кібербезпеки та кіберзахисту. Навч. посіб. У 3-х част. Ч.3. Основи кіберзахисту. К.: Нац. акад. СБУ, 2020. – 272 с.

Допоміжна література:

5. Основи кіберпростору, кібербезпеки та кіберзахисту / В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін. Навч. посіб. під ред. В. М. Богуша. – К.: Видавництво Ліра-К, 2020. – 554 с.

Нормативно-правові акти

1. Закон України Про національну безпеку України. Голос України від 07.07.2018 - № 122.
2. Закон України Про основні засади забезпечення кібербезпеки України. Голос України від 09.11.2017 - № 208.
3. Стратегія кібербезпеки України. Затверджена Указом Президента України від 15 березня 2016 року №96/2016.
4. Стратегія інформаційної безпеки Затверджена Указом Президента України від 28 грудня 2021 року № 685/2021
5. Концепція створення державної системи захисту критичної інфраструктури. Схвалена розпорядженням КМ України від 6 грудня 2017 р. № 1009-р.
6. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту.
7. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT).

Інформаційні ресурси (відповідно до завдання, визначеного в методичних рекомендаціях до самостійної роботи).

Заняття проводяться в комп'ютерних класах за наявності підключення до Інтернету та мультимедійної апаратури.

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.			
…			

29/2/1/4 – 133 від 23.01.2025