**Силабус курсу «ІНФОРМАЦІЙНА ПОЛІТИКА ДЕРЖАВИ»**

**2019**–**2020 навчального року**

|  |  |
| --- | --- |
| **Назва курсу** | Інформаційна політика держави |
| **Адреса викладання курсу** | м. Львів, Львівський національний університет імені Івана Франка, вул. Університетська 1, ауд. 362 (лекційні заняття); ауд. 116 (семінарські заняття) |
| **Факультет та кафедра дисципліни** | філософський факультеткафедра політології |
| **Галузь знань, шифр та назва спеціальності** | Галузь знань: 05 – соціальні та поведінкові наукиСпеціальність: 052 – політологія |
| **Викладачі курсу** | Осадчук Ігор Юрійович, кандидат політичних наук, доцент кафедри політології |
| **Контактна інформація викладачів** | Е-mail: ihor.osadchuk@lnu.edu.ua; ihorosadchuk89@gmail.comПерсональна сторінка: <http://filos.lnu.edu.ua/employee/8032> |
| **Консультації по курсу відбуваються** | Щопонеділка,13:30–14:30 год.  (м. Львів, вул. Університетська, 1, ауд. 206) |
| **Сторінка курсу** | <https://filos.lnu.edu.ua/course/informatsiyna-polityka-derzhavy> |
| **Інформація про курс** | «Інформаційна політика держави» – вибіркова навчальна дисципліна, що вивчається студентами третього курсу спеціальності «політологія» філософського факультету. Дисципліна є складовою частиною вивчення політичної науки і викладається в шостому семестрі в обсязі 3,5 кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| **Коротка анотація курсу** | Курс є елементом такого напряму сучасної політичної науки, як національна безпека. Курс було розроблено з прицілом на усталені й новітні якісні та кількісні механізми, методики, інструменти аналізу інформаційної політики України, США та країн Західної Європи. Методологічною основою курсу є постбіхевіоралізм та неоінституціоналізм. У науковому та навчальному плані курс використаний як механізм диверсифікації та поглиблення (звуження) сфери наукового політологічного аналізу. Курс розділено на два змістові модулі: 1. Інформаційна політика держави на сучасному етапі. Інформаційна політика в Україні, США і країнах Західної Європи; 2. Інформаційні операції та інформаційні війни. Інтернет-ресурси та інформаційна безпека держави. |
| **Мета та цілі курсу** | **Мета курсу** – сформувати у студентів розуміння сутності явища інформаційна політика держави, ознайомити з особливостями формування та реалізації інформаційної політики в Україні, США та країнах Західної Європи. **Завдання курсу:*** розкрити ознаки феномена «інформаційна політика держави»;
* прищепити у студентів навики самостійного аналізу інформаційних стратегій в контексті інформаційної політики держави;
* ознайомити з особливостями формування та реалізації інформаційної політики в Україні, США та країнах Західної Європи;
* сформувати навики виокремлення чинників і наслідків інформаційних війн;
* ознайомитись з методиками оцінювання загроз інформаційній безпеці держави у соціальних Інтернет-сервісах.
 |
| **Література для вивчення дисципліни** | **Основна література:**1. Горбулін В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.
2. Качинський А. Індикатори національної безпеки: визначення та застосування їх граничних значень. К.: НІСД, 2013. 104 с.
3. Нестеряк Ю. Державна інформаційна політика: теоретико-методологічні засади: моногорафія. К.: НАДУ, 2014. 292 с.
4. Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.
5. Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с.

**Додаткова література:**1. Вакулич В., Бухтатий О. Державна інформаційна політика як механізм реалізації інформаційної функції сучасної держави. Публічне управління: теорія та практика. 2014. №. 1. С. 97–107.
2. Валюшко І. Еволюція інформаційних війн: минуле і сучасність. Історико-політичні студії. Збірник наукових праць. 2015. № 2. С. 127–134.
3. [Грищук Р.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A=&S21COLORTERMS=1&S21STR=%D0%93%D1%80%D0%B8%D1%89%D1%83%D0%BA%20%D0%A0$), Мамарєв В., Молодецька-Гринчук К. Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблоку Twitter). [Інформаційні технології та комп’ютерна інженерія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9625260). 2017. № 2. С. 12–19.
4. Еделєва М. Концепт державної інформаційної політики в сучасних умовах. Грані. 2016. № 3 (131). С. 62–67.
5. 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.
