ФІЛОСОФСЬКІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ВІЙНИ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Третій (доктор філософії)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітня програма	*КОМП'ЮТЕРНІ НАУКИ*
Статус дисципліни	***Блок вибіркових навчальних дисциплін***
Форма навчання	***очна(денна)***
Рік підготовки, семестр	*2 курс, весінній семестр*
Обсяг дисципліни	*2 кредити (60 годин)*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	*Перший тиждень:* ***лекція/практична робота****, _____, on-line* *Другий тиждень:* ***лекція/практична робота****, _____, on-line*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *к.т.н. Бакалинський Олександр Олегович, контактні дані:* ***baov@ukr.net*** Практичні: *к.т.н. Бакалинський Олександр Олегович, контактні дані:* ***baov@ukr.net***
Розміщення курсу	Посилання на дистанційний ресурс (Moodle, Google Classroom, тощо):

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Дисципліна «Філософські аспекти інформаційної війни», (ІІВ3) є вибірковою дисципліною навчального плану підготовки докторів філософії з спеціальності «Комп'ютерні науки» і грає важливу роль у підготовці фахівців.

Метою навчальної дисципліни є формування у аспірантів компетентностей та підготовка науковця, здатного виявити ознаки спеціальних інформаційних операцій, визначити об'єкт їх спрямування, розпізнати техніки маніпулювання інформацією, здійснювати професійну діяльність в умовах швидкозмінного стану суспільства, яке знаходиться у стані інформаційної війни. Використовувати критичне мислення формувати власну психологічну стійкість в умовах ескалації інформаційних та гібридних впливів.

Метою кредитного модуля є формування у аспірантів загальних і спеціальних професійних та системних компетентностей:

– ЗК 01 – Здатність до абстрактного мислення, аналізу та синтезу;

– ЗК 03– здатність працювати в міжнародному контексті;

– СК05 – здатність планувати й організовувати роботу дослідницьких колективів з рішення наукових і науково-освітніх завдань.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Пререквізити: навички використання інформаційних і комунікаційних технологій. Цей курс базується на таких забезпечуючих дисциплінах: Сучасні проблеми і тенденції розвитку комп'ютерних наук та інформаційних технологій, філософські проблеми наукового пізнання, фахова іноземна мова.

Постреквізити: Перелік напрямків діяльності, що забезпечуються: за рахунок сформованого критичного мислення вміння виявляти акції інформаційного впливу, спеціальні інформаційні операції, визначати їх мету та цілі, використовувати ці навички при проведенні наукових досліджень.

3. Зміст навчальної дисципліни

Розділ 1. Вступ до дисципліни.

Лекція 1. Інформаційні війни. Інформаційна безпека держави

Лекція 2. Інформаційно-психологічний вплив. Спеціальні інформаційні операції та акції інформаційного впливу.

Розділ 2. Особливості сучасного періоду інформаційно-психологічного протиборства.

Лекція 3. Глобальне інформаційне протиборство нового тип, інформаційна зброя в сучасних умовах.

Лекція 4. Засоби масової комунікації: маніпулятивні техніки ведення інформаційних війн.

4. Навчальні матеріали та ресурси

Базові

1. Інформаційна безпека. підручник / [В.В.Остроухов, М.М.Присяжнюк, В.М.Петрик та ін.]; / під. ред. В.В.Остроухова. – К. : Вид-во Літера-К, 2021. – 412 с
2. Толубко, В. Б., С. Я. Жук, and В. О. Косевцов. "Концептуальні основи інформаційної безпеки України." ВБ Толубко, СЯ Жук, К.- 2004.
3. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник / [В.М. Петрик, С.О. Гнатюк, М.М. Присяжнюк та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика та О.А Смірнова. — К., 2022. – 328 с.
4. Сучасні технології нейролінгвістичного програмування: навчальний посібник. / [Петрик В.М., Гнатюк С.О., Черненко О.Є. та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика, О.А. Смірнова. – К.: Центр учбової літератури, 2020. – 200 с.
5. Соціальна інженерія (системний аналіз): навч. посіб. / [В.М.Петрик, В.І.Курганевич, В.Г.Кононович та ін.] / за заг. ред. В.І.Курганевича та В.М.Петрика. – К., 2019. – 200 с.
6. 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. – 388с.
7. Богданов О.М., Петрик В.М. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. / за заг. ред. В.М.Петрика. – К.: Вид-во ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. – 80 с.
8. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене / [В.М. Петрик, М.М. Присяжнюк, Я.М. Жарков та ін.]; за заг. ред. В. М. Петрика. — К.: Вид-во ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. − 388 с.

Додаткові

9. Жук, С. Я., В. О. Чмельов, and Т. М. Дзюба. "Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї." (2006): 35-41.
10. Пєвцов, Г. В., et al. "Основні особливості ознак проведення інформаційно-психологічної операції Російської Федерації в Автономній Республіці Крим." Наука і техніка Повітряних Сил Збройних Сил України 1 (2014): 35-37.
11. Пєвцов Г. В., et al. Основні особливості ознак проведення інформаційно-психологічної операції Російської Федерації в Автономній Республіці Крим. Наука і техніка Повітряних Сил Збройних Сил України, 2014, 1: 35-37.
12. Бакалинський О.О., Інформаційний «бліцкриг», "Правова інформатика", № 2(42)/2014.
13. Пєвцов, Г. В., Залкін, С. В., Сідченко, С. О., Хударковський, К. І., Феклістов, А. О., & Антонов, А. В. (2014). Основні особливості ознак проведення інформаційно-психологічної операції Російської Федерації в Автономній Республіці Крим. Наука і техніка Повітряних Сил Збройних Сил України, (1), 35-37.
14. Пєвцов, Г. В., С. В. Залкин, and А. О. Феклістов. "Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері." Системи обробки інформації 2 (2011): 57-59.
15. Петрик В.М., Новицька Н.Б., Кудирко В.М. Дезінформування як засіб ведення інформаційної війни російської федерації проти України // Ірпінський юридичний часопис : науковий журнал / редкол. : В. В. Топчій (голов. ред.) та ін. – Ірпінь : Університет державної фіскальної служби України, 2022. – Випуск 1 (8). – С. 118-130.
16. О.Бакалинський, О.Бакалінська, Правове забезпечення кібербезпеки в Україні, 2019, Журнал Entrepreneurship, Economy and Law, Стор.100-108.
17. Ryabchuk N., Grishko N., Rudenko A., Petryk V., Bapiyev I. and Fedushko S. Artificial intelligence technologies using in social engineering attacks, CEUR Workshop Proceedings, Vol. 2654, 2020, pp. 546-555.
18. Петрик В., Давидюк А. Система автоматизованого аналізування даних про терористичну діяльність з ресурсів мережі Інтернет // Information Technology and Security, vol. 7, iss. 1, January-June 2019, pp. 48-57.

Інтернет-ресурси

19. Stein G. J. AWC INFORMATION WARFARE [Electronic resource] / George J. Stein. – Режим доступу: http://www.airpower.maxwell.af.mil/airchronicles/apj/ apj95/spr95_files/stein.htm.
20. Szafranski R. Theory of Information Warfare: Preparing For 2020. Official Site of "Airpower Journal". URL: http://www.airpower.au.af.mil/airchronicles/ apj/apj95/spr95_files/szfran.htm.
21. Rethinking Warfare in the 21st Century The Influence and Effects of the Politics, Information and Communication Mix, pp. 20 – 57 Cambridge University Press, 2023, https://doi.org/10.1017/9781009355247.002[Opens in a new window].
22. Undermining Ukraine: How Russia widened its global information war in 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/
23. Російська інформаційна війна проти України, https://en.wikipedia.org/wiki/Russian_information_war_against_Ukraine
24. OSINT розвідка з відкритих джерел та інформаційна безпека, https://prometheus.org.ua/course/course-v1:Prometheus+OSINT101+2024_T3.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№ з/п	Назва практичної роботи	Кількість ауд. годин
1	2	3
	Розділ 1. Вступ до дисципліни.	
1	***Лекція 1. Інформаційні війни. Інформаційна безпека держави.*** *Визначення та задачі ІВ. Об'єкти посягань та складові ІВ. Філософські аспекти інформаційної безпеки держави, суспільства та громадянина.* *Навчальні матеріали та ресурси:* *Основні – 1, 2,3, 4, 7, 8* *Додаткові – 9, 10, 11,12* *Інтернет-ресурси – 21* *Самостійна робота:* *Підготовка до практичної роботи.*	2
2	***Лекція 2. Інформаційно-психологічний вплив. Спеціальні інформаційні операції та акції інформаційного впливу.*** *Об'єкти впливу. Методи впливу. Спрямування та мета впливу. Алгоритм проведення спеціальної інформаційної операції. Ознаки проведення СІО.* *Навчальні матеріали та ресурси:* *Основні – 1, 2, 3, 4, 5, 7* *Додаткові – 11, 12, 13* *Інтернет-ресурси – 24* *Самостійна робота: Підготовка до практичної роботи.*	2
	Розділ 2. Особливості сучасного періоду інформаційно-психологічного протиборства.	
3	***Лекція 3. Глобальне інформаційне протиборство нового типу, інформаційна зброя в сучасних умовах.*** *Філософія проведення інформаційного протиборства в технічній та психологічній складовій. Пошук інформації, спотворення та знищення інформації, впливи на інформаційні системи.* *Навчальні матеріали та ресурси:* *Основні – 3, 4, 5, 7,* *Додаткові – 14, 15, 16, 17* *Інтернет-ресурси – 20, 22,23* *Самостійна робота:* *Підготовка до практичної роботи.*	2
4	***Лекція 4. Засоби масової комунікації: маніпулятивні техніки ведення інформаційних війн.*** *Характеристика інформаційно-психологічного впливу через засоби масової комунікації: етапи, моделі, принципи. Тренди розвитку засобів масової комунікації як підґрунтя інформаційно-психологічного протиборства. Аудиторія, тиражі й рейтинги засобів масової комунікації. Засоби масової комунікації: маніпулятивні техніки ведення інформаційно-психологічного протиборства.*	2

	Навчальні матеріали та ресурси: *Основні – 8* *Додаткові – 17, 18* *Інтернет-ресурси – 19, 20, 22, 23* *Самостійна робота:* *Підготовка до практичної роботи.*	
	Разом	**8/2**

Практичні заняття

№ з/п	Назва практичної роботи	Кількість ауд. годин
1	2	3
1	***Практична робота 1****. Особливості забезпечення інформаційної безпеки в епоху глобалізації.* *Література: 1, 2, 3, 7, 11, 15, 20.*	2
2	***Практична робота 2.*** *Пошук та аналіз сучасних інформаційних операцій з використанням ЗМІ та соціальних мереж.* *Література: 3, 4, 7, 8, 14, 15.*	2
3	***Практична робота 3****.Аналіз філософії проведення найвідоміших інформаційних операцій періоду 2014-2019 років.* *Література: 1, 4, 12, 10, 15.*	2
4	***Практична робота 4.*** *Дослідження особливостей розвитку інформаційно-психологічного протиборства в історичній ретроспективі від Середньовіччя до часів «холодної війни».* *Література: 2, 4, 7, 11, 15.*	2
5	***Практична робота 5.*** *Аналіз сучасних ЗМІ, пошук та аналіз комплексних гібридних впливів на прикладі подій січня – лютого 2022 року* *Література: 6, 9, 16, 17.*	2
	Разом	**10/2**

6. Самостійна робота аспіранта

№ з/п	Назви тем і питань, що виноситься на самостійне опрацювання та посилання на навчальну літературу	Кількість годин СРС
1	2	2
1	*Теорія інформаційних війн [21]*	2
2	*Особливості проведення агітації на виборах президента України 2004, 2019 року [2,3]*	2
3	*Планування проведення СІО [2, 4, 7, 11, 15]*	2
4	*Кібербезпека, як складова гібридних впливів в рамках проведення СІО [17,18, 24]*	2
5	*Робота зі ЗМІ, через ЗМІ, соціальні мережі [15, 21,22, 23]*	2
6	*OSINT розвідка з відкритих джерел та інформаційна безпека [24]*	30
	Разом	**42/65**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Відвідування лекцій переконливо рекомендується, але штрафних санкцій за пропуски лекцій не передбачено. Відвідування занять комп'ютерного практикуму необхідно в обсязі, достатньому для виконання вимог викладача щодо виконання і своєчасної здачі практичних робіт та індивідуального завдання.

Пропущені контрольні заходи

Практичні роботи можна здавати у відведений за розкладом час як до, так і після встановленого терміну здачі практичної роботи. Додаткові години для здачі індивідуального завдання призначаються викладачем в межах часу практичних занять. За відсутності поважних причин пропуску (медична довідка тощо) штрафні бали не нараховуються.

Процедура оскарження результатів контрольних заходів

Аспіранти мають можливість підняти будь-яке питання, яке стосується процедури контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: виконані практичні роботи захищаються у відведений за розкладом час.

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

Семестровий контроль: залік.

Умови допуску до семестрового контролю: мінімально позитивна оцінка за індивідуальне завдання /зарахування усіх практичних робіт/семестровий рейтинг більше 30 балів.

Рейтинг аспіранта з дисципліни складається з двох складових: стартової – призначена для оцінювання заходів поточного контролю впродовж семестру та екзаменаційної – призначена для оцінювання окремих запитань (завдань) на екзамені і формується з балів, що він отримує за:

1) поточний контроль;

2) виконання індивідуальних завдань для самостійної роботи;

3) відповідь на екзамені.

1. Практичні заняття

Ваговий бал – 10 за кожну практичну роботу. Максимальна кількість балів на всіх практичних заняттях дорівнює 10*5= 50 балів.

2. Індивідуальне завдання

Кожний аспірант виконує індивідуальні завдання для самостійної роботи, яке передбачає використання всього матеріалу, що вивчається в рамках курсу. Ваговий бал – 25 за всю самостійну роботу загалом.

3. Відповідь на заліку

Кількість балів по відповіді на кожне питання визначається викладачем з врахуванням складності питання та якості відповіді. Максимальна кількість балів 25.

Штрафні та заохочувальні бали:

– за виконання завдань із удосконалення дидактичних матеріалів з дисципліни надається від 2 до 5 заохочувальних балів.

Розрахунок шкали (R) рейтингу

Сума вагових балів контрольних заходів протягом семестру складає:

RC = 50 + 25 + 25 = 100 балів

Для отримання аспірантом відповідних оцінок (ECTS та традиційних) його рейтингова оцінка *R* переводиться згідно з таблицею відповідності рейтингових балів оцінкам за університетською шкалою.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

1. Існує можливість зарахування сертифікатів проходження дистанційних чи онлайн курсів за тематикою дисципліни «Філософія інформаційної війни».

2. Застосовуються стратегії активного і колективного навчання, які визначаються наступними методами і технологіями:

– кредитно-модульна технологія навчання;

– особистісно-орієнтовані (розвиваючі) технології, засновані на активних формах і методах навчання («аналіз ситуацій», ділові, імітаційні ігри, дискусія, експрес-конференція, навчальні дебати);

– інформаційно-комунікаційні технології, що забезпечують проблемно-дослідницький характер процесу навчання та активізацію самостійної роботи аспірантів (електронні презентації для лекційних занять, використання аудіо- та відео-підтримки навчальних занять, розробка і застосування на основі комп'ютерних і мультимедійних засобів творчих завдань, доповнення традиційних навчальних занять засобами взаємодії на основі мережевих комунікаційних можливостей).

Робочу програму навчальної дисципліни (силабус):

Складено: к.т.н., ст.дослідником Бакалинським Олександром Олеговичем

Ухвалено: : Вченою радою ІПМЕ ім. Г.Є. Пухова НАН України (протокол №10 від 26 вересня 2024р.)