Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»

Кафедра політичних наук і права

Т.О. Каменчук

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

щодо проведення практичної та самостійної роботи з курсу «Інформаційні та психологічні війни» (для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 05 «Соціальні та поведінкові науки» Спеціальність: 052 «Політологія», 281 «Публічне управління та адміністрування», денної та заочної форми навчання)

ОПП: Політологія.
Публічне управління та адміністрування

Спеціальність: 052 Політологія, 281 Публічне управління та адміністрування
Рівень вищої освіти: перший (бакалаврський)
Рік навчання: 4
Мова навчання: українська
Факультет: соціально-гуманітарний

Одеса – 2024

УДК: 3.073.1:342.72:[004+159](076)

Рекомендовано до друку науково-методичною комісією Державного закладу «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського. (Протокол № 6 від 05.01.2024 року).

Рецензенти:

Кокорєв О.В.- доктор політичних наук, завідувач кафедри міжнародних відносин, суспільних комунікацій та ІТ-права, ДЕРЖАВНОГО УНІВЕРСИТЕТУ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ ЯЗКУ.

Наумкіна С.М. – доктор політичних наук завідувач кафеди політичних наук і права, ДЕРЖАВНОГО ЗАКЛАДУ Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»

Методичні рекомендації Каменчук Т.О. щодо проведення практичних занять та самостійної роботи з курсу «**Інформаційні та психологічні війни» (для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 05 «Соціальні та поведінкові науки» Спеціальність: 052 «Політологія», 281 «Публічне управління та адміністрування», денної та заочної форми навчання)**» Одеса : Університет Ушинського, 2024 28 с.

Методичні рекомендації та поради укладені відповідно до Освітньо-професійних програм «**Інформаційні та психологічні війни» (для здобувачів четвертого (бакалаврського) рівня вищої освіти галузі знань 05 «Соціальні та поведінкові науки» Спеціальність: 052 «Політологія», 281 «Публічне управління та адміністрування**

Мета вивчення дисципліни – формування у здобувачів системи знань та цілісне уявлення про інформаційні та психологічні війни, їхню історію, особливості прояву в сучасному світі, загрози в інформаційній сфері та участі в цих процесах ЗМІ.

Очікувані результати вивчення дисципліни

У результаті вивчення навчальної дисципліни здобувач повинен:

знати:

- теоретичні основи дослідження інформаційних війн та психологічних операцій;
- основні принципи психологічних операцій та інформаційної війни;
- основні напрямки інформаційної війни;
- відмінні риси інформаційної війни різних країн;
- характеристики, особливості та властивості всіх існуючих видів інформаційної війни в сучасному світі;
- особливості 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 свідомістю телеглядачів, слухачів і читачів тощо.
- інструментарій інформаційно - психологічного впливу та протидії.

уміти:

- визначати специфіку кожного з видів інформаційної війни, з урахуванням правових, національних та інших особливостей;
- вивчати та формувати громадську думку;
- застосовувати прийоми, процедури і технології маніпулятивного впливу з метою захисту інформаційного простору держави.
- розрізняти інформаційні війни в політиці.
- розпізнати інформаційну атаку, інформаційну війну в професійній сфері, вміти їм протистояти;
- застосувати отримані знання в професійній діяльності, міжособистісному спілкуванні,
- визначати найважливіші правові засадт інформаційної війни;
- знаходити сильні і слабкі сторони ведення інформаційної війни;
- практично реалізувати теоретичний інструментарій при проведенні психологічних операцій та інформаційних кампаній;
- застосовувати отримані знання в галузі професійної діяльності;

Міждисциплінарні зв'язки: «Загальна теорія політики», «Політична психологія», «Прикладна політологія», «Національна безпека», «Міжнародні відносини», «Політична конфліктологія», «Технологія управління та урегулювання конфліктів», «Політичні комунікації та PR»

ВКАЗІВКИ ДО ОРГАНІЗАЦІЇ САМОСТІЙНОЇ РОБОТИ

Серед усіх видів навчальної роботи важливе місце належить самостійності у навчанні, тобто пошуку і відбору літератури, її опрацюванню, робота підготовка, доповідей, повідомлень, наукових статей тощо.

