СИЛАБУС КУРСУ

«Медіабезпека»

2022/2023 н. р.

Ступінь вищої освіти - **бакалавр**
Освітньо-професійна програма: «Видавнича справа та медіакомунікації»
Галузь знань: **06 “Журналістика”**
Спеціальність: **061 Журналістика**
Компонент освітньої програми – обовязкова дисципліна
Рік підготовки – 3 (1), семестр – 5 (1)
Кількість кредитів: 3
Мова викладання: українська
Дні занять: згідно з розкладом
Консультації: понеділок, згідно з розкладом

Керівник курсу - **Фінклер Юрій Едуардович**, викладач ЦК журналістики, доктор філологічних наук, професор
Контактна інформація – *bubabu@meta.ua*

АНОТАЦІЯ ДИСЦИПЛІНИ

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.

Мета курсу. Сформувати у студентів розуміння сутності явища інформаційна війна, інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки держави.

Набути практичних навиків у протистоянні новітнім методам інформаційної агресії в нинішніх умовах, коли ЗМІ стали визначальним елементом сучасного суспільства, коли інформація почала виконувати й «убивчу» роль, перетворюючи народ у натовп, оскільки одним із найефективніших методів відучити людей думати — це закидати їх величезним обсягом інформації, яка не має державних орієнтирів, або ж під виглядом наявності їх в інформаційному потоці маскувати інші цілі, ставити зовсім іншу мету.

Ознайомити студентів з методами агресії, 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.

СТРУКТУРА КУРСУ ТА ЗАВДАННЯ ВИВЧЕННЯ ДИСЦИПЛІНИ

ДЕННА ФОРМА НАВЧАННЯ

Кількість годин (аудит./ самост.)	Тема	Результати навчання	Форми контролю
12/23	**Змістовий модуль І ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ**		
4/2	Тема 1. Інформація в житті людини. Інформаційний вплив та інформаційні війни.	Знати специфіку відмінностей між пропагандою та інформаційною війною, ментальною агресією та психологічною війною у контексті функціонування соціально-політичної системи.	Питання, дискусія, написання ессе.
2/7	Тема 2. Типи інформаційної війни.	Знати класичні вияви психологічної війни.	Презентації-повідомлення, питання, обговорення.
4/7	Тема 3. Специфіка ведення інформаційної війни. Електронна війна — війна третього тисячоліття.	Вміти застосовувати прийоми, процедури і технології маніпулятивного впливу з метою захисту інформаційного простору держави; розрізняти інформаційні війни в політиці.	Презентації-повідомлення, питання, обговорення. ІНДЗ
2/7	Тема 4. Національна безпека в умовах інформаційної війни	Знати основні ознаки інформаційної безпеки.	Презентації-повідомлення, питання, обговорення. **Модульний контроль.**
20/35	**Змістовий модуль ІІ. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ**		
4/7	Тема 5. Інформаційна безпека: підходи до концептуалізації та індикатори визначення.	Вміти користуватися знанням підходів до визначення інформаційної безпеки.	Презентації-повідомлення, виконання творчо-пошукових завдань, питання, обговорення.
4/7	Тема 6. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах	Знати методики оцінювання загроз інформаційній безпеці у соціальних Інтернет- сервісах.	Презентації-повідомлення, питання, обговорення.
4/7	Тема 7. Теорія і практика інформаційно-психологічного протиборства у ХХ – на початку ХХІ ст.	Вміти виявляти причини інформаційних воєн	Презентації-повідомлення, питання, обговорення.

Кількість годин (аудит./ самост.)	Тема	Результати навчання	Форми контролю
4/7	Тема 8. Інститути й інструменти забезпечення інформаційної безпеки України.	Розрізняти основні напрями і можливості вдосконалення системи забезпечення інформаційної безпеки на національному і міжнародному рівнях, її проблемні аспекти.	Презентації-повідомлення, питання, обговорення. ІНДЗ
4/7	Тема 9. Загрози інформаційній безпеці України	Оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та воєн.	**Модульний контроль.**

