МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Кафедра політичних теорій

КІБЕРЗАГРОЗИ В СУЧАСНОМУ ПОЛІТИЧНОМУ ПРОСТОРІ

МЕТОДИЧНІ ВКАЗІВКИ

для підготовки до практичних занять та самостійної роботи здобувачів вищої освіти другого (магістерського) рівня

галузі знань – 05 «Соціальні та поведінкові науки»,

спеціальність – 052 «Політологія»

Одеса
2024

УДК: 323.269
З133

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»
(*протокол № 1 від* 24 *вересня 2024 р.*)

Укладач:
Юлія ЗАВГОРОДНЯ –кандидат політичних наук, доцент, доцент кафедри політичних теорій, Національного університету «Одеська юридична академія».
ORCID ID 0000-0003-3500-8638

Рецензенти:

Алла СІЛЕНКО– доктор політичних наук, професор, професор кафедри мовної та психолого-педагогічної підготовки Одеського національного економічного університету;

Юлія ШМАЛЕНКО **–** кандидат політичних наук, доцент, доцент кафедри психології Національного університету «Одеська юридична академія».

З133 **Кіберзагрози в сучасному політичному просторі**: метод. вказівки для підготовки до практичних занять та самостійної роботи здобувачів вищої освіти другого (магістерського) рівня галузі знань – 05 «Соціальні та поведінкові науки», спеціальності – 052 «Політологія» [Електронне видання] / Ю. В. Завгородня; Нац. ун-т «Одеська юрид. академія». – Одеса, 2024. – 30 с. Режим доступу: https://hdl.handle.net/11300/28400

Методичні вказівки призначені для здобувачів вищої освіти галузі знань 052 Політологія з метою закріплення лекційного матеріалу та підготовки до практичних занять з дисципліни «Кіберзагрози в сучасному політичному просторі». Містять завдання до практичних занять та самостійної роботи.

УДК: 323.269

ЗМІСТ

ВСТУП

Навчальний курс «Кіберзагрози в сучасному політичному просторі» направлений на деталізацію вивчення кіберпростору, який активно використовується політичними суб'єктами з метою досягнення поставлених цілей. Окрім цього, кіберплощина використовується, як платформа для політичного протистояння, що може дестабілізувати політичні процеси та руйнувати усталені політичні порядки. Вивчення курсу допоможе сформувати цілісне уявлення про кіберзагрози у різних проявах, які притаманні кіберпростору; удосконалити знання про різновиди протиборства; отриманні знань про кібербезпеку; вивченню досвіду провідних країнах світу щодо кіберзахисту.

Метою викладання навчальної дисципліни «Кіберзагрози в сучасному політичному просторі» є формування системи знань про кіберзагрози в політичному процесі з деталізацією сучасних форм боротьби, з негативним впливом, який проявляється у кіберборотьбі, яка виходить за будь які сталі рамки розуміння кордонів держави.

Завданням курсу «Кіберзагрози в сучасному політичному просторі» є дослідження характеристики політичної діяльності в кіберпросторі; визначення індикаторів кіберзагроз в політичній взаємодії; оцінка політико-правових аспектів кібербезпеки України; характеристика деструктивних форм прояву політичної активності в кіберпросторі; дослідження кібервійни у сучасному геополітичному просторі; характеристика кіберконфліктів, як сучасної форми політичної взаємодії; визначення національних механізмів протидії кіберзагрозам; оцінка сучасних форм кіберзахисту політичних процесів у провідних країнах світу; дослідження проблем та перспектив удосконалення політичної діяльності щодо кіберзахисту.

На вивчення дисципліни відводиться 90 годин, 3 кредити ECTS (з них, 14 – лекційних, 16 – практичних, 60 – самостійна робота).

Форма підсумкового контролю – залік.

Перелік тем практичних занять:

№	Назва теми	Год.
Практичне заняття № 1.	Тема 1. Загальна характеристика політичної діяльності в кіберпросторі. Тема 2. Індикатори кіберзагроз в політичній взаємодії.	2
Практичне заняття № 2.	Тема 3. Політико-правові аспекти кібербезпеки України Тема 4. Деструктивні форми прояву політичної активності в кіберпросторі	2
Практичне заняття № 3.	Тема 5. Кібервійни у сучасному геополітичному просторі	2
Практичне заняття № 4.	Тема 6. Кіберконфлікти, як сучасна форма політичної взаємодії	2
Практичне заняття № 5.	Тема 7. Національні механізми протидії кіберзагрозам	2
Практичне заняття № 6.	Тема 8. Сучасні форми кіберзахисту політичних процесів у провідних країнах світу	2
Практичне заняття № 7.	Тема 9. Проблеми та перспективи удосконалення політичної діяльності щодо кіберзахисту	2
Практичне заняття №8.	Тема 9. Проблеми та перспективи удосконалення політичної діяльності щодо кіберзахисту	2

Рекомендації щодо підготовки здобувачів вищої освіти до практичних занять:

Ефективне проведення практичних занять потребує від здобувачів вищої освіти ґрунтовної попередньої підготовки за таким алгоритмом:

- Детально ознайомтеся з темою, метою та планом заняття.
- Проаналізуйте ключові проблеми, які потрібно розглянути.
- Опрацюйте рекомендовану літературу, зокрема наукові статті та методичні матеріали з теми. Робіть необхідні нотатки та виписки.
- Сформулюйте свою точку зору з дискусійних питань із відповідною аргументацією.
- Складіть чіткий план заняття, з визначенням ключового змісту, очікуваних проблем та етапів їх розв'язання під час аудиторної роботи.
- Заздалегідь підготуйте запитання до тих аспектів теми, які потребують обговорення чи уточнення під час заняття.

Рекомендації щодо організації самостійної роботи здобувачів вищої освіти:

Самостійна робота є важливою складовою навчання, оскільки сприяє кращому засвоєнню матеріалу та формуванню навичок у час, вільний від аудиторних занять.