Самостійна робота над навчальним матеріалом є індивідуальним видом роботи на практични заняттях, передбачає виконання практичних завдань та контрольних робіт. Вона здійснюється відповідно до навчальних планів, навчальної і робочої програм з курсу.

Метою самостійної роботи є:

• забезпечення фундаментальної загальноосвітньої та практичної підготовки;

• засвоєння методів і навичок самостійного глибокого вивчення навчального матеріалу;

• підвищення ефективності навчального процесу за допомогою організації позааудиторного навчання відповідно до особистих здібностей;

• оволодіння культурою розумової праці, вмінням орієнтуватися у потоці наукової інформації, розвиток незалежності мислення, формування власного погляду на питання, що вивчаються.

Ефективність самоосвіти, яка є одним із основних методів навчання здобувачів, визначається постійністю, послідовністю і наполегливістю в роботі з навчальним матеріалом, здійсненням самоконтролю за систематичним засвоєнням знань, вмінням поєднати практичні навички з теорією.

Самостійна робота здобувачів заочної форми навчання починається після вступної лекції, на якій викладач дає рекомендації щодо методики самостійного опанування курсом.

Основними формами самостійної роботи є:

• робота з підручниками та посібниками;

• робота з науковою літературою;

• самостійне вивчення окремих тем і питань до семінарських та практичних занять на основі навчальної, монографічної літератури, документів, матеріалів, періодичних видань; • підготовка презентації;

• підготовка до консультації з викладачем;

• підготовка до заліку.

ТЕМАТИЧНИЙ ПЛАН дисципліни

«Інформаційні та психологічні війни»

№ з/п	Назва теми	Кількість годин
Змістовий модуль1. Теоретико-методологічні засади дослідження інформаційної війни. Теорія і практика інформаційно-психологічного протиборства		
1	Інформація в житті людини. Інформаційний вплив та інформаційні війни	9
2	Типи інформаційної війни	9
3	Специфіка ведення інформаційної війни. Електронна війна – війна третього тисячоліття	8
4	Національна безпека в умовах інформаційної війни	9
Змістовий модуль 2. Теоретико-методологічні засади дослідження інформаційно психологичної безпеки		
5	Інформаційно психологична безпека: підходи до концептуалізації та індикатори визначення	9
6.	. Загрози інформаційно психологтчної	9

	безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних інтернет-сервісах	
7	Теорія і практика інформаційно-психологічного протиборства у XX – на початку XXI ст	8
8	Інститути й інструменти забезпечення інформаційної безпеки України	9
	Всього	70

Змістовий модуль 1. Теоретико-методологічні засади дослідження інформаційної війни. Теорія і практика інформаційно-психологічного протиборства

Тема 1. Інформація в житті людини. Інформаційний вплив та інформаційні війни (9 год)

План

1. Поняття «інформація», «інформаційне середовище», «інформація явища».

2. Поняття «інформаційний ресурс», «інформаційний простір» та «інформаційний суверенітет».

3. Поняття «інформаційний вплив». Інформаційні технології як засіб інформаційного впливу.

4. Поняття «інформаційна протидія» та «інформаційна війна».

5. Інформаційні війни в історії людства.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Розкрийте зміст понять «інформація», «інформаційне середовище», «інформація явища».

2. З'ясуйте значення понять та наведіть приклади порогових і безпорогових явищ інформації.

3. Поясніть значення понять «інформаційний ресурс», «інформаційний простір» та «інформаційний суверенітет».

4. Проаналізуйте, як формується і яке має значення інформаційне поле життєвого середовища людини/суспільства.

5. Дайте визначення поняття «інформаційний вплив».

6. Поясніть, чому інформаційні технології вважають дієвим засобом інформаційного впливу.

7. Які цілі та завдання інформаційно-психологічного впливу на людину, суспільство, державу. Відповідь проілюструйте прикладами.

8. Поясніть, чи може інформаційний вплив спрямовуватися на моральну та духовну сфери людини чи суспільства, на індивідуальну чи колективну психіку. Відповідь обґрунтуйте.