ЗАОЧНА ФОРМА НАВЧАННЯ

Кількість годин (аудит./ самост.)	Тема	Результати навчання	Форми контролю
8/40	**Змістовий модуль І ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ**		
2/10	Тема 1. Інформація в житті людини. Інформаційний вплив та інформаційні війни.	Знати специфіку відмінностей між пропагандою та інформаційною війною, ментальною агресією та психологічною війною у контексті функціонування соціально-політичної системи.	Питання, дискусія, написання ессе.
2/10	Тема 2. Типи інформаційної війни.	Знати класичні вияви психологічної війни.	Презентації-повідомлення, питання, обговорення.
2/10	Тема 3. Специфіка ведення інформаційної війни. Електронна війна — війна третього тисячоліття.	Вміти застосовувати прийоми, процедури і технології маніпулятивного впливу з метою захисту інформаційного простору держави; розрізняти інформаційні війни в політиці.	Презентації-повідомлення, питання, обговорення. ІНДЗ
2/10	Тема 4. Національна безпека в умовах інформаційної війни	Знати основні ознаки інформаційної безпеки.	Презентації-повідомлення, питання, обговорення. **Модульний контроль.**

Кількість годин (аудит./ самост.)	Тема	Результати навчання	Форми контролю
8/34	**Змістовий модуль ІІ Інформаційна безпека України**		
4/10	Тема 5. Інформаційна безпека: підходи до концептуалізації та індикатори визначення.	Вміти користуватися знанням підходів до визначення інформаційної безпеки.	Презентації-повідомлення, виконання творчо-пошукових завдань, питання, обговорення.
2/10	Тема 6. Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах	Знати методики оцінювання загроз інформаційній безпеці у соціальних Інтернет- сервісах.	Презентації-повідомлення, питання, обговорення.
-/10	Тема 7. Теорія і практика інформаційно-психологічного протиборства у ХХ – на початку ХХІ ст.	Вміти виявляти причини інформаційних воєн	Презентації-повідомлення, питання, обговорення.
-/4	Тема 8. Інститути й інструменти забезпечення інформаційної безпеки України.	Розрізняти основні напрями і можливості вдосконалення системи забезпечення інформаційної безпеки на національному і міжнародному рівнях, її проблемні аспекти.	Презентації-повідомлення, питання, обговорення. ІНДЗ
2/-	Тема 9. Загрози інформаційній безпеці України	Оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та воєн.	**Модульний контроль.**

ПОЛІТИКА ПРОВЕДЕННЯ АУДИТОРНИХ ЗАНЯТЬ

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

При проведенні аудиторних занять домінуючими є проблемні, індивідуально-диференційовані, особистісно-орієнтовані форми проведення занять та технології компетентнісного навчання.

При проведенні практичних занять використовуються різні активності: евристичні бесіди, дискусії, ситуативні кейси.

На лекціях у формі активної бесіди з елементами дискусії розглядаються основні теоретичні положення теми, які вимагають роз’яснення та уточнення з боку викладача. На лекціях вимагається активна участь студентів у обговоренні ключових положень теми, ведення стислого конспекту лекції.

Теоретичні знання, отримані студентами під час лекцій, обговорюються більш детально на практичних заняттях у формі міні-дискусій, представлення міні-проектів, заслуховування та аналізу тематичних доповідей та рефератів.

У процесі практичного (семінарського) заняття студенти вчаться формулювати свою точку зору, логічно викладати матеріал, підбирати докази у підтвердження своїх думок, вчаться публічно виступати.

ВИМОГИ ДО САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Основним завданням самостійної роботи студентів є набуття навичок самостійного опрацювання фахових інформаційних джерел.

Самостійна робота студента в процесі вивчення курсу «Медіабезпека» полягає у додатковому опрацюванні загальної та спеціальної літератури з тем, що не увійшли до лекційного матеріалу, підготовці до семінарських та практичних занять, підготовці відповідних презентацій щодо найбільш важливих питань.

Формами контролю виконання самостійної роботи студентами є відповіді на семінарських заняттях, тестування та письмове опитування.

Обсяг самостійної роботи визначається кількістю годин, передбачених робочою програмою.

ПОЛІТИКА ОЦІНЮВАННЯ ТА АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Оцінювання здійснюється за 100-бальною шкалою відповідно до **Положення про порядок рейтингового оцінювання знань (освітніх досягнень) здобувачів вищої освіти.**

Оцінювання знань студентів із 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 та семінарських занять і має на меті перевірку знань студентів із окремих тем та рівня їх підготовленості до виконання конкретної роботи.

На семінарських заняттях використовуються: дискусія, проблемно-пошуковий, репродуктивний, інтерактивний *методи* тощо.

