Галицький фаховий коледж імені В'ячеслава Чорновола

юридичне відділення

назва відділення

Циклова комісія ***журналістики***

повна назва циклової комісії

ЗАТВЕРДЖУЮ
Заступник директора
з навчальної, наукової
роботи та міжнародного
співробітництва
_____ Ірина Гелецька
«__30__» «____09____» 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕДІАБЕЗПЕКА

назва навчальної дисципліни

НАЙМЕНУВАННЯ ПОКАЗНИКІВ	ГАЛУЗЬ ЗНАНЬ, СПЕЦІАЛЬНІСТЬ, ОСВІТНІЙ РІВЕНЬ	ХАРАКТЕРИСТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	
		денна форма навчання	**заочна форма навчання**
Кількість кредитів ECTS – 3 **Загальна кількість годин** – 90 год.	**Галузь знань –** 06 Журналістика **Спеціальність –** 061 Журналістика **Освітня програма –** Видавнича справа та медіакомунікації **Освітній рівень:** перший (бакалаврський)	**Обов'язкова** (нормативна) **Мова викладання**: українська	
Кількість змістових модулів – 2		**Рік підготовки (семестр):**	
Тижневих годин для денної форми навчання: **аудиторних** – 2/2		3-й (5-й)	1-й (1-й)
		Лекції:	
		18	12
		Практичні, семінарські:	
		14	4
		Самостійна робота:	
		58	74
		Вид підсумкового контролю: залік	

Розробник:

Фінклер Юрій Едуардович, викладач циклової комісії журналістики, доктор філологічних наук, професор, (*buibabu@meta.ua)*

РЕКОМЕНДОВАНО:

Цикловою комісією журналістики
Протокол № 1 від 30.08.2022 р.

Голова ЦК
_____ Г. Б. Вищневська

ПОГОДЖЕНО:

Гарант освітньо-професійної програми
_____Ю.Е. Фінклер

ПОГОДЖЕНО:

Завідувач відділення
_____М.Д. Денисовський

ВСТУП

Курс є елементом такого напряму сучасної комунікативістики як національна інформаційна безпека. Курс було розроблено з прицілом на усталені й новітні якісні та кількісні механізми, методики, інструменти аналізу інформаційної безпеки України та країн Європейського Союзу і НАТО. Методологічною основою курсу є комунікаційні постбіхевіоралізм та неоінституціоналізм. У науковому та навчальному плані курс використаний як механізм диверсифікації та поглиблення (звуження) сфери наукового і практичного контент- аналізу.

Курс розділено на два змістові модулі:

1. Теоретико-методологічні засади дослідження інформаційної війни.
2. Інформаційна безпека України.

Метою викладання навчальної дисципліни «Медіабезпека» є формування у майбутніх медіапрацівників розуміння сутності явища інформаційна війна, інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки держави.

Завдання курсу.

1. З'ясувати роль інформаційно-психологічних операцій в інформаційному просторі України в контексті гарантування інформаційної безпеки як складової національної безпеки держави. Ознайомити студентів з методами агресії проти розуму/інтелекту, що стало можливим завдяки «розвитку засобів масової комунікації і вдосконалення технологій психологічного впливу на індивідуальну і масову свідомість. За допомогою спеціальних психотехнологій здійснюються цілеспрямовані зміни масової свідомості з метою закладання певної інформації (від комерційної до світоглядної). За мету можуть ставитися також зміни культурної і навіть етнічної самоідентифікації великих груп людей для включення їх у психокультуру агресора або для досягнення інших цілей.
2. Розкрити ознаки феномена «медіабезпека», прищепити у студентів навики самостійного аналізу загроз інформаційній безпеці держави.
3. Сформувати навики виокремлення тенденцій, які властиві сучасним загрозам інформаційній безпеці у соціальних медіях.
4. Визначити напрями і можливості вдосконалення системи забезпечення інформаційної безпеки України.

Об'єктом навчальної дисципліни «Медіабезпека» є визначення методами агресії, що стало можливим завдяки розвитку засобів масової комунікації і вдосконалення технологій психологічного впливу на індивідуальну і масову свідомість.

Предметом навчальної дисципліни «Медіабезпека» є спеціальні психотехнології, які здійснюються для цілеспрямованої зміни масової свідомості з метою закладання певної інформації (від комерційної до світоглядної)..