9. Назвіть сучасні вимоги до інформаційна складової ефективного інформаційного впливу. Відповідь обґрунтуйте.

10. З'ясуйте значення понять «інформаційна протидія» та «інформаційна війна».

11. Поясніть сутність та витоки інформаційних воєн в історії людства.

12. Практичне завдання. Використовуючи медійні повідомлення, спираючись на власний досвід чи спостереження, продемонструйте, як на практиці реалізується інформаційний вплив між окремими людьми чи групами осіб.

Перелік літератури до вивчення теми:

1. .Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
2. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.
3. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
4. 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.
5. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. К. : КНТ, 2006. 280 с.
6. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». 2012.Вип. 32. С. 20–27.
7. Присяжнюк М. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету імені Тараса Шевченка. Військово- спеціальні науки. 2013. Вип. 30. С. 42–46.

Тема 2. Типи інформаційної війни (9 год)

План

1. Основи ведення інформаційної війни. Типологія інформаційних війн.

2. Політичні інформаційні війни.

3. Типові тактики та стратегії інформаційних війн.

4. Чинники інформаційної війни.

5. Психологічні аспекти інформаційної війни.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Вкажіть на основні принципи, засади та умови ведення сучасних інформаційних війн.

2. З'ясуйте типологію інформаційних війн.

3. Поясніть сутність та природу політичних інформаційних війн.

4. Прокоментуйте тезу: «Інформаційна війна – складова частина ідеологічної боротьби».

5. Розкажіть про типові тактики та стратегії інформаційних війн.

6. З'ясуйте мету та завдання інформаційних війн різних типів.

7. Якими методами досягається головна мета політичних інформаційних війн – дискредитація і деморалізація політичного опонента. Відповідь аргументуйте прикладами.

8. Окресліть чинники інформаційної війни.

9. Обґрунтуйте зміст поняття «інформаційно-психологічний вплив».

10. Вкажіть на психологічні аспекти інформаційної війни.

11. Практичне завдання. Змоделюйте інформаційні війни різних типів. Проаналізуйте перебіг інформаційних війн за схемою: причини передумови – привід – мета – завдання – ресурси(засоби) – тактика стратегія – результати – наслідки.

Перелік літератури до вивчення теми:

1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
2. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.
3. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
4. 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.
5. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. К. : КНТ, 2006. 280 с.
6. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45.
7. Пилипчук В. Реформування і розвиток Служби безпеки в контексті євроінтеграції України : науково-методичний посібник. К. : Нац. акад. СБУ, 2017. 260 с.

Тема 3. Специфіка ведення інформаційної війни. Електронна війна – війна третього тисячоліття (8 год)

План

1. Інформаційні війни в сучасному соціально-політичному вимірі.

2. Технології проведення інформаційних операцій.

3. Основні принципи, завдання, цілі та методи геополітичного стратегічного аналізу та прогнозування.

4. Сучасна світова/регіональна політика та Інтернет. Особливості інформаційно-психологічного впливу через Інтернет.

5. Комп’ютерні інформаційні технології як невід’ємна частина озброєння сучасних армій.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Поясніть специфіку інформаційних війн у сучасному соціальнополітичному вимірі.

2. З’ясуйте значення поняття «технологія інформаційного впливу».

3. Схарактеризуйте технології проведення інформаційних операцій.

4. З’ясуйте основні принципи, завдання, цілі і методи геополітичного стратегічного аналізу та прогнозування.

5. Яким чином глобальні інформаційні мережі пов’язані з явищем інформаційних війн? Відповідь обґрунтуйте.

6. Поясніть зв'язок сучасної світової/регіональної політики та мережі «Інтернет».

7. У чому полягають особливості інформаційно-психологічного впливу через мережу «Інтернет». Вкажіть на переваги і недоліки такого впливу.

8. Прокоментуйте тезу: «Комп’ютерні інформаційні технології – невід’ємна частина озброєння сучасних армій».

9. Аргументуйте значення сучасних комп’ютерних інформаційних технологій для забезпечення ефективного функціонування органів державної влади та діяльності військових структур.