Серед основних видів самостійної роботи здобувачів вищої освіти з дисципліни «Кіберзагрози в сучасному політичному просторі» можна виділити:

- Підготовка доповідей та повідомлень за темами практичних занять.
- Опрацювання рекомендованої літератури для обговорення проблемних питань.
- Пошук та огляд актуальних публікацій з досліджуваної тематики.
- Виконання навчальних завдань (кейсів, ситуативних вправ, тестів тощо).
- Підготовка аналітичних оглядів та есе з відповідних тем.

Завдання для самостійного опрацювання видаються на початку вивчення дисципліни, а терміни їх виконання чітко регламентуються. Передбачено поточний та підсумковий контроль результатів такої роботи здобувачів вищої освіти з боку викладача.

Вимоги академічної доброчесності:

Усі завдання, винесені на практичні заняття чи для самостійного опрацювання, мають виконуватися здобувачем вищої освіти особисто на основі здобутих знань та компетентностей.

При використанні ідей, тверджень, відомостей з літературних джерел чи інших інформаційних ресурсів обов'язково робити посилання на автора і джерело із дотриманням правил цитування.

При написанні роботи неприпустимим є плагіат, фабрикування джерел, списування, а також будь-яке спотворення чи приховування даних щодо авторського внеску здобувача вищої освіти.

Результати практичних завдань, досліджень, опитувань мають бути справжніми і не фабрикованими, отриманими самостійно, а не запозиченими без відповідних посилань.

Коректне представлення спільної роботи. Якщо завдання виконувалось у співавторстві з іншими здобувачами вищої освіти, то обов'язково зазначити особистий внесок в роботу та контрибуторів.

Дотримання цих та інших норм академічної доброчесності сприяє чесному і прозорому оцінюванню результатів навчання. Порушення принципів академічної доброчесності тягне за собою відмову у зарахуванні роботи.

Вимоги викладача:

Регулярне відвідування навчальних занять є необхідною умовою якісного засвоєння матеріалу дисципліни та набуття фахових компетентностей майбутніми спеціалістами.

Очікується, що здобувачі вищої освіти будуть присутні на всіх лекційних та практичних заняттях відповідно до розкладу та сумлінно виконуватимуть усі навчальні завдання. У випадку неможливості відвідати заняття (через хворобу тощо), здобувачі вищої освіти зобов'язані завчасно попередити про це викладача та у терміни, що не перевищують пропущені заняття, відпрацювати навчальний матеріал

та виконати поставлені завдання.

Користування електронними пристроями (телефони, планшетні ПК тощо) під час аудиторної роботи дозволяється тільки з дозволу викладача та у відповідних до навчального курсу цілях.

Для уникнення відставання у навчанні та отриманні своєчасного зворотного зв'язку вкрай важливо дотримуватися встановлених викладачем часових меж для подання робіт та оприлюднення результатів їх перевірки.

Оцінювання результатів навчання здобувачів вищої освіти щодо опанування навчальної дисципліни здійснюється відповідно до Положення про організацію освітнього процесу в Національному університеті «Одеська юридична академія».

Система нарахування балів з курсу базується на об'єктивному оцінюванні знань та вмінь здобувачів вищої освіти, продемонстрованих ними впродовж семестру під час практичних занять, виконання індивідуальних завдань та екзамену.

При цьому враховуються такі ключові аспекти:

- Сумлінна присутність та активна участь в обговореннях на заняттях.
- Успішне та своєчасне виконання поточних завдань згідно визначених вимог.
- Демонстрація глибоких знань та здатності їх самостійного застосування при вирішенні практичних кейсів.
- Ініціативність у навчанні та пошуку додаткових матеріалів для вивчення.

За певні порушення академічної доброчесності (списування, плагіат, фабрикація даних, порушення термінів подання робіт) передбачено зниження підсумкової оцінки або незарахування результатів навчання.

<table>
<tr><th colspan="4">Шкала оцінювання</th></tr>
<tr><td rowspan="2">100-бальною шкалою</td><td rowspan="2">Шкала за ECTS</td><td colspan="2">За національною шкалою</td></tr>
<tr><td>Екзамен</td><td>Залік</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>Fx</td><td rowspan="2">Незадовільно</td><td rowspan="2">Не зараховано</td></tr>
<tr><td>1-34</td><td>F</td></tr>
<tr><td colspan="4">Поточний контроль знань здобувачів освіти оцінюється за шкалою («2», «3», «4», «5»), з обов'язковим переведенням при підсумковому контролі оцінок в бали за допомогою шкали Університету до національної шкали та шкали ECTS.
Для отримання підсумкової оцінки здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних/лабораторних занять та поточних контрольних заходів (реферату, контрольної роботи, завдань до самостійної роботи тощо).
Для переводу підсумкової оцінки у 100 бальну шкалу оцінювання знань середньоарифметична підсумкова оцінка множиться на коефіцієнт 20.
Якщо протягом вивчення навчальної дисципліни здобувач освіти, який складає екзамен, набрав не менше ніж ½ від загальної кількості оцінок суму балів 90 та більше за шкалою оцінювання ECTS, то він має право отримати оцінку за набраними балами A/Відмінно без складання підсумкового контролю.
Здобувач освіти, який складає залік та набрав суму балів 60 та більше за шкалою оцінювання ECTS, отримує оцінку за набраними балами без складання підсумкового контролю. Якщо</td></tr>
</table>

здобувач освіти бажає покращити оцінку, отриману як середньоарифметичну результатів поточного контролю, то він може скласти залік.
Здобувач освіти, який набрав менше ніж ½ від загальної кількості оцінок на практичних/лабораторних занять та поточних контрольних заходах та/або менше ніж 60 балів (для залікової дисципліни) та менше ніж 90 балів (для екзаменаційної дисципліни) складає залік/екзамен відповідно в обов'язковому порядку.

Практичне заняття 1.
ТЕМА 1. Загальна характеристика політичної діяльності в кіберпросторі
ТЕМА 2. Індикатори кіберзагроз в політичній взаємодії

Теми загального циклу спрямовані на спрямована на розуміння політичної діяльності у кіберпросторі, що охоплює використання цифрових платформ для ведення агітації, організації кампаній, мобілізації виборців і впливу на громадську думку. Соціальні мережі, блоги та інші інтернет-ресурси стали важливими інструментами політичної комунікації, оскільки вони забезпечують швидке поширення інформації і можливість прямого зв'язку з аудиторією. Політичні партії, уряди та активісти все частіше використовують онлайн-середовище для просування своїх ідей і досягнення підтримки серед населення.