У результаті вивчення навчальної дисципліни студент повинен

знати:

- специфіку відмінностей між пропагандою та інформаційною війною, ментальною агресією та психологічною війною у контексті функціонування

соціально-політичної системи;

•роль і значення інформаційно-психологічних операцій в інформаційному просторі України в контексті гарантування інформаційної безпеки як складової національної безпеки держави;

•класичні вияви психологічної війни - тотальне пересмикування фактів, маніпулювання свідомостю телеглядачів, слухачів і читачів тощо;

•методи, які впливають на зміну етнокультурної само ідентифікації;

основні ознаки інформаційної безпеки;

•загрози інформаційній безпеці та їх різновиди;

•методики оцінювання загроз інформаційній безпеці у соціальних Інтернет-сервісах;

• особливості інформаційно-психологічного протиборства у XX – на початку XXI ст.;

• інститути й інструменти забезпечення інформаційної безпеки України;

• причини та методи ведення інформаційної війни Російської Федерації проти України;

• стандарти Європейського Союзу та НАТО у сфері інформаційної безпеки;

вміти:

- формувати громадську думку;
- застосовувати прийоми, процедури і технології маніпулятивного впливу з метою захисту інформаційного простору держави;
- розрізняти інформаційні війни в політиці;
- належним чином оперувати такими поняттями як “інформація”, “знання”, “інформаційне суспільство”;
- користуватися знанням підходів до визначення інформаційної безпеки;
- розуміти проблематику і специфіку загроз інформаційній безпеці;
- знати основні різновиди загроз інформаційній безпеці;
- розрізняти основні напрями і можливості вдосконалення системи забезпечення інформаційної безпеки на національному і міжнародному рівнях, її проблемні аспекти;
- виявляти причини інформаційних воєн;
- оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та воєн.

У результаті вивчення навчальної дисципліни студент повинен набути таких компетентностей:

Загальні компетентності:

ЗК04. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК05. Навички використання інформаційних і комунікаційних технологій.

ЗК07. Здатність працювати в команді.

ЗК08. Здатність навчатися і оволодівати сучасними знаннями.

ЗК09. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та

необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Спеціальні (фахові, предметні) компетентності:

СК06. Здатність до провадження безпечної медіадіяльності.

СК07. Здатність володіти технологіями цифрової безпеки.

СК09. Здатність застосовувати технології медіа-аналізу в умовах інформаційних війн.

Після вивчення дисципліни студенти повинні показати такі **результати навчання:**

ПР04 Виконувати пошук, оброблення та аналіз інформації з різних джерел.

ПР05 Використовувати сучасні інформаційні й комунікаційні технології та спеціалізоване програмне забезпечення для вирішення професійних завдань.

ПР07 Координувати виконання особистого завдання із завданнями колег.

ПР08 Виокремлювати у виробничих ситуаціях факти, події, відомості, процеси, про які бракує знань, і розкривати способи та джерела здобування тих знань.

ПР09 Оцінювати діяльність колег як носіїв прав і обов'язків членів суспільства, представників громадянського суспільства.

ПР18 Використовувати необхідні знання й технології для виходу з кризових комунікаційний ситуацій на засадах толерантності, діалогу й співробітництва.

ПР19 Застосовувати знання технологій цифрової безпеки для створення якісного медіа продукту.

ПР21 Застосовувати знання в своїй професійній діяльності.

Матриця компетентностей та програмних результатів навчання, які формуються під час вивчення навчальної дисципліни «Медіабезпека» відповідно до освітньо-професійної програми «Видавнича справа та медіакомунікації»

Шифр компетентності	Компетентності	Шифр програмних результатів	Програмні результати навчання
Загальні компетентності (ЗК)			
ЗК 04	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	**ПР04**	Виконувати пошук, оброблення та аналіз інформації з різних джерел
ЗК 05	Навички використання інформаційних і комунікаційних технологій.	**ПР05**	Використовувати сучасні інформаційні й комунікаційні технології та спеціалізоване програмне забезпечення для вирішення професійних завдань.
ЗК 07	Здатність працювати в команді.	**ПР07**	Координувати виконання особистого завдання із завданнями колег.
ЗК 08	Здатність навчатися і оволодівати сучасними знаннями.	**ПР08**	Виокремлювати у виробничих ситуаціях факти, події, відомості, процеси, про які бракує знань, і розкривати способи та джерела здобування тих знань.
ЗК 09	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	**ПР09**	Оцінювати діяльність колег як носіїв прав і обов'язків членів суспільства, представників громадянського суспільства.
Спеціальні (фахові) компетентності (СК)			
СК06	Здатність застосовувати знання зі сфери соціальних комунікацій у своїй професійній діяльності.	**ПР18**	Використовувати необхідні знання й технології для виходу з кризових комунікаційний ситуацій на засадах толерантності, діалогу й співробітництва.
СК07	Здатність організовувати й контролювати командну професійну діяльність.	**ПР19**	Застосовувати знання технологій цифрової безпеки для створення якісного медіапродукту.
СК09	Здатність застосовувати технології медіа-аналізу в умовах інформаційних війн.	**ПР21**	Застосовувати знання в своїй професійній діяльності