10. Практичне завдання. На підставі обраних і проаналізованих медійних повідомлень поясніть механізм реалізації технології інформаційного впливу.

Для виконання завдання використайте насамперед приклади (кейси), пов’язані з явищем глобальних інформаційних мереж.

Перелік літератури до вивчення теми:

1. Валюшко І. Кібербезпека України: наукові та практичні виміри сучасності. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2016. № 3/4 (31–32). С. 117–124.
2. Гнатюк С. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: Аналітична доповідь. К. : Нац. ін-тстратегічних досліджень, 2013. 51 с.
3. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
4. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.

5. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
6. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. К. : КНТ, 2006. 280 с.
7. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45.
8. Ніщименко О. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.
9. Сасин Г. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). Грані. 2015. № 3. С. 18–23. 25
10. Сопілко І. Інформаційні загрози та безпека сучасного українського суспільства. Юридичний вісник. 2015. № 1 (34). С. 75–80.

Тема 4. Національна безпека в умовах інформаційної війни (9 год)

План

1. Інформаційні потоки в політико-соціальних системах.

2. Поняття «національна безпека». Види безпеки.

3. Основні види загроз національній безпеці.

4. Інформаційна безпека як складова національної безпеки.

5. Роль держави в забезпеченні інформаційної безпеки країни.

6. Українська державність як об’єкт інформаційної агресії.

7. Державна мова як важливий елемент національної безпеки країни.

8. Типи і класи загроз інформаційній безпеці.

9. Методи запобігання і ліквідації загроз інформаційній безпеці держави.

10. Поняття «політика безпеки». Принципи побудови політики безпеки та її впровадження.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Поясніть, як функціонують інформаційні потоки в політико-соціальних системах. Доберіть приклади з медіасфери.

2. Вкажіть, у чому полягає явище деформації механізмів збору розсіяної інформації.

3. З’ясуйте значення поняття «національна безпека».

4. Схарактеризуйте види безпеки.

5. Проаналізуйте такі види безпеки: державна, економічна, суспільна, військова, екологічна, інформаційна. Доберіть приклади з медіа сфери.

6. Вкажіть на основні види загроз національній безпеці.

7. Поясніть значення поняття «інформаційна безпека».

8. Обґрунтуйте взаємозв'язок інформаційної та інших видів безпеки.

9. Доберіть з медіа приклади різних типів загроз: загрози інформаційній інфраструктурі, загрози безпеці інформації, загрози духовному життю суспільства, загрози правам і свободам громадян.

10. Прокоментуйте тезу: «Інформаційна безпека є складовою національної безпеки».

11. У чому полягає роль держави в забезпеченні інформаційної безпеки країни?

12. Теза для аналізу й обговорення «Українська державність як об’єкт інформаційної агресії».

13. Поясніть, чому державна мова є важливим елементом національної безпеки України.

14. Схарактеризуйте типи і класи загроз інформаційній безпеці.

15. Доберіть з медіа приклади зовнішніх і внутрішніх загроз інформаційній безпеці, різних типів і класів загроз, джерел, засобів реалізації, можливих і реальних наслідків загроз.

16. Проаналізуйте методи запобігання і ліквідації загроз інформаційній безпеці держави.

17. Розкрийте зміст поняття «політика безпеки».

18. Розкрийте принципи побудови політики безпеки та засоби її впровадження.

19. Практичне завдання. Підготуйтеся до дискусії на тему «Українська державність як об'єкт інформаційної агресії». Доберіть аргументи, які підтверджують чи спростовують цю тезу. Підготуйте усний тезовий виступ (5-6 аргументів) або тематичну мультимедійну презентацію (5-6 слайдів) на запропоновану тему.

Перелік літератури до вивчення теми:

1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
2. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.
3. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
4. Качинський А. Індикатори національної безпеки: визначення та застосування їхграничних значень. К. : НІСД, 2013. 104 с.
5. Левченко О. Система заходів протидії інформаційним операціям. Збірник наукових праць Харківського університету Повітряних Сил. 2016. Вип. 3. С. 57–60.
6. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. К. : КНТ, 2006. 280 с.
7. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45.
8. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». 2012.Вип. 32. С. 20–27.
9. Сніцаренко П., Саричев Ю. Роль та місце інформаційного забезпечення в системі державного управління. Державне управління: теорія та практика. 2016. № 1. С. 46–56.
10. 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.
11. Чекаленко Л. Національна безпека України: система реалізації. Зовнішні справи. 2016. № 11. С. 17–19.