У фокусі уваги - загрози, зокрема кіберзлочинність, дезінформація, втручання у вибори та кібератаками. Основні індикатори загроз включають кібератаки на політичні сайти, крадіжку або підробку персональних даних, маніпуляцію громадською думкою через фейкові новини та бот-мережі, а також втручання іноземних держав у внутрішню політику. Небезпечні дії в кіберпросторі можуть мати серйозні наслідки для демократичних процесів, створюючи дестабілізацію та підриваючи довіру громадськості до політичних інститутів.

Відстеження таких загроз потребує системного підходу та використання сучасних інструментів кібербезпеки, зокрема моніторингу активності в соціальних мережах, аналізу інформаційних потоків і реагування на аномалії в поведінці користувачів. Важливою є також співпраця держав, міжнародних організацій та приватних компаній для забезпечення безпеки цифрової інфраструктури й захисту політичних процесів від зовнішніх впливів.

План практичного заняття:

1. Сутнісна характеристика кіберпростору в розвитку політичних процесів.
2. Кібермогутність і національна безпека держави.
3. Кіберпростір як сфера глобальних конфронтацій.
4. Основи безпеки кіберпростору в сучасному світі.
5. Науковий аналіз кібернетичних меж політичного протиборства.
6. Співвідношення понять «кіберзагрози» , «кібербезпека», «кіберконфлікти» в політичному аспекті.
7. Кіберпростір як новий вимір геополітичного суперництва. Різновиди кіберзагроз.
8. Відносини США – КНР як ключовий геополітичний наратив початку XXI сторіччя: співробітництво, суперництво, протистояння
9. Механізми реалізації кіберконфліктів у міжнародній політиці XXI сторіччя: хактивізм, кібершпигунство та кібердиверсії
10. Російсько-українська війна, як чинник кіберпротиборства.

Методичні вказівки до теми:

1. Опрацюйте базові поняття: «кіберзагрози» , «кібербезпека», «кіберконфлікти» в політичному аспекті. Зверніть увагу на визначення цих термінів та їх взаємозв'язок.

2. Вивчіть історію виникнення та становлення меж політичного протиборства в кіберпросторі.

3. Дослідіть основні теоретичні підходи та концепції, що застосовуються у світі щодо кібербезпеки.

4. Проаналізуйте відносини США – КНР. Визначити їх сильні та слабкі сторони.

5. Визначте механізми реалізації кіберконфліктів у міжнародній політиці XXI сторіччя.

6. Проаналізуйте актуальні напрями наукових досліджень у сучасній кібербезпеці. Наведіть конкретні приклади.

7. Дайте оцінку перспективам подальшого розвитку кіберпротиборства.

8. Підготуйте аналітичну доповідь за обраною Вами проблематикою в межах теми. Використовуйте різноманітні джерела.

Проблемні питання для обговорення:

1. Як кіберпростір впливає на трансформацію політичних процесів у сучасному світі?

2. Яким чином цифрові технології змінюють політичну комунікацію та взаємодію між громадянами і державою?

3. Що таке кібермогутність і як вона визначає роль держави у міжнародній системі безпеки?

4. Які компоненти формують кібермогутність держави і як вони впливають на її національну безпеку?

5. Які основні фактори провокують конфронтації у кіберпросторі між державами?

6. Як кіберпростір використовується державами як арена для міжнародних конфліктів?

7. Які головні принципи забезпечення кібербезпеки держави?

8. Які глобальні ініціативи існують для регулювання безпеки у кіберпросторі?

9. Які основні механізми кіберконфліктів використовуються у міжнародній політиці XXI століття?

10. Як хактивізм, кібершпигунство та кібердиверсії впливають на міжнародні відносини?

Завдання для самостійної роботи:

1. Оцінити роль кіберпростору в політичних процесах.
2. Провести аналіз кібернетичних меж політичного протиборства.
3. Підготувати порівняльний аналіз щодо кіберзагроз в країні тоталітарного режиму та демократичного режиму.
4. Дослідити кібердиверсії, як вплив на політичні рішення.

Практичне заняття 2
ТЕМА 3. Політико-правові аспекти кібербезпеки України
ТЕМА 4. Деструктивні форми прояву політичної активності в кіберпросторі

Тема спрямована на розуміння кібербезпеки як критично важливої складової національної безпеки України, особливо в умовах гібридної війни та зростаючої кіберзагрози з боку зовнішніх і внутрішніх акторів. Політико-правові аспекти кібербезпеки включають систему законодавчих та нормативних актів, які регулюють дії у сфері захисту кіберпростору. Україна, адаптуючись до європейських і міжнародних стандартів, запроваджує закони, спрямовані на боротьбу з кіберзлочинністю, захист критичної інфраструктури та інформаційних систем.

Зокрема, одним із важливих елементів є інтеграція України в глобальну систему кібербезпеки. Закон "Про основні засади забезпечення кібербезпеки України" визначає правові основи, механізми захисту кіберпростору та заходи протидії кіберзагрозам. Окрім того, тісна співпраця з ЄС, НАТО та іншими міжнародними організаціями дозволяє Україні отримувати експертну підтримку та розробляти ефективні стратегії кіберзахисту.

У фокусі уваги - кількісні та якісні методи аналізу, а також методи прогнозування міжнародних відносин. Розглядаються можливості і обмеження застосування різних методів. Окрема увага приділяється кількісним і якісним методам аналізу даних та моделям прогнозування розвитку кібернетичних відносин. Висвітлюються методи збору емпіричних даних в міжнародних дослідженнях: аналіз документів, опитування, інтерв'ю, фокус-групи, спостереження. Акцентується важливість комплексного методологічного підходу в аналізі та прогнозуванні кібернетичних тенденцій.

