Форма № Н - 3.04

Національний університет біоресурсів і природокористування України
Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»

_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

"Інформаційно-психологічне протиборство"

зі спеціальності 125 – «Кібербезпека»
(шифр і назва напряму підготовки)

Освітня програма «Кібербезпека»

факультет інформаційних технологій
(назва факультету)

спеціальність	125 "Кібербезпека"
освітня програма	Кібербезпека
Факультет	Інформаційних технологій
Розробник:	д.пед.н., професор Мамченко С.М.

Київ – 2023 р.

Опис навчальної дисципліни
Інформаційно-психологічне протиборство
(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2023-2024	
Семестр	7	
Лекційні заняття	30 год.	
Практичні, семінарські заняття		
Лабораторні заняття	30 год.	
Самостійна робота	60 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	4 год.	

1. Мета та завдання навчальної дисципліни

Мета навчальної дисципліни «Інформаційно-психологічне протиборство» полягає у набутті компетенцій, знань, умінь і навичок для подальшого використання у своїй практичній діяльності по захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів з урахуванням досягнень науково-технічного прогресу та міжнародного досвіду.

Основні завдання навчальної дисципліни:

- розширити і систематизувати знання щодо загроз національній безпеці в інформаційній сфері;
- набути знання щодо історії та сучасності проведення акцій інформаційного впливу, спеціальних інформаційних операцій, інформаційних війн;
- сформувати критичне мислення для набуття навичок із захисту від маніпулятиного впливу;
- розвити вміння щодо управління інформаційною безпекою держави.

Навчальна дисципліна «Інформаційно-психологічне протиборство» надає можливості отримання таких знань, вмінь і досвіду.

Знати:

види та сучасні технології інформаційних впливів;

сутність форми і види інформаційного протиборства;

етапи, ознаки, суб'єкти та методи проведення спеціальних інформаційних операцій;

завдання, об'єкти посягань, форми проведення інформаційної війни;

історію і особливості сучасного стану інформаційно-психологічного протиборства;

особливості інформаційного впливу через ЗМІ;

особливості діяльності неурядових організацій в контексті впливу на інформаційний простір;

основні методи, головні вектори та види атак з використанням соціальної інженерії.

Вміти:

узагальнювати теоретичні уявлення щодо сутності інформаційної безпеки;

виявляти приховані та шкідливі інформаційно-психологічні впливи;

здійснювати порівняльний аналіз форм, методів, засобів та технологій проведення інформаційних війн, акцій інформаційного впливу та спеціальних інформаційних операцій;

здійснювати прогнози щодо можливих небезпек інформаційному простору держави;

використовувати світовий досвід щодо захисту інформаційного простору для його творчого впровадження на українських теренах.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Спеціальні (фахові) компетентності:

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки.

Навчальна програма розрахована на здобувачів вищої освіти, які навчаються за освітньою програмою підготовки бакалаврів за спеціальністю 125 «Кібербезпека».

Робоча програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Навчальна програма розроблена на підставі наступних документів:

-освітньо-професійна програма підготовки фахівців за спеціальністю «Кібербезпека»;

-навчальний план підготовки бакалаврів за спеціальністю «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення є курс «Інформаційна безпека держави».

2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Моніторинг мережевої безпеки.												
Тема №1. Становлення і розвиток інформаційно-психологічного протиборства (ІПсП).	7	2		0		5						
Тема №2. Інформаційна війна як форма ІПсП.	11	2		4		5						
Тема №3. Сучасні технології проведення спеціальних інформаційних операцій.	11	2		4		5						
Тема №4. Становлення та розвиток ІПсП.	9	2		2		5						
Тема №5. Формування основ теорії і практики ІПсП на початку XX-го сторіччя.	9	2		2		5						
Тема №6. Інформаційно-психологічне протиборство в роки Другої світової війни.	9	2		2		5						
Разом за змістовим модулем 1	**56**	**12**		**14**		**30**						
Змістовий модуль 2. Інформаційна зброя в сучасних умовах.												
Тема № 7. Інформаційна зброя в сучасних умовах.	9	2		2		5						
Тема №8. Засоби масової інформації як засіб впливу на інформаційний простір.	7	2		0		5						
Тема № 9. Особливості впливу на інформаційний простір України російських та проросійських неурядових	13	2		6		5						

організацій.												
Тема № 10. Інформаційна складова терористичної діяльності.	11	4		2		5						
Тема № 11. Базові методи та організаційні заходи захисту від атак за допомогою соціальної інженерії.	13	4		4		5						
Тема № 12. Особистісно-психологічний захист від застосування методів соціальної інженерії.	11	4		2		5						
Разом за змістовим модулем 2	**64**	**18**		**16**		**30**						
Усього годин за курс	**120**	**30**		**30**		**60**						