Змістовий модуль 2. Теоретико-методологічні засади дослідження інформаційної безпеки

Тема 5. Інформаційна безпека: підходи до концептуалізації та індикатори визначення (9 год)

План

1. Інформаційна безпека в добу інформаційного суспільства. Кібернетична безпека.

2. Підходи до дослідження інформаційної безпеки.

3. Система забезпечення інформаційної безпеки.

4. Поняття «національний інтерес». Класифікація національних інтересів,

5. Національний інтерес в інформаційній сфері.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Вкажіть на специфічні риси інформаційної безпеки в добу інформаційного суспільства.

2. З'ясуйте значення поняття «кібернетична безпека».

3. Схарактеризуйте та порівняйте статичний, діяльнісний і комплексний підходи до дослідження інформаційної безпеки.

4. З яких компонентів складається і як практично функціонує система забезпечення інформаційної безпеки?

5. Розкрийте зміст поняття «національний інтерес».

6. Дайте класифікацію національних інтересів,

7. Обґрунтуйте національний інтерес в інформаційній сфері.

8. Практичне завдання. Складіть опорну схему до теми «Система інформаційної безпеки України».

Виконане завдання представте у формі усного виступу чи мультимедійної презентації.

Перелік літератури до вивчення теми:

1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
2. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.
3. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
4. 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.
5. Грищук Р., Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. Сучасний захист інформації. 2017. Т. 19. № 4. С. 254– 262.
6. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник. К. : КНТ, 2006. 280 с.
7. 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.
8. Молодецька-Гринчук К. Аналіз впливу загроз інформаційній безпеці держави у соціальних інтернет-сервісах на сфери суспільної діяльності. Управліннярозвитком складних систем. 2017. Вип. 30. С. 121– 127.
9. Сніцаренко П., Саричев Ю. Роль та місце інформаційного забезпечення в системі державного управління. Державне управління: теорія та практика. 2016. № 1. С. 46–56.
10. 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.
11. Чекаленко Л. Національна безпека України: система реалізації. Зовнішні справи. 2016. № 11. С. 17–19.

Тема 6. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних інтернет-сервісах (9 год)

План

1. Поняття «інформаційне протиборство», «інформаційна експансія», «інформаційна війна», «інформаційний тероризм».

2. Поняття «інформаційна акція», «інформаційна атака», «інформаційна операція», «інформаційна кампанія».

3. Форми та способи інформаційної протидії негативним інформаційним впливам.

4. Механізми реагування на загрози інформаційній безпеці.

5. Принципи інформаційної війни.

6. Логіка інформаційної війни.

7. Моделі інформаційної війни.

8. Різновиди інформаційних воєн. Засоби, методи і технології інформаційних воєн.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Поясніть зміст понять «інформаційне протиборство», «інформаційна експансія», «інформаційна війна», «інформаційний тероризм». Доберіть історичні або актуальні приклади для обґрунтування відповіді.

2. Дайте визначення поняттям «інформаційна акція», «інформаційна атака», «інформаційна операція», «інформаційна кампанія». Відповідь проілюструйте історичними або сучасними прикладами.

3. Розкрийте зміст понять «інформаційно-психологічна протидія», «контроль каналів передачі інформації», «система моніторингу та прогнозування негативних інформаційно-психологічних впливів».

4. З’ясуйте принципи інформаційної війни.

5. Поясніть логіку та закономірності ведення інформаційної війни.

6. Що таке «моделі інформаційної війни». Як і з якою метою відбувається моделювання інформаційних війн?

7. Які існують різновиди інформаційних війн?

8. Поясніть, які засоби, методи і технології застосовуються під час проведення інформаційних війн.

9. Вкажіть на реальні механізми реагування на загрози інформаційній безпеці.