Кіберпростір сьогодні стає не лише платформою для комунікації та обміну інформацією, але й ареною для деструктивних форм політичної активності. До таких проявів можна віднести хактивізм, кібератаки на державні установи, пропаганду, дезінформацію та поширення фейкових новин. Політичні актори, як державні, так і недержавні, використовують кіберпростір для маніпуляцій громадською думкою та дестабілізації політичних процесів в окремих країнах.

План практичного заняття:

1. Особливості забезпечення принципів кібербезпеки в Україні.
2. Суб'єкти забезпечення кібербезпеки в державі.
3. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.
4. Міжнародне співробітництво у сфері кібербезпеки.
5. Місце і роль кіберзахисту в Збройних Силах України.
6. Сучасні форми політичної активності в кіберпросторі.
7. Деструкція, як специфічна форма прояву політичної взаємодії в кіберпросторі.
8. Способи та механізми впливу на політичне життя суб'єктів політики в кіберпросторі.

9. Виклики щодо використання кіберпростру суб'єктами політики : культурний та ідеологічний аспект.

Методичні вказівки до теми:

1. Опрацюйте базові поняття: «міжнародне співробітництво», «кібербезпека», «диструкція». Зверніть увагу на визначення цих термінів, їх сутнісні характеристики.

2. Вивчіть історію становлення та розвитку міжнародного співробітництва як напряму наукових досліджень.

3. Дослідіть еволюцію кібербезпеки від зародження до сучасного стану в світі.

4. Визначте роль кібербезпеки для міжнародної комунікації.

5. Дайте визначення поняттю «світова політика». Охарактеризуйте її структуру та учасників.

6. Проаналізуйте роль і значення аналізу та прогнозування міжнародного співробітництва у формуванні зовнішньої політики держав. Наведіть конкретні приклади.

7. Підготуйте письмову аналітичну доповідь за обраною вами проблематикою теми. Використовуйте додаткові наукові та аналітичні джерела.

Проблемні питання для обговорення:

1. Як українське законодавство адаптується до нових викликів у сфері кібербезпеки та чи відповідає воно міжнародним стандартам?

2. Які основні бар'єри заважають ефективній реалізації принципів кібербезпеки в Україні (інституційні, фінансові, технічні)?

3. Які державні інституції є ключовими суб'єктами забезпечення кібербезпеки в Україні, і як вони взаємодіють між собою?

4. Наскільки ефективно діє співпраця між державними і приватними суб'єктами у сфері кібербезпеки?

5. Які основні виклики стикаються з CERT-UA у питаннях реагування на комп'ютерні інциденти на національному рівні?

6. Яким чином CERT-UA співпрацює з міжнародними партнерами для протидії кіберзагрозам?

7. Які основні форми міжнародного співробітництва Україна використовує для зміцнення своєї кібербезпеки?

8. Як глобальні альянси (ЄС, НАТО) допомагають Україні у забезпеченні кіберзахисту, і чи існують перешкоди для подальшої інтеграції?

9. Яке значення надається розвитку кіберзахисту в рамках Збройних Сил України в умовах сучасних військових конфліктів?

10. Чи вистачає ресурсів для ефективного функціонування підрозділів кіберзахисту в ЗСУ?

Завдання для самостійної роботи:

1. Провести контент-аналіз законодавства України щодо кібербезпеки.

2. Оцінити технологічні аспекти потреб кіберзахисту в Збройних Силах України.

3. Визначити наслідки руйнівних дій політичних суб'єктів у кіберпросторі.

4. Провести компаративістський аналіз ролі ідеології та культури США та Китаю у кіберпротиборстві.

Практичне заняття 3.
ТЕМА 5. Кібервійни у сучасному геополітичному просторі

Тема присвячена аналізу кібервійни в сучасному геополітичному просторі , що стала невід'ємною частиною конфліктів між державами. Вона передбачає використання кіберінструментів для здійснення атак на інформаційну інфраструктуру супротивника з метою збору розвідданих, дезорганізації управління, а також для підриву економічних і військових систем. Кібератаки, такі як DDoS, зломи, крадіжка даних або впровадження шкідливого програмного забезпечення, стають ключовими елементами гібридних воєн, де традиційні військові дії поєднуються з цифровими атаками.

Основними цілями кібервійни є державні інституції, критична інфраструктура (енергетика, транспорт, фінанси), військові об'єкти, а також засоби масової інформації. Кібероперації можуть бути націлені як на безпосереднє завдання шкоди, так і на стратегічне маніпулювання інформаційними потоками, впливаючи на громадську думку чи виборчі процеси. У зв'язку з цим кібератаки стали інструментом політичного тиску та навіть способом досягнення військових або дипломатичних цілей без прямої збройної конфронтації.

На тлі глобальної цифровізації і зростаючої залежності від інформаційних технологій кібервійна становить серйозну загрозу міжнародній безпеці. Держави інвестують у розробку кіберзахисту та створення кіберпідрозділів у збройних силах. Водночас міжнародні організації та країни шукають способи вироблення норм і правил ведення кіберконфліктів, аби зменшити ризики ескалації та уникнути неконтрольованих наслідків кібероперацій на глобальному рівні.

План практичного заняття:

1. Історія становлення знань про кіберпотиборство.
2. Сутність поняття кібервійна: визначення, види, ознаки.
3. Предумови до розвитку кібервійни.
4. Перша світова кібервійна: причини та перспективи.
5. Проблеми щодо врегулювання кібервійни в межах кіберпростору: політичний аспект.

Методичні вказівки до теми:

1. Опрацюйте базове поняття «кібервійна». З’ясуйте роль кібервійни у розвитку кібербезпеки.
2. Вивчіть основні форми кібервійни.
3. Дослідіть базові засади передумов кібервійни.
4. Вивчіть основні відмінності між кіберконфліктом та кібервійною.
5. Проаналізуйте сильні та слабкі сторони реалізації кібервійни в сучасному світі.
6. Проаналізуйте проблеми щодо врегулювання кібервійни в сучасному кіберпросторі?
7. Здійсніть порівняння різних форм атак під час кібердій.

8. Підготуйте аналітичну доповідь щодо обраної Вами проблематики у межах теми.