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. Макаренко Є. Європейська інформаційна політика: монографія. К.: Наша культура і наука, 2000. 368 с.
8. Молодецька-Гринчук К. Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня. [Системи обробки інформації](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9670474). 2017. Вип. 5. С. 122–129.
9. Мохова Ю., Луцька А. Сутність та головні напрямки державної інформаційної політики України. Державне управління: удосконалення та розвиток. 2018. № 12. DOI: 10.32702/2307-2156-2018.12.25.
10. Нестеряк Ю. Технології та моделі державної інформаційної політики. Ефективність державного управління: зб. наук. пр. Львів. регіон. ін-ту держ. упр. Нац. акад. держ. упр. при Президентові України. Львів: ЛРІДУ НАДУ, 2012. Вип. 30. С. 227–234.
11. Панченко В. Інформаційні операціїв асиметричній війні Росії проти України*:*підходи до моделювання. Інформація і право. 2014. № 3. С. 13–16.
12. Пахнін М. Особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. 2014. Вип. 4. С. 414–422.
13. Рябоконь О. Державна інформаційна політика формування інформаційного суспільства: зарубіжний досвід. Наук. пр. Нац. б-ки України ім. В. І. Вернадського: зб. наук. пр. / НАН України, Нац. б-ка України ім. В. І. Вернадського, Асоц. б-к України. Київ, 2016. Вип. 43. C. 97–114.
14. Сасин Г. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). [Грані](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9669893). 2015. № 3. С. 18–23.
15. Снитко О. Проекти тотального зомбування в інформаційному просторі України. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С. 207–215.

**Інтернет-джерела:**1. Міністерство закордонних справ України: Офіційний веб-сайт. URL: <https://mfa.gov.ua/ua>.
2. Міністерство оборони України: Офіційний веб-сайт. URL: <http://www.mil.gov.ua/>.
3. Офіційний портал Верховної Ради України. URL: <https://rada.gov.ua/>.
4. Президент України. Офіційне інтернет-представництво. URL: <https://www.president.gov.ua/>.
5. Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.bsi.bund.de/DE/Home/home\_node.html.
6. U.S. Cyber Command. URL: https://www.cybercom.mil/.
 |
| **Тривалість курсу** | 105 год. |
| **Обсяг курсу** | 64 години аудиторних занять. З них: 32 години лекцій, 32 години практичних занять та 41 година самостійної роботи |
| **Очікувані результати навчання** | Після завершення цього курсу студент буде ***знати:**** основні ознаки інформаційної політики держави;
* сутність та різновиди інформаційних стратегій в контексті інформаційної політики держави;
* методики оцінювання загроз інформаційній безпеці держави у соціальних Інтернет-сервісах;
* причини та методи ведення інформаційних війн;
* особливості формування та реалізації інформаційної політики в Україні, США та країнах Західної Європи;

***вміти:**** користуватися знанням підходів до визначення інформаційної політики держави;
* розуміти проблематику, специфіку й різновиди загроз інформаційній безпеці держави;
* розрізняти основні напрями і можливості вдосконалення інформаційної політики держави;
* оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та війн.
 |
| **Ключові слова** | Інформаційна сфера, інформаційна політика держави, інформаційна безпека держави, національна безпека, кібернетична безпека, інформаційне суспільство, інформаційна війна, інформаційна акція, інформаційна атака, інформаційна операція. |
| **Формат курсу** | Очний |
| **Аудиторні особливості курсу** | Проведення лекцій, семінарських занять та консультацій для кращого розуміння тем дисципліни. |
| **Підсумковий контроль, форма** | Залік в кінці семестру (усна форма). |
| **Пререквізити** | Для вивчення курсу студенти потребують базових знань, достатніх для сприйняття категоріального апарату і розуміння джерел з таких дисциплін: «Політичні конфлікти», «Національна безпека», «Інформаційна безпека». |
| **Навчальні методи та техніки, які будуть використовуватися під час викладання курсу** | Навчальний процес здійснюється за традиційною технологією: лекції, практичні (семінарські) заняття, самостійна робота. На лекційних заняттях використовуються: словесні методи (розповідь, бесіда, пояснення, діалог); наочні та практичні методи (ілюстрація, демонстрація); методи синтезу, аналізу, індукції, дедукції тощо. На семінарських заняттях використовуються: дискусія, проблемно-пошуковий, інтерактивний методи тощо. У межах самостійної роботи застосовуються дослідницькі методи. |
| **Необхідне обладнання** | Персональний комп’ютер з відповідним програмним забезпеченням (Microsoft Office) та мультимедійний проектор.  |
| **Критерії оцінювання (окремо для кожного виду навчальної діяльності)** | Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співідношенням: практичні/самостійні – 30 % семестрової оцінки; максимальна кількість 30 балів; контрольні заміри (модулі) – 20 % семестрової оцінки; максимальна кількість 20 балів; залік – 50 % семестрової оцінки (максимальна кількість 50 балів). Максимальна кількість 100 балів.Оцінювання знань студентів відбувається на основі результатів поточного контролю знань та підсумкового контролю знань (залік). Поточний контроль знань студентів проводять за трьома складовими: контроль систематичності та активності роботи студента протягом семестру; контроль за виконанням модульних завдань; контроль за виконанням завдань самостійного опрацювання. При контролі систематичності і активності роботи студента оцінці підлягають: самостійна робота студентів; відвідування й активність на семінарських занять; рівень засвоєння знань програмного матеріалу.Поточний контроль успішності здійснюється за п’ятибальною шкалою: «5» – відмінно, «4» – добре, «3» – задовільно, «2» – доповнення, «1» – коментарі (участь у дискусії). Контроль знань за результатами вивчення окремого змістового модуля оцінюється в 10 балів. **Письмові роботи:** очікується, що студенти виконають декілька видів письмових робіт (вирішення кейсу, есе). **Академічна доброчесність**: очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування і втручання в роботу інших студентів становлять, однак не обмежують прикладів можливої академічної недоброчесності. Виявлення ознак цього є підставою для незарахування роботи студента викладачем, незалежно від масштабів плагіату чи обману. **Відвідування занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов’язані дотримуватися усіх термінів, визначених для виконання усіх видів робіт, передбачених курсом.**Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих і обов’язкових.**Політика виставлення балів.** Враховуються бали, набрані на поточному тестуванні, в самостійній роботі і бали підсумкового контролю знань (залік). При цьому, обов’язково враховуються присутність на заняттях й активність студента під час практичного заняття, списування і плагіат, а також несвоєчасне виконання поставлених завдань.Жодні форми порушення академічної доброчесності не толеруються. |
| **Питання до заліку** | 1. Інформація: суть, види і властивості.
2. Інформаційне суспільство: підходи до визначення та моделі.
3. Інформаційна політика держави: основні принципи, напрями та механізми реалізації.
4. Інформаційна безпека як функція інформаційної політики держави.
5. Виклики та загрози інформаційній безпеці держави в сучасних умовах.
6. Ознаки інформаційних стратегій.
7. Різновиди інформаційних стратегій.
8. Специфіка реалізації інформаційних стратегій в контексті інформаційної політики держави.
9. Ознаки інформаційних технологій.
10. Різновиди інформаційних технологій.
11. Особливості використання інформаційних технологій в інформаційній політиці держави.
12. Правове регулювання державної інформаційної політики України.
13. Завдання і напрями державної інформаційної політики України.
14. Механізми реагування на загрози інформаційній безпеці України.
15. Шляхи вдосконалення державної інформаційної політики України.
16. Правове забезпечення інформаційної політики США.
17. Завдання і напрями інформаційної політики США.
18. Механізми реагування на загрози інформаційній безпеці США.
19. Шляхи вдосконалення інформаційної політики США.
20. Правове забезпечення інформаційної політики у країнах Західної Європи.
21. Завдання і напрями інформаційної політики у країнах Західної Європи.
22. Механізми реагування на загрози інформаційній безпеці у країнах Західної Європи.
23. Шляхи вдосконалення інформаційної політики у країнах Західної Європи.
24. Сутність та різновиди інформаційних операцій.
25. Ознаки й логіка інформаційної війни.
26. Методи ведення інформаційних війн.
27. Різновиди інформаційних війн.
28. Причини інформаційної війни Російської Федерації проти України.
29. Методи ведення інформаційної війни Російської Федерації проти України.
30. Нормативно-правові механізми протидії інформаційній війні Російської Федерації проти України.
31. Інституційні механізми протидії інформаційній війні Російської Федерації проти України.
32. Інтернет-ресурси як об’єкти загроз інформаційній безпеці держави.
33. Профілі інформаційної безпеки акторів у соціальних Інтернет-сервісах.
34. Методи виявлення загроз інформаційній безпеці держави у соціальних Інтернет-сервісах.
35. Оцінювання загроз інформаційній безпеці держави у соціальних Інтернет-сервісах.
 |
| **Опитування** | Анкету-оцінку для оцінювання якості курсу буде надано по його завершенню. |

**Схема курсу**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Тиж. / дата / год. | Тема | План заняття | Форма діяльності (заняття) лекція, самостійна, дискусія, групова робота) | Література / Ресурси в інтернеті |
| 1/10.02; 12.02 | Інформаційна політика держави на сучасному етапі (частина 1) | 1.Інформація: суть, види і властивості. 2.Інформаційне суспільство: підходи до визначення та моделі.3.Інформаційна політика держави: основні принципи, напрями та механізми реалізації. | Лекція; семінарське заняття(дискусія, групова робота) | 1. Еделєва М. Концепт державної інформаційної політики в сучасних умовах. Грані. 2016. № 3 (131). С. 62–67.2. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A=&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A$) Основні суб’єкти та інститути інформаційної безпеки. [Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9669749:%D0%A4%D1%96%D0%BB%D0%BE%D1%81." \o "Періодичне видання). 2017. Вип. 48 (1). С. 212–219.3. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.4.Нестеряк Ю. Державна інформаційна політика: теоретико-методологічні засади : Моногорафія. К.: НАДУ, 2014. 292 с.5.Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с. |
| 2/17.02;19.02 | Інформаційна політика держави на сучасному етапі(частина 2) | 1.Інформаційна безпека як функція інформаційної політики держави.2.Виклики та загрози інформаційній безпеці держави в сучасних умовах. | Лекція; семінарське заняття(дискусія, групова робота) | 1. [Захаренко К.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A=&S21COLORTERMS=1&S21STR=%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9A$) Основні суб’єкти та інститути інформаційної безпеки. [Вісник Харківського національного педагогічного університету імені Г. С. Сковороди. Філософія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9669749:%D0%A4%D1%96%D0%BB%D0%BE%D1%81." \o "Періодичне видання). 2017. Вип. 48 (1). С. 212–219.2. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.3.Нестеряк Ю. Державна інформаційна політика: теоретико-методологічні засади : Моногорафія. К.: НАДУ, 2014. 292 с.4.Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с. |
| 3/24.02;26.02 | Інформаційні стратегії та інформаційні технології в контексті інформаційної політики держави (частина 1) | 1.Ознаки інформаційних стратегій.2.Різновиди інформаційних стратегій.3.Специфіка реалізації інформаційних стратегій в контексті інформаційної політики держави. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Воскобойнікова-Гузєва О. Стратегічний менеджмент інформаційної діяльності: базові засади. Вісник Книжкової палати. 2017. № 11. С. 15–19.2.Латинін М. Стратегічні пріоритети розбудови інформаційного суспільства в Україні. Публічне управління: теорія та практика: Зб. наук. праць Асоціації докторів наук з державного управління. Х.: Вид-во «ДокНаукДержУпр», 2011. № 2 (6). С. 185–191.3.Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с. |
| 4/2.03; 4.03 | Інформаційні стратегії та інформаційні технології в контексті інформаційної політики держави (частина 2) | 1.Ознаки інформаційних технологій.2.Різновиди інформаційних технологій.3.Особливості використання інформаційних технологій в інформаційній політиці держави | Лекція; семінарське заняття(дискусія, групова робота) | 1.Воскобойнікова-Гузєва О. Стратегічний менеджмент інформаційної діяльності: базові засади. Вісник Книжкової палати. 2017. № 11. С. 15–19.2.Латинін М. Стратегічні пріоритети розбудови інформаційного суспільства в Україні. Публічне управління: теорія та практика: Зб. наук. праць Асоціації докторів наук з державного управління. Х.: Вид-во «ДокНаукДержУпр», 2011. № 2 (6). С. 185–191.3.Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с. |
| 5/9.03; 11.03 | Державна інформаційна політика України(частина 1) | 1.Правове регулювання державної інформаційної політики України.2.Завдання і напрями державної інформаційної політики України. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Дрешпак В. Періоди розвитку державної інформаційної політики України: зміст і хронологічні межі. Державне управління та місцеве самоврядування : зб. наук. праць. Дніпропетровськ: ДРІДУ НАДУ, 2014. Вип. 1 (20). С. 3–14.2.Еделєва М. Державна інформаційна політика України: аналіз вітчизняного та закордонного досвіду. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». 2016. № 3 (30). C. 272–274.3.Мохова Ю., Луцька А. Сутність та головні напрямки державної інформаційної політики України. Державне управління: удосконалення та розвиток. 2018. № 12. DOI: 10.32702/2307-2156-2018.12.25.4.Негодченко В. Основні напрями державної інформаційної політики в Україні. Підприємництво, господарство і право. 2016. №4. С. 77–81.5.Нестеряк Ю. Державна інформаційна політика: теоретико-методологічні засади: моногорафія. К.: НАДУ, 2014. 292 с. |
| 6/16.03; 18.03 | Державна інформаційна політика України(частина 2) | 1.Механізми реагування на загрози інформаційній безпеці України.2.Шляхи вдосконалення державної інформаційної політики України. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Еделєва М. Державна інформаційна політика України: аналіз вітчизняного та закордонного досвіду. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». 2016. № 3 (30). C. 272–274.2.Нестеряк Ю. Державна інформаційна політика: теоретико-методологічні засади: моногорафія. К.: НАДУ, 2014. 292 с. |
| 7/23.03;25.03 | Інформаційна політика США(частина 1) | 1.Правове забезпечення інформаційної політики США.2.Завдання і напрями інформаційної політики США. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. Центр досліджень соціальних комунікацій НБУВ. URL: http://nbuviap.gov.ua/index.php?option=com\_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350.2.Пахнін М. Особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. 2014. Вип. 4. С. 414–422.3.Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с.4. National Security Strategy of the United States of America. Washington. 2010. 52 p. White House. URL: http://www.whitehouse.gov/sites/default/files/r.5.US Cybersecurity: Progress stalled Key findings from the 2015 US State of Cybercrime Survey. URL: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf. |
| 8/30.03;1.04 | Інформаційна політика США(частина 2) | 1.Механізми реагування на загрози інформаційній безпеці США.2.Шляхи вдосконалення інформаційної політики США. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Пахнін М. Особливості державної інформаційної політики в розвинених країнах світу. Теорія та практика державного управління. 2014. Вип. 4. С. 414–422.2.Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с.3. National Security Strategy of the United States of America. Washington. 2010. 52 p. White House. URL: http://www.whitehouse.gov/sites/default/files/r.4.US Cybersecurity: Progress stalled Key findings from the 2015 US State of Cybercrime Survey. URL: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf. |
| 9/6.04; 8.04 | Інформаційна політикау країнах Західної Європи(частина 1) | 1.Правове забезпечення інформаційної політики у країнах Західної Європи.2.Завдання і напрями інформаційної політики у країнах Західної Європи. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Макаренко Є. Європейська інформаційна політика: монографія. К.: Наша культура і наука, 2000. 368 с.2.Почепцов Г., Чукут С. Інформаційна політика: навч. посіб. К.: Вид-во «Знання», 2008. 663 с.3.Твердохліб О. Європейський підхід до розроблення інформаційної політики держави: актуальні проблеми. Економіка. 2016. №3 (177). С. 429–435. |
| 10/13.04; 15.04 | Інформаційна політикау країнах Західної Європи(частина 2) | 1.Механізми реагування на загрози інформаційній безпеці у країнах Західної Європи.2. Шляхи вдосконалення інформаційної політики у країнах Західної Європи. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Барановська А. Інституційне забезпечення державної комунікативної політики Великої Британії. Стратегічні пріоритети. 2013. № 4 (29). С. 85–90.2.Буга Л. Досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах. Наук. зап. Львів. ун-ту бізнесу та права: зб. наук. пр. з екон. та юрид. наук. Серія юридична. Львів, 2018. Вип. 19. С. 174–178.3.Макаренко Є. Європейська інформаційна політика: монографія. К.: Наша культура і наука, 2000. 368 с.4.Чернухін І. Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. Інформаційна безпека людини, суспільства, держави. 2014. № 1. С. 27–43. |
| 11/20.04;22.04 | Інформаційні операції та інформаційні війни(частина 1) | 1.Сутність та різновиди інформаційних операцій.2.Ознаки й логіка інформаційної війни. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Валюшко І. Еволюція інформаційних війн: минуле і сучасність. Історико-політичні студії. Збірник наукових праць. 2015. № 2. С. 127–134.2.Горбулін В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.3.Панченко В. Інформаційні операції в системі стратегічних комунікацій. [Стратегічні пріоритети. Серія: Політика](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9625775:%D0%9F). 2016. № 4. С. 72–79.4.Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с. |
| 12/27.04;29.04 | Інформаційні операції та інформаційні війни(частина 2) | 1.Методи ведення інформаційних війн.2.Різновиди інформаційних війн. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Горбулін В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.2.Панченко В. Інформаційні операції в системі стратегічних комунікацій. [Стратегічні пріоритети. Серія: Політика](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9625775:%D0%9F). 2016. № 4. С. 72–79.3.Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с. |
| 13/4.05; 6.05 | Інформаційна війна Російської Федерації проти України(частина 1) | 1.Причини інформаційної війни Російської Федерації проти України.2.Методи ведення інформаційної війни Російської Федерації проти України. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Валюшко І. Інформаційна безпека України в контексті російсько-українського конфлікту: дис… канд. політ. наук. Дипломатична академія України при МЗС України, Київ; Чорноморський національний університет імені Петра Могили, Миколаїв, 2018. 210 с.2.Гай-Нижник П. Руйнація і поглинання: плани керівництва Російської Федерації щодо розколу і зруйнування держави Україна (2014–2015 рр.). Гілея: зб. наук. пр. / Нац. пед. ун-т ім. М. П. Драгоманова. Київ, 2018. Вип. 134 (7). С. 358–370.3.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. 180–190.4.Панченко В. Інформаційні операціїв асиметричній війні Росії проти України*:*підходи до моделювання. Інформація і право. 2014. № 3. С. 13–16. |
| 14/11.05;13.05 | Інформаційна війна Російської Федерації проти України(частина 2) | 1.Нормативно-правові механізми протидії інформаційній війні Російської Федерації проти України.2.Інституційні механізми протидії інформаційній війні Російської Федерації проти України.  | Лекція; семінарське заняття(дискусія, групова робота) | 1.Валюшко І. Інформаційна безпека України в контексті російсько-українського конфлікту: дис… канд. політ. наук. Дипломатична академія України при МЗС України, Київ; Чорноморський національний університет імені Петра Могили, Миколаїв, 2018. 210 с.2.Панченко В. Інформаційні операціїв асиметричній війні Росії проти України*:*підходи до моделювання. Інформація і право. 2014. № 3. С. 13–16. |
| 15/18.05;20.05 | Інтернет-ресурси та інформаційна безпека держави | 1.Інтернет-ресурси як об’єкти загроз інформаційній безпеці держави.2. Профілі інформаційної безпеки акторів у соціальних Інтернет-сервісах. | Лекція; семінарське заняття(дискусія, групова робота) | 1.[Грищук Р.](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=A=&S21COLORTERMS=1&S21STR=%D0%93%D1%80%D0%B8%D1%89%D1%83%D0%BA%20%D0%A0$" \o "Пошук за автором), Мамарєв В., Молодецька-Гринчук К. Класифікація профілів інформаційної безпеки акторів у соціальних Інтернет-сервісах (на прикладі мікроблоку Twitter). [Інформаційні технології та комп’ютерна інженерія](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9625260). 2017. № 2. С. 12–19.2.Молодецька-Гринчук К. Метод виявлення ознак інформаційних впливів у соціальних Інтернет-сервісах за змістовними ознаками. [Радіоелектроніка, інформатика, управління](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9616683" \o "Періодичне видання). 2017. № 2. С. 117–126. |
| 16/25.05;27.05 | Інтернет-ресурси та інформаційна безпека держави | 1. Методи виявлення загроз інформаційній безпеці держави у соціальних Інтернет-сервісах.2. Оцінювання загроз інформаційній безпеці держави у соціальних Інтернет-сервісах. | Лекція; семінарське заняття(дискусія, групова робота) | 1.Молодецька-Гринчук К. Метод виявлення ознак інформаційних впливів у соціальних Інтернет-сервісах за змістовними ознаками. [Радіоелектроніка, інформатика, управління](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9616683" \o "Періодичне видання). 2017. № 2. С. 117–126.2.Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних Інтернет-сервісах. [Автоматизация технологических и бизнес-процессов](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%96100466). 2017. Вип. 9. № 2. С. 36–42.3.Молодецька-Гринчук К. Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних Інтернет-сервісах та оцінювання їх рівня. [Системи обробки інформації](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=JUU_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=IJ=&S21COLORTERMS=1&S21STR=%D0%9670474). 2017. Вип. 5. С. 122–129. |