Міністерство освіти і науки України
Карпатський національний університет імені Василя Стефаника
Факультет історії, політології та міжнародних відносин
Кафедра політичних наук

Ломака Іванна Іванівна

Соціокультурна та інформаційна безпека

Навчально – методичний посібник для студентів

Факультету історії, політології та міжнародних відносин

галузь знань - 05 Соціальні та поведінкові науки

напрям підготовки - 052 Політологія

Івано-Франківськ
2026

ББК 351.746.1:004:316.7

УДК 66.4(4Укр), 60.56

Ломака І. І. Соціокультурна та інформаційна безпека: навчально – методичний посібник для студентів Факультету історії, політології та міжнародних відносин. Галузь знань - 05 «Соціальні та поведінкові науки», напрям підготовки - 052 «Політологія». Івано – Франківськ. 2026. – 56с.

Рецензенти:
В. Й. Климончук, доктор політичних наук, професор кафедри політичних наук Карпатського національного університету імені Василя Стефаника

О. І. Липчук, кандидат політичних наук, доцент кафедри політичних наук Карпатського національного університету імені Василя Стефаника.

Рекомендовано до друку Вченою радою Факультету історії, політології та міжнародних відносин Карпатського національного університету імені Василя Стефаника (протокол № 4 від 25 листопада 2025 року)

ЗМІСТ

Вступ……. 4

Тематичний план…… 11

Навчальна програма курсу…….. 12

Плани та методичні рекомендації до семінарських занять…… 24

Теми індивідуальних завдань…….. 39

Курси на платформах самоосвіти…….. 44

Програмові вимоги до курсу…… 45

Термінологічний словник…… 47

Рекомендована навчальна і додаткова література…….. 53

Вступ

Інформація – чи не головна цінність у сучасному світі. Всі знають знамениту фразу: ***«Хто володіє інформацією — той володіє світом»***. Сьогодні світом рухає інформація. Це можуть бути будь-які відомості, які передаються між людьми усілякими способами: усним, письмовим, візуальним та іншими. Із середини 20 століття роль інформації внаслідок соціального прогресу і бурхливого розвитку науки і техніки незмірно зросла. Світовою тенденцією став перехід на цифрові технології, розвиток високошвидкісного Інтернету і мобільного зв'язку.

Інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Знання в цій сфері дозволять студенту зрозуміти природу інформації та її властивостей, усвідомити сутність інформаційної небезпеки і шляхів її запобігання та усунення.

Предметом вивчення навчальної дисципліни є суспільні відносини, які виникають з приводу соціокультурної безпеки, культурної експансії, функціонування інформаційної сфери у контексті переходу до інформаційного суспільства, захисту інформації конфіденційного характеру, діяльності щодо поширення та захисту інформації, а також види відповідальності за інформаційні правопорушення.

Навчальний план підготовки здобувачів вищої освіти першого рівня передбачає вивчення дисципліни «Соціокультурна та інформаційна безпека держави» за денною формою навчання в обсязі 180 годин, в тому числі: 30 годин лекцій, 30 години семінарських занять і 120 години самостійної роботи. Навчальна дисципліна вивчається протягом одного семестру; результатом засвоєння матеріалу є складання здобувачами вищої освіти першого рівня екзамену.

У методичному посібнику пропонується програма нормативного курсу,

подається орієнтовний план семінарських занять до курсу, який включає основні питання що виносяться на розгляд, тематику рефератів для самостійної роботи студентів, перелік запитань для самоперевірки та закріплення знань. В кінці кожної теми та кожного семінарського заняття вказаний список літератури. Включений перелік програмових вимог, що виносяться на іспит, який завершує вивчення нормативного курсу «Соціокультурна та інформаційна безпека». В посібнику зазначений перелік базової,та допоміжної літератури з курсу.

Мета і завдання дисципліни

Метою викладання навчальної дисципліни “Соціокультурна та інформаційна безпека держави” є формування у здобувачів освіти системи ґрунтовних теоретичних знань щодо загроз національній безпеці України в соціокультурній та інформаційній сферах, методів та заходів забезпечення інформаційної безпеки держави, зв’язків з громадськістю в секторі забезпечення інформаційної та культурної безпеки, чорних маніпулятивних технологій, піару, комунікацій, а також здатності оцінювати і підвищувати ефективність нормативно-правової бази забезпечення інформаційної безпеки держави в умовах глобалізації інформаційного простору та побудови інформаційного суспільства та трансформаційних змін, які відбуваються у європейської та світової системах забезпечення безпеки.

Основними цілями вивчення дисципліни є вивчення сутності та властивостей інформації,її впливу на свідомість та поведінку людини, суспільства, сучасних механізмів маніпулювання свідомістю, а також вивчення інформаційного законодавства як правової бази забезпечення інформаційної безпеки, особливо в умовах розбудови інформаційного суспільства та змін, які відбуваються у європейській та світових системах забезпечення безпеки. Навчити майбутніх політологів, фахівців у сфері національної безпеки аналізувати національний інформаційний простір в контексті формування суспільної думки та забезпечення інформаційної безпеки особи, суспільства та держави; з’ясовувати фактори, що визначають функціонування інформаційних потоків національного й іноземного походження; використовувати у практичній діяльності сукупність знань, професійних прийомів і методів, які впливають на формування національної інформаційної політики.

Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

- сутність основних понять та термінів, їх тотожностей та відмінностей у сфері інформаційної безпеки;
- методи маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;
- взаємозв’язок інформаційної безпеки з інформаційним суверенітетом та національною безпекою;
- основи державної політики у сфері забезпечення інформаційної безпеки;
- склад правової бази забезпечення інформаційної безпеки та зміст основних нормативно - правових актів у сфері інформаційної безпеки;

- проблеми правового забезпечення інформаційної безпеки;

- специфіку інформаційної безпеки в умовах формування нових світових та регіональних безпекових систем;

- особливості правової охорони комп'ютерної інформації: комп'ютерних програм, автоматизованих баз даних і знань;

- основи охорони та захисту інформації в автоматизованих (комп'ютерних) системах як вид інформаційної діяльності;

- проблеми правового регулювання Інтернет - правовідносин щодо засобів, способів і методів охорони та захисту електронних даних;

- реальні та потенційні шляхи запобігання інформаційної небезпеки.

вміти:

- орієнтуватися у чинному законодавстві, яке стосується регулювання інформаційних правовідносин та шукати необхідні нормативно-правові акти та інформаційно-правові положення чинного законодавства, що стосуються питань забезпечення інформаційної безпеки;

- застосовувати зазначені акти та інформаційно-правові положення у практичної діяльності, у тому числі, і під час використання інформаційних технологій.

Організаційно-методичні вказівки

Вивчення курсу «Соціокультурна та інформаційна безпека держави» передбачає засвоєння теоретичного матеріалу в сфері соціокультурної безпеки, інформаційної безпеки та ознайомлення з національним законодавством в інформаційній сфері. Проведення *практичних та семінарських занять* має на меті надати здобувачам вищої освіти першого рівня навички практичного застосовувати набутих під час лекцій теоретичних знань при вирішенні складних завдань, що можуть виникати в сфері національної безпеки.

З метою кращої організації самостійної роботи студентів визначаються основні проблеми політологічного курсу для підготовки питань зазначених для розгляду на семінарських заняттях, теми повідомлень, рефератів, есе. Також зазначено теми та методичні поради для самостійної розробки лекцій, семінарів, поза аудиторних навчальних заходів. Поточний контроль за навчальним процесом здійснюється під

час проведення семінарських занять шляхом усного опитування, заслуховування рефератів, огляду літератури, журнальних публікацій, та тестуванням. Дієвим засобом контролю за якістю навчання є участь студентів у дискусіях на семінарських заняттях, у науково-практичних конференціях.

Форми організації занять. Основними видами навчальних занять є: лекції, семінарські заняття, самостійна робота, індивідуально-консультаційна робота під керівництвом викладача.

Лекційні заняття системно охоплюють увесь курс, допомагають здобувачам освіти усвідомити його значення, обсяг і структуру, зміст окремих розділів і тем, надають змістовну, організаційну та методичну допомогу у самостійному їх вивченні, визначають найбільш складні теми та питання. Тематика лекцій визначається робочою програмою навчальної дисципліни.

Семінарські заняття.

Семінарські заняття проводяться, в основному, шляхом всебічного обговорення питань теми без попереднього призначення доповідачів. Завданням семінарських занять є закріплення і поглиблення знань, отриманих здобувачами вищої освіти при вивченні лекційного матеріалу, а також організація їх систематичної роботи зі спеціальною літературою. На семінарських заняттях оцінці підлягають: рівень знань, продемонстрований у виступах, активність при обговоренні питань, відповіді на питання експрес-контролю тощо. Критеріями оцінки при усних відповідях можуть бути: повнота розкриття питання; логіка викладення; впевненість та переконливість; культура мови; використання основної та додаткової літератури (монографій, навчальних посібників, журналів, інших періодичних видань тощо); аналітичність міркування, вміння робити порівняння, висновки.

Індивідуально-консультаційна робота під керівництвом викладача виконується у вигляді написання рефератів, доповідей, есе, підготовки презентацій, тез на наукові конференції, проведення опитування.

Самостійна робота студентів.

Самостійна робота здобувачів освіти є невід'ємною складовою частиною навчального процесу. Основна мета самостійної роботи – засвоєння навчального матеріалу, передбаченого програмою курсу і не охопленого іншими видами занять – лекційними, семінарськими тощо. Самостійна робота здобувачів освіти сприяє розвитку у них критичного мислення та формування навичок цілеспрямованої самостійної роботи з літературними джерелами, нормативними документами, інформацією в

цілому та вміння на їх основі аналізувати та вирішувати проблемні питання і робити власні висновки та обґрунтування як теоретичного, так і практичного характеру.

При контролі виконання завдань для самостійного опрацювання оцінці можуть підлягати: самостійне опрацювання тем загалом чи окремих питань; самостійна підготовка конспектів лекцій, семінарів, презентацій, поза аудиторних заходів; написання та публічний захист рефератів, есе; підготовка конспектів навчальних чи наукових текстів.

Інформаційні джерела

Базові підручники, навчальні посібники – основна література; підручники, монографії, словники, енциклопедії, наукові статті – додаткова література, інтернет- джерела.

Опанувавши курс, здобувачі вищої освіти будуть ґрунтовно знати й розуміти національні інтереси держави в інформаційній сфері, джерела загроз та нормативно-правові документи у сфері забезпечення інформаційної безпеки України, завдання і систему суб'єктів забезпечення інформаційної безпеки України, а також вмітимуть оцінювати ефективність нормативно-правової бази щодо забезпечення інформаційної безпеки держави, практично реалізовувати методи забезпечення інформаційної безпеки країни, розробляти інформаційне забезпечення зв'язків з громадськістю у секторі безпеки, концепції суспільних зв'язків у секторі безпеки, методи й прийоми "чорного" піару, "чорної" риторики, комунікації у сучасних відношеннях, у політиці та секторі безпеки для забезпечення інформаційної безпеки держави.

Методи та форми навчання. Під час проведення занять з навчальної дисципліни «Академічна доброчесність» використовуються такі методи навчання, як:

- пояснювально-ілюстративний (з метою розуміння сутності соціокультурної та інформаційної безпеки), пов'язаний із використанням засобів наочності (схем, таблиць, графіків);

- проблемний (з метою розв'язання проблемних ситуацій, які виникають під час організації вивчення курсу);

- пошуковий метод (шляхом формулювання проблем з питань організації вивчення курсу);

- дослідницький (шляхом формулювання проблем розглядуваних питань самими здобувачами вищої освіти та самостійне їх вирішення).

- активні та інтерактивні методи навчання.

Організація поточного та підсумкового контролю знань. Поточний контроль проводиться у формі усного опитування, письмового експрес-контролю або тестування на семінарських заняттях, виступів здобувачів вищої освіти при обговоренні питань на семінарських заняттях.