Матриця відповідності компетентностей результатам навчання за дисципліною «Медіабезпека»

Компетентності		Результати навчання			
		Знання	**Уміння**	**Комунікація**	**Автономність та відповідальність**
ЗК04.	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.		ПР04 Виконувати пошук, оброблення та аналіз інформації з різних джерел		
ЗК05.	Навички використання інформаційних і комунікаційних технологій.		ПР 05 Використовувати сучасні інформаційні й комунікаційні технології та спеціалізоване програмне забезпечення для вирішення професійних завдань.		
ЗК07.	Здатність працювати в команді.			ПР 07 Координувати виконання особистого завдання із завданнями колег.	
ЗК08.	Здатність навчатися і оволодівати сучасними знаннями.				ПР 08 Виокремлювати у виробничих ситуаціях факти, події, відомості, процеси, про які бракує знань, і розкривати способи та джерела здобування тих знань.
ЗК09	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і				ПР 09 Оцінювати діяльність колег як носіїв прав і обов'язків членів суспільства, представників громадянського суспільства.

	громадянина в Україні.				
Спеціальні (фахові) компетентності (СК)					
СК06.	Здатність застосовувати знання зі сфери соціальних комунікацій у своїй професійній діяльності.	ПР 18 Використовувати необхідні знання й технології для виходу з кризових комунікаційний ситуацій на засадах толерантності, діалогу й співробітництва.			
СК07.	Здатність організовувати й контролювати командну професійну діяльність.		ПР 19 Застосовувати знання зі сфери предметної спеціалізації для створення інформаційного продукту .		
СК09.	Здатність застосовувати технології медіа-аналізу в умовах інформаційних війн.				ПР 21 Застосовувати знання в своїй професійній діяльності

1. ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	Денна форма навчання				Заочна форма навчання			
	всього	у тому числі			всього	у тому числі		
		л	с	с. р.		л	с	с. р.
Змістовий модуль І ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ								
Тема 1. Інформація в житті людини. Інформаційний вплив та інформаційні війни.	6	2	2	2	12	2		10
Тема 2. Типи інформаційної війни.	9	2		7	12	2		10
Тема 3. Специфіка ведення інформаційної війни. Електронна війна — війна третього тисячоліття	11	2	2	7	12	2		10
Тема 4. Національна безпека в умовах інформаційної війни	9	2		7	12	2		10
Змістовий модуль ІІ ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ								
Тема 5. Інформаційна безпека: підходи до концептуалізації та індикатори визначення.	11	2	2	7	14	2	2	10
Тема 6. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах.	11	2	2	7	12	2		10
Тема 7. Теорія і практика інформаційно-психологічного протиборства у XX – на початку XXI ст.	11	2	2	7	10			10
Тема 8. Інститути й інструменти забезпечення інформаційної безпеки України.	11	2	2	7	4			4
Тема 9. Загрози інформаційній безпеці України.	11	2	2	7	2		2	
Всього	**90**	**18**	**14**	**58**	**90**	**12**	**4**	**74**

2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МЕДІАБЕЗПЕКА» за темами

Змістовий модуль 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ.

Тема 1. Інформація в житті людини. Інформаційний вплив та інформаційні війни.

Визначення поняття «інформація». Інформаційне середовище. Інформація явища. Порогові й безпорогові явища. Вплив інформаційного поля життєвого середовища людини. Найважливіші властивості розумної системи: сприйняття, збереження та обробка інформації. Сприйняття інформації — певна зміна системи під тим чи іншим впливом. Поняття інформаційного ресурсу, інформаційного простору та інформаційного суверенітету. Поняття інформаційного впливу. Інформаційні технології як засіб інформаційного впливу. Цілі та завдання інформаційно-психологічного впливу. Інформаційний вплив на моральну та духовну стійкість супротивника, вплив на його психіку. Інформаційна складова: актуальність, своєчасність, достовірність, якість, обсяг. Інформаційна протидія. Поняття інформаційної війни. Інформаційні війни в історії.

Тема 2. Типи інформаційної війни.

Основи ведення інформаційної війни. Інформаційна війна — складова частина ідеологічної боротьби. Політичні інформаційні війни: головна мета — дискредитація і деморалізація політичного опонента. Типові тактики та стратегії. Мета інформаційної війни. Чинники інформаційної війни. Психологія інформаційної війни.