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

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

Індивідуальне навчально-дослідне завдання (ІНДЗ) студенти виконують самостійно під керівництвом викладача. Індивідуальні завдання можуть бути як груповими, так і виконуватися 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. Це завершена теоретична або практична робота в межах навчальної програми курсу, яка виконується на основі знань, вмінь і навичок, отриманих у процесі лекційних, практичних занять, охоплює тему, декілька тем або зміст навчальної дисципліни загалом.

Політика щодо академічної доброчесності

Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування (в т.ч. із використанням мобільних девайсів), втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування, незалежно від масштабів плагіату чи обману.

Студенти як відповідальні учасники освітнього процесу дотримуються норм **академічної доброчесності**, усвідомлюють наслідки її порушення, що визначаються

Положенням про академічну доброчесність у Галицькому фаховому коледжі імені В'ячеслава Чорновола.

Списування під час контрольних заходів заборонені (в т. ч. із використанням мобільних девайсів).

ТАБЛИЦЯ
розподілу балів за підсумковими контрольними заходами
та відповідними ваговими коефіцієнтами

	Модуль 1 (поточне опитування)	**Модуль 2 (підс. мод. контр.)**	**Модуль 3 (ІНДЗ)**	**Підсумкова оцінка**
Вагові коефіцієнти, %	70	20	10	100
Розрахунок оцінки в балах	80	83	70	82

Приклад розрахунку підсумкової оцінки в балах:

О = 80*0,7+83*0,2+70*0,1=82

Студенти як відповідальні учасники освітнього процесу дотримуються норм **академічної доброчесності**, усвідомлюють наслідки її порушення, що визначаються **Положенням про академічну доброчесність у Галицькому фаховому коледжі імені В'ячеслава Чорновола.**

Списування під час контрольних заходів та екзаменів заборонені (в т. ч. із використанням мобільних девайсів).

ПОЛІТИКА ЩОДО ВІДВІДУВАННЯ, ДЕДЛАЙНІВ ТА ПЕРЕСКЛАДАННЯ

Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, відрядження, участь у науково-дослідницьких заходах, міжнародне стажування) навчання може відбуватись в онлайн форматі за погодженням із керівником курсу. Пропущені заняття та незадовільні оцінки (поточний контроль, ПМК) повинні бути відпрацьовані згідно графіку консультацій викладача.

ІНДЗ, ПМК, які здаються із порушенням термінів без поважних причин можуть бути оцінені на нижчу оцінку (до 10 балів).

До початку сесії студенти повинні виконати усі підсумкові контрольні заходи і отримати по кожному з Модулів 1, 2, 3 не менше 60 балів.

Студент має право оскаржити оцінку, отриману за результатами підсумкового семестрового контролю у формі іспиту (крім незадовільної оцінки). Такі випадки регулюються **Положенням про апеляцію результатів підсумкового контролю знань студентів.**

Перескладання незадовільних оцінок здійснюється відповідно до **Положення про порядок ліквідації академічних заборгованостей здобувачами вищої освіти**.

ЛІТЕРАТУРНІ ТА ІНФОРМАЦІЙНІ ДЖЕРЕЛА КУРСУ

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-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. Системно-концептуальні засади стратегіїнаціональної 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. 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-Могилянська академія», 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.

Допоміжна:

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).

СХЕМА ВИВЧЕННЯ ДИСЦИПЛІНИ

І семестр

	1 тиждень	2 тиждень	3 тиждень	4 тиждень	5 тиждень	6 тиждень	7 тиждень	8 тиждень	9 тиждень	10 тиждень	11 тиждень	12 тиждень	13 тиждень	14 тиждень	15 тиждень	16 тиждень
Лекції	**Л1**		**Л2**	**Л3**	**Л4**		**Л5**		**Л6**		**Л7**		**Л8**		**Л9**	
Семінарські		**С1**				**С2**		**С3**		**С4**		**С5**		**С6**		**С7**
Контроль знань		**ПО**				**МК1**		**ПО**		**ПО**		**ПО**		**ПО**	**ІНДЗ**	**МК2**

Л1 – лекційне заняття по темі 1

С1 – семінарське заняття по темі 1

МК1 – модульний контроль 1

ІНДЗ – індивідуальне навчально-дослідне завдання

ПО – поточне опитування