10. Практичне завдання. Змоделюйте окрему інформаційну акцію чи цілісну інформаційну кампанію, спрямовану на 1) протидію негативним інформаційним впливам і на захист національних інтересів в інформаційній сфері та 2) на завдання негативного інформаційнопсихологічного впливу (шкоди) країні-противнику (реальному чи уявному агресору) й на зміцнення позицій країни в інформаційній війні.

Перелік літератури до вивчення теми:

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. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
3. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.
4. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
5. Левченко О. Система заходів протидії інформаційним операціям. Збірник наукових праць Харківського університету Повітряних Сил. 2016. Вип. 3. С. 57–60.
6. 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.
7. 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.
8. Сопілко І. Інформаційні загрози та безпека сучасного українського суспільства. Юридичний вісник. 2015. № 1 (34). С. 75–80.

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

Тема 7. Теорія і практика інформаційно-психологічного протиборства у XX – на початку XXI ст. (8 год)

План

1. Інформаційно-психологічне протиборство у XX – XXI ст.: періодизація, технології, історичне значення, глобальні наслідки.

2. Інформаційно-психологічне протиборство під час Першої світової війни та у міжвоєнний період (1919–1939).

3. Інформаційно-психологічне протиборство в роки Другої світової війни (1939–1945).

4. Інформаційно-психологічне протиборство в умовах Холодної війни (1946–1991).

5. Специфіка глобального інформаційно-психологічного протиборства на початку XXI ст.

6. Сучасний стан і провідні тенденції інформаційно-психологічного протиборства у світі.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Проаналізуйте періодизацію, технології, історичне значення та глобальні насідки інформаційно-психологічне протиборства у XX – XXI ст.

2. Прокоментуйте основні етапи та специфічні риси інформаційнопсихологічного протиборства під час Першої світової війни та у міжвоєнний період (1919–1939).

3. Поясніть сутність конфліктів, позиції учасників та технологічну складову інформаційно-психологічного протиборства в роки Другої світової війни (1939–1945).

4. Схарактеризуйте природу та засоби інформаційно-психологічного протиборства в умовах Холодної війни (1946–1991).

5. Назвіть основні конфлікти, учасників і специфіку глобального інформаційно-психологічного протиборства на початку XXI ст.

6. Схарактеризуйте сучасний стан і провідні тенденції інформаційнопсихологічного протиборства у світі.

7. Вкажіть на сучасні тренди розвитку засобів масової комунікації як основи інформаційно-психологічного протиборства у XXI ст.

8. Поясніть сутність поняття «інформаційні маніпуляції».

9. Як працюють маніпулятивні технології ведення інформаційнопсихологічного протиборства в сучасних умовах. Відповідь ілюструйте прикладами з медіасфери.

10. Практичне завдання. Підготуйте приклади з історії XX ст. та сучасного стану інформаційно-психологічного протиборства у світі, в яких активно застосовувалися інформаційні маніпуляції та маніпулятивні техніки.

Перелік літератури до вивчення теми:

1. Валюшко І. Еволюція інформаційних війн: минуле і сучасність. Історико- політичні студії. Збірник наукових праць. 2015. №2. С. 127–134.
2. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
3. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.
4. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
5. 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.
6. 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.
7. Левченко О. Система заходів протидії інформаційним операціям. Збірник наукових праць Харківського університету Повітряних Сил. 2016. Вип. 3. С. 57–60.

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

9. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико- методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45.
10. Ніщименко О. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.
11. Сопілко І. Інформаційні загрози та безпека сучасного українського суспільства. Юридичний вісник. 2015. № 1 (34). С. 75–80.
12. Чекаленко Л. Національна безпека України: система реалізації. Зовнішні справи. 2016. № 11. С. 17–19.

Тема 8. Інститути й інструменти забезпечення інформаційної безпеки України (9 год)

План

1. Правові засади організації системи інформаційної безпеки в Україні.

2. Державна політика забезпечення інформаційної безпеки України.

3. Інститути забезпечення інформаційної безпеки України.

4. Механізми реагування на загрози інформаційній безпеці України.

