**Силабус курсу «ІНФОРМАЦІЙНА БЕЗПЕКА»**

**2019**–**2020 навчального року**

|  |  |
| --- | --- |
| **Назва курсу** | Інформаційна безпека |
| **Адреса викладання курсу** | м. Львів, Львівський національний університет імені  Івана Франка, вул. Університетська 1, ауд. 206  (лекційні заняття) |
| **Факультет та кафедра дисципліни** | філософський факультет  кафедра політології |
| **Галузь знань, шифр та назва спеціальності** | Галузь знань: 05 – соціальні та поведінкові науки  Спеціальність: 052 – політологія |
| **Викладачі курсу** | Осадчук Ігор Юрійович, кандидат політичних наук,  доцент кафедри політології |
| **Контактна інформація викладачів** | Е-mail: [ihor.osadchuk@lnu.edu.ua](mailto:ihor.osadchuk@lnu.edu.ua); [ihorosadchuk89@gmail.com](mailto:ihorosadchuk89@gmail.com)  Персональна сторінка: <http://filos.lnu.edu.ua/employee/8032> |
| **Консультації по курсу відбуваються** | Щоп’ятниці,10:30–11:30 год.  (м. Львів, вул. Університетська, 1, ауд. 206) |
| **Сторінка курсу** | <http://filos.lnu.edu.ua/course/informatsiyna-bezpeka> |
| **Інформація про курс** | «Інформаційна безпека» – вибіркова навчальна дисципліна, що вивчається магістрами другого курсу спеціальності «політологія» філософського факультету. Дисципліна є складовою частиною вивчення політичної науки і викладається в третьому семестрі в обсязі 3 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 безпеки України, країн Європейського Союзу і НАТО. 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. Теоретико-методологічні засади дослідження інформаційної безпеки. Загрози інформаційній безпеці. Теорія і практика інформаційно-психологічного протиборства; 2. Інформаційна безпека України. Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки. |
| **Мета та цілі курсу** | **Мета курсу** – сформувати у студентів розуміння сутності явища інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки держави.  **Завдання курсу:**   * розкрити ознаки феномена «інформаційна безпека»; * прищепити у студентів навики самостійного аналізу загроз інформаційній безпеці держави; * сформувати навики виокремлення тенденцій, які властиві сучасним загрозам інформаційній безпеці у соціальних Інтернет-сервісах; * визначити напрями і можливості вдосконалення системи забезпечення інформаційної безпеки України. |
| **Література для вивчення дисципліни** | **Основна література:**   1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с. 2. Історія інформаційно-психологічного протиборства: підручник / Скулиш Є.Д., Жарков Я.М., Компанцева Л.Ф., Остроухов В.В., Петрик В.М., Присяжнюк М.М.; за заг. ред. Є.Д. Скулиша. К.: Наук.-вид. відділ НА СБ України, 2012. 212 с. 3. Качинський А. Індикатори національної безпеки: визначення та застосування їх граничних значень. К.: НІСД, 2013. 104 с. 4. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с. 5. Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.   **Додаткова література:**   1. Бєлоусова Н., Афанасьєва П. Основні вимоги НАТО щодо забезпеченння безпеки інформаційного простору. Актуальні проблеми міжнародних відносин. Вип. 102. Ч. І. 2011. С. 196–202. 2. Валюшко І. Дипломатія України у вимірі інформаційної безпеки країни. Вісник Львівського університету. Серія філос.-політолог. студії. 2017. Вип. 13. С. 137–142. 3. Валюшко І. Еволюція інформаційних війн: минуле і сучасність. Історико-політичні студії. Збірник наукових праць. 2015. №2. С. 127–134. 4. Валюшко І. Кібербезпека України: наукові та практичні виміри сучасності. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2016. № 3/4 (31–32). С. 117–124. 5. [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. 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. Нестеряк Ю. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40–45. 8. Ніщименко О. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23. 9. 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. 10. 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. 11. 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. 12. Панченко В. Інформаційні операціїв асиметричній війні Росії проти України*:*підходи до моделювання. Інформація і право. 2014. № 3. С. 13–16. 13. 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. 14. Снитко О. Проекти тотального зомбування в інформаційному просторі України. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С. 207–215. 15. 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](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%9670384). 2016. Вип. 13. С. 12–19.   **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** | 90 годин |
| **Обсяг курсу** | 36 годин аудиторних занять. З них 24 години лекцій, 12 годин практичних занять та 54 години самостійної роботи. |
| **Очікувані результати навчання** | Після завершення цього курсу студент буде:  ***знати***   * основні ознаки інформаційної безпеки; * загрози інформаційній безпеці та їх різновиди; * методики оцінювання загроз інформаційній безпеці у соціальних Інтернет-сервісах; * особливості інформаційно-психологічного протиборства у XX – на початку XXІ ст.; * інститути й інструменти забезпечення інформаційної безпеки України; * причини та методи ведення інформаційної війни Російської Федерації проти України; * cтандарти Європейського Союзу та НАТО у сфері інформаційної безпеки;   ***вміти:***   * користуватися знанням підходів до визначення інформаційної безпеки; * розуміти проблематику і специфіку загроз інформаційній безпеці; * знати основні різновиди загроз інформаційній безпеці; * розрізняти основні напрями і можливості вдосконалення системи забезпечення інформаційної безпеки на національному та міжнародному рівнях, її проблемні аспекти; * виявляти причини інформаційних війн; * оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та війн. |
| **Ключові слова** | Інформаційна сфера, інформаційна політика держави, національний інтерес, інформаційна безпека держави, національна безпека, кібернетична безпека, інформаційне суспільство, система забезпечення інформаційної безпеки, загрози інформаційній безпеці, інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія, інформаційно-психологічна протидія, інформаційна війна, механізми реагування на загрози інформаційній безпеці. |
| **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 політика держави». |
| **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. Підходи до дослідження інформаційної безпеки. 2. Система забезпечення інформаційної безпеки. 3. Національний інтерес в інформаційній сфері. 4. Поняття і різновиди загроз інформаційній безпеці. 5. Принципи і логіка інформаційної війни. 6. Методи і технології інформаційних війн. Різновиди інформаційних війн. 7. Механізми реагування на загрози інформаційній безпеці. 8. Інтернет-ресурси як об’єкти загроз інформаційній безпеці держави. 9. Методики оцінювання загроз інформаційній безпеці у соціальних Інтернет-сервісах. 10. Інформаційно-психологічне протиборство під час Першої світової війни та у міжвоєнний період (1919–1939). 11. Інформаційно-психологічне протиборство в роки Другої світової війни (1939–1945). 12. Інформаційно-психологічне протиборство в умовах «Холодної війни» (1946–1991). 13. Специфіка глобального інформаційно-психологічного протиборства на початку XXI cт. 14. Правові засади організації системи інформаційної безпеки України. 15. Інституціональне забезпечення інформаційної безпеки України. 16. Механізми реагування на загрози інформаційній безпеці України. 17. ЗМІ як інструмент інформаційної безпеки України. 18. Громадські організації в контексті інформаційної безпеки України. 19. Різновиди загроз інформаційній безпеці України. 20. Патерни інформаційних операцій Російської Федерації проти України. 21. Інформаційна війна Російської Федерації проти України. 22. Дипломатія України в контексті інформаційної війни Російської Федерації проти України. 23. Інституціональне забезпечення інформаційної безпеки Європейського Союзу. 24. Правові засади політики інформаційної безпеки НАТО. 25. Механізми забезпечення інформаційної безпеки НАТО. |
| **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 |
| 1/4.09; 5.09 | Інформаційна безпека: підходи до концептуалізації та індикатори визначення | 1.Підходи до дослідження інформаційної безпеки.  2.Система забезпечення інформаційної безпеки.  3.Національний інтерес в інформаційній сфері. | Лекція; семінарське заняття  (дискусія, групова робота) | 1.Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.  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.). 2017. Вип. 48 (1). С. 212–219.  3.Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.  4.Ліпкан В. Національна безпека України: навчальний посібник. Київ: КНТ, 2009. 576 с.  5.Прозоров А. Ціннісні основи інформаційної безпеки особи, суспільства та держави. Інформаційна безпека людини, суспільства, держави. 2016. № 1 (20). С. 29–37. |
| 2/11.09; 12.09 | Загрози інформаційній безпеці. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах | 1.Поняття і різновиди загроз інформаційній безпеці.  2.Принципи і логіка інформаційної війни.  3.Методи і технології інформаційних війн.  4. Різновиди інформаційних війн. 5.Механізми реагування на загрози інформаційній безпеці.  6.Інтернет-ресурси як об’єкти загроз інформаційній безпеці держави.  7.Методики оцінювання загроз інформаційній безпеці у соціальних Інтернет-сервісах. | Лекція; семінарське заняття  (дискусія, групова робота) | 1.Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. К.: Інтертехнологія, 2009. 164 с.  2.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.  3.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). 2017. № 2. С. 117–126.  4.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.  5.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.  6.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.  7.Почепцов Г. Сучасні інформаційні війни. К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с. |
| 3/18.09; 19.09 | Теорія і практика інформаційно-психологічного протиборства у XX – на початку XXI cт. | 1.Інформаційно-психологічне протиборство під час Першої світової війни та у міжвоєнний період (1919–1939).  2.Інформаційно-психологічне протиборство в роки Другої світової війни (1939–1945).  3.Інформаційно-психологічне протиборство в умовах «Холодної війни» (1946–1991).  4.Специфіка глобального інформаційно-психологічного протиборства на початку XXI cт. | Лекція; семінарське заняття  (дискусія, групова робота) | 1.Зозуля О. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства: дис…канд. наук з держ. управл. Національна академія державного управління при Президентові України, Київ, 2017. 251 с.  2.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.  3.Історія інформаційно-психологічного протиборства: підручник / Скулиш Є.Д., Жарков Я.М., Компанцева Л.Ф., Остроухов В.В., Петрик В.М., Присяжнюк М.М.; за заг. ред. Є.Д.Скулиша. К.: Наук.-вид. відділ НА СБ України, 2012. 212 с. |
| 4/25.09; 26.09 | Інформаційна безпека України в сучасних умовах | 1.Правові засади організації системи інформаційної безпеки України.  2.Інституціональне забезпечення інформаційної безпеки України.  3.Механізми реагування на загрози інформаційній безпеці України.  4.ЗМІ як інструмент інформаційної безпеки України.  5.Громадські організації в контексті інформаційної безпеки України. | Лекція; семінарське заняття  (дискусія, групова робота) | 1.Горбулін В., Качинський А. Засади національної безпеки України: підручник. К.: Інтертехнологія, 2009. 272 с.  2.Дмитренко М. Зовнішньополітичні впливи як пріоритети діяльності зовнішньої розвідки. Збірник наукових праць Інституту Служби зовнішньої розвідки України. 2013. № 5. С. 31−46.  3.[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$) Ефективність використання потенціалу недержавних суб’єктів інформаційної безпеки. [Мультиверсум. Філософський альманах](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%9670616). 2016. Вип. 1–2. С. 58–70.  4.Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.  5.Пилипчук В. Реформування і розвиток Служби безпеки в контексті євроінтеграції України: Науково-методичний посібник. К.: Нац. акад. СБУ, 2017. 260 с.  6.Ткачук Т. Ю.Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис… д. юрид. наук. ДВНЗ «Ужгородський національний університет», Ужгород, 2019. 487 с. |
| 5/2.10; 3.10 | Загрози інформаційній безпеці України | 1.Різновиди загроз інформаційній безпеці України.  2.Патерни інформаційних операцій Російської Федерації проти України.  3.Інформаційна війна Російської Федерації проти України.  4.Дипломатія України в контексті інформаційної війни Російської Федерації проти України. | Лекція; семінарське заняття  (дискусія, групова робота) | 1.Валюшко І.О. 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.Горбулін В., Качинський А. Засади національної безпеки України: підручник. К.: Інтертехнологія, 2009. 272 с.  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.Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.  5.Панченко В. Інформаційні операціїв асиметричній війні Росії проти України*:*підходи до моделювання. Інформація і право. 2014. № 3. С. 13–16. |
| 6/9.10; 10.10 | Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки | 1.Інституціональне забезпечення інформаційної безпеки Європейського Союзу.  2.Правові засади політики інформаційної безпеки НАТО.  3.Механізми забезпечення інформаційної безпеки НАТО. | Лекція; семінарське заняття  (дискусія, групова робота) | 1.Бєлоусова Н., Афанасьєва П. Основні вимоги НАТО щодо забезпеченння безпеки інформаційного простору. Актуальні проблеми міжнародних відносин. Вип. 102. Ч. І. 2011. С. 196–202.  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.Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 2013. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN>.  5.Kovács L. Cyber Security Policy and Strategy in the European Union and NATO. Land Forces Academy Review. 2018. Vol. 23. No. 1(89). P. 16–24. |