СИЛАБУС ДИСЦИПЛІНИ
«ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНЕ ПРОТИБОРСТВО»

Ступінь вищої освіти – бакалавр
Спеціальність 125 – Кібербезпека
Освітня програма «Кібербезпека»
Рік навчання 4, семестр 7
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	 **Мамченко Сергій Миколайович, д.пед.н., професор (портфоліо)**
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail s.mamchenko@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (7 семестр)**

ОПИС 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.

Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання.

СТРУКТУРА КУРСУ

Тема	Години (лекції/ Лабораторні,)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Становлення і розвиток інформаційно-психологічного протиборства.				
Тема №1. Становлення і розвиток інформаційно-психологічного протиборства (ІПсП).	**2/0**	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.	Опитування.	-
Тема №2. Інформаційна війна як форма ІПсП.	**2/4**		Захист лабораторної роботи.	**10**
Тема №3. Сучасні технології проведення спеціальних інформаційних операцій.	**2/4**		Захист лабораторної роботи.	**10**
Тема №4. Становлення та розвиток ІПсП.	**2/2**		Опитування.	**2**
Тема №5. Формування основ теорії і практики ІПсП на початку XX-го сторіччя.	**2/2**		Опитування.	**2**
Тема №6. Інформаційно-психологічне протиборство в роки Другої світової війни.	**2/2**			
Модульний контроль			Підсумковий тест в ЕНК.	**30**
Модуль 2. Інформаційна зброя в сучасних умовах.				
Тема № 7. Інформаційна зброя в сучасних умовах.	**2/2**	ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.	Захист лабораторної роботи.	**10**
Тема №8. Засоби масової	**2/0**	ПРН 52. Використовувати	Опитування.	-

інформації як засіб впливу на інформаційний простір.		інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.		
Тема № 9. Особливості впливу на інформаційний простір України російських та проросійських неурядових організацій.	**2/6**		Опитування.	**2**
Тема № 10. Інформаційна складова терористичної діяльності.	**4/2**		Опитування.	**2**
Тема № 11. Базові методи та організаційні заходи захисту від атак за допомогою соціальної інженерії.	**4/4**		Опитування.	**2**
Тема № 12. Особистісно-психологічний захист від застосування методів соціальної інженерії.	**4/2**		Опитування.	**2**
Модульний контроль			Підсумковий тест в ЕНК.	**30**
Всього за семестр				**70**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету).

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

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