Тема 3. Специфіка ведення інформаційної війни. Електронна війна — війна третього тисячоліття.

Інформаційні війни в сучасному соціально-політичному вимірі. Технології проведення інформаційних операцій. Основні принципи, завдання, цілі та методи геополітичного стратегічного аналізу та прогнозування. Глобальні інформаційні мережі. Сучасна світова/регіональна політика та Інтернет. Особливості інформаційно-психологічного впливу через Інтернет.

Комп’ютерні інформаційні технології як невід’ємна частина озброєння сучасних армій, принципово важливий компонент, від якого залежить діяльність багатьох військових структур і чим при нагоді може скористатися супротивник.

Тема 4. Національна безпека в умовах інформаційної війни.

Інформаційні потоки в політико-соціальних системах. Деформація механізмів збору розсіяної інформації. Поняття "національна безпека". Види безпеки: державна, економічна, суспільна, військова, екологічна, інформаційна.

Взаємозв'язок інформаційної та інших видів безпеки. Основні види загроз національній безпеці: загрози інформаційній інфраструктурі, загрози безпеці інформації, загрози духовному життю суспільства, загрози правам і свободам громадян. Інформаційна безпека як складова національної безпеки. Зовнішні і внутрішні загрози інформаційній безпеці: типи і класи загроз, джерела, засоби реалізації загроз та їхні наслідки. Роль держави в забезпеченні інформаційної безпеки країни. Українська державність як об’єкт інформаційної агресії. Державна мова як важливий елемент національної безпеки країни. Методи запобігання і ліквідації загроз інформаційній безпеці держави. Поняття політики безпеки. Принципи побудови політики безпеки та її впровадження.

Змістовий модуль 2. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

Тема 5. Інформаційна безпека: підходи до концептуалізації та індикатори визначення.

Інформаційна сфера, інформаційна безпека, національна безпека, кібернетична безпека. Інформаційне суспільство. Підходи до дослідження інформаційної безпеки. Статичний, діяльнісний, комплексний підходи. Система забезпечення інформаційної безпеки. Національний інтерес, класифікація національних інтересів, національний інтерес в інформаційній сфері.

Тема 6. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах.

Поняття і різновиди загроз інформаційній безпеці. Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційний тероризм. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія. Інформаційно-психологічна протидія, контроль каналів передачі інформації, система моніторингу та прогнозування негативних інформаційно-психологічних впливів. Принципи інформаційної війни. Логіка інформаційної війни. Моделі інформаційної війни. Різновиди інформаційних воєн. Засоби, методи і технології інформаційних воєн. Механізми реагування на загрози інформаційній безпеці.

Тема 7. Теорія і практика інформаційно-психологічного протиборства у XX – на початку XXI ст.

Інформаційно-психологічне протиборство під час Першої світової війни та у міжвоєнний період (1919–1939). Інформаційно-психологічне протиборство в роки Другої світової війни (1939–1945). Інформаційно-психологічне протиборство в умовах «Холодної війни» (1946–1991). Специфіка глобального інформаційно- психологічного протиборства на початку XXI ст. Сучасні тренди розвитку засобів масової комунікації як основи інформаційно-психологічного протиборства. Маніпулятивні техніки ведення інформаційно-психологічного протиборства в сучасних умовах.

Тема 8. Інститути й інструменти забезпечення інформаційної безпеки України.

Правові засади організації системи інформаційної безпеки в Україні. Державна політика забезпечення інформаційної безпеки України. Інститути забезпечення інформаційної безпеки України. Механізми реагування на загрози інформаційній безпеці України. ЗМІ як інструмент інформаційної безпеки України. Громадські організації в контексті інформаційної безпеки України.

Тема 9. Загрози інформаційній безпеці України.

Різновиди загроз інформаційній безпеці України. Патерни інформаційних операцій Російської Федерації проти України. Інформаційна війна Російської Федерації проти України. Дипломатія України в контексті інформаційної війни Російської Федерації проти України. Інститути й інструменти забезпечення інформаційної безпеки Європейського Союзу. Нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки.

Тематика практичних, семінарських занять та самостійної роботи студентів визначені у тематичному плані дисципліни. Питання та завдання практичної та самостійної роботи студентів деталізовані у відповідних методичних вказівках.