Проблемні питання для обговорення:

1. Які політичні перешкоди існують для створення міжнародних угод щодо регулювання кібервійни?
2. Чому досягнення міжнародного консенсусу щодо правил кібервійни є складним завданням для світової спільноти?
3. Яку роль відіграють великі держави та їхні інтереси у блокуванні ініціатив по врегулюванню кібервійни на міжнародному рівні?
4. Як еволюціонували підходи до захисту інформаційних систем у різних етапах розвитку технологій?
5. Які історичні події стали ключовими в становленні знань про кіберконфлікти між державами?
6. Яке є найбільш загальновизнане визначення терміну "кібервійна", і в чому полягають основні труднощі його формулювання?
7. Які основні види кібервійни існують, і чим вони відрізняються за своїми методами та цілями?
8. Які ознаки кібервійни відрізняють її від інших видів кіберконфліктів, таких як кіберзлочинність чи інформаційні війни?
9. Як розвиток глобальної цифровізації та інтернету створив передумови для ведення кібервійни?
10. Які технологічні прориви в інформаційній безпеці стимулювали зростання загроз кібервійни?

Завдання для самостійної роботи:

1. Визначити інцидент (причину, що спонукала сторони), як основу кіберпротиборства, на прикладі кібервійни сучасності 2022-2024 років.
2. Оцінити проблеми щодо врегулювання кібервійни.

Практичне заняття 4.
ТЕМА 6. Кіберконфлікти, як сучасна форма політичної взаємодії

Тема спрямована на розкриття кіберконфліктів, які стали новою формою політичної взаємодії в сучасному світі, що суттєво змінює традиційні методи впливу на держави та міжнародні організації. Усе частіше кіберпростір використовується як арена для здійснення атак, спрямованих на дестабілізацію політичної системи або втручання у внутрішні справи країн. Атаки можуть мати різний характер — від викрадення даних та маніпуляції громадською думкою до атак на критичну інфраструктуру. Ця форма конфлікту дозволяє державам уникати відкритих військових дій, використовуючи цифрові інструменти для досягнення політичних або економічних цілей.

Кіберконфлікти відкривають нові можливості для держав та недержавних акторів впливати на міжнародну політику без прямого збройного втручання. Атаки у кіберпросторі можуть бути непомітними, складно визначити їх джерело, що дає можливість уникати відповідальності або прямих наслідків. Зокрема, це дозволяє вести "гібридні" війни, де кібероперації стають доповненням до інших форм політичного тиску, таких як економічні санкції, дипломатичні маніпуляції або інформаційні кампанії.

Водночас зростає важливість міжнародного співробітництва та вироблення спільних правил і норм поведінки в кіберпросторі. Оскільки кіберконфлікти можуть мати глобальні наслідки, держави все частіше визнають необхідність спільних ініціатив для кібербезпеки. Проте, політичні та стратегічні інтереси великих гравців часто ускладнюють процес створення міжнародних угод, що регулювали б кіберконфлікти, роблячи цей вид взаємодії особливо небезпечним і нестабільним у довгостроковій перспективі.

План практичного заняття:

1. Категоріально-понятійне осмислення політичних кіберконфліктів в сучасному світосприйнятті.
2. Доктринальні засади управління інформаційно-комунікаційними політичними процесами.
3. Типологізація політичних конфліктів в кіберпросторі.
4. Шляхи управління кіберконфліктами.

Методичні вказівки до теми:

1. Опрацюйте базове поняття «кіберконфлікти». Визначте його складові елементи.
2. Проаналізуйте еволюцію системи конфліктної взаємодії у світі.
3. Порівняйте однополярну, біполярну та багатополярну структури міжнародних систем щодо розвитку кіберконфліктів. Визначити їх особливості.
4. Проаналізуйте рівні розвитку кіберконфліктів: глобальний, регіональний, локальний. З'ясуйте їх специфіку.
5. Дослідіть основних суб'єктів кіберпротиборства: держави, міжурядові організації, ТНК, громадські організації тощо.

6. Вивчіть роль кіберконфліктів у світовій політиці. Наведіть конкретні приклади кіберконфліктів.

7. Проаналізуйте вплив транснаціональних корпорацій на кібернетичну стабільність.

Проблемні питання для обговорення:

1. Які стратегії та методи використовуються для врегулювання політичних конфліктів у кіберпросторі?

2. Яка роль міжнародних організацій, таких як ООН чи НАТО, у розробці інструментів для управління кіберконфліктами?

3. Які технологічні та дипломатичні підходи можна використовувати для зменшення ризиків ескалації кіберконфліктів у міжнародній політиці?

4. Як змінюються категорії та поняття політичних конфліктів у контексті їх переходу в кіберпростір?

5. Які головні концептуальні підходи до аналізу кіберконфліктів використовуються в сучасній політології?

6. Як сприйняття кіберконфліктів формує нові парадигми політичної взаємодії в глобальному масштабі?

7. Які основні типи кіберконфліктів існують у політичному контексті, і як вони класифікуються за характером і масштабом?

8. Як відрізняються між собою політичні кіберконфлікти за участю держав та недержавних акторів?

9. Які основні чинники впливають на ескалацію та поширення політичних конфліктів у кіберпросторі?

10. Яка роль державних інституцій та міжнародних організацій у формуванні політики кібербезпеки та управлінні кіберконфліктами?

Завдання для самостійної роботи:

1. Здійснити характеристику різновидів політичних конфліктів в кіберпросторі у вигляді таблиці з оцінкою кожного виду та прикладу його використання на практиці.

2. Визначити різницю між «політичним конфліктом» та «політичним кіберконфліктом».

3. Проаналізувати у вигляді таблиці інститути кібербезпеки на державному та міжнародному рівні.

Практичне заняття 5
ТЕМА 7. Національні механізми протидії кіберзагрозам

Тема спрямована на розуміння національних механізмів протидії кіберзагрозам, які ґрунтуються на комплексному підході до забезпечення кібербезпеки держави. Основою такої системи є нормативно-правова база, яка регулює використання інформаційно-комунікаційних технологій, а також визначає обов'язки державних органів і приватних компаній у сфері захисту кіберпростору. У багатьох країнах прийнято національні стратегії кібербезпеки, які окреслюють основні пріоритети, цілі та методи реагування на кіберзагрози. Ключову роль у цьому відіграють спеціальні державні структури, такі як кіберпідрозділи в рамках національних сил оборони або окремі агентства з кібербезпеки, які відповідають за моніторинг, попередження та реагування на інциденти.

