Міністерство освіти і науки України
Національний університет водного господарства та природокористування

Навчально-науковий інститут економіки та менеджменту
Кафедра журналістики та українознавства

06-10-58М

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних завдань та самостійної роботи
з навчальної дисципліни
«Інформаційна безпека та інформаційна війна»
для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Журналістика» спеціальності 061 «Журналістика» денної форми навчання

Рекомендовано радою з якості ННІЕМ
Протокол № 3
від 22 листопада 2021 року

Рівне – 2021

Методичні вказівки до виконання практичних завдань та самостійної роботи з навчальної дисципліни **«Інформаційна безпека та інформаційна війна»** для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Журналістика» спеціальності 061 «Журналістика» денної форми навчання [Електронне видання] / Фінклер Ю. Е., Крупка О. В. - Рівне : НУВГП, 2021. – 28 с.

Укладачі: Фінклер Ю. Е., доктор філологічних наук, професор кафедри журналістики та українознавства; Крупка О. В., кандидат історичних наук, доцент кафедри журналістики та українознавства.

Відповідальна за випуск – Малевич Л. Д., кандидатка філологічних наук, доцентка, завідувачка кафедри журналістики та українознавства.

Керівник групи забезпечення – Супрун В. М., доктор філологічних наук, професор кафедри журналістики та українознавства.

Передмова

«Інформаційна безпека та інформаційна війна» – навчальна дисципліна вибіркового блоку, що вивчається студентами четвертого року навчання спеціальності «журналістика». Курс розрахований на 120 навчальних годин. Структура годин курсу: лекційні заняття – 22 год., практичні заняття – 20 год., самостійні завдання – 78 год.

Навчальний курс є складовою сучасної комунікативістики, зокрема розділу про теоретичні та практичні аспекти глобальної та національної інформаційної безпеки. Зміст дисципліни розроблено на основі узагальнення досвіду усталених новітніх практик ефективного аналізу і забезпечення інформаційної безпеки України, а також провідних постіндустріальних держав світу, зокрема країн Європейського Союзу і НАТО.

Методологічною основою курсу є комунікаційні теорії постбіхевіоризму та неоінституціоналізму. У науковому і навчальному плані курс адаптовано як прикладна методологія, а також механізм диверсифікації та поглиблення сфери теоретичного і практичного контент-аналізу.

Предметом вивчення дисципліни є новітні практики, механізми, методики, інструменти аналізу інформаційної безпеки України та країн Європейського Союзу і НАТО.

Мета вивчення дисципліни – сформувати у студентів розуміння природи та сутності сучасних інформаційних явищ – інформаційної війни, інформаційної безпеки; ознайомити здобувачів освіти з основними загрозами глобальній і національній інформаційній безпеці; на основі сучасних знань з теорії глобальної комунікативістики виробити практичні

вміння самостійно застосовувати методики критичного аналізу ефективності забезпечення інформаційної безпеки держави.

Курс розділено на два змістові модулі:

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

2. Інформаційна безпека України. Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки.

Основні завдання вивчення дисципліни:

- 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;
- опанувати понятійно-категоріальний апарат сучасної комунікативістики, зокрема у сфері глобальної та національної інформаційної безпеки («інформаційна протидія», «інформаційна безпека», «інформаційна агресія», «інформаційна війна» тощо);
- формувати у студентів навички самостійного аналізу загроз інформаційній безпеці держави, вміння виокремлювати тенденції, які властиві сучасним загрозам інформаційній безпеці у соціальних медіях, уміння визначати напрями і можливості вдосконалення системи забезпечення національної інформаційної безпеки України.

У процесі викладання курсу передбачено формування таких **компетентностей:**

а) загальних: здатність до абстрактного мислення, аналізу та синтезу, пошуку та опрацювання інформації з різних джерел; здатність усно й

писемно спілкуватися українською мовою як державною в усіх сферах суспільного життя; здатність здобувати знання й розуміти площину їхнього застосування в професійній діяльності; здатність до адаптації та дії в новій ситуації й організації безпечної діяльності; знання правових та морально-етичних аспектів діяльності, а також професійних кодексів поведінки (ЗК);

б) спеціальних (фахових): здатність надавати аргументовану експертну оцінку щодо можливостей та реальних випадків використання патогенної інформації для здійснення деструктивних впливів на свідомість і психіку людей; здатність до визначення та розробки стратегічних пріоритетів в галузі інформаційної безпеки України, розпізнавати найбільш поширені маніпулятивні стратегії інформаційних воєн; виявлення основних тенденцій формування сучасного інформаційного простору, зокрема впливів на його зміст, форму та обсяг процесів глобалізації; виявляти уміння розпізнавати найбільш поширені маніпулятивні стратегії деструктивних інформаційних і гібридних воєн, об’єктивно висвітлювати події в зоні конфліктів; виявляти вміння безпечно працювати в екстремальних умовах (ФК).

У процесі викладання курсу передбачено досягнення таких **програмних результатів навчання:**

дотримуватися принципів і правил безпечної діяльності; виокремлювати у виробничих ситуаціях факти, події, інформаційні процеси, про які бракує знань і які не вдається відтворити, що викликає необхідність у самоосвіті та професійному вдосконаленні; виявляти кризові стани суспільства, певної соціальної групи та окремої особистості, розкриваючи їх причини й прогнозуючи наслідки, шукати адекватні способи виходу з них (ПРН).

Міждисциплінарні зв’язки. Навчальна дисципліна «Інформаційна

безпека та інформаційна війна» є складовою частиною циклу дисциплін професійної (фахової) підготовки студентів за спеціальністю 061 «Журналістика». Її вивчення пов'язане з вивченням курсів «Безпека життєдіяльності та цивільний захист», «Інформаційна журналістика», «Фотожурналістика», «Теорія соціальних комунікацій», «Види журналістики за проблематикою», «Теле-, радіожурналістика», «Теорія масової комунікації».

Вимоги до знань та умінь студентів визначаються «Стандартом вищої освіти для першого (бакалаврського) рівня вищої освіти спеціальності 061 «Журналістика» (Київ, 2019).

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 (2 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. Для обґрунтування послуговуйтеся понятійно-категоріальним апаратом теми 1.

Література (*Тут і далі вказано номери джерел у списку рекомендованої літератури). [7, 8, 9, 14, 28, 37, 45]

Тема 2. Типи інформаційної війни (2 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.

Література [7, 8, 9, 14, 28, 35, 43]

Тема 3. Специфіка ведення інформаційної війни. Електронна війна – війна третього тисячоліття (2 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 соціально-політичному 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.

Література [5, 6, 7, 8, 9, 28, 35, 36, 47, 51]

Тема 4. Національна безпека в умовах інформаційної війни (4 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.

Література [7, 8, 9, 24, 26, 28, 35, 37, 49, 50, 57]

Змістовий модуль 2.
Теоретико-методологічні засади дослідження інформаційної безпеки

Тема 5. Інформаційна безпека: підходи до концептуалізації та індикатори визначення (2 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.

Література [7, 8, 9, 10, 11, 28, 31, 32, 49, 54, 57]

Тема 6. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних інтернет-сервісах (2 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 інформаційно-психологічного впливу (шкоди) країні-противнику (реальному чи уявному агресору) й на зміцнення позицій країни в інформаційній війні.

Література [1, 7, 8, 9, 26, 31, 42, 51, 57]

Тема 7. Теорія і практика інформаційно-психологічного протиборства у XX – на початку XXI ст. (2 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 інформаційно-психологічного 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 інформаційно-психологічного 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 інформаційно-психологічного 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.

Література [4, 7, 8, 9, 19, 25, 26, 33, 35, 36, 51, 57]

Тема 8. Інститути й інструменти забезпечення інформаційної безпеки України (2 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

день (один номер для пресового видання) з позицій забезпечення інформаційної безпеки України. Результати дослідження представте у формі усного виступу чи мультимедійної презентації.

Література [7, 8, 9, 10, 16, 17, 18, 25, 52, 57]

Тема 9. Загрози інформаційній безпеці України (4 год)

План

1. Різновиди загроз інформаційній безпеці України.
2. Інформаційна війна Російської Федерації проти України.
3. Дипломатія України в контексті інформаційної війни Російської Федерації проти України.
4. Інститути й інструменти забезпечення інформаційної безпеки Європейського Союзу.
5. Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки.
6. Нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки.

Запитання для актуалізації знань та завдання для самостійної роботи

1. Вкажіть на різновиди загроз інформаційній безпеці України.
2. Обґрунтуйте тезу «Російської Федерації веде інформаційну війну проти України». Відповідь проілюструйте прикладами з українських, російських та інших медій.
3. Проаналізуйте основні патерни інформаційних операцій Російської Федерації проти України.
4. Поясніть роль, яку виконує дипломатія України в контексті протидії інформаційній війни Російської Федерації проти України.
5. Схарактеризуйте діяльність інститутів та ефективність інструментів забезпечення інформаційної безпеки Європейського Союзу.

6. Назвіть стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки.
7. Проаналізуйте нормативно-правові акти ЄС у сфері забезпечення інформаційної безпеки.
8. Практичне завдання. Готуємося до командної рольової гри на тему «Засідання РНБО України з актуальних питань інформаційної політики та забезпечення належної інформаційної безпеки України (2021-2031)». Учасники виступають з доповідями про сучасний стан та поточні й імовірні загрози інформаційній безпеці України (російський, білоруський кейси, європейські напрямки політики, гуманітарна політика, освіта, ЗМІ тощо). Також доповідачі висловлюють та обґрунтовують пропозиції щодо ефективної протидії загрозам інформаційній безпеці та застосування дієвих заходів для зміцнення національних інтересів в інформаційній сфері. У підсумку формується стратегічний документ про пріоритети інформаційної політики у визначений термін, який ухвалюється в режимі поіменного голосування учасниками засідання.

Література [1, 2, 3, 23, 25, 28, 51, 58]

Рекомендована література

Основна література

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-тстратегічних 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. *Сучасний 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 їхграничних 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. Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. *Автоматизация технологических и бизнес-процессов*. 2017. Вип. 9. № 2. С. 36–42.

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

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

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

38. Панченко В. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. *Інформація і право*. 2014.

№ 3. С. 13–16.

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

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

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

42. 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.

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

44. Почепцов Г. Сучасні інформаційні війни. К. : Вид. дім «Києво-Могилянськаакадемія», 2015. 497 с.

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

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

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

48. 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.

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

50. 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.

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

52. Ткачук Т. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. *Наук. вісник УжНУ.* Серія: Право. 2017. № 46. Т. 2. С. 39–43.

53. 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.

54. 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.

55. 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.

56. 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.

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

58. 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.

Додаткова література

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.

Інтернет-ресурси

1. Міністерство закордонних справ України: Офіційний вебсайт. URL: https://mfa.gov.ua/ (дата звернення: 24.09.2021).
2. Міністерство оборони України: Офіційний вебсайт. URL: https: https://www.mil.gov.ua/ (дата звернення: 24.09.2021).
3. Офіційний портал Верховної Ради України. URL: https://rada.gov.ua/ (дата звернення: 24.09.2021).
4. Президент України. Офіційне інтернет-представництво. URL: https://www.president.gov.ua/ (дата звернення: 24.09.2021).
5. Рада національної безпеки і оборони України: Офіційний вебсайт. URL: https://www.rnbo.gov.ua/ (дата звернення: 24.09.2021).
6. Служба безпеки України: Офіційний вебсайт. URL: https://ssu.gov.ua/ (дата звернення: 24.09.2021).