3. ПОРЯДОК ПОТОЧНОГО ТА ПІДСУМКОВОГО ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ СТУДЕНТІВ

Оцінювання знань студентів з навчальної дисципліни здійснюється шляхом проведення контрольних заходів, які включають:

- *поточний контроль,*
- *модульний контроль,*

- *виконання індивідуального навчально-дослідного завдання.*

Поточний контроль здійснюється під час проведення практичних і семінарських занять і має на меті перевірку знань студентів з окремих тем та рівня їх підготовленості до виконання конкретної роботи.

Ключовими формами та методами демонстрації студентами результатів навчання при поточному контролі є:

- робота в малих групах - спільне опрацювання групою студентів окремих проблемних питань з наступною демонстрацією результатів та засвоєння навчального матеріалу;
- презентація - виступи перед аудиторією для висвітлення окремих питань, індивідуальних завдань, реферативних досліджень тощо;
- дискусія - обґрунтування власної позиції у вирішенні проблемних питань;
- кейс-метод - аналіз конкретних ситуацій, що дає змогу наблизити процес навчання до реальної практичної діяльності.

Результати поточного контролю за семестр визначаються як середня з усіх поточних оцінок за 100-бальною шкалою, відображених у журналах обліку відвідування та успішності академічної групи.

Модульний контроль проводиться з метою оцінки результатів навчання після закінчення логічно завершеної частини лекційних та практично-семінарських занять з певного змістового модуля.

Основною формою модульного контролю є завдання, які включають як і перевірку теоретичних положень курсу, так і розв'язування практичних завдань.

Оцінки з модульного контролю за 100-бальною шкалою відображаються у журналах обліку відвідування та успішності академічної групи і включаються як окремий заліковий модуль до залікового кредиту.

Індивідуальне навчально-дослідне завдання (ІНДЗ) – це форма організації навчання, яка має на меті поглиблення, узагальнення та закріплення знань, які студенти отримують у процесі навчання, а також застосування цих знань на практиці. Індивідуальні завдання виконують студенти самостійно і звичайно під керівництвом викладачів. Як правило, індивідуальні завдання виконуються окремо кожним студентом.

ІНДЗ є видом позааудиторної індивідуальної роботи студента навчального, навчально-дослідницького характеру, яке використовується в процесі вивчення програмного матеріалу навчальної дисципліни і завершується оцінюванням.

ІНДЗ – це завершена теоретична або практична робота в межах навчальної програми курсу, яка виконується на основі знань, вмінь і навичок, отриманих у процесі лекційних, семінарських занять, охоплює тему, декілька тем або зміст навчальної дисципліни вцілому.

У процесі відповіді виявляються наступні рівні знань: високий, добрий, посередній, недостатній.

Високий рівень знань: оцінка в межах від 90 до 100 балів. Ставиться за повні і правильні відповіді студента на усі запитання. При цьому необхідно, щоб студент умів логічно мислити, вільно використовувати набуті теоретичні

знання при аналізі проблем галузі, застосовувати знання з суміжних галузей журналістики та видавничої справи.

Добрий рівень знань оцінюється у межах 75 – 89 балів. Студент аргументовано викладає матеріал, висловлює свої міркування з приводу тих чи інших проблем, але припускається певних неточностей та похибок у логіці викладу теоретичного матеріалу. Він володіє базовими термінами, поняттями та категоріями з вказаної теми, але самостійно нездатний аналізувати матеріал, застосовувати їх в конкретній ситуації.

Посередній рівень знань оцінюється в межах 60 – 74 балів. Студент в основному знає матеріал теми, рекомендовану літературу, але непереконливо відповідає, плутає поняття, додаткові питання викликають невпевненість або відсутність стабільних знань, відповідаючи на запитання практичного характеру, виявляє неточності у знаннях, не вміє оцінювати факти та явища, пов'язувати їх із майбутнім фахом.

Недостатній рівень знань оцінюється в межах до 60 балів. Студент не опанував зміст теми, вкрай слабо знає рекомендовану літературу, не володіє базовими поняттями, термінами, категоріми. Відсутнє логічне та наукове мислення, практичними навичками не володіє.

ШКАЛА ОЦІНЮВАННЯ:

За шкалою коледжу	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (добре)
84-75		C (добре)
67–74	задовільно	D (задовільно)
60-66		E (задовільно)
35 – 59	незадовільно	FX (незадовільно з можливістю повторного складання)
0 – 34		F (незадовільно з обов’язковим повторним курсом)

Підсумкова оцінка за 100-бальною шкалою розраховується як середня у відповідності з ваговими коефіцієнтами, величина яких залежить від значення кожного з контрольних заходів, що проводяться під час вивчення навчальної дисципліни**.**

ТАБЛИЦЯ
розподілу балів за підсумковими контрольними заходами та відповідними ваговими коефіцієнтами

	Модуль 1 (поточне опитування)	**Модуль 2 (підс. мод. контроль)**	**Модуль 3 (ІНДЗ)**	**Підсумкова оцінка**
Вагові коефіцієнти, %	70	20	10	100
Розрахунок оцінки в балах	80	85	90	82

Приклад розрахунку підсумкової оцінки в балах:

О= 80*0,7+85*0,2+90*0,1=82

4. ОРГАНІЗАЦІЙНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Для якісного засвоєння курсу необхідна систематична та усвідомлена робота студентів в усіх видах навчальної діяльності: лекції, семінарські та практичні заняття, консультації, самостійна робота як індивідуальна, так і під керівництвом викладача.

При проведенні аудиторних занять домінуючими є лекційно-проблемні, індивідуально-диференційовані, особистісно-орієнтовані форми проведення занять та технології, спрямовані на організацію якісної освіти студента.

При проведенні практичних занять використовуються активні форми їх проведення: евристичні бесіди, дискусії, вправи.

Крім того, така робота повинна бути індивідуалізованою з врахуванням рівня творчих можливостей студента, його навчальних здобутків, інтересів, навчальної активності тощо.

Самостійна робота, зокрема, включає: вивчення теоретичних аспектів, насамперед на основі прослуханого лекційного матеріалу; поглиблене вивчення окремих питань передбачених тем (дослідження наукової літератури на задану тему та пошук додаткової інформації); підготовку до семінарських занять; узагальнення вивченого матеріалу перед поточним контролем тощо.

Склад методичного забезпечення дисципліни:

Аудиторна та самостійна робота студента забезпечується усіма необхідними навчально-методичними засобами задля належного вивчення навчальної дисципліни чи окремої її теми, а саме: робочою програмою навчальної дисципліни; силабусом; підручниками, навчальними та навчально-методичними посібниками, методичними рекомендаціями, конспектами лекцій, науковою літературою та періодичними виданнями, засобами поточного

контролю (завдання для підсумкових модульних робіт), завдання для виконання самостійної роботи та індивідуальних навчально-дослідних завдань.

Навчально-методичне забезпечення розміщено в електронному форматі в навчально-інформаційному середовищі коледжу на базі Moodle з відкритим доступом для студентів.

Інструменти, обладнання та комп'ютерне забезпечення

Електронні енциклопедії, довідники, мультимедійні засоби у вільному доступі в Інтернет, комп'ютерні презентації за темами курсу.

5. РЕКОМЕНДОВАНІ ІНФОРМАЦІЙНІ ДЖЕРЕЛА

Основні:

1. Барабаш О., Грищук Р., Молодецька-Гринчук К. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних Інтернет-сервісів. Наукоємні технології. 2018. № 2. С. 232–239.
2. Бєлоусова Н., Афанасьєва П. Основні вимоги НАТО щодо забезпеченння безпеки інформаційного простору. Актуальні проблеми міжнародних відносин. Вип. 102. Ч. І. 2011. С. 196–202.
3. Валюшко І. Дипломатія України у вимірі інформаційної безпеки країни. Вісник Львівського університету. Серія філос.-політолог. студії. 2017. Вип. 13. С. 137– 142.
4. Валюшко І. Еволюція інформаційних війн: минуле і сучасність. Історико- політичні студії. Збірник наукових праць. 2015. №2. С. 127–134.
5. Валюшко І. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2016. № 3/4 (31–32). С. 117–124.
6. Гнатюк С. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: Аналітична доповідь. К.: Нац. ін-т стратегічних досліджень, 2013. 51 с.
7. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.
8. Горбулін В., Качинський А. Засади національної безпеки України: підручник. К.: Інтертехнологія, 2009. 272 с.
9. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України: монографія. К., 2007. 592 с.
10. Грищук Р., Мамарєв В., Молодецька-Гринчук К. Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблоку Twitter). Інформаційні технології та комп'ютерна

інженерія. 2017. № 2. С. 12–19.

11. Грищук Р., Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. *Захист інформації.* 2017. Т. 19. № 4. С. 254–262.

12. Грищук Р., Молодецька-Гринчук К. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. *Сучасний захист інформації.* 2017. № 3. С. 86–96.

13. Дереко В. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С.16–22.

14. Дмитренко М. Спеціальні заходи впливу як механізм протистояння зовнішньополітичним впливам в інформаційних війнах. Збірник наукових праць Інституту Служби зовнішньої розвідки України. 2016. № 12. С. 21–37.

15. Дмитренко М. Спеціальні інформаційні впливи. Збірник наукових праць Інституту Служби зовнішньої розвідки України. 2014. № 8. С. 156–167.

16. Захаренко К. Глобальна природа інформаційної безпеки. Політологічний вісник. 2015. Вип. 79. С. 181–189.

17. Захаренко К. Держава як суб'єкт інформаційної безпеки суспільства. Гілея: науковий вісник. 2017. Вип. 124. С. 295–299.

18. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки. Мультиверсум. Філософський альманах. 2016. Вип. 1– 2. С. 58–70.

19. Захаренко К. Інформаційні впливи як джерела загострення інформаційної небезпеки. Науковий часопис НПУ імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2015. Вип. 34. С. 167–175.

20. Захаренко К. Категорія «інформаційної безпеки» у вітчизняному науковому дискурсі. Гуманітарний вісник державного вищого навчального закладу «Переяслав-Хмельницький державний педагогічний університет ім. Г. С. Сковороди». Філософія. 2015. Вип. 37. С. 106–117.

21. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія. 2017. Вип. 48 (1). С. 212–219.

22. Захаренко К. Проблеми формування ефективної державної інформаційної політики. Науковий часопис НПУ імені М. П. Драгоманова. Серія 7: Релігієзнавство. Культурологія. Філософія. 2016. Вип. 36. С. 202–209.

23. Зозуля О. Зарубіжний досвід державного управління забезпеченням інформаційної безпеки в умовах інформаційно-психологічного протиборства. *Науково-інформаційний вісник Академії національної безпеки.* 2016. № 1–2. С. 28–38.

24. Качинський А. Індикатори національної безпеки: визначення та застосування їх граничних значень. К.: НІСД, 2013. 104 с.

25. Куцька О. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України. Інформаційна безпека людини, суспільства, держави. 2017. № 1(21). С.180–190.

26. Левченко О. Система заходів протидії інформаційним операціям. Збірник наукових праць Харківського університету Повітряних Сил. 2016. Вип. 3. С. 57–60.

27. Левченко О. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату. *Наука і оборона*. 2013. № 3. С. 21–26.

28. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.

29. Ліпкан В. Національна безпека України: навчальний посібник. Київ: КНТ, 2009. 576 с.

30. Ліпкан В. Теоретико-методологічні засади управління у сфері національної безпеки України. К.: Видавництво Національної академії внутрішніх справ України, 2005. 350 с.

31. Молодецька-Гринчук К. Адаптація методів теорії динамічного хаосу для забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. *Вісник Житомирського національного агроекологічного університету*. 2017. № 2 (1). С. 180–187.

32. Молодецька-Гринчук К. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності. Управління розвитком складних систем. 2017. Вип. 30. С. 121–127.

33. Молодецька-Гринчук К. Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками. *Радіоелектроніка, інформатика, управління*. 2017. № 2. С. 117–126.

34. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз. *Вісник НАДУ*. № 3. 2013. С. 40–45.

35. Ніщименко О. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23.

36. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». 2012. Вип. 32. С. 20–27.

37. Панченко В. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. *Інформація і право*. 2014. № 3. С. 13–16.

38. Панченко В. Інформаційні операції в системі стратегічних комунікацій. *Стратегічні пріоритети. Серія: Політика*. 2016. № 4. С. 72–79.

39. Панченко В. Концептуальні вимоги до якості розвідувальної інформації в умовах суспільства знань. *Інформаційна безпека людини, суспільства, держави*. 2013. № 3. С. 6–11.

40. Пелещишин А., Гумінський Р. Загрози інформаційної безпеки держави в соціальних мережах. *Наука і техніка Повітряних Сил Збройних Сил України*. 2013. № 2. С. 192–199.

41. Пилипчук В. Інформаційна сфера як складова гібридної війни. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ: Нац. акад. СБУ, 2018. 408 с.

42. Пилипчук В. Реформування і розвиток Служби безпеки в контексті євроінтеграції України: Науково-методичний посібник. К.: Нац. акад. СБУ, 2017. 260 с.

43. Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.

44. Присяжнюк М. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету імені Тараса Шевченка. *Військово- спеціальні науки.* 2013. Вип. 30. С. 42–46.

45. Прозоров А. Ціннісні основи інформаційної безпеки особи, суспільства та держави. *Інформаційна безпека людини, суспільства, держави.* 2016. № 1 (20). С. 29–37.

46. Сасин Г. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). *Грані*. 2015. № 3. С. 18–23.

47. Сніцаренко П., Міхєєв Ю., Чернявський Г. Методичний підхід до оцінювання рівня інтенсивності деструктивного інформаційно-психологічного впливу на цільову аудиторію. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2016. Вип. 13. С. 12–19.

48. Сніцаренко П., Саричев Ю. Роль та місце інформаційного забезпечення в системі державного управління. *Державне управління: теорія та практика*. 2016. № 1. С. 46–56.

49. Сніцаренко П., Саричев Ю. Теоретичні підходи до визначення сутності інформаційного забезпечення в системі державного управління. *Науково- інформаційний вісник Академії національної безпеки*. 2016. № 1–2. С. 7–19.

50. Сопілко І. Інформаційні загрози та безпека сучасного українського суспільства. *Юридичний вісник.* 2015. № 1 (34). С. 75–80.

51. Ткачук Т. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. *Наук. вісник УжНУ. Серія: Право.* 2017. № 46. Т. 2.

С. 39–43.

52. Ткачук Т. Захист національних інформаційних ресурсів як пріоритетна складова інформаційної політики держави в умовах глобалізації. Розвиток України в 21 ст.: економічні, соціальні, екологічні, гуманітарні та правові проблеми: мат. міжнарод. наук.-практ. конф. (Тернопіль, 30 березня 2012 р.). С. 209–212.

53. Ткачук Т. Інформаційний чинник у гібридній війні. Кібербезпека у системі нац. безпеки України: пріоритетні напрями розвитку: мат. наук. круглого столу (Маріуполь, 26 квітня 2018 р.). МДУ, 2018. С. 39–42.

54. Ткачук Т. Кібербезпека: підходи до визначення в окремих країнах. Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, 24 травня 2017 р.). 2017. С. 142–144.

55. Ткачук Т. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. Теоретико-правові основи формування та розвитку інформаційного суспільства: мат. наук.-практ. конф. (Київ, 29 листопада 2017 р.). 2017. С. 111–114.

56. Чекаленко Л. Національна безпека України: система реалізації. *Зовнішні справи.* 2016. № 11. С. 17–19.

57. Штельмах О. Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. Актуальні проблеми управління державною безпекою: зб. Матер.наук.-практ. Конф (Київ, 19 березня 2015 р.). К.: Центр навч., наук. та період. видань НА СБ України, 2015. С. 393–396.

Допоміжні:

1. Дмитренко М. Зовнішньополітичні впливи як пріоритети діяльності зовнішньої розвідки. *Збірник наукових праць Інституту Служби зовнішньої розвідки України.* 2013. № 5. С. 31−46.

2.Климчук О. Ткачук Н. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3 (19). С.75–83.

3.Коваленко Є., Плетньов О. Діяльність контррозвідувальних органів в державній системі забезпечення інформаційної безпеки: досвід країн НАТО та українські реалії. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право».* 2018. Вип. 26. С. 136–139.

4.Левченко О. Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел. *Системи обробки інформації*. 2016. Вип. 1 (138). С. 100–102.

5.Молодецька-Гринчук К. Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та

оцінювання їх рівня. *Системи обробки інформації.* 2017. Вип. 5. С. 122–129.

6.Пономаренко Л. Інноваційні підходи до попередження радикалізації настроїв і проявів екстремізму в контексті забезпечення сталого демократичного розвитку. *Інформаційна безпека людини, суспільства, держави.* 2017. № 1 (21). С. 74–81.

7.Снитко О. Проекти тотального зомбування в інформаційному просторі України. *Інформаційна безпека людини, суспільства, держави*. 2017. № 1 (21). С. 207– 215.

8.Ярема О. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ. Серія: Право*. 2016. № 2. С. 244–252.

9.Яцик Т. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2014. № 2. С. 55–60.

10. Rasmussen M. The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century. Cambridge: Cambridge University Press, 2007. 234 p.

Інформаційні ресурси:

1. Міністерство закордонних справ України: Офіційний веб-сайт.URL: https://mfa.gov.ua/ua (дата звернення: 26.08.2019).

2. Міністерство оборони України: Офіційний веб-сайт. URL: http://www.mil.gov.ua/ (дата звернення: 26.08.2019).

3. Офіційний портал Верховної Ради України. URL: https://rada.gov.ua/ (дата звернення: 26.08.2019).

4. Президент України. Офіційне інтернет-представництво. URL: https://www.president.gov.ua/ (дата звернення: 26.08.2019)

5. Рада національної безпеки і оборони України: Офіційний веб-сайт. URL: http://www.rnbo.gov.ua/ (дата звернення: 26.08.2019).

6. Служба безпеки України: Офіційний веб-сайт. URL: https://ssu.gov.ua/ (дата звернення: 26.08.2019).