Підсумковий контроль проводиться з метою оцінки результатів навчання на певному освітньо-професійному рівні або на окремих його завершальних етапах за національною шкалою і шкалою ЄКТС.

Підсумковий контроль включає, зокрема, семестровий контроль, який проводиться у формі екзамену в обсязі навчального матеріалу, визначеного робочою програмою навчальної дисципліни,і в терміни, встановлені графіком освітнього процесу, індивідуальним планом здобувача вищої освіти.

Екзамен – це форма підсумкового контролю, що полягає в оцінці засвоєння здобувачем вищої освіти навчального матеріалу з певної дисципліни на підставі результатів виконаних поточних визначених завдань (50 балів) і підсумкового екзамену (50 балів).

Підводячи підсумки практичного (семінарського) заняття, викладач робить висновки, в яких зазначає правильну позицію при відповідях на теоретичні питання, робить висновок щодо загального рівня підготовки, оцінює відповіді та виступи здобувачів вищої освіти. Здобувачем вищої освіти вважається виконаним семестровий контроль з конкретної навчальної дисципліни, якщо він виконав усі види робіт, передбачені робочою програмою цієї навчальної дисципліни та набрав мінімальну кількість балів, що має дорівнювати 50.

Дисципліна оцінюється максимальною оцінкою у 100 балів.

Види, методи та форми контролю.

Види: поточний контроль, підсумковий контроль, семестровий контроль (екзамен).

Методи: перевірка самостійної роботи, усне опитування. Форми:

індивідуальна та фронтальна перевірка.

Організаційні процедури та порядок виявлення якості засвоєння навчального матеріалу, рівня відповідності отриманих знань, умінь і навичок здобутій кваліфікації в межах освітнього процесу здійснюється відповідно до Положення про контрольні заходи у Карпатському національному університеті імені Василя Стефаника.

Оцінювання результатів навчання здобувачів вищої освіти, отриманих під час практичних занять, здійснюється за такимикритеріями:

Оцінка зараховано (A) виставляється, коли здобувач вищої освіти дає абсолютно правильні відповіді на питання з викладенням оригінальних висновків, отриманих на основі програмного, додаткового матеріалу та нормативних документів. Здобувач вищої освіти застосовує системні знання навчального матеріалу, передбачені навчальною програмою.

Оцінка зараховано (B) виставляється здобувачеві вищої освіти, який повністю розкрив питання на основі програмного та додаткового матеріалу. При виконанні практичних завдань здобувач застосовує узагальнені знання навчального матеріалу, передбачені навчальною програмою.

Оцінка зараховано (C) виставляється здобувачеві вищої освіти, який повністю розкрив питання, але мають місце окремі неточності.

Оцінка зараховано (D) виставляється, коли здобувач розкрив питання, проте при викладенні програмного матеріалу допущені окремі помилки. Здобувач вищої освіти припускається помилок, за рахунок недостатнього розуміння програмного матеріалу.

Оцінка зараховано (E) виставляється, коли здобувач неповністю розкрив питання, відповідь містить суттєві помилки.

Оцінка не зарахховано з можливістю повторного складання (FX) виставляється здобувачеві, який не розкрив питання Як правило такий здобувач виявляє здатність до викладення думки лише на елементарному рівні.

Оцінка не зараховано з обов'язковим повторним вивченням дисципліни (F) виставляється здобувачеві, який не виконав навчальну програму або якийсь елемент її складової, має фрагментарні знання, які не дозволяють розкрити питання. Такий здобувач не може викласти свою думку навіть на елементарному рівні.

За результатами контролю знань здобувачеві вищої освіти, дозволяється виставлення залікової оцінки – «зараховано», «не зараховано з можливістю повторного складання», та «не зараховано з обов'язковим повторним вивченням дисципліни».

Політика щодо дедлайнів та перескладань, академічної доброчесності, відвідування: перездача та повторне вивчення дисципліни здійснюється відповідно до Положення про організацію освітнього процесу та розробку основних документів з організації освітнього процесу в Карпатському національному університеті Імені Василя Стефаника та Положення про порядок повторного вивчення навчальних дисциплін (кредитів ECTS) в умовах ECTS. Перескладання відбувається з дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Положення про запобігання академічному плагіату та іншим порушенням академічної доброчесності у навчальній та науково-дослідній роботі здобувачів освіти Прикарпатського національного університету імені Василя Стефаника.

Структура розподілу балів передбачає:

1) відповіді на семінарських заняттях – 50 балів;

2) написання контрольної письмової роботи – 20 балів;

3)виконання індивідуального завдання – створення та представлення графічної презентації з визначеної проблеми навчального курсу – 30 балів (з них 15 балів – за проєкт, 15 балів – за представлення).

Загальна кількість – *100 балів*.

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою. Для екзамену, курсового проекту (роботи), практики	Оцінка за національною шкалою. Для заліку
90 10	**A**	відмінно	зараховано
80 – 89	**B**	добре	зарахован
70 – 79	**C**	добре	зараховано
60 – 69	**D**	задовільно	зараховано
50 – 59	**E**	задовільно	зараховано
26 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-25	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципл ни

Політика навчальної дисципліни

Письмові роботи: студент зобов'язаний добросовісно готуватися до усіх видів поточного та підсумкового контролю, які виносяться на практичні заняття та самостійну роботу. вчасно виконати письмове завдання (підготовка реферату; виконати підсумковий тест у зазначений день. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Академічна доброчесність: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв, планшету чи іншого мобільного пристрою під час опитування, виконання письмового завдання чи тестування є недопустимими та призводять до не зарахування результатів чи не складання тестування відповідно до Положення про запобігання академічному плагіату та іншим порушенням академічної доброчесності у навчальній та науково-дослідній роботі здобувачів освіти Прикарпатського національного університету імені Василя Стефаника.

Відвідування занять. При виставленні рейтингового підсумкового балу обов'язково враховується присутність студента на заняттях (у тому числі на лекційних), пропуски та спізнення без поважної причини, що передбачено Положенням про організацію освітнього процесу та розробку основних документів з організації освітнього процесу у Прикарпатському національному університеті імені Василя Стефаника. Студенти мають можливість відпрацювати заняття, які було пропущено з поважних причин, а також отримати роз'яснення питань, з якими виникли труднощі у процесі підготовки до семінарських занять і письмових робіт, на консультаціях викладача кожного вівторка о 15.00.

Навчання за індивідуальним графіком: студенти, котрі навчаються за індивідуальним графіком, опрацьовують частину теоретичного матеріалу самостійно з обов'язковим проходженням усіх тестувань. системі дистанційного навчання d-learn.pnu.edu.ua та виконанням усіх завдань відповідно до індивідуального графіку навчання, складеного та погодженого з викладачем на початку семестру. Умови навчання за індивідуальним графіком регламентуються Положенням про порядок навчання здобувачів вищої освіти за індивідуальним графіком у Карпатському національному університеті імені Василя Стефаника.

Неформальна освіта: порядок перезарахування результатів неформальної освіти в межах курсу (наприклад, результати проходження курсів на платформах самоосвіти Prometeus, EdEra, Coursera, Udemy, наявність сертифікатів, котрі підтверджують проходження відповідних професійних курсів / тренінгів, тощо) регламентується Положенням про визнання результатів навчання, здобутих шляхом неформальної освіти, в Прикарпатському національному університеті імені Василя Стефаника.

Повторне вивчення дисципліни: студент, який не набрав 50 балів за відомістю №3, направляється на проходження курсу вдруге відповідно до Положення про порядок повторного вивчення навчальних дисциплін (кредитів ECTS) в умовах ECTS або відраховується з навчального закладу.

Наприкінці курсу студенти мають можливість надати відгуки та пропозиції щодо якості викладання дисципліни на сайті https://d-learn.pnu.edu.ua

Тематичний план

5. Організація навчання			
Обсяг навчальної дисципліни			
Лекції	30		
семінарські заняття / практичні / лабораторні	30		
самостійна робота	120		
Ознаки навчальної дисципліни			
Семестр	Спеціальність	Курс (рік навчання)	Нормативний / вибірковий
3	052 Політологія. Національна безпека	2	нормативний

Тематика навчальної дисципліни			
Тема	кількість год.		
	лекції	заняття	сам. роб.
Тема 1 Соціокультурна безпека в сучасному світі	2		5
Тема 2 Вплив глобалізації на національний культурний простір народів	2	2	5
Тема 3 Протистояння етнокультур масовій культурі	2		5
Тема 4 Культурна експансія як загроза соціальній стабільності та національній безпеці	2		5
Тема 5 Релігійна політика держави та етноконфесійні відносини	2		5
Тема 6 Мовна політика як елемент безпеки	2		5
Тема 7 Національна самоідентифікація	2		5
Тема 8 Основи державної інформаційної політики	2	2	5
Тема 9 Основні положення інформаційної безпеки	2	2	5
Тема 10 Основні поняття інформаційного протиборства	2	2	5
Тема 11 Інформаційна безпека України. Сучасний стан. Проблеми та перспективи.	2	2	5
Тема 12 Методи та заходи забезпечення інформаційної безпеки України	2		5
Тема 13 Система та політика забезпечення інформаційної безпеки України	2		5
Тема 14 Політико- правові основи інформаційної безпеки	4		5
Тема 15 Правова відповідальність за правопорушення в		2	5

інформаційній сфері			
Тема 16 Основи національної безпеки держави		2	5
Тема 17 Культурна безпека як складова національної безпеки		2	5
Тема 18 Сучасні релігійно - церковні процеси в Україні		2	5
Тема 19 Методи та заходи забезпечення інформаційної безпеки		2	5
Тема 20 Система і політика забезпечення інформаційної безпеки та інформаційного простору в інших державах		4	5
Тема 21 Інформаційна зброя та світові інформаційні мережі		2	5
Тема 22 Інформаційні війни та інформаційно – психологічна безпека держави		2	5
Тема 23 Інформаційна безпека в умовах кіберцивілізації		2	10
ЗАГ:	30	30	120

Згідно з навчальним планом курс розраховано на один семестр. Його загальний обсяг – 180 годин аудиторного навантаження- 60 годин та 120 годин самостійної роботи.. Підсумкова форма контролю – екзамен. Курс передбачає аудиторне обговорення рефератів та повідомлень, підготовлених студентами на основі самостійного вивчення рекомендованої і довідкової літератури.

Навчальна програма курсу

«Соцокультурна та інформаційна безпека»

Тема 1. Соціокультурна безпека в сучасному світі (2 год.)

Соціокультурна безпека є важливою складовою системи національної безпеки держави та пов'язана із захистом духовних, культурних і ціннісних основ суспільства. Вона охоплює систему заходів, спрямованих на збереження культурної спадщини, мови, традицій та національної ідентичності. У сучасному світі соціокультурна безпека перебуває під впливом глобалізаційних процесів, інтенсивного розвитку інформаційних технологій та міжкультурної взаємодії. Значну загрозу становлять процеси культурної уніфікації, поширення масової культури та інформаційні маніпуляції, ідеологічна експансія. Важливим чинником забезпечення соціокультурної стабільності є збереження духовних цінностей суспільства. Держава відіграє ключову роль у формуванні політики культурного розвитку та захисту національного культурного простору. Соціокультурна безпека також передбачає розвиток освіти, науки, культури та мистецтва. Значну роль у цьому процесі відіграють громадянське суспільство, культурні інституції та засоби масової інформації. Забезпечення соціокультурної безпеки сприяє зміцненню національної єдності та суспільної стабільності. У сучасних умовах вона стає одним із стратегічних факторів розвитку держави.

Тема 2. Вплив глобалізації на національний культурний простір народів (2 год.)