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Нові форми і методи інформаційного впливу на психіку людини.	4
2.	Індивідуальна, групова і масова свідомість людей - основні об'єкти агресивного ІПсВ.	4
3.	ІПсП крізь призму засобів масової комунікації.	4
4.	Техніки маніпуляції, що застосовуються ЗМК при здійсненні інформаційно-психологічних впливів.	4
5.	Головні вектори нападу при проведенні атак за допомогою методів соціальної інженері.	6
6.	Характеристика основних методів соціальної інженерії.	4
7.	Види атак з використанням соціальної інженерії.	4
	Разом	**30**

7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Основні способи і методи застосування інформаційної зброї.	5
2	Міжнародний "кібертероризм", інформаційні та інформаційно-іміджеві війни сучасності.	5
3	Нові форми і методи інформаційного впливу на психіку людини.	5
4	Індивідуальна, групова і масова свідомість людей - основні об'єкти агресивного ІПсВ.	5
5	ІПсП крізь призму засобів масової комунікації.	5
6	Сутність переваг та проблем, що виникають при веденні ІПП за допомогою ЗМК.	5
7	Характеристика ІПсП, що здійснюється за допомогою ЗМК.	5
8	Тренди у сфері комунікацій, які впливають на участь сучасних ЗМК в ІПсП.	5
9	ехніки маніпуляції, що застосовуються ЗМК при здійсненні інформаційно-психологічних впливів.	5
10	Головні вектори нападу при проведенні атак за допомогою методів соціальної інженері.	5
11	Характеристика основних методів соціальної інженерії.	5
12	Види атак з використанням соціальної інженерії.	5
	Разом	**60**

8. Контрольні питання для перевірки знань студентів (приклади питань)

1. Становлення і розвиток ІПсП
2. Китайські стратегеми і положення про ІПсП "Трактату про військове мистецтво" Сунь-Цзи.
3. Зародження пропаганди як форми інформаційно-психологічноговпливу в епоху Середньовіччя.
4. Особливості ІПсП за часів українського козацтва.
5. Особливості спецпропаганди у роки Першої світової війни.
6. Політичний досвід використання пропаганди у Першій світовій війні.
7. Роль воєнної пропаганди Німеччини у збройних конфліктах.
8. Особливості здійснення інформаційно-психологічного впливу фашистською Німеччиною на території України.
9. Заходи радянського уряду напередодні Другої світової війни для зміцнення апарату спецпропаганди.
10. Особливості та напрями ведення спецпропаганди СРСР у роки Другої світової війни.
11. Нові концепції та погляди США на ведення психологічної війни у Кореї (1950-1953 рр.).
12. Випробування концепції спеціальних методів війни США під час війни у В'єтнамі (1964-1975).
13. Особливості психологічних операцій ЗС США у Перській затоці (1991).
14. Недооцінка військово-політичним керівництвом СРСР ролі та значення інформаційних факторів "холодної війни".
15. Основні тенденції зміни характеру геополітичної боротьби держав та розвиток процесу глобалізації сучасності.
16. Інформаційно-психологічні операції, як альтернатива бойовим діям.
17. Лінійний та синергетичний підходи до спеціальнихінформаційних операцій.
18. Інформаційний простір - театр сучасних військових дій.
19. Класифікація сучасної інформаційної зброї.
20. Основні способи і методи застосування інформаційної зброї.
21. Міжнародний "кібертероризм", інформаційніта інформаційно-іміджеві війни сучасності.
22. Нові форми і методи інформаційного впливу на психіку людини. Індивідуальна, групова і масова свідомість людей - основні об'єкти агресивного ІПсВ.
23. ІПсП крізь призму засобів масової комунікації
24. Взаємозалежність та взаємозумовленість ІПсП й модифікацій засобів ма- сової комунікації (ЗМК).
25. Сутність переваг та проблем, що виникають при веденні ІПП за допомогою ЗМК.
26. Характеристика ІПсП, що здійснюється за допомогою ЗМК.
27. Етапи становлення ЗМК.
28. Тренди у сфері комунікацій, які впливають на участь сучасних ЗМК в ІПсП.
29. Техніки маніпуляції, що застосовуються ЗМК при здійсненні інформаційно-психологічних впливів.
30. Характеристика військових ЗМК

9. Методи навчання

Проведення лекцій з використанням технічних засобів навчання.

Виконання лабораторних робіт з використанням наочних технічних засобів навчання у вигляді систем моделювання за допомогою інженерних пакетів проектування цифрових пристроїв.

Проведення самостійної роботи засобами інформаційно-комунікаційних технологій в освіті.