Інтеграція державних механізмів протидії кіберзагрозам із приватним сектором є важливою складовою стратегії безпеки. Приватні компанії, зокрема ті, що керують критичною інфраструктурою (енергетика, транспорт, фінанси), часто стають головними цілями кіберзлочинців. Тому співпраця між державою і бізнесом через обмін інформацією, запровадження стандартів безпеки і проведення спільних навчань є необхідною для ефективного захисту від кібератак. Крім того, важливим є впровадження інструментів кіберрозвідки та кібермоніторингу, які дозволяють виявляти потенційні загрози на ранніх стадіях.

Міжнародне співробітництво також відіграє важливу роль у протидії кіберзагрозам. Оскільки кібератаки часто не мають чітких кордонів, держави активно взаємодіють з міжнародними організаціями, такими як НАТО, Європейський Союз або ООН, для координації зусиль і обміну інформацією про нові загрози. Створення загальноприйнятих стандартів і правил поведінки в кіберпросторі сприяє підвищенню рівня глобальної кібербезпеки і допомагає запобігати ескалації кіберконфліктів на міжнародній арені.

План практичного заняття:

1. Стан розвитку національних механізмів протидії кіберзагрозам.
2. Особливості організаційного забезпечення органів державної протидії кіберзагрозам.
3. Розбудова Національної системи кібернетичної безпеки: регіональний та глобальний аспект.

Методичні вказівки до теми:

1. Вивчіть поняття «кіберзагрози», «кібербезпека» та їхні складники у контексті міжнародниго співробітництва.
2. Дослідіть роль громадської думки в міжнародному співробітництві щодо протидії кіберзагрозам, проаналізуйте шляхи її формування та впливу.
3. Проаналізуйте вплив ЗМІ на формування громадської думки з питань міжнародної політики щодо кіберзагроз. Наведіть конкретні приклади.
4. Розгляньте вплив етнічного та релігійного факторів на характер протидії кіберзагрозам.

5. Дослідити роль політичного режиму на формування системи кіберзахисту окремими державами.

6. Проаналізуйте вплив російсько-української війни на розвиток міжнародної системи кібербезпеки.

7. Проаналізуйте окремі країни у їх діяльності щодо кіберзахисту.

Проблемні питання для обговорення:

1. Які міжнародні стандарти та практики кібербезпеки найчастіше використовуються для побудови національних систем кіберзахисту?

2. Які моделі співпраці між державами найбільш ефективні для глобального протидії кіберзагрозам?

3. Як регіональні організації, такі як ЄС або НАТО, сприяють розвитку національних систем кібербезпеки у своїх країнах-членах?

4. Які перспективи створення глобальної системи кібербезпеки та які ключові виклики стоять на шляху її реалізації?

5. Як оцінюється ефективність національних стратегій кібербезпеки у різних країнах?

6. Які фактори впливають на нерівномірний розвиток механізмів кіберзахисту між різними державами?

7. Яку роль відіграють державні та приватні сектори у формуванні національної політики протидії кіберзагрозам?

8. Які основні органи державної влади відповідають за протидію кіберзагрозам, і як між ними розподіляються повноваження?

9. Як організована міжвідомча взаємодія між різними структурами, що займаються кібербезпекою на державному рівні?

10. Як впроваджуються технології кібермоніторингу та кіберрозвідки в державні структури для боротьби з кіберзагрозами?

Завдання для самостійної роботи:

1. Відтворити структуру системи органів щодо національної кібернетичної безпеки.

2. Оцінити роль безпекових міжнародних організацій для захисту національної кібербезпеки.

Практичне заняття 6.
ТЕМА 8. Сучасні форми кіберзахисту політичних процесів у провідних країнах світу

Тема спрямована на розуміння сучасних форм кіберзахисту політичних процесів у провідних країнах світу, що базуються на розробці комплексних національних стратегій кібербезпеки, які охоплюють різні аспекти політичної та економічної діяльності. Наприклад, у США існують окремі програми для захисту виборчих процесів, розроблені після інцидентів втручання в вибори 2016 року. Основна увага приділяється захисту виборчих систем, попередженню кібератак на політичні партії та кандидатів, а також активній співпраці з приватним сектором для моніторингу кіберзагроз. Подібний підхід демонструють країни ЄС, де на основі GDPR (Загального регламенту захисту даних) вибудувана система захисту персональних даних, що включає політичну комунікацію та захист від інформаційних атак.

Кіберзахист політичних процесів також активно впроваджується у таких країнах, як Німеччина, Велика Британія та Франція, де було створено спеціальні урядові органи для боротьби з кіберзагрозами. Німеччина, наприклад, має Федеральне відомство з інформаційної безпеки (BSI), яке відповідає за забезпечення кібербезпеки державних установ та ключових політичних процесів, таких як вибори. Велика Британія та Франція також зміцнили свої структури кібербезпеки через створення національних центрів кібербезпеки, які координують захист виборчих процесів, а також проводять аналіз загроз і надають підтримку державним установам.

Міжнародне співробітництво є важливою частиною захисту політичних процесів від кібератак. Країни-члени НАТО, ЄС та інші міжнародні організації тісно співпрацюють у питаннях кібербезпеки, обмінюються інформацією та спільно розробляють стратегії захисту. Такі ініціативи, як Програма кіберзахисту НАТО, передбачають спільне навчання фахівців, тестування кіберсистем та реалізацію програм швидкого реагування на кібератаки. Це дозволяє підвищити стійкість політичних систем до втручання та забезпечити прозорість і безпеку демократичних процесів.

План практичного заняття:

1. Сполучені Штати Америки, як показник високого розвитку кібербезпеки.
2. Позиція Китаю щодо кіберзахисту в глобальному світі.
3. Особливості політичних дій щодо кібербезпеки європейськими країнами.
4. Виклики кіберзлочинності в цифрову епоху країн Африканського континенту.

Методичні вказівки до теми:

1. Вивчіть визначення поняття «дипломатія», її функції та роль у міжнародній співпраці.
2. Проаналізуйте роль дипломатії у кіберзахисті на глобальному рівні.

3. Визначте особливості позиції щодо кіберзахисту Балтійських країн.

4. Дослідіть види кіберзлочинності. Опрацюйте основні форми кіберзлочинності.

5. Проаналізуйте сутність і типологію кіберконфліктів.

4. Дослідіть роль міжнародних організацій у дипломатичному вирішенні кіберзагроз. Наведіть приклади.

5. Вивчіть поняття «третьої сторони» та її функції у вирішенні кіберзагроз.

6. Підготуйте аналітичну доповідь у межах теми.

Проблемні питання для обговорення:

1. Чи ефективна багатостороння система кіберзахисту у світі?

2. Чому міжнародна комунікація не запобігла російській агресії проти України в кібернетичному просторі?

3. Вчому специфіка політики КНР щодо кіберзахисту? Аналіз наслідків.

4. Чому саме ООН найчастіше виконує функції посередника у міжнародних протиріччях, конфліктах, війнах? Які її переваги та недоліки посереднецтва ООН у кібервійні?

5. Чи ефективною є «м'яка сила» ЄС у подоланні сучасної кібервійни?

6. Які проблеми у притягненні до відповідальності за кіберзлочини?

Завдання для самостійної роботи:

1. Проаналізувати систему кібербезпеки країн Балтії.

2. Дослідити геолокацію здійснення кібератак на країни європейського континенту.

Практичне заняття 7,8
ТЕМА 9. Проблеми та перспективи удосконалення політичної діяльності щодо кіберзахисту

Тема спрямована на розуміння проблем, які сформувалися у кіберпросторі щодо кіберпростору та потребують політичної комунікації на усіх рівнях управління з метою подолання критичних викликів. У темі аналізуються сутність, причини та перпективи можливого покращення політичної діяльності. Розглядаються ключові моделі глобального управління та їх вплив на формування системи кіберзахисту.

У фокусі уваги - проблеми ефективності та легітимності глобального управління в умовах кіберзагроз. Обговорюються шляхи удосконалення системи глобального управління. Розглядається роль глобальних гравців та інших багатосторонніх інституцій у забезпеченні миру, кібербезпеки, сталого розвитку. Аналізується діяльність регіональних організацій.

Окрема увага приділяється співпраці держав з неурядовими організаціями та бізнесом у глобальному управлінні з метою формування кіберзахисту. Аналізуються ключові виклики та проблеми політичної діяльності щодо кіберзахисту: демократичний дефіцит, неефективність, обмежений вплив. Обговорюються напрями покращення системи глобального управління, посилення її легітимності та ефективності в сучасному світі. Акцентується необхідність посилення багатостороннього співробітництва держав для розв'язання проблем кіберзахисту.

План практичного заняття:

1. Стратегічне управління розвитком кіберзахисту критичної інформаційної інфраструктури.
2. Глобалізація проблеми кіберзахисту у викликах сучасності.
3. Перспективи удосконалення політичної діяльності, щодо безпеки в кіберпросторі.
4. Удосконалення механізмів формування системи підготовки кадрів у сфері кібербезпеки.
5. Національна стійкість в умовах мінливого безпекового середовища.

Методичні вказівки до теми:

1. Опрацюйте поняття «критична інформаційна інфраструктура», з'ясуйте його основні види.
2. Проаналізуйте ключові теорії глобального управління.
3. Розгляньте роль міжнародних організацій у кіберзахисті.
4. Дослідіть структуру, основні цілі та напрями діяльності НАТО щодо кібернетичної безпеки.
5. Проаналізуйте провідні регіональні міжнародні організації та їхню роль у кіберзахисті.
6. Проаналізуйте діяльність G7 та G20 як механізмів глобального управління та впливу на кібернетичні процеси атак та їх попередження.
7. Розгляньте питання безпеки, екології, прав людини у контексті кіберзахисту.

8. Визначте проблеми ефективності й легітимності кіберзахисту.

9. Проаналізуйте роль регіональних міжнародних організацій в сучасному кіберзахисті. Наведіть 2-3 приклади.

10. Підготуйте аналітичну доповідь за обраною Вами проблематикою теми.

Проблемні питання для обговорення:

1. Чи ефективна діяльність ООН щодо кіберзахисту?
2. Чому підготовка кадрів у сфері кібербезпеки продовжує бути актуальною?
3. Чи виправдовують себе санкції ЄС проти Росії за агресію проти України?
4. Наскільки успішно НАТО реагує на кібератаки зі сторони Росії?
5. Чому кіберпростір як зручний комунікатор викликає ряд загроз для поличних та суспільних процесів?
6. Чи ефективною є кібербезпека на національному рівні держав?
7. Які перспективи формування системи кіберзахисту та кібербезпеки на глобальному рівні?
8. Які основні виклики постають перед глобальним управлінням у XXI столітті щодо кіберзагроз?

Завдання для самостійної роботи:

1. Проаналізувати кадровий потенціал у сфері кібербезпеки у США.
2. Визначити основні перспективи щодо кіберзахисту України, її роль у вдосконаленні кібербезпеки в Європі.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Здобувачеві другого рівня освіти обрати самостійно країну світу та провести аналіз щодо:

- форм кібервпливу, які вчинялись на таку країну за останні 5 років (кібератаки, хакерство, кібершпигунство та ін.);
- дослідити, яку шкоду було завдано державі та суспільству (майнову, репутаційну, інфраструктурна та ін.);
- оцінити чи покращується рівень кібербезпеки країни в сучасних тенденціях;

охарактеризувати державну політику обраної країни щодо кіберзахисту.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Сутнісна характеристика кіберпростору в розвитку політичних процесів.
2. Кібермогутність і національна безпека держави.
3. Кіберпростір як сфера глобальних конфронтацій.
4. Основи безпеки кіберпростору в сучасному світі.
5. Науковий аналіз кібернетичних меж політичного протиборства.
6. Співвідношення понять «кіберзагрози» , «кібербезпека», «кіберконфлікти» в політичному аспекті.
7. Кіберпростір як новий вимір геополітичного суперництва. Різновиди кіберзагроз.
8. Відносини США – КНР як ключовий геополітичний наратив початку XXI сторіччя: співробітництво, суперництво, протистояння
9. Механізми реалізації кіберконфліктів у міжнародній політиці XXI сторіччя: хактивізм, кібершпигунство та кібердиверсії
10. Російсько-українська війна, як чинник кіберпротиборства.
11. Особливості забезпечення принципів кібербезпеки в Україні.
12. Суб'єкти забезпечення кібербезпеки в державі.
13. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.
14. Міжнародне співробітництво у сфері кібербезпеки.
15. Місце і роль кіберзахисту в Збройних Силах України.
16. Сучасні форми політичної активності в кіберпросторі.
17. Деструкція, як специфічна форма прояву політичної взаємодії в кіберпросторі.
18. Способи та механізми впливу на політичне життя суб'єктів політики в кіберпросторі.
19. Виклики щодо використання кіберпростру суб'єктами політики : культурний та ідеологічний аспект.
20. Історія становлення знань про кіберпотиборство.
21. Сутність поняття кібервійна: визначення, види, ознаки.
22. Предумови до розвитку кібервійни.
23. Перша світова кібервійна.
24. Проблеми щодо врегулювання кібервійни в межах кіберпростору: політичний аспект.
25. Категоріально-понятійне осмислення політичних кіберконфліктів в сучасному світосприйнятті.
26. Доктринальні засади управління інформаційно-комунікаційними політичними процесами.
27. Типологізація політичних конфліктів в кіберпросторі.
28. Шляхи управління кіберконфліктами.
29. Стан розвитку національних механізмів протидії кіберзагрозам.

30. Особливості організаційного забезпечення органів державної протидії кіберзагрозам.
31. Розбудова Національної системи кібернетичної безпеки: регіональний та глобальний аспект.
32. Сполучені Штати Америки, як показник високого розвитку кібербезпеки.
33. Позиція Китаю щодо кіберзахисту в глобальному світі.
34. Особливості політичних дій щодо кібербезпеки європейськими країнами.
35. Виклики кіберзлочинності в цифрову епоху країн Африканського континенту.
36. Стратегічне управління розвитком кіберзахисту критичної інформаційної інфраструктури.
37. Глобалізація проблеми кіберзахисту у викликах сучасності.
38. Перспективи удосконалення політичної діяльності, щодо безпеки в кіберпросторі.
39. Удосконалення механізмів формування системи підготовки кадрів у сфері кібербезпеки.
40. Національна стійкість в умовах мінливого безпекового середовища.
41. Кібербезпека країн Балтії.
42. Особливості кіберзахисту в Німеччині.
43. Концепт правового захисту кіберпростору в Польщі.
44. Основи кібербезпеки в Італії.
45. Методика кібербезпеки в Фінляндії.
46. Роль політичної системи в формуванні кібербезпеки держави.
47. Діяльність політичних інститутів щодо кібербезпеки.
48. Роль переговорного процесу в кіберконфліктах.
49. Глобальні аспекти кіберзахисту.
50. Реакція міжнародних організацій щодо кіберзагроз.

РЕКОМЕНДОВАНИХ ПЕРЕЛІК ДЖЕРЕЛ

Основні джерела:

1. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч.посіб. Ліра-К. 2021. 554с.
2. Веселова Л.Ю. Кібернетична безпека в умовах гібридної війни: адміністративно-правові засади. Монографія. Видавничий дім «Гельветика». 2020. 488с.
3. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак К.: Видавництво НА СБ України, 2020. 256 с.
4. Пєтков С.В., Журавльов Д.В., Дрозд О.Ю., Дрозд В.Г. Кібербезпека в Україні. Навч.посіб. ЦУЛ. 2022. 460с.
5. Zavhorodnia Yu. V. Political conflicts as a prerequisite for the Russian-Ukrainian war: manipulative features. The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects : Scientific monograph. Riga, Latvia : «Baltija Publishing», 2022. С. 911-918. (1436 p.)

Допоміжні джерела:

1. Завгородня Ю.В. «Кіберконфлікти» та «політичні конфлікти»: співвідношення понять. Актуальні проблеми політики. Одеса, 2022. Вип.70. С. 95-100.
2. Завгородня Ю.В. Історія становлення кібервійни як складової політичного процесу. Актуальні проблеми політики. Одеса, 2023. Вип. 72 С.42-46
3. Завгородня Ю.В. Кібербезпека, як інноваційний захист у політичному просторі України. Вісник національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право: зб.наук.праць. 2021. №4(52). С. 33-39
4. Завгородня Ю.В. Кіберконфлікти як сучасна загроза цифровізації суспільства: політичний аспект. Актуальні проблеми філософії та соціології. № 35. 2022. Видавничий дім «Гельветика». С.88-92
5. Завгородня Ю.В. Кіберконфлікти, як елемент політичних технологій в інформаційному просторі. Актуальні проблеми філософії та соціології. № 32. 2021. Видавничий дім «Гельветика». С. 144-148.
6. Завгородня Ю.В. Краудсорсинг як політична складова кіберконфліктів (концепт кібердій України та агресора). 2024. Міжнародні та політичні дослідження. № 37. 2024. С.186-1931
7. Завгородня Ю.В. Можливості політики кіберзахисту в зовнішніх та внутрішніх процесах. Актуальні проблеми філософії та соціології. № 48/2024. Видавничий дім «Гельветика» - С.187-191 http://apfs.nuoua.od.ua/archive/48_2024/31.pdf
8. Завгородня Ю.В. Особливості поведінки учасників політичного процесу під час конфронтації в інформаційному просторі. Політикус. Випуск 4. 2022. Видавничий дім «Гельветика». С. 29-34
9. Завгородня Ю.В. Плюралізм різновекторних поглядів в інформаційному просторі: конфліктологічний аспект. Політикус. Випуск 1. 2022. Видавничий дім «Гельветика». С. 49-54

10. Завгородня Ю.В. Політичне протистояння в кіберпросторі: глобалізаційний аспект. Вісник Львівського університету. Філософсