Прим. №1

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Кафедра інформаційної безпеки держави

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Інформаційне протиборство»

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 – 2023

29/3/3 - 772/Bi
25. 09. 2023

1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	1
Семестр (и)	1, 2
Обсяг *(кредити ЄКТС/години)*	5 /150
Кількість змістових модулів	**3**
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	**8**
семінарські заняття (СЗ)	**8**
практичні заняття (ПЗ)	
лабораторні заняття (ЛЗ)	
індивідуальні завдання (ІЗ)	
самостійна робота (СР)	**134**
форма підсумкового контролю *(семестр)*	Екзамен

2. Мета та завдання навчальної дисципліни

2.1. Мета – формування у студентів сучасного рівня інформаційно-психологічної та комп'ютерної культури, набуття знань про організаційно-правові основи, принципи, методи та засоби інформаційного протиборства, набуття практичних навичок підготовки та ведення інформаційних операцій, використання новітніх інформаційно-психологічних, інформаційно-комунікаційних технологій для вирішення різноманітних завдань у професійній діяльності.

2.2. Завдання:

Основними завданнями вивчення дисципліни «Інформаційне протиборство» є:

вивчення нормативних документів в сфері інформаційного протиборства;

вивчення основних понять, які пов'язані з інформаційним протиборством;

вивчення принципів та методів інформаційного протиборства;

вивчення рефлексивного управління як теоретичної основи інформаційного протиборства;

вивчення основ використання можливостей глобальної мережі Internet в інтересах інформаційного протиборства;

проведення моніторингу соціально-орієнтованих ресурсів мережі Internet як складової національного інформаційного простору;

вивчення використання відкритих даних у веденні інформаційного протиборства;

надбання вмінь та навичок ефективного використання сучасних комп'ютерних інформаційних технологій при вирішенні практичних завдань інформаційного протиборства, освоєння нових програмних продуктів;

вивчення основ автоматизації обробки документів в ході інформаційного протиборства.

2.3. Результати навчання

Обов'язкова навчальна дисципліна «Інформаційне протиборство» 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 __.__.202__ № _____),* а саме:

РН-02.	Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.
РН-03.	Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог
РН-05.	Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів
РН-08.	Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності.
РН-11.	Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності .
РН-13.	Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.
РН-15.	Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.
РН-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.
РН-20.	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН-24.	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів 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. *Інформаційне протиборство як механізм забезпечення національної безпеки в інформаційній сфері*						
Тема 1. Генезис інформаційного протиборства	**16**	**2**	**2**	**-**	**-**	**12**
Лекція 1. Сутність та зміст інформаційного протиборства		2				
Семінар 1. Еволюція інформаційного протиборства			2			
Самостійна робота 1. Загрози національним інтересам в сфері інформаційного протиборства						12
Тема 2. Сучасні стратегії та концепції інформаційного протиборства	**26**	**2**	**-**	**-**		**24**
Лекція 1. Стратегія інформаційного протиборства держави		2				24
Самостійна робота 1. Стратегія національної безпеки України: інформаційний аспект						12
Самостійна робота 2. Концепції інформаційного протиборства провідних країн світу						12
Модульна контрольна робота 1 (за рахунок бюджету часу сем. 1)						
Всього годин за модуль І	**42**	**4**	**2**	**-**		**36**
Модуль 2. Теоретичні та технологічні основи інформаційного протиборства						
Тема. 3 Теоретичні основи інформаційного протиборства	**16**	**2**	**2**			**12**
Лекція 1. Рефлексивне управління як теоретична основа інформаційного протиборства		2				
Семінар 1. Когнітивне моделювання інформаційного протиборства			2			
Самостійна робота 1. Теоретичний доробок Володимира Лефевра						12
Тема 4. Технології та засоби інформаційного протиборства	**26**	**-**	**-**			**26**
Самостійна робота 2. Технології та засоби захисту у сфері інформаційної безпеки та кіберсфері						12
Самостійна робота 3. Технології та засоби інформаційного протиборства в сфері кібербезпеки						14
Модульна контрольна робота 2 (за рахунок бюджету часу сем. 1)						
Всього годин за модуль 2	**42**	**2**	**2**	**-**		**38**
Модуль 3. Організаційні аспекти підготовки та ведення інформаційного протиборства						

1	2	3	4	5	6	7
Тема 5. Форми ведення інформаційного протиборства	**14**	**2**	**2**			**10**
Лекція 1. Форми ведення інформаційного протиборства		2				
Семінар 1. «Використання відкритих даних у веденні інформаційного протиборства»			2			
Самостійна робота 1. Особливості ведення інформаційно-психологічної операції на державному та військовому рівнях						10
Тема 6. Підготовка та ведення інформаційного протиборства з використанням соціально-орієнтованих ресурсів мережі Internet та відкритих даних	**32**		**2**			**30**
Самостійна робота 1. Система інформаційного протиборства держави						10
Семінар 1. «Моніторинг соціально-орієнтованих ресурсів мережі Internet як складової національного інформаційного простору»			2			
Самостійна робота 1 «Моніторинг початку спеціальної інформаційної операції»						10
Самостійна робота 2. «Спеціальна інформаційна операція у протидії загрозам національній безпеці»						10
Тема 7. Перспективи ведення інформаційного протиборства в соціальних мережах	**20**	**-**	**-**	**-**		**20**
Самостійна робота 1. Технології використання сервісів та прикладних програмних засобів для ведення інформаційного протиборства в соціальних мережах						10
Самостійна робота 2. Інформаційне протиборство в соціальних мережах в системі стратегічних комунікацій						10
Модульна контрольна робота 3 (за рахунок бюджету часу сем. 1)						
Всього годин за модуль 3.	**66**	**2**	**4**			**60**
Підсумковий контроль (екзамен)						
Всього годин за навчальну дисципліну	**150**	**8**	**8**			**134**
Кількість кредитів ЄКТС	5					

4. Основні методи навчання

І. Методи організації та здійснення навчально-пізнавальної діяльності:

1. За джерелом інформації:

словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда;

наочні: спостереження, ілюстрація, демонстрація.

2. За логікою передачі і сприймання навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні.

3. За ступенем самостійності мислення: репродуктивні, пошукові, дослідницькі.

4. За ступенем керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів.

ІІ. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності:

навчальні дискусії;

створення ситуації пізнавальної новизни;

створення ситуацій зацікавленості (метод цікавих аналогій тощо).

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)	1
Робота на семінарських заняттях	5
Робота на практичних заняттях	-
Робота на лабораторних заняттях	-
Виконання завдань для самостійної роботи	1
Виконання індивідуальних та/або групових завдань	-
Виконання модульної контрольної роботи	5

Мінімальна кількість балів для допуску до підсумкового контролю 36

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

Основна література:

1. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніка, 2019. – 580 с.

2. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

3. Мужанова Т.М. Інформаційна безпека держави: навчальний посібник. – К., 2019. – 131 с.

4. 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.

5. Інформаційна безпека: навч. посіб. / Лісовська Ю.П. — Київ: Видавничий дім «Кондор», 2018. – 172 с.

6. Є. Яковенко, І. Журавель, І. Горбатий, А. Бондарєв. Інформаційна безпека. Видавництво Львівська політехніка. 2019. - 580с.

7. Г. Почепцов. Пропаганда 2.0. Х.: Вид-во Фоліо, 2018.- 796 с.

Нормативно-правові акти:

1. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96

2. Про Стратегію воєнної безпеки України: Указ Президента України від 25.03.2021 № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021

3. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII . URL: https://zakon.rada.gov.ua/laws/show/2469-19

4. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98

5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17

6. Стратегія національної безпеки України «Безпека людини – безпека країни». Затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020

7. Стратегія інформаційної безпеки України. Затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

8. Стратегія кібербезпеки України. «Безпечний кіберпростір – запорука успішного розвитку країни». Затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

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[1]

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри
	29.08.2024р., протокол №1	Актуальна для набору 2024р. ОПП реєст. №29/3/1/1-1276/ві від 11.07.2024 р.	[підпис]

[1] Перегляд робочої програми навчальної дисципліни відбувається щорічно, з урахуванням результатів моніторингу та періодичного перегляду освітньої програми і, зокрема, отриманих від здобувачів вищої освіти та інших стейкхолдерів побажань та зауважень.