Використовується електронний навчальний курс на платформі Moodle.

10. Форми контролю

Захист результатів виконання лабораторних робіт.

Контрольне тестування відповідно до кожного змістовного модуля, що створений у комп’ютерному навчальному середовищі.

Підсумкова атестація: іспит.

11. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10)

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

12. Методичне забезпечення

Електронний навчальний курс на платформі Moodle вміщує методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

13. Рекомендована література

Базова

1. Інформаційна безпека (соціально-правові аспекти) : підруч. / [В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк та ін.] ; за ред. Є.Д.Скулиша. - К.:КНТ, 2010.-776 с.
2. Інформаційна безпека держави: підручник / [В.М.Петрик, М.М.Присяжнюк, Д.С.Мельник та ін.]; в 2 т. / – К. : Вид-во ІСЗЗІ НТУУ “КПІ”, 2016. – Т. 1. – 264 с.
3. Інформаційно-психологічне протиборство (еволюція та сучасність): навч. посіб. / Я.М.Жарков, В.М.Петрик, М.М.Присяжнюк та ін. - К.: ЗАТ "ВІПОЛ", 2013.-246 с.
4. Інформаційно-психологічне протиборство : підручник. Видання третє доповнене та перероблене / [В.М.Петрик, В.В.Бедь, М.М.Присяжнюк та ін.]; за заг. ред. В.В.Бедь, В.М.Петрика. - К.: ПАТ «ВІПОЛ», 2018. - 388 с.
5. Історія інформаційно-психологічного протиборства : підруч. / [Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш] ; за заг. ред. Є.Д.Скулиша. - К. : Наук.-вид. відділ НА СБ України, 2012.-208 с.
6. Петрик В.М., Бакалинський О.О., Жарков Я.М. та ін. Інформаційно-психологічне протиборство (еволюція та сучасність) : навч. посіб. – К.: Вид-во ІСЗЗІ НТУУ “КПІ”, 2012. – 248 с.
7. Петрик В.М., Присяжнюк М.М., Мельник Д.С. та ін. Забезпечення інформаційної безпеки держави: підручник ; за заг. ред. О.А.Семченка та В.М.Петрика. – К.: ДНУ «Книжкова палата України», 2015. – 672 с.
8. Соціальна інженерія (системний аналіз): навч. посіб. / за заг. ред. В.І.Курганевича та В.М.Петрика. – К., 2019. – 200 с.
9. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. / [О.М.Богданов, В.М.Петрик, Д.В.Пахольченко] / за заг. ред. В.М.Петрика. – К., 2018. –80 с.
10. Соціальна інженерія в контексті кібернетичної безпеки України (сучасні технології та шляхи захисту): навч. посіб. / [Ю.Г.Куцан, О.М.Богданов, В.М.Петрик, Д.В.Пахольченко, А.В.Давидюк] / за заг. ред. В.М.Петрика. – К., 2017. – 80 с.

11. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева та ін.]; за заг. ред. Є.Д.Скулиша. - К.: Наук.-вид. відділ НА СБ України, 2010. - 248 с..

Допоміжна

1. Безбах В.Г., Онищук М.І. Протидія інформаційно-психологічному впливу противника: навч.-метод. посібник. – К.: НАОУ, 2002. – 40 с.

2. Бірюков В.О., Есаулов М.Ю., Жук П.В., Міночкін А.І., Павлов І.М. Теоретичні основи інформаційної боротьби в сучасних війнах, воєнних конфліктах та у війнах майбутнього. – К.: ВІТІ ДУТ, 2013. – 322 с.

3. Богданович В.Ю., Свида І.Ю., Скулиш Є.Д. Теоретико-методологічні основи забезпечення національної безпеки України: Теоретичні основи, методи й технології забезпечення національної безпеки України. – К.: Наук. вид. від НА СБУ, 2012. – 548 с.

4. Бурячок В.Л., Хорошко В.О. Технологія прийняття рішень у складних соціотехнічних системах – К.: ДУІКТ, 2012. – 344 с.

5. Бурячок В.Л, Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки. – К: ПВП «Задруга», 2014. – 222 с.

14. Інформаційні ресурси

1. http://www.rsasecurity.com
2. http://www.nist.gov
3. http://www.eprint.iacr.org
4. http://www.citeseer.ist.psu.edu
5. http://www.ansi.org
6. http://www.cryptography.org
7. http://www.iso.org
8. http://www.linuxiso.org
9. http://www.cryptography.com
10. http://www.springerlink.com
11. http://www.cacr.math.uwaterloo.ca
12. http://www.financialcryptography.com
13. http://www.austinlinks.com
14. http://world.std.com/~franl/crypto.html
15. http://www.cryptonessie.org