5. ЗМІ як інструмент інформаційної безпеки України.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Проаналізуйте правові засади організації системи інформаційної безпеки в Україні.

2. Схарактеризуйте основні принципи та засади державної політики забезпечення інформаційної безпеки України.

3. Назвіть провідні інститути забезпечення інформаційної безпеки України. Оцініть ефективність діяльності цих інститутів.

4. Поясніть, як практично діють правові та інституційні механізми реагування на загрози інформаційній безпеці України.

5. Прокоментуйте тезу: «ЗМІ є інструментом інформаційної безпеки України».

6. Обґрунтуйте роль, яку відіграють громадські організації (спілки, товариства, НУО) в посиленні інформаційної безпеки України.

7. Практичне завдання. Підготуйтеся до експертного «круглого столу» на тему «Роль ЗМІ в утвердженні та зміцненні інформаційної безпеки України». Оберіть одне медіа за видом (радіо, ТБ, паперове чи електронне видання). Здійсніть вибірковий аналіз (моніторинг) контенту медій за один 18 день (один номер для пресового видання) з позицій забезпечення інформаційної безпеки України. Результати дослідження представте у формі усного виступу чи мультимедійної презентації.

Перелік літератури до вивчення теми:

1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К. : Інтертехнологія, 2009. 164 с.
2. Горбулін В., Качинський А. Засади національної безпеки України : підручник.К. : Інтертехнологія, 2009. 272 с.
3. Горбулін В., Качинський А. Системно-концептуальні засади стратегії національної безпеки України : монографія. К., 2007. 592 с.
4. 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.
5. Захаренко К. Глобальна природа інформаційної безпеки. Політологічний вісник. 2015. Вип. 79. С. 181–189.
6. Захаренко К. Держава як суб'єкт інформаційної безпеки суспільства. Гілея: науковий вісник. 2017. Вип. 124. С. 295–299.
7. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки. Мультиверсум. Філософський альманах. 2016. Вип. 1–2. С. 58–70.
8. 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.
9. Ткачук Т. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Наук. вісник УжНУ. Серія: Право. 2017. № 46. Т. 2. С. 39–43.
10. Чекаленко Л. Національна безпека України: система реалізації. Зовнішні справи. 2016. № 11. С. 17–19.

Теми презентацій

1. Відповідальність за розміщення недостовірної інформації на вебресурсі
2. Строки позовної давності для звернень з питань спростування недостовірної інформації
3. Способи фіксації доказів та інформації, розміщеної в Інтернеті
4. Проблеми надання нотаріусам права здійснювати нотаріальне посвідчення витягів з веб-сайтів.
5. Актуальність вивчення інформаційного права в сучасних умовах глобалізації
6. Предмет, об'єкт та структура інформаційного права як галузі права
7. Основні цілі та функції інформаційного права
8. Теоретико-методологічні засади та концептуальні підходи до визначення інформаційного права Термінолого-понятійний інструмент інформаційного права як галузі права
9. Інформаційна цивілізація
10. Процеси інформатизації у сучасному світі
11. Роль та призначення ІТ-права
12. Характеристика структури ІТ-права та Інформаційного права
13. Інформаційний кодекс: «за» та «проти»
14. Джерела інформаційного права
15. Податкові пільги для суб'єктів індустрії програмної продукції
16. Інформаційні правовідносини
17. Предмет і об'єкти інформаційних правовідносин
18. Суб'єкти інформаційних правовідносин
19. Відкриття ІТ-компанії в Україні
20. Юридичні особливості відкриття ІТ-бізнесу в Україні
21. Найпоширеніші моделі структурування ІТ-бізнесу в Україні
22. Порядок Висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні
23. Забезпечення права на приватність при використанні інформації
24. Правовий статус друкованих ЗМІ
25. Суб'єкти видавничої справи
26. Бібліотечна справа, архівний фонд
27. Положення про не конкуренцію та його чинність за законодавством України
28. Юридичні механізми захисту новацій, ноу-хау, комерційних таємниць компаній
29. Укладення з працівниками компанії договір про неконкуренцію
30. Конфіденційність та способи захисту комерційної таємниці
31. Доведення розголошення конфіденційної інформації