Глобалізація є одним із найважливіших процесів сучасного світу, що охоплює економічну, політичну та культурну сфери життя суспільства. У культурному вимірі глобалізація проявляється у поширенні загальносвітових культурних стандартів та інтенсивному міжкультурному обміні. Вона сприяє активному поширенню інформації, розвитку комунікацій та взаємодії культур різних народів. Разом з тим глобалізація створює загрозу уніфікації культур та втрати національної самобутності. В умовах глобального інформаційного простору посилюється вплив масової культури на традиційні культурні системи. Важливим завданням державної культурної політики є підтримка національної культури та захист культурної спадщини. Значну роль у цьому процесі відіграють освітні інституції, культурні організації та засоби масової інформації. Збереження культурного різноманіття є важливою умовою гармонійного розвитку людства. Міжкультурний діалог сприяє взаємному збагаченню культур та формуванню атмосфери взаєморозуміння між народами. Таким чином, глобалізація має як позитивні, так і негативні наслідки для розвитку національних культур.

Тема 3. Протистояння етнокультур масовій культурі (2 год.)

Масова культура є характерною ознакою сучасного інформаційного суспільства та формується під впливом глобальних медіа і культурної індустрії. Вона орієнтована на широке коло споживачів і часто характеризується стандартизацією культурних продуктів. Поширення масової культури може призводити до витіснення традиційних культурних форм і цінностей. Етнокультура, навпаки, відображає

історичний досвід, традиції, звичаї та духовні цінності конкретного народу. Вона є важливим елементом національної ідентичності та культурної спадщини. У сучасних умовах етнокультури стикаються з викликами культурної глобалізації та інформаційного впливу. Збереження етнокультурної самобутності потребує активної державної підтримки та розвитку культурних інституцій. Важливу роль у цьому процесі відіграє освіта, яка формує повагу до національних традицій та історії. Також значення має розвиток культурних програм, фестивалів та інших форм популяризації народної культури. Гармонійне поєднання традиційної та сучасної культури сприяє духовному розвитку суспільства.

Тема 4. Культурна експансія як загроза соціальній стабільності та національній безпеці (2 год.)

Культурна експансія є одним із інструментів впливу держав та міжнародних акторів на інші суспільства. Вона проявляється у поширенні певних культурних цінностей, моделей поведінки та світоглядних установок через медіа, освіту, мистецтво та інформаційні ресурси. Часто культурна експансія використовується як елемент політики «м'якої сили». У результаті такого впливу можуть змінюватися культурні орієнтири суспільства та послаблюватися національні традиції. Особливо значним є вплив глобальних медіакорпорацій і цифрових платформ. Культурна експансія може призводити до формування залежності від чужих культурних стандартів. Це створює ризики для соціальної стабільності та культурної самобутності держави. Тому важливим завданням державної політики є підтримка національного культурного продукту. Важливу роль відіграє розвиток національної освіти, культури та інформаційної політики. Захист культурного простору є важливою складовою забезпечення національної безпеки.

Тема 5. Релігійна політика держави та етноконфесійні відносини (2 год.)

Релігійна політика держави визначає принципи взаємовідносин між державними інституціями та релігійними організаціями. Вона базується на принципах свободи совісті, рівності конфесій та відокремлення церкви від держави. У демократичних суспільствах держава гарантує громадянам право на свободу світогляду і віросповідання. Етноконфесійні відносини є важливим елементом суспільної стабільності. Релігійні організації можуть відігравати значну роль у формуванні духовних цінностей та моральних норм суспільства. Водночас міжконфесійні суперечності можуть ставати джерелом соціальних конфліктів. Тому важливим завданням державної політики є забезпечення міжконфесійної толерантності та діалогу. Особливу роль у цьому процесі відіграють міжрелігійні ініціативи та громадські організації. Релігійна політика має сприяти збереженню духовної спадщини та культурних традицій. Гармонійні етноконфесійні відносини сприяють зміцненню соціальної стабільності держави.

Тема 6. Мовна політика як елемент безпеки (2 год.)

Мовна політика є важливим напрямом державної політики, що визначає принципи використання мов у суспільстві. Мова виступає одним із головних елементів національної ідентичності та культурної єдності народу. Державна мовна політика

спрямована на забезпечення функціонування державної мови в усіх сферах суспільного життя. Водночас вона повинна гарантувати права національних меншин на збереження і розвиток власних мов. Неврегульованість мовних питань може призводити до соціальної напруги та політичних конфліктів. Тому мовна політика повинна бути зваженою та спрямованою на консолідацію суспільства. Важливим напрямом є розвиток освіти державною мовою та підтримка національної культури. Мова також відіграє важливу роль у формуванні інформаційного простору держави. Поширення державної мови сприяє зміцненню національної єдності. Таким чином мовна політика виступає важливим елементом соціокультурної та інформаційної безпеки.

Тема 7. Національна самоідентифікація (2 год.)

Національна самоідентифікація є процесом усвідомлення людиною своєї належності до певної нації. Вона формується під впливом історичних, культурних, мовних та духовних чинників. Важливу роль у формуванні національної ідентичності відіграє історична пам'ять народу. Також значення мають традиції, культура, релігія та система освіти. У сучасному світі процеси глобалізації можуть впливати на формування національної самосвідомості. Збереження національної ідентичності є важливим завданням державної культурної та освітньої політики. Патріотичне виховання сприяє зміцненню національної єдності та громадянської відповідальності. Важливим чинником є розвиток національної культури та підтримка культурних традицій. Національна самоідентифікація також пов'язана з усвідомленням спільних цінностей і історичної долі народу. Вона є основою формування громадянської солідарності та суспільної стабільності.

Тема 8. Основи державної інформаційної політики (2 год.)

Державна інформаційна політика є важливою складовою діяльності держави, спрямованою на регулювання інформаційних процесів у суспільстві. Вона визначає основні принципи, цілі та механізми функціонування інформаційного простору держави. Інформаційна політика спрямована на забезпечення доступу громадян до достовірної інформації та розвиток демократичних комунікацій. Важливим завданням держави є формування національного інформаційного простору та захист інформаційного суверенітету. Державна інформаційна політика передбачає розвиток засобів масової інформації, інформаційних технологій та систем комунікації. Вона також включає підтримку національного інформаційного продукту. Особливе значення має забезпечення свободи слова та плюралізму думок. Разом з тим держава повинна протидіяти поширенню дезінформації та інформаційних маніпуляцій. Інформаційна політика повинна сприяти розвитку інформаційної культури суспільства. Ефективна державна інформаційна політика є важливим чинником забезпечення інформаційної безпеки держави.

Тема 9. Основні положення інформаційної безпеки (2 год.)

Інформаційна безпека є складовою національної безпеки та спрямована на захист інформаційного простору держави. Вона включає систему заходів, спрямованих на захист інформації, інформаційних ресурсів і комунікаційних систем. Основними

загрозами інформаційній безпеці є дезінформація, пропаганда, маніпуляція суспільною свідомістю та кіберзлочинність. В умовах інформаційного суспільства інформаційна безпека набуває особливого значення. Важливим завданням держави є створення ефективної системи захисту інформаційних ресурсів. Інформаційна безпека також передбачає захист прав громадян на доступ до інформації. Вона спрямована на забезпечення стабільності інформаційного середовища. Значну роль у забезпеченні інформаційної безпеки відіграють державні органи, засоби масової інформації та громадянське суспільство. Важливим напрямом є розвиток інформаційної культури населення. Таким чином інформаційна безпека є важливим фактором стабільності сучасної держави.

Тема 10. Основні поняття інформаційного протиборства (2 год.)

Інформаційне протиборство є важливим елементом сучасних міжнародних відносин та політичних конфліктів. Воно передбачає використання інформації як інструменту впливу на суспільну свідомість та політичні процеси. Основними формами інформаційного протиборства є пропаганда, інформаційні операції та психологічний вплив. У сучасних умовах інформаційні технології значно розширюють можливості такого впливу. Інформаційне протиборство може здійснюватися через засоби масової інформації, соціальні мережі та інші комунікаційні канали. Метою інформаційних операцій є формування певних політичних установок і поведінкових моделей у суспільстві. Такі процеси можуть використовуватися як інструмент політичної боротьби. Інформаційне протиборство часто є складовою гібридних конфліктів. Тому держави повинні розробляти ефективні механізми протидії інформаційним загрозам. Розуміння основ інформаційного протиборства є необхідним для забезпечення інформаційної безпеки держави.

Тема 11. Інформаційна безпека України. Сучасний стан, проблеми та перспективи (2 год.)

Інформаційна безпека України є важливим елементом національної безпеки держави. В умовах сучасних геополітичних викликів питання захисту інформаційного простору набуває особливої актуальності. Україна стикається з різноманітними інформаційними загрозами, серед яких пропаганда, дезінформація та інформаційні атаки. Важливим завданням держави є формування ефективної системи протидії таким загрозам. Значну роль у цьому процесі відіграє розвиток національних медіа та інформаційних ресурсів. Важливим напрямом є також підвищення рівня медіаграмотності населення. Інформаційна безпека передбачає захист національних інтересів у інформаційному просторі. Для цього необхідне вдосконалення законодавчої бази та інституційних механізмів. Перспективи розвитку інформаційної безпеки пов’язані з інтеграцією до міжнародних систем безпеки. Ефективна інформаційна політика сприяє зміцненню державного суверенітету України.

Тема 12. Методи та заходи забезпечення інформаційної безпеки України (2 год.)

Забезпечення інформаційної безпеки держави передбачає застосування комплексу правових, організаційних та технічних заходів. Важливим елементом є створення ефективної системи державного управління інформаційною сферою. До методів забезпечення інформаційної безпеки належать правове регулювання інформаційних відносин та контроль за дотриманням законодавства. Значну роль відіграють технологічні засоби захисту інформаційних систем. Важливим напрямом є протидія дезінформації та інформаційним маніпуляціям. Не менш важливою є підготовка фахівців у сфері інформаційної безпеки. Держава повинна підтримувати розвиток національного інформаційного простору. Значення має також міжнародне співробітництво у сфері кібербезпеки. Комплексний підхід до забезпечення інформаційної безпеки дозволяє ефективно протидіяти сучасним загрозам. Це сприяє стабільності інформаційного середовища держави.

Тема 13. Система та політика забезпечення інформаційної безпеки України (2 год.)

Система забезпечення інформаційної безпеки України включає сукупність державних органів, правових норм та організаційних механізмів. Вона спрямована на захист інформаційного простору та національних інтересів держави. Основними суб'єктами забезпечення інформаційної безпеки є державні інституції, правоохоронні органи та спеціалізовані служби. Важливу роль відіграють також засоби масової інформації та громадянське суспільство. Державна політика у цій сфері визначає стратегічні напрями розвитку інформаційної безпеки. Вона передбачає формування ефективної системи моніторингу інформаційних загроз. Важливим завданням є координація діяльності різних органів влади. Політика інформаційної безпеки повинна відповідати сучасним викликам інформаційного суспільства. Значну роль відіграє міжнародна співпраця у сфері інформаційної безпеки. Розвиток цієї системи є важливою умовою захисту інформаційного суверенітету держави.

Тема 14. Політико-правові основи інформаційної безпеки (2 год.)

Політико-правові основи інформаційної безпеки визначають правові принципи функціонування інформаційної сфери. Вони формуються на основі національного законодавства та міжнародних правових норм. Основними принципами є захист прав людини, свобода слова та інформаційна безпека держави. Законодавство регулює відносини у сфері створення, поширення та використання інформації. Важливим завданням є забезпечення балансу між свободою інформації та захистом національних інтересів. Правові норми також визначають відповідальність за порушення інформаційного законодавства. У сучасному світі політико-правове регулювання інформаційної сфери постійно удосконалюється. Важливу роль відіграє гармонізація національного законодавства з міжнародними стандартами. Політико-правові механізми сприяють формуванню безпечного інформаційного середовища. Вони є важливою складовою системи інформаційної безпеки держави.

Тема 15. Правова відповідальність за правопорушення в інформаційній сфері (2 год.)

Правопорушення в інформаційній сфері становлять серйозну загрозу для функціонування інформаційного простору держави. До таких правопорушень належать незаконне поширення інформації, кіберзлочини, маніпуляції інформацією та порушення авторських прав. Законодавство передбачає різні види відповідальності за порушення інформаційних правовідносин. Це може бути адміністративна, цивільна або кримінальна відповідальність. Особливу небезпеку становлять кіберзлочини та незаконне втручання у роботу інформаційних систем. Правові механізми спрямовані на запобігання таким правопорушенням. Важливим є розвиток міжнародного співробітництва у боротьбі з кіберзлочинністю. Значну роль відіграють правоохоронні органи та спеціалізовані служби. Підвищення рівня правової культури населення також сприяє зменшенню кількості інформаційних правопорушень. Ефективна система відповідальності забезпечує стабільність інформаційного простору держави.

Тема 16. Основи національної безпеки держави (2 год.)

Національна безпека є комплексною системою захисту життєво важливих інтересів держави, суспільства та особи. Вона охоплює політичну, економічну, соціальну, військову, культурну та інформаційну сфери. Основною метою національної безпеки є забезпечення стабільності та суверенітету держави. Важливу роль у цій системі відіграє державна політика безпеки. Національна безпека передбачає захист територіальної цілісності та конституційного ладу. Вона також спрямована на забезпечення прав і свобод громадян. У сучасних умовах значення набувають нові загрози, пов’язані з інформаційними та кібернетичними впливами. Система національної безпеки включає діяльність державних інституцій та спеціалізованих органів. Важливим є також розвиток міжнародного співробітництва у сфері безпеки. Ефективна система національної безпеки є основою стабільного розвитку держави.

Тема 17. Культурна безпека як складова національної безпеки (2 год.)

Культурна безпека є важливим елементом національної безпеки держави. Вона пов’язана із захистом культурної спадщини, традицій та духовних цінностей суспільства. Культура відіграє важливу роль у формуванні національної ідентичності. Втрата культурної самобутності може призвести до ослаблення національної єдності. У сучасному світі культурна безпека зазнає впливу глобалізаційних процесів. Поширення масової культури може призводити до витіснення традиційних культурних форм. Тому важливим завданням державної політики є підтримка національної культури. Значну роль у цьому процесі відіграють освіта, наука та мистецтво. Культурна безпека також передбачає розвиток культурного простору держави. Забезпечення культурної безпеки сприяє збереженню духовної спадщини народу.

Тема 18. Сучасні релігійно-церковні процеси в Україні (2 год.)

Релігійне життя України характеризується значним конфесійним різноманіттям. На території держави діють різні християнські конфесії, а також інші релігійні спільноти. Релігійні організації відіграють важливу роль у духовному житті

суспільства. Вони сприяють формуванню моральних цінностей та духовного розвитку людини. Сучасні релігійно-церковні процеси пов'язані з активізацією міжконфесійного діалогу. Водночас у релігійній сфері можуть виникати конфлікти та суперечності. Держава повинна забезпечувати рівність усіх конфесій перед законом. Важливим принципом є свобода совісті та віросповідання. Релігійні організації також беруть участь у суспільному та благодійному житті країни. Гармонійні міжконфесійні відносини сприяють соціальній стабільності.

Тема 19. Методи та заходи забезпечення інформаційної безпеки (2 год.)

Забезпечення інформаційної безпеки передбачає використання комплексу різноманітних методів і заходів. До них належать правові, організаційні, технічні та освітні механізми захисту інформаційного простору. Важливим напрямом є створення ефективної системи інформаційного моніторингу. Також необхідно розвивати засоби протидії інформаційним загрозам. Значну роль відіграє підвищення рівня медіаграмотності населення. Освітні програми сприяють формуванню критичного мислення. Держава повинна підтримувати розвиток національного інформаційного продукту. Важливим є також розвиток кіберзахисту інформаційних систем. Комплексний підхід дозволяє ефективно протидіяти сучасним інформаційним викликам. Це сприяє формуванню стабільного інформаційного середовища.

Тема 20–21. Система і політика забезпечення інформаційної безпеки та інформаційного простору в інших державах (4 год.)

Різні держави світу розробляють власні системи забезпечення інформаційної безпеки. Вони враховують національні особливості, політичну систему та рівень розвитку інформаційних технологій. У багатьох країнах створено спеціалізовані органи, що відповідають за захист інформаційного простору. Важливу роль відіграє державна інформаційна політика. Значну увагу приділяють протидії дезінформації та інформаційним атакам. Розвинені країни активно впроваджують системи кіберзахисту. Вони також розвивають міжнародне співробітництво у сфері інформаційної безпеки. Значення має і розвиток медіаграмотності населення. Порівняльний аналіз міжнародного досвіду дозволяє визначити ефективні механізми захисту інформаційного простору. Цей досвід може бути використаний для вдосконалення системи інформаційної безпеки України.

Тема 22. Інформаційні війни та інформаційно-психологічна безпека держави (2 год.)

Інформаційні війни є важливим елементом сучасних конфліктів. Вони передбачають використання інформації як засобу впливу на суспільну свідомість. Основною метою інформаційної війни є формування потрібних політичних установок у населення. Інформаційно-психологічний вплив може здійснюватися через медіа, соціальні мережі та інші канали комунікації. Значну роль відіграють пропаганда та дезінформація. Інформаційні операції можуть впливати на політичні процеси та громадську думку. У сучасному світі інформаційні війни часто є складовою гібридних конфліктів. Тому держави повинні розробляти ефективні

механізми протидії таким загрозам. Важливим є розвиток системи інформаційно-психологічного захисту. Це сприяє зміцненню національної безпеки держави.

Тема 23. Інформаційна безпека в умовах кіберцивілізації (2 год.)

Сучасне суспільство характеризується стрімким розвитком інформаційних технологій та формуванням глобального кіберпростору. Це створює нові можливості для комунікації, обміну інформацією та розвитку економіки. Водночас виникають нові загрози інформаційній безпеці. Серед них особливе місце займають кіберзлочини, хакерські атаки та незаконне втручання у роботу інформаційних систем. Кіберпростір стає важливою сферою міжнародного протиборства. Тому держави приділяють значну увагу розвитку систем кібербезпеки. Важливим є також захист персональних даних та інформаційних ресурсів. Значну роль відіграє підвищення цифрової грамотності населення. Формування культури безпечної поведінки у цифровому середовищі є необхідною умовою сучасного суспільства. Забезпечення інформаційної безпеки в умовах кіберцивілізації є одним із ключових завдань державної політики.

Тематика та зміст практичних(семінарських) занять

Семінарське заняття № 1

Основи національної безпеки держави

Термінологічний мінімум: безпека, національна безпека, нація, життєво важливі інтереси, особистість, суспільство, держава, національні інтереси, теорія національної безпеки, концепція, загроза, безпека особистості, безпека суспільства, безпека держави, система забезпеченнянаціональної безпеки.

Зміст семінарського заняття

1. Основні поняття національної безпеки:
   1.1. Визначення національної безпеки.
   1.2. Основні категорії теорії національної безпеки.
   1.3. Фактори та засоби забезпечення національної безпеки.
2. Характеристика основних видів національної безпеки:
   2.1. Рівні національної безпеки.
   2.2. Види національної безпеки.
3. Система забезпечення національної безпеки в Україні.
   3.1. Визначення системи забезпечення національної безпеки.
   3.2. Функції системи забезпечення національної безпеки.
   3.3. Повноваження суб'єктів забезпечення національної безпеки.

Завдання для обов'язкового виконання

Матеріали лекції доповнити за посібником Кормич Б. Інформаційна безпека: організаційно-правові основи : [навч. посіб.] / Кормич Б. – К. : Кондор, 2004. – 384 с. Законспектувати параграфи:

- історія формування категорії „національна безпека". – С. 8 – 16;
- правове регулювання питань національної безпеки. – С. 16 – 31;
- національна безпека та національні інтереси. – С. 31 – 39.

Рекомендована література

1. Карпенко В. Основи професіональної комунікації / Карпенко В. – К. : Нора-прінт, 2002. – 348 с.
2. Кормич Б. Інформаційна безпека: організаційно-правові основи : [навч. посіб.] / Кормич Б. – К. : Кондор, 2004. – 384 с.
3. Основи інформаційного права України : [навч. посіб.] / [Цимбалюк В., Павловський В., Грищенко В. та ін.] ; за ред. М. Швеця, Р. Калюжного, П. Мельника. – К. : Знання, 2004. – 274 с.
4. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. – К. : Текст,2004. – 136 с.
5. Юдін О. Інформаційна безпека держави : [навч. посіб.] / О. Юдін, В. Богуш. – Х. : Консул, 2005. – 576 с.

Семінарське заняття № 2

Культурна безпека як складова національної безпеки

Термінологічний мінімум: безпека, національна безпека, нація, життєво важливі інтереси, особистість, суспільство, держава, національні інтереси, теорія національної безпеки, концепція, загроза, безпека особистості, безпека суспільства, безпека держави, система забезпеченнянаціональної безпеки.

Зміст семінарського заняття

1. Культурна політика як інструмент політики національної безпеки держави

2. Культурна безпека особистості.

3. Культурна безпека як складова національної безпеки.

4. Культурна самобутність як чинник та основа національної безпеки держави.

Завдання для повторення.

С. Хантінгтон «Зіткнення цивілізацій». Концепція «Конфлікту цивілізацій» С. Хантінгтон
https://www.academia.edu/7883787/%D0%A2%D0%B5%D0%BE%D1%80%D1%96%D1%8F_%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D1%96%D0%BA%D1%82%D1%83_%D1%86%D0%B8%D0%B2%D1%96%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9_%D0%A5%D0%B0%D0%BD%D1%82%D1%96%D0%BD%D0%B3%D1%82%D0%BE%D0%BD%D0%B0

Завдання для самостійної роботи.

Опрацюйте статтю

«Інститут Тараса Шевченка»: культурний ресурс національної безпеки .
https://www.prostir.ua/?blogs=instytut-tarasa-shevchenka-kulturnyj-resurs-natsionalnoji-bezpeky

Рекомендована література

1. А. Борканюк file:///C:/Users/Home/Downloads/Nznuoafs_2011_9_11%20(1).pdf

2. В. Малімон . Культурна безпека як важлива складова сталого розвитку та національної безпеки.

https://molodyivchenyi.ua/index.php/journal/article/view/2695/2677

3. І. Каріх. Культурна політика як інструмент політики національної безпеки. https://eppd13.cz/wp-content/uploads/2017/2017-4-2/23.pdf

Семінар 3-4

Сучасні релігійно-церковні процеси в Україні. Релігійна політика як фактор безпеки. (4 год)

Термінологічний мінімум: Релігія, церква, релігійна організація, конфесія, державно-церковні відносини, свобода совісті, релігійна політика держави, релігійний плюралізм, міжконфесійні відносини, релігійна безпека, національна безпека, духовна безпека, міжрелігійний діалог.

Зміст семінарського заняття

1.Філософсько-релігійні та соціально-культурні підвалини формування ідеї Бога в християнстві.

2.Тенденції церковно-релігійного життя в період незалежності:

-Українська Православна Церква Московського Патріархату.

-УАПЦ в період незалежності України.

-Українська Православна Церква Київського Патріархату.

-Православна Церква України.

-Українська Греко – Католицька Церква,Римо – Католицька Церква.

- Етноконфесійні та нові релігійні організації в Україні (Іслам, Іудаїзм, Караїзм та ін)

3.Релігійний чинник у процесах національної консолідації. Український екуменізм як шлях до гармонізації міжконфесійних відносин.

4.Релігійна свобода і безпека в Україні в умовах російської агресії.

Завдання для обов'язкового виконання

Підготувати доповіді на такі теми:

1. Особливості розвитку релігійного життя в Україні у XXI столітті.

2. Конфесійна структура сучасної України.
3. Основні принципи державної політики у сфері свободи совісті.
4. Роль міжконфесійного діалогу у зміцненні суспільної стабільності.
5. Вплив релігійних організацій на формування духовної та національної безпеки держави.

