ФІЛОСОФСЬКІ ТА МЕТОДОЛОГІЧНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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	*Вибіркова*
Форма навчання	*очна (денна)*
Рік підготовки, семестр	*2 курс, осінній семестр*
Обсяг дисципліни	*2 кредити (60 годин), в т.ч. лекції - 8 годин, практичні – 10 годин*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *д.т.н., ст. досл. Зубок Віталій Юрійович,контактні дані:* vitalii.zubok@pimee.ua Практичні : *д.т.н., ст. досл. Зубок Віталій Юрійович,контактні дані:* vitalii.zubok@pimee.ua
Розміщення курсу	Посилання на дистанційний ресурс: https://classroom.google.com/ генерується на початку семестру

Програма навчальної дисципліни

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

В останні роки чітко фіксуються дезорганізуючі та дисфункціональні тенденції, що безпосередньо пов'язані з високою швидкістю зміни інформації. Традиційна практика інформаційної безпеки та захисту від інформації ускладнюється у зв'язку з розвитком віртуальної соціальної реальності кіберпростору. Сучасні комунікаційні процеси призводять до надмірності інформації та посилюють «розрив» між віртуальним та реальним світами, що впливає на зростання умовностей мережевих практик інформаційної безпеки. Надлишок інформації низької якості, що спостерігається на даному етапі розвитку інформаційного суспільства, не є єдиною проблемою інформаційної безпеки. До таких питань належить і проблема формування відповідного рівня інформаційної культури, який запобігав би виникненню у неї стресових ситуацій при роботі з інформацією та інформаційними технологіями.

Дисципліна «Філософські та методологічні проблеми теорії інформаційної безпеки» (ІІВ2) є нормативною дисципліною навчального плану підготовки докторів філософії з спеціальності «Комп'ютерні науки» і грає важливу роль у підготовці фахівців.

Завдання дисципліни:

– ознайомити здобувачів із визначенням, класифікацією та характеристиками інформаційної

безпеки;
- вивчити організаційні та економічні аспекти роботи з інформаційними ресурсами і методи оцінки їхньої безпеки;
- надати уявлення про особливості інформаційної безпеки, сегменти та учасників інформаційного ринку, а також про формування безпеки інформації;
- розглянути основні технологічні принципи захисту світових інформаційних ресурсів на базі глобальної мережі Інтернет;
- дослідити можливості застосування заходів захисту для інформаційних ресурсів у кіберпросторі.

Кінцевою метою дисципліни є формування розуміння сучасних тенденцій в галузі інформаційних технологій та їхніх бізнес-можливостей, а також основних загроз.

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

ЗК 01 Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 04 Здатність розв'язувати комплексні проблеми комп'ютерних наук на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.

СК 05 Здатність здійснювати науково-педагогічну діяльність у вищій освіті у сфері комп'ютерних наук

СК 06 Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку комп'ютерних наук та інформаційних технологій

ПРН 01 Мати передові концептуальні та методологічні знання з комп'ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.

ПРН 07 Розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми комп'ютерної науки з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.

ПРН 08 Визначати актуальні наукові та практичні проблеми у сфері комп'ютерних наук, глибоко розуміти загальні принципи та методи комп'ютерних наук, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері комп'ютерних наук та у викладацькій практиці.

ПРН 09 Вивчати, узагальнювати та впроваджувати в навчальний процес інновації комп'ютерних наук.

ПРН 11 Організовувати і здійснювати освітній процес у сфері комп'ютерних наук, його наукове, навчально-методичне та нормативне забезпечення, застосувати ефективні методики викладання навчальних дисциплін

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

Пререквізитами даної дисципліни є:

- пов'язані навчальні дисципліни «Сучасні проблеми і тенденції розвитку комп'ютерних наук та інформаційних технологій»;

– знання, отримані на попередніх рівнях вищої освіти.

Постреквізити: Перелік напрямків діяльності, що забезпечуються: науково-технічні публікації за результатами виконаних досліджень, підготовка та захист дисертаційної роботи.

3. Зміст навчальної дисципліни

Тема 1. Загальні поняття і проблеми теорії інформаційної безпеки.

Основні визначення інформації
Термінологія сучасних документів
Інформаційна безпека в цифровому світі
Інформаційна безпека в аспекті інформаційного протиборства

Тема 2. Суб'єкти, об'єкти та моделі інформаційної безпеки.

види політик ІБ
оцінки поточного стану ІБ
оцінювання захищеності як ефективності політик ІБ
моделі ІБ та захищеність від інформаційних впливів

Тема 3. Класифікування порушників та загроз.

Класифікування та оцінювання порушників
Популярні моделі загроз
Проблеми традиційного підходу до моделювання загроз

Тема 4. Соціальні та психологічні аспекти кібербезпеки.

Інформаційні впливи та інформаційні війни
Інформаційно-технічна та інформаційно-психологічна боротьба
Теорія інформаційної безпеки та захист об’єктів інформаційно-психологічної боротьби

4. Навчальні матеріали та ресурси

Базові

1. Закон України «Про основні засади забезпечення кібербезпеки України». – К.: Відомості Верховної Ради. – 2017. – № 45. – с.403.
2. Рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". – Введено в дію Указом Президента України №447/2021.
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – Наказ ДСТСЗІ СБУ від 28.04.99 № 22.
4. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. – Наказ ДСТСЗІ СБУ від 28.04.99 (зі змінами).
5. Грайворонський М.В., Новіков О.М. «Безпека інформаційно-комунікаційних систем». — К.:БХВ. – 2009.

Додаткові

6. В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. - К.: Інтертехнологія, 2009. - 164 с. ISBN 978-966-1648-12-7
7. А.Г. Додонов, Д.В. Ландэ, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Грайворонская. Распознавание информационных операций: Монография. - К.: Инжиниринг, 2017. - 282 с. ISBN 978-966-2344-60-8

Навчальний контент

5. Методика опанування навчальної дисципліни(освітнього компонента)

Лекційні заняття

№ з/п	Назва практичної роботи	Кількість ауд. годин
1	2	3
1	**Лекція 1. Загальні поняття і проблеми теорії інформаційної безпеки.** – Основні визначення інформації – Термінологія сучасних документів – Інформаційна безпека в цифровому світі – Інформаційна безпека в аспекті інформаційного протиборства Література: [1,2,7]	2
2	**Лекція 2. Суб'єкти, об'єкти та моделі інформаційної безпеки.** – види політик ІБ – оцінки поточного стану ІБ – оцінювання захищеності як ефективності політик ІБ – моделі ІБ та захищеність від інформаційних впливів Література: [1,4,5]	2
3	**Лекція 3. Класифікування порушників та загроз.** – Класифікування та оцінювання порушників – Популярні моделі загроз – Проблеми традиційного підходу до моделювання загроз Література: [4,5,7]	2
4	**Лекція 4. Соціальні та психологічні аспекти кібербезпеки.** – Інформаційні впливи та інформаційні війни – Інформаційно-технічна та інформаційно-психологічна боротьба – Теорія інформаційної безпеки та захист об'єктів інформаційно-психологічної боротьби Література: [6,7]	2
	Разом	**8**

Практичні заняття

№ з/п	Назва практичної роботи	Кількість ауд. годин
1	2	3
1	***Практичне заняття 1.*** Інформаційна безпека, комп'ютерна безпека, кібербезпека. Кейс-стаді.	2
2	***Практичне заняття 2.*** Побудова моделі інформаційної безпеки для захисту від інформаційного впливу. *Література: [2-4].*	2
3	***Практичне заняття 3.*** Аналіз захищеності від інформаційних впливів за допомогою моделей загроз. Кейс-стаді.	2
4	***Практичне заняття 4.*** Аналіз ефективності технічних засобів для запобігання розповсюдженню	2

	відкритої інформації. *Література: [2,6,7]*	
5	***Практичне заняття 5.*** Узагальнення навчальних результатів та підведення підсумків курсу. Відповіді на тестові запитання. *Література: [1-6]*	2
	Разом	**10**

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**	**3**
1	Соціально-психологічні аспекти цифрової резильєнтності	12
2	Роль цифрової грамотності в інформаційному протиборстві	8
3	Вивчення світового досвіду з інтернет-цензури	14
4	Індивідуальне завдання. Написання есею за тематикою дисципліни.	8
	Разом	**42**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Відвідування лекцій переконливо рекомендується, але штрафних санкцій за пропуски лекцій не передбачено. Відвідування практичних занять 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 практичних занять, як до, так і після встановленого терміну здачі конкретної роботи. Додаткові години для здачі індивідуального завдання призначаються викладачем в межах часу практичних занять. Практичні завдання, виконані та здані по-за межами відведених годин, можуть бути оцінені з нижчим балом (до 1 балу). За наявності поважних причин пропуску (медична довідка тощо) штрафні балине нараховуються.

Процедура оскарження результатів контрольних заходів

Здобувачі 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: не передбачений у зв'язку з короткою тривалістю курсу.

Семестровий контроль: залік з оцінкою.

Умови допуску до семестрового контролю: успішність протягом семестру не нижче 60%.

Рейтинг здобувача з дисципліни формується з балів, що він отримує за:

1) виконання завдань на практичних заняттях;

2) індивідуальне завдання

1. Індивідуальне завдання

Ваговий бал – 25. Кожний здобувач виконує індивідуальне завдання щодо написання есею за темою дисципліни.

2. Робота на практичних заняттях

Ваговий бал – 15. Максимальна кількість балів на всіх практичних заняттях дорівнює 5*15= 75 балів.

Штрафні та заохочувальні бали за:

- виконання завдань із удосконалення дидактичних матеріалів з дисципліни надається від 1 до 5 заохочувальних балів.

Розрахунок шкали (R) рейтингу

Сума вагових балів контрольних заходів протягом семестру складає:

RC = 75 + 25 = 100 балів.

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 «Філософські та методологічні проблеми інформаційної безпеки».

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: д.т.н., ст.досл. Зубком Віталієм Юрійовичем

Ухвалено: : Вченою радою ІПМЕ ім. Г.Є. Пухова НАН України (протокол №10 від 26.09.2024 р.)