Рекомендована література:

Основна:

1. Бондарчук П. М., Даниленко В. М., Крупина В. О., Кубальський О. Н. Релігійна політика в Україні у 1960-х – 1980-х роках і сучасна практика міжконфесійних відносин. Київ: Інститут історії України НАН України, 2010. 210 с.
2. Державно-конфесійні відносини в Україні: сучасний стан та тенденції розвитку / За ред. В. Д. Бондаренка, І. М. Мищака. Київ: Видав- ництво НПУ ім. М. П. Драгоманова, 2012. 518 с.
3. Історія православної церкви в Україні: збірка наукових праць. Київ: Четверта хвиля, 1997. 292 с.
4. Історія релігії в Україні: навчальний посібник / За ред. А. М. Колодного, П. Л. Яроцького. Київ: Знання, КОО, 1999. 735 с.
5. Історія релігії в Україні: у 10 т. Т. 10. Релігія і Церква років незалежності України / За ред. А. Колодного. Дрогобич: Коло, 2003. 616 с.
6. Колодний А. Україна в її релігійних виявах. Львів: СПОЛОМ, 2005. 336 с.
7. Панченко П. П. Релігійні конфесії в Україні (40-і – початок 90-х рр.). Київ: Інститут історії України АН України, 1993. 49 с.
8. Україна. Закони. Закон України «Про свободу совісті та релігійні організації». Київ: Парламентське видавництво, 1998. 23 с.

Додаткова:

1. Арістова А. В. Релігійні конфлікти в сучасному світі: природа, вияви, шляхи врегулювання. Київ: НТУ, 2007. 336 с.
2. Войналович В., Єленський В., Кирюшко М., Кочан Н., Рубльова Н. Релігійний чинник у процесах націє- та державотворення: досвід сучасної України. Київ: Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України, 2012. 272 с.
3. Екуменізм і проблеми міжконфесійних відносин в Україні / За заг. ред. А. Колодного, П. Яроцького, О. Сагана. Київ: Гносис, 2001. 278 с.
4. Здіорук С. І. Суспільно-релігійні відносини: виклики XXI століття. Київ: Знання України, 2005. 552 с.
5. Україна релігійна. Колективна монографія. Кн. 1: Стан релігійного життя України. Київ, 2008. 436 с.
6. Україна релігійна. Колективна монографія. Кн. 2: Прогнози релігійних процесів України. Київ, 2008. 341 с.
7. Шуба О. В. Релігія в етнонаціональному розвитку України: політо-

логічний аналіз. Київ: Криниця, 1999. 323 с.

Інтернет-ресурси:

1. Всеукраїнська Рада Церков і релігійних організацій. Режим доступу: http://www.vrciro.org.ua/ua/
2. Інститут релігійної свободи. Режим доступу: https://irs.in.ua/ua
3. Православна Церква України. Режим доступу: https://www.pomisna.info/uk/
4. Релігійно-інформаційна служба України. Режим доступу: https://risu.org.ua
5. Українська Православна Церква [Московський патріархат]. Режим доступу: http://orthodox.org.ua
6. Держава і Церква в Україні-2019: підсумки року і перспективи розвитку відносин (інформаційні матеріали) // Інформаційні матеріали, підготовлені до чергового засідання постійно діючого круглого столу «Релігія і влада в Україні: проблеми взаємовідносин», 14 листопада 2019 р. за сприяння Представництва Фонду Конрада Аденауера в Україні. Київ, 201

Переглянути документальний кінофільм «Церква без Христа».
https://www.youtube.com/watch?v=iNtUcdzLfHo

Семінарське заняття № 5-6

(4 год.)

Основи державної інформаційної політики

Термінологічний мінімум: Державна інформаційна політика, інформаційна безпека, інформаційний суверенітет, стратегічні комунікації, національний інформаційний простір, медіа, державне регулювання інформації, дезінформація, пропаганда, інформаційний контроль, інформаційні ресурси, кібербезпека, громадська думка.

Зміст семінарського заняття

1.Основні положення державної інформаційної політики:

1.1. Визначення державної інформаційної політики.

1.2. Поняття про програму входження держави в інформаційне суспільство.

2. Основні напрями національної інформаційної політики:

2.1. Основні напрями національної інформаційної політики у сфері суспільних відносин.

2.1. Основні напрями національної інформаційної політики векономічній сфері.

2.1. Основні напрями національної інформаційної політики ворганізаційній сфері.

3. Державна політика забезпечення інформаційної безпеки:

3.1. Основні поняття політики забезпечення інформаційної безпеки держави.

3.2. Основні загрози інформаційній безпеці держави.

3.3. Організаційний напрям протидії загрозам у сфері інформаційної безпеки.

3.3. Захист прав і свобод людини та громадянина.

3.5. Розвиток матеріально-технічної бази системи інформаційної безпеки особи, держави та суспільства.

3.6. Науково-практична робота щодо забезпечення інформаційної безпеки.

3.7. Удосконалення нормативно-правової бази забезпечення загальнодержавної системи інформаційної безпеки.

Завдання для обов'язкового виконання

Підготувати доповіді на такі теми:

1. Основні цілі та завдання державної інформаційної політики України.
2. Законодавче забезпечення інформаційної політики в Україні.
3. Механізми реалізації державної інформаційної політики.
4. Роль стратегічних комунікацій у забезпеченні національної інформаційної безпеки.
5. Перспективи розвитку державної інформаційної політики у цифрову епоху.

Рекомендована література

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін**.** Інформаційна безпека : навчальний посібник. Львів : Львівська політехніка, 2019.
2. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. Інформаційна безпека : підручник. Київ : Ліра-К, 2021.
3. Макаренко Є. А. **Міжнародна інформаційна безпека : підручник.** Київ : КНУ ім. Т. Шевченка, 2021.
4. Дубов Д. В**.** Кібербезпека та інформаційна безпека держави. Київ : НІСД, 2021.
5. Стратегія інформаційної безпеки України. Указ Президента України, 2021.
6. Закон України «Про національну безпеку України». Київ, 2018.

7. Закон України «Про основні засади забезпечення кібербезпеки України». Київ, 2017.

Семінарське заняття № 7
Основні положення інформаційної безпеки

Термінологічний мінімум: інформаційна безпека, інформаційне середовище, національний інформаційний простір, поінформованість особистості, інформаційна безпека особистості, інформаційна безпека держави (суспільства), концепція інформаційної безпеки держави, дестабілізуючі фактори, міждержавні дестабілізуючі фактори, загрози інформаційній безпеці, інформаційна зброя, забезпечення інформаційної безпеки, державна система забезпечення інформаційної безпеки держави, інформаційний патронат, інформаційне забезпечення інформаційної безпеки, інформаційний захист, інформаційна кооперація, інформаційна могутність, інформаційний потенціал.

Зміст семінарського заняття

1. Поняття інформаційної безпеки:
   - 1.1. Визначення інформаційної безпеки.
   - 1.2. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.
   - 1.3. Об'єкти та суб'єкти інформаційної безпеки.
   - 1.4. Види інформаційної безпеки.
   - 1.5. Концепція інформаційної безпеки держави.
2. Загрози інформаційній безпеці:
   - 2.1. Дестабілізуючі фактори інформаційної безпеки.
   - 2.2. Класифікація загроз інформаційній безпеці.
   - 2.3. Джерела загроз інформаційній безпеці.
3. Методи й засоби забезпечення інформаційної безпеки:
   - 3.1. Основні принципи забезпечення інформаційної безпеки.
   - 3.2. Система забезпечення інформаційної безпеки держави.
   - 3.3. Основні форми і способи забезпечення інформаційної безпеки держави.
4. Країни Європи в світовому інформаційному просторі і системи інформаційної безпеки:
   - 4.1. Конфігурація світового інформаційного простору і місце країн Європив ньому.
   - 4.2. Системи інформаційної безпеки в країнах Європи (Великобританія, Німеччина, Росія).

Завдання для обов'язкового виконання

1. Перше питання доповнити за такими джерелами:
   - Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. –К. : Текст, 2004. – 136 с. (С. 46 – 47);
   - Основи інформаційного права України : [навч. посіб.] / [Цимбалюк В., Павловський В., Грищенко В. та ін.] ; за ред. М. Швеця, Р. Калюжного, П. Мельника. – К. : Знання, 2004. – 274 с. (С. 219 – 220).
2. До другого питання. Основні типи інформаційних загроз виписати з таких джерел:
   - Литвиненко О. Інформаційна безпека Європи / Литвиненко В. – К., 1999. (С. 4 – 7);
   - 10. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. – К. : Текст, 2004. – 136 с. (С. 34).
3. Третє питання доповнити за такими джерелами:
   - Литвиненко О. Інформаційна безпека Європи / Литвиненко В. – К., 1999. (С. 10 – 24) /Напрями забезпечення інформаційної безпеки/;
   - Основи інформаційного права України : [навч. посіб.] / [Цимбалюк В., Павловський В., Грищенко В. та ін.] ; за ред. М. Швеця, Р. Калюжного, П. Мельника. – К. : Знання, 2004. – 274 с. (С. 217) /Напрями інформаційної безпеки/.
4. Четверте питання опрацювати самостійно за посібником Литвиненко О. Інформаційна безпека Європи / Литвиненко В. – К., 1999. /крім України/ (С. 25 – 33). Звернути особливу увагу на критерії, щохарактеризують такі поняття як інформаційна могутність та інформаційний потенціал (С. 27).
5. Накреслити самостійно схеми на основі матеріалів лекції та опрацьованих самостійно джерел:
   1) основні типи інформаційних загроз;
   2) напрями забезпечення інформаційної безпеки.

Рекомендована література

1. Кормич Б. Інформаційна безпека: організаційно-правові основи : [навч. посіб.] / Кормич Б. – К. : Кондор, 2004. – 384 с.
2. Литвиненко О. Інформаційна безпека Європи / Литвиненко В. – К., 1999.
3. Основи інформаційного права України : [навч. посіб.] / [Цимбалюк В., Павловський В., Грищенко В. та ін.] ; за ред. М. Швеця, Р. Калюжного, П. Мельника. – К. : Знання, 2004. – 274 с.
4. Юдін О. Інформаційна безпека держави : [навч. посіб.] / О. Юдін, В. Богуш. –Х. : Консул, 2005. – 576 с.

Семінарське заняття № 8-9
Основні поняття інформаційного протиборства

Термінологічний мінімум: інформаційне протиборство, інформаційна сфера, інформаційна війна, інформаційна перевага, концепція інформаційної війни, тероризм, інформаційні злочини, пасивне забезпечення інформаційної безпеки, активне забезпечення інформаційної безпеки.

Зміст семінарського заняття

1. Визначення поняття "інформаційне протиборство".
2. Інформаційна війна.
3. Інформаційний тероризм.
4. Інформаційна злочинність.
5. Інформаційне протиборство як форма забезпечення. інформаційної безпеки.

Завдання для обов'язкового виконання

Підготувати доповіді на такі теми:

1. Основні поняття інформаційної війни: історія і сучасність.
2. Основні поняття та форми психологічної війни.
3. Дезінформування як особливий прийом психологічної війни.
4. Патогенний текст як загроза інформаційно-психологічній безпеці.

Рекомендована література

1. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. – К. : Текст,2004. – 136 с.
2. Потятиник Б. Патогенний текст / Б. Потятиник, М. Лозинський. – Львів : Місіонер, 1996. – 296 с.
3. Почепцов Г. Информация & дезинформація / Почепцов Г. – К. : Ника-центр, Эльга, 2001. – 256 с.
4. Почепцов Г. Как ведутся тайные войны: Психологические операции в современном мире / Почепцов Г. – Х. : Консум, 2000. – 200 с.
5. Почепцов Г. Теорія комунікації / Почепцов Г. – К. : Видавничо-поліграфічний центр „Київський університет", 1999. – 308 с.

Семінарське заняття № 10 -11
Інформаційна політика та інформаційна безпека в Україні (4 год.)

Термінологічний мінімум: Інформаційна політика держави, інформаційна безпека, інформаційний простір, національні інтереси в інформаційній сфері, інформаційний суверенітет, інформаційні загрози, дезінформація, пропаганда, кібербезпека, інформаційна агресія, медіаграмотність, стратегічні комунікації, кіберзагрози, інформаційна інфраструктура.

Зміст семінарського заняття

1. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
2. Загрози інформаційній безпеці України.
3. Джерела загроз інформаційній безпеці України.
4. Стан інформаційної безпеки України.
5. Завдання і забезпечення інформаційної безпеки України.

Завдання для обов'язкового виконання

Підготувати доповіді на такі теми:

1. Інформаційна політика України в умовах гібридної війни.
2. Дезінформація та пропаганда як загрози інформаційній безпеці держави.
3. Роль кібербезпеки у забезпеченні інформаційної безпеки України.
4. Медіаграмотність як засіб протидії інформаційним загрозам.
5. Інформаційний суверенітет держави: зміст та механізми забезпечення.

Рекомендована література

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. Інформаційна безпека : навч. посіб. Львів : Львівська політехніка, 2019.
2. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. Інформаційна безпека : підручник. Київ : Ліра-К, 2021.
3. Почепцов Г. Г. Пропаганда та інформаційні війни. Київ : Києво-Могилянська академія, 2019.
4. Макаренко Є. А. Міжнародна інформаційна безпека : підручник. Київ : КНУ ім. Тараса Шевченка, 2021.
5. Дубов Д. В. Кібербезпека та інформаційна безпека держави. Київ : НІСД, 2021.

6. Стратегія інформаційної безпеки України. Указ Президента України, 2021.
7. Закон України «Про національну безпеку України». Київ, 2018.
8. Закон України «Про основні засади забезпечення кібербезпеки України». Київ, 2017.

Семінарське заняття № 12-13
Методи та заходи забезпечення інформаційної безпеки України
(4 год.)

Термінологічний мінімум: Інформаційна безпека, інформаційна політика держави, захист інформаційного простору, інформаційна інфраструктура, кібербезпека, інформаційні загрози, інформаційна агресія, стратегічні комунікації, інформаційні системи, телекомунікаційні системи, інформаційний суверенітет, національна інформаційна безпека, інформаційний захист, кіберзахист.

Зміст семінарського заняття

1. Загальні методи забезпечення інформаційної безпеки України.
2. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя:
   2.1. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.
   2.2. Забезпечення інформаційної безпеки України у сфері зовнішньої політики.
   2.3. Забезпечення інформаційної безпеки України в галузі науки та техніки.
   2.4. Забезпечення інформаційної безпеки України у сфері духовного життя.
   2.5. Забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах.
   2.6. Забезпечення інформаційної безпеки України у сфері оборони.
   2.7. Забезпечення інформаційної безпеки України у правоохоронній і судовій сферах.
   2.8. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.
   3.Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки.

Завдання для обов'язкового виконання

Підготувати доповіді на такі теми:

1. Методи державної політики у сфері забезпечення інформаційної безпеки України.
2. Роль стратегічних комунікацій у протидії інформаційним загрозам.

3. Кібербезпека як складова національної безпеки держави.
4. Захист інформаційної інфраструктури України в умовах цифровізації.
5. Інформаційна безпека в умовах гібридної війни.

Рекомендована література

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. **Інформаційна безпека : навчальний посібник.** Львів : Львівська політехніка, 2019.
2. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. **Інформаційна безпека : підручник.** Київ : Ліра-К, 2021.
3. Почепцов Г. Г. **Пропаганда та інформаційні війни.** Київ : Києво-Могилянська академія, 2019.
4. Макаренко Є. А. **Міжнародна інформаційна безпека : підручник.** Київ : КНУ ім. Тараса Шевченка, 2021.
5. Дубов Д. В. **Кібербезпека та інформаційна безпека держави.** Київ : НІСД, 2021.
6. **Закон України «Про національну безпеку України».** Київ, 2018.
7. **Закон України «Про основні засади забезпечення кібербезпеки України».** Київ, 2017.
8. **Стратегія інформаційної безпеки України.** Указ Президента України, 2021.

Семінарське заняття № 14
Система та політика забезпеченняінформаційної безпеки України
(2год.)

Термінологічний мінімум: Система інформаційної безпеки, інформаційна політика держави, національна безпека, інформаційний суверенітет, інформаційний простір, стратегічні комунікації, державне управління інформаційною сферою, кібербезпека, інформаційна інфраструктура, інформаційні загрози, державна інформаційна політика, інформаційний захист.

Зміст семінарського заняття

1. Основні функції системи забезпечення інформаційної безпеки України.
2. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
3. Основні положення політики забезпечення інформаційної безпеки України.

4. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.

Завдання для обов'язкового виконання

1. Із посібника Кудрявцева С. Міжнародна інформація : [навч. посіб.] /С. Кудрявцева, В. Колос. – К. : Видавничий Дім „Слово", 2005. – 400 с. виписати:
   - взаємодія категорій інформація та державна політика (С. 246 – 250);
   - основні напрями державної інформаційної політики (С. 250 – 254);
   - захист національного інформаційного простору (С. 255 – 262).

Завдання для обов'язкового виконання

Підготувати доповіді на такі теми:

1. Система забезпечення інформаційної безпеки України: структура та функції.
2. Роль державних інституцій у формуванні інформаційної політики України.
3. Стратегія інформаційної безпеки України: основні положення та напрями реалізації.
4. Механізми протидії дезінформації та інформаційній агресії.
5. Роль громадянського суспільства у забезпеченні інформаційної безпеки держави.

Рекомендована література

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. Інформаційна безпека : навчальний посібник. Львів : Львівська політехніка, 2019.
2. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. Інформаційна безпека : підручник. Київ : Ліра-К, 2021.
3. Почепцов Г. Г. Пропаганда та інформаційні війни. Київ : Києво-Могилянська академія, 2019.
4. Макаренко Є. А. Міжнародна інформаційна безпека : підручник. Київ : КНУ ім. Тараса Шевченка, 2021.
5. Дубов Д. В. Кібербезпека та інформаційна безпека держави. Київ : НІСД, 2021.
6. Закон України «Про національну безпеку України». Київ, 2018.
7. Закон України «Про основні засади забезпечення кібербезпеки України». Київ, 2017.
8. Стратегія інформаційної безпеки України. Указ Президента України, 2021.
9. Кудрявцева С. Міжнародна інформація : [навч. посіб.] / С. Кудрявцева, В. Колос. – К. : Видавничий Дім „Слово", 2005. – 400 с.

10. Гриценко О. Основи теорії міжнародної журналістики / О. Гриценко, В. Шкляр. – К. : Видавничо-поліграфічний центр „Київський університет”,2002. – 304 с.

11. Дубас О. Інформаційний розвиток сучасної України у світовому контексті /Дубас О. – К. : Генеза, 2004. – 208 с.

12. Карпенко В. Антиукраїнські тенденції в українській державі / Карпнко В. – : Акціонерне товариство „Київська книжкова фабрика”, 2001. – 112 с.

13. Литвиненко О. Інформаційна безпека Європи / Литвиненко В. – К., 1999.

14. Юдін О. Інформаційна безпека держави : [навч. посіб.] / О. Юдін,В. Богуш. – Х. : Консул, 2005. – 576 с.

15. Климчук О. О. Забезпечення інформаційної безпеки у провідних країнах світу : навч. посіб. / [О. О. Климчук, Д. С. Мельник, В. М. Панченко, В. М. Петрикта ін.] ; за заг. ред. В. М. Петрика. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. – 260 с.

Семінарське заняття № 15
Система та політика забезпечення інформаційної безпеки та інформаційного простору в інших державах
(4 год.)
Зміст семінарського заняття

Термінологічний мінімум: Інформаційна безпека держави, інформаційна політика, інформаційний суверенітет, кібербезпека, національна інформаційна інфраструктура, стратегічні комунікації, інформаційна війна, кіберзахист, інформаційний простір, цифрова безпека, державне регулювання інформаційної сфери, міжнародна інформаційна безпека.

Зміст семінарського заняття

1. Загальні підходи до формування системи інформаційної безпеки в зарубіжних державах.

2. Особливості політики інформаційної безпеки у країнах Європейського Союзу.

3. Система забезпечення інформаційної безпеки у Сполучених Штатах Америки.

4. Особливості забезпечення інформаційної безпеки у країнах Азії.

5. Міжнародне співробітництво у сфері інформаційної безпеки.

Завдання для обов’язкового виконання

Підготуйте порівняльну таблицю моделей інформаційної безпеки (США – ЄС – Китай – Україна)

Підготувати доповіді на такі теми:

1. Моделі забезпечення інформаційної безпеки у зарубіжних державах.
2. Політика інформаційної безпеки Європейського Союзу.
3. Система кібербезпеки Сполучених Штатів Америки.
4. Особливості державного контролю інформаційного простору у країнах Азії.
5. Роль міжнародного співробітництва у забезпеченні глобальної інформаційної безпеки.

Рекомендована література

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. **Інформаційна безпека : навчальний посібник.** Львів : Львівська політехніка, 2019.
2. Остроухов В. В., Присяжнюк М. М., Фармагей О. І. **Інформаційна безпека : підручник.** Київ : Ліра-К, 2021.
3. Почепцов Г. Г. **Інформаційні війни та інформаційна політика.** Київ : Києво-Могилянська академія, 2018.
4. Макаренко Є. А. **Міжнародна інформаційна безпека : підручник.** Київ : КНУ ім. Тараса Шевченка, 2021.
5. Дубов Д. В. **Кібербезпека та інформаційна безпека держави.** Київ : НІСД, 2021.
6. **Стратегія інформаційної безпеки України.** Указ Президента України, 2021.
7. **Закон України «Про основні засади забезпечення кібербезпеки України».** Київ, 2017.

Індивідуальні завдання(тематика есе)

1. Вплив глобалізації на національний культурний простір різних народів.
2. Протистояння етнокультур масовій культурі.
3. Культурна експансія як загроза соціальній стабільності.
4. Релігійна політика держави та етноконфесійні відносини.
5. Мова як чинник національної ідентичності. Мовна політика.
6. Національна самоідентифікація.
7. Інформаційна безпека як вид національної безпеки.
8. Загрози інформаційній безпеці.
9. Методи й засоби забезпечення інформаційної безпеки.
10. Країни Європи у світовому інформаційному просторі й системи інформаційної безпеки.
11. Патогенний текст як загроза інформаційно-психологічній безпеці.
12. Основні поняття інформаційної війни: історія і сучасність.
13. Основні поняття та форми психологічної війни.
14. Дезінформування як особливий прийом психологічної війни.
15. Державна політика забезпечення інформаційної безпеки.
16. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
17. Система та політика забезпечення інформаційної безпеки України.
18. Інформаційний простір України як чинник національної безпеки.
19. Інформаційна експансія Росії в український інформаційний простіряк загроза національній державності.
20. Український книжковий ринок та стратегія державної інформаційної політики.
21. Створення та розбудова мережі книгорозповсюдження та книжкової

торгівлі.

22. Інформаційне забезпечення функціонування українського книжкового ринку засобами масової комунікації України.
23. Програма підтримки перекладів українських книжок іноземними мовами.
24. Видання перекладів іноземних книг українською мовою.
25. Участь українських видавців та авторів у міжнародних та національних книжкових ярмарках, форумах, виставках тощо.
26. Роль дитячої книги у формуванні національної самосвідомості.
27. Функціонування бібліотечної системи України.
28. Підготовка і видання підручників для початкової, середньої та вищої школи в Україні
29. Характеристика новин загальнонаціональних телеканалів.
30. Тема України в закордонних ЗМІ.

Питання на колоквіуми

Колоквіум № 1

Поняття інформаційної безпеки та інформаційноїполітики

1. Визначення національної безпеки.
2. Основні категорії теорії національної безпеки.
3. Фактори та засоби забезпечення національної безпеки.
4. Рівні національної безпеки.
5. Види національної безпеки.
6. Визначення системи забезпечення національної безпеки.
7. Функції системи забезпечення національної безпеки.
8. Повноваження суб'єктів забезпечення національної безпеки.
9. Визначення інформаційної безпеки.
10. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.
11. Об'єкти та суб'єкти інформаційної безпеки.
12. Види інформаційної безпеки.
13. Концепція інформаційної безпеки держави.
14. Дестабілізуючі фактори інформаційної безпеки.
15. Класифікація загроз інформаційній безпеці.
16. Джерела загроз інформаційній безпеці.
17. Основні принципи забезпечення інформаційної безпеки.
18. Система забезпечення інформаційної безпеки держави.
19. Основні форми і способи забезпечення інформаційної безпеки держави.
20. Визначення поняття "інформаційне протиборство".
21. Інформаційна війна.
22. Інформаційний тероризм.
23. Інформаційна злочинність.
24. Інформаційне протиборство як форма забезпечення інформаційної безпеки.
25. Визначення державної інформаційної політики.
26. Поняття про програму входження держави в інформаційне суспільство.
27. Основні напрями національної інформаційної політики у сфері суспільних відносин.
28. Основні напрями національної інформаційної політики в економічній сфері.
29. Основні напрями національної інформаційної політики в

організаційній сфері.

30. Основні поняття політики забезпечення інформаційної безпеки держави.
31. Основні загрози інформаційній безпеці держави.
32. Організаційний напрям протидії загрозам у сфері інформаційної безпеки.
33. Захист прав і свобод людини та громадянина.
34. Розвиток матеріально-технічної бази системи інформаційної безпеки особи, держави та суспільства.
35. Науково-практична робота щодо забезпечення інформаційної безпеки.
36. Удосконалення нормативно-правової бази забезпечення загальнодержавної системи інформаційної безпеки.

Колоквіум № 2

Інформаційна політика та інформаційна безпека вУкраїні

1. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
2. Загрози інформаційній безпеці України.
3. Джерела загроз інформаційній безпеці України.
4. Стан інформаційної безпеки України.
5. Завдання і забезпечення інформаційної безпеки України.
6. Загальні методи забезпечення інформаційної безпеки України.
7. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.
8. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.
9. Забезпечення інформаційної безпеки України у сфері зовнішньої політики.
10. Забезпечення інформаційної безпеки України в галузі науки та техніки.
11. Забезпечення інформаційної безпеки України у сфері духовного життя.
12. Забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах.
13. Забезпечення інформаційної безпеки України у сфері оборони.
14. Забезпечення інформаційної безпеки України в правоохоронній і судовій сферах.
15. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.
16. Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки.

17. Основні функції системи забезпечення інформаційної безпеки України.
18. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
19. Основні положення політики забезпечення інформаційної безпеки України.
20. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.

Рекомендовані до опрацювання курси на платформах самоосвіти (або інші на вибір студента).

Prometheus

- Prometheus. Медіаграмотність: як не піддаватися маніпуляціям? https://prometheus.org.ua/course/course-v1:Prometheus+MEDIA_L101+2022_T3
- Prometheus. Культура та політика: багатозначність (взаємо)зв'язків https://prometheus.org.ua/course/course-v1:UCF+PCR101+2019_T3
- Prometheus. Інформаційна гігієна під час війни. https://prometheus.org.ua/course/course-v1:Prometheus+IHWAR101+2022_T2
- Prometheus. Інформаційна безпека. https://prometheus.org.ua/course/course-v1:Internews+INFOS101+UA_2021_T3
- Prometheus. Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні https://prometheus.org.ua/course/course-v1:Prometheus+IH101+2021_T3
- Prometheus. Дезінформація: види, інструменти та способи захисту. https://prometheus.org.ua/course/course-v1:Prometheus+DISINFO101+2021_T2
- Prometheus. Захист релігійних прав та свобод в Україні в умовах змін. https://prometheus.org.ua/course/course-v1:LCILHR+PRRF101+2021_T1
- Prometheus. Інформаційні війни. https://prometheus.org.ua/course/course-v1:KNU+102+2015_T2
- Prometheus. Основи інформаційної безпеки. https://prometheus.org.ua/course/course-v1:KPI+IS101+2014_T

ED ERA

- Знай свою Україну. Онлайн- курс про українську традиційну культуру.
  .

Питання на екзамен

1. Визначення національної безпеки.
2. Основні категорії теорії національної безпеки.
3. Фактори та засоби забезпечення національної безпеки.
4. Рівні національної безпеки.
5. Види національної безпеки.
6. Визначення системи забезпечення національної безпеки.
7. Функції системи забезпечення національної безпеки.
8. Повноваження суб'єктів забезпечення національної безпеки.
9. Визначення інформаційної безпеки.
10. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.
11. Об'єкти та суб'єкти інформаційної безпеки.
12. Види інформаційної безпеки.
13. Концепція інформаційної безпеки держави.
14. Дестабілізуючі фактори інформаційної безпеки.
15. Класифікація загроз інформаційній безпеці.
16. Джерела загроз інформаційній безпеці.
17. Основні принципи забезпечення інформаційної безпеки.
18. Система забезпечення інформаційної безпеки держави.
19. Основні форми і способи забезпечення інформаційної безпеки держави.
20. Визначення поняття "інформаційне протиборство".
21. Інформаційна війна.
22. Інформаційний тероризм.
23. Інформаційна злочинність.
24. Інформаційне протиборство як форма забезпечення інформаційної безпеки.
25. Визначення державної інформаційної політики.
26. Поняття про програму входження держави в інформаційне суспільство.
27. Основні напрями національної інформаційної політики у сфері суспільних відносин.
28. Основні напрями національної інформаційної політики в економічній сфері.
29. Основні напрями національної інформаційної політики в організаційній сфері.
30. Основні поняття політики забезпечення інформаційної безпеки держави.
31. Основні загрози інформаційній безпеці держави.
32. Організаційний напрям протидії загрозам у сфері інформаційної

безпеки.

33. Захист прав і свобод людини та громадянина.
34. Розвиток матеріально-технічної бази системи інформаційної безпеки особи, держави та суспільства.
35. Науково-практична робота щодо забезпечення інформаційної безпеки.
36. Вдосконалення нормативно-правової бази забезпечення загальнодержавної системи інформаційної безпеки.
37. Національні інтереси України в інформаційній сфері та шляхи їхнього забезпечення.
38. Загрози інформаційній безпеці України.
39. Джерела загроз інформаційній безпеці України.
40. Стан інформаційної безпеки України.
41. Завдання і забезпечення інформаційної безпеки України.
42. Загальні методи забезпечення інформаційної безпеки України.
43. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.
44. Забезпечення інформаційної безпеки України у сфері внутрішньої політики.
45. Забезпечення інформаційної безпеки України у сфері зовнішньої політики.
46. Забезпечення інформаційної безпеки України в галузі науки та техніки.
47. Забезпечення інформаційної безпеки України усфері духовного життя.
48. Забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах.
49. Забезпечення інформаційної безпеки України у сфері оборони.
50. Забезпечення інформаційної безпеки України в правоохоронній і судовій сферах.
51. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.
52. Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки.
53. Основні функції системи забезпечення інформаційної безпеки України.
54. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
55. Основні положення політики забезпечення інформаційної безпеки України.
56. Першочергові заходи щодо реалізації політики забезпечення інформаційної безпеки України.

Термінологічний мінімум

Активне забезпечення інформаційної безпеки спрямоване на завчасне виявлення та попередження загроз.

Безпека – стан, при якому кому-небудь, чому-небудь не загрожує небезпека будь-якого виду, існує захист від небезпеки.

Безпека держави – положення, при якому державі не загрожує небезпека. Досягається наявністю ефективного механізму управління і координації діяльності політичних сил та громадських груп, а також активних інститутів (органів) їхнього захисту.

Безпека особистості – положення, при якому особистості не загрожує небезпека. Безпека особистості полягає у формуванні комплексу правових і моральних норм, суспільних інститутів та організацій, що дозволили розвивати й реалізовувати соціально значущі здібності й потреби, не зазнаючи при цьому протидії держави й суспільства.

Безпека суспільства – наявність суспільних інститутів, норм, розвинених форм суспільної свідомості, які дозволяють реалізувати права та свободи всіх груп населення і протистояти діям, що ведуть до розколу суспільства (зокрема і з боку держави).

Держава – сукупність офіційних органів влади в цій чи іншій країні, основний заклад і спосіб політико-правової організації життя суспільства начолі з одноособовим або колективним правителем, органами виконавчої та інших видів влади й вертикальною системою управління, за допомогою якої здійснюється влада, охороняється існуючий лад, забезпечується нормальне життя людей.

Державна система забезпечення інформаційної безпеки держави являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система становить найважливішу ланку системи інформаційної безпеки особистості, суспільства й держави в правовій державі.

Життєво важливі інтереси – сукупність потреб, задовольняння яких надійно забезпечує існування і можливості прогресивного розвитку особистості, суспільства й держави.

Дестабілізуючі фактори – явища та процеси природного й штучного походжень, що породжують інформаційні загрози.

Забезпечення інформаційної безпеки – сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства й держави в інформації.

Загроза – можлива небезпека, тобто здатність заподіяти будь-якушкоду, призвести до будь-якого нещастя.

Загрози інформаційній безпеці – 1. сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері; 2. дія чи подія, що може призвести до руйнування, спотворення чи несанкціонованого власником чи володільцем доступу до інформаційних ресурсів.

Найбільшу загрозу інформаційній безпеці становить: можливість утрати, порушення цілісності або блокування інформації; відкриття конфіденційної інформації; несанкціоноване використання ресурсів; помилкове використання ресурсів; несанкціонований обмін інформацією; відмова від інформації; відмова від обслуговування.

Інтереси держави в інформаційній сфері полягають у:

– створенні умов для гармонічного розвитку інформаційної інфраструктури України;

– реалізації конституційних прав і свобод людини й громадянина в галузі одержання інформації й користування нею з метою забезпечення непорушності конституційного ладу, суверенітету й територіальної цілісності України, політичної, економічної та соціальної стабільності;

– забезпеченні законності та правопорядку, розвитку рівноправного й взаємовигідного міжнародного співробітництва.

Інтереси особистості в інформаційній сфері полягають у:

– реалізації конституційних прав особи й громадянина на доступ до інформації, а також на використання інформації в інтересах здійснення діяльності, яка не заборонена законом;

– у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають у:

– забезпеченні інтересів особистості в цій сфері;
– зміцненні демократії;
– створенні правової соціальної держави;
– досягненні й підтримці суспільної злагоди;
– у духовному відновленні України.

Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційною безпекою варто розуміти єдність захисту наступних компонентів:

– системи виробництва інформаційних продуктів;
– системи доставки інформаційних продуктів до споживача;
– системи виробництва засобів виробництва інформаційних продуктівта їх доставки;
– системи виробництва інформаційних технологій;
– системи накопичення і збереження інформаційних продуктів;
– системи сервісного обслуговування елементів інформаційної інфраструктури;
– системи підготовки кадрів.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, уражаючих державні інтереси тощо) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Інформаційна безпека особистості – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо.

Інформаційна безпека України – стан захищеності її національних інтересів у інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства й держави.

Інформаційна війна – комплекс заходів і операцій, спрямованих на забезпечення інформаційної переваги щодо потенційного або реального противника.

Інформаційна зброя – сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу протилежної сторони з метою руйнування її інформаційної інфраструктури, системи управління державою, зниження духовного потенціалу суспільства.

Інформаційна кооперація – форма забезпечення інформаційної безпеки між рівноправними суб’єктами інформаційного процесу (фізичними,

юридичними, міжнародними), що включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі та інформаційні загрози й захист від них доступними законними способами й засобами.

Інформаційна перевага розуміють ситуацію, що надає можливість змінити уявлення противника про дійсну обстановку й позбавити його здатності прогнозувати подальші події та впливати на них.

Інформаційна політика держави – це головні напрями й предмет діяльності держави в галузі інформації.

Інформаційна сфера – сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації.

Інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхнє оброблення, обмін інформацією між органами управління і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Інформаційне середовище – сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням та споживанням інформації.

Інформаційне суспільство – 1. органічний сегмент глобального інформаційного товариства, а також забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захист національних моральних і культурних цінностей, забезпечення конституційних прав на свободу слова та вільний доступ до інформації; 2. суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її вищої форми – знань; 3. суспільство, в якому діяльність людей грунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

Інформаційний патронат (захисник) є формою забезпечення інформаційної безпеки фізичних і юридичних осіб із боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори й загрози стану поінформованості фізичних і юридичних осіб (інформаційне забезпечення

інформаційної безпеки) та власне захист життєво важливих інтересів цих осібвід інформаційних загроз, або, як ще кажуть, інформаційний захист.

Інформаційні злочини можуть вчинятися із використанням як інформаційно комп'ютерних, так й інформаційно психологічних методів впливу.

Концепція слугує юридичним актом, що містить керівні принципи та цільові настанови щодо шляхів, засобів та методів захисту життєво важливих інтересів людини, групи, суспільства та держави.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення.

Концепція інформаційної війни – система поглядів на інформаційну війну та шляхи її ведення.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Національна безпека – категорія політичної науки (політології), що характеризує стан соціальних інститутів, що забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості, суспільства та держави. Вона відображає зв'язок безпеки з нацією.

Національний інформаційний простір – інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрація, накопичення, збереження, захист і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави.

Національні інтереси держави відображають фундаментальні цінності та прагнення народу, його потреби в гідних умовах життєдіяльності, а також цивілізовані шляхи їх створення й способи задоволення. Національні інтереси держави та їхня пріоритетність обумовлюються конкретною ситуацією, що складається в країні та за її межами.

Нація – стійка історична спільність людей, що визначається соціальними зв'язками певної формації і характеризується специфічними етнічними рисами, зумовленими особливостями економічного й культурного розвитку, спільністю території, мови, побуту, традицій і звичаїв, а також відображенням цих факторів у суспільній свідомості та суспільній психології.

Особистість – людина як суб'єкт відносин і свідомої діяльності. До життєво важливих інтересів особистості належать, насамперед права і свободи людини й громадянина, зокрема інформаційні.

Пасивне забезпечення інформаційної безпеки передбачає реагування на вже наявні загрози, спрямоване на безпосередню протидію акціям, що є деструктивними щодо соціальної системи.

Поінформованість особистості (суспільства та держави) – задоволення в будь-якій мірі потреб в інформації, що призводить до оволодіння відомостями про навколишній світ та процеси, що відбуваються у ньому.

Система забезпечення національної безпеки – організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства держави.

Суспільство – сукупність форм сумісної діяльності людей, що утворилися в процесі історичного розвитку. Життєво важливі інтереси суспільства зв'язані зі створенням і розвитком вільного, гуманного, високоосвіченого, гармонійного суспільства, заснованого на принципах демократи, бережливого ставлення до своїх традицій і національного надбання, суспільства, що підтримує і всіляко охороняє основний свій осередок – сім'ю.

Теорія національної безпеки – наука, що поєднує у собі прикладні аспекти соціальних, воєнних, гуманітарних, технічних, психологічних, біологічних та інших наук із метою дослідження суті, змісту, методів, форм і засобів забезпечення безпеки особистості, суспільства та держави.

Тероризм – загроза або використання насильства в політичних цілях окремими особами або групами, що можуть діяти як на боці, так і проти існуючого уряду, коли такі дії, спрямовані на те, щоб уплинути на більше число людей, ніж безпосередні жертви.

Список рекомендованої літератури

Література:

Нормативно-правові акти

1.Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки"

2. Розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року»

3. Рішення Ради національної безпеки і оборони України від 15.10.2021 «Про Стратегію інформаційної безпеки»

4. Закон України «Про інформацію»

5. Закон України «Про медіа»

6. Закон України «Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста»

7. Закон України «Про правовий режим воєнного стану»

8. Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції»

9. Указ Президента України від 24.02.2022 № 64/2022 «Про введення воєнного стану в Україні»

10. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану"

11. Наказ Головнокомандувача Збройних Сил України від 03.03.2022 № 73 «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану»

Підручники, посібники, статті:

1. Карпенко В. Основи професіональної комунікації / Карпенко В. – К. : Нора-прінт, 2002. – 348 с.
2. Кормич Б. Інформаційна безпека: організаційно-правові основи : [навч. посіб.] / Кормич Б. – К. : Кондор, 2004. – 384 с.
3. Основи інформаційного права України : [навч. посіб.] / [Цимбалюк В.,

Павловський В., Грищенко В. та ін.] ; за ред. М. Швеця, Р. Калюжного, П. Мельника. – К. : Знання, 2004. – 274 с.
4. Харченко Л. Інформаційна безпека України: Глосарій / Харченко Л., Ліпка В., Логінов О. / За заг. ред д. юрид. н., проф. Р. Калюжного. – К. : Текст, 2004. – 136 с.
5. Юдін О. Інформаційна безпека держави : [навч. посіб.] / О. Юдін, В. Богуш. – Х. : Консул, 2005. – 576 с.
6. А. Борканюк file:///C:/Users/Home/Downloads/Nznuoafs_2011_9_11%20(1).pdf
7. В. Малімон . Культурна безпека як важлива складова сталого розвитку та національної безпеки. https://molodyivchenyi.ua/index.php/journal/article/view/2695/2677
8. І. Каріх. Культурна політика як інструмент політики національної безпеки. https://eppd13.cz/wp-content/uploads/2017/2017-4-2/23.pdf
9. Україна релігійна. Колективна монографія. Кн. 1: Стан релігійного життя України. Київ, 2008. 436 с.
10. Україна релігійна. Колективна монографія. Кн. 2: Прогнози релігійних процесів України. Київ, 2008. 341 с.
11. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. **Інформаційна безпека : навч. посіб.** Львів : Львівська політехніка, 2019. 580 с.
12. Лизанчук В. В. **Інформаційна безпека України: теорія і практика : підручник.** Львів : ЛНУ ім. Івана Франка, 2017. 728 с.
13. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М., Петрикт В. М. **Інформаційна безпека : підручник.** Київ : Ліра-К, 2021. 411 с.
14. Макаренко Є. А., Рижков М. М., Кучмій О. П., Фролова О. М., Литвиненко Н. П. **Міжнародна інформаційна безпека : підручник.** Київ : Київський національний університет імені Тараса Шевченка, 2021.
15. Яковенко Є., Журавель І., Горбатий І., Бондарєв А. **Інформаційна безпека : навчальний посібник.** Київ : Центр навчальної літератури, 2018.
16. Ломака І.І., Липчук О.І., Кобець Ю.В. Інформаційна безпека держави: теоретико – методологічні засади та особливості в умовах збройного конфлікту // Регіональні студії № 31, ВД «Гельветика», 2022 р., с. 113 – 119. http://regionalstudies.uzhnu.uz.ua/index.php/31
17. Ломака І.І., Війна як чинник нестабільності в сучасній Україні та її вплив на сфери національної безпеки//Вісник Прикарпатського університету. Серія: Політологія / Прикарпатський національний університет імені Василя Стефаника. Одеса: Гельветика. 2024. Вип. 17. с 82 - 90. https://journals.pnu.if.ua/index.php/politology/issue/view/19/19
18. Липчук О.І., Ломака І. І.Співпраця України та міжнародних інституцій в контексті проблем застосування біологічної та хімічної зброї під час російської агресії в Україні. Вісник Прикарпатського університету. Серія: Політологія / Прикарпатський національний університет імені Василя Стефаника. Одеса: Гельветика. 2024. Вип. 19. с.105 -113.

https://journals.pnu.if.ua/index.php/politology/issue/view/21/21
19. Ломака І. І., Микитин А. Релігійна складова національної безпеки в Україні. Вісник Прикарпатського університету. Серія: Політологія / Прикарпатський національний університет імені Василя Стефаника. Одеса: Гельветика. 2024. Вип. 19. с.113 - 122. https://journals.pnu.if.ua/index.php/politology/issue/view/21/21
20.. Collins A. Contemporary Security Studies. 3rd ed. United Kingdom: Oxford University Press, 2013. 478 p.
21.. Potts M. The State Information Security. Network Security. 2012. Volume 2012. Issue 7. P. 9–
17. URL: https://www.sciencedirect.com/science/article/pii/S1353485812700648 (Last Accessed: 20.08.2020)

Додаткова література

1. Зубок М. І. Інформаційна безпека в підприємницькій діяльності : навчальний посібник**.** Київ : Кондор, 2014.
2. Почепцов Г. Г. Інформаційні війни. Київ : Києво-Могилянська академія, 2015.
3. Литвиненко О. В. Інформаційна безпека держави. **Київ** : НІСД, 2016.
4. Кастельс М. Влада комунікації. Київ : Ваклер, 2016.
5. Почепцов Г. Г. Пропаганда та інформаційні війни. Київ : Києво-Могилянська академія, 2019.
6. Гуревич С. М. Інформаційна політика та безпека держави. Київ : Академвидав, 2018.
7. Дзьобань О. П. Інформаційна безпека: філософські та соціальні аспекти. Харків : Право, 2017.
8. Токар Б. І. Інформаційна безпека України в умовах гібридної війни. Київ : НІСД, 2020.
9. Даниленко С. І. Інформаційна політика та національна безпека. Київ : КНЕУ, 2019.
10. Дубов Д. В. Кібербезпека та інформаційна безпека держави. Київ : НІСД, 2021.

Інтернет ресурси

1. Незалежний аналітичний центр геополітичних досліджень «БОРИСФЕН ІНТЕЛ» [Електронний ресурс]. - Режим доступу: http://bintel.com.ua/uk/page/about/
2. Міжнародні відносини і світова політика [Електронний ресурс]. - Режим доступу: http://iir-mp.narod.ru/irip.htm
3. Портал зовнішньої політики [Електронний ресурс]. - Режим доступу:

http://fpp.com.ua/analytics/
4. Близький схід та Африка. Міністерство закордонних справ України [Електронний ресурс]. - Режим доступу: https://mfa.gov.ua/dvostoronnye-spivrobitnictvo/blizkij-shid-ta-afrika
5. Національний інститут стратегічних досліджень [Електронний ресурс]. - Режим доступу: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosini/suchasni- tendencii-regionalizmu-v-skhidniy-azii-mozhlivosti
6. Рада зовнішньої політики «Українська призма» [Електронний ресурс]. - Режим доступу: http://prismua.org/regions/asia-and-pacific/
7. Глобал-аналітик [Електронний ресурс].Режим доступу: http://www.global-analityk.com/category/%d0%bc%d1%96%d0%b6%d0%bd%d0%b0%d1%80%d0%be%d0%b4%d0%bd%d0%b5-%d0%b6%d0%b8%d1%82%d1%82%d1%8f/
7. Майдан закордонних справ [Електронний ресурс]. - Режим доступу: https://www.mfaua.org/uk
8. https://ssu.gov.ua/ – офіційний сайт Служби безпеки України
9. http://itlaw.wikia.com/wiki/Profiling – Центр оцінки достовірності інформації «ДетектІнфо».
10. Глосарій гібридних загроз URL: https://warn-erasmus.eu/ua/glossary/
11. Електронний ресурс: Європейський центр з протидії гібридним загрозам Hybrid CoE URL: https://www.hybridcoe.fi/
12. Thiele R. D. Hybrid Threats – And how to counter them / R. D Thiele // ISPSW Strategy Series: Focus on Defense and International Security. – Issue No. 448, Sep 2016. – S. 2. URL : http://www.ispsw.com/wp-content/uploads/2016/09/448_Thiele_Oslo.pdf.
13. Understanding hybrid threats. Briefing European parliamentary research service. – June, 2015. URL : http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.

Інформаційні ресурси

14. **https://www.coursera.org**
15. **https://www.udemy.com/**
16. **https://prometheus.org.ua**
17. **https://www.ed-era.com**
18. **https://www.futurelearn.com**
19. **https://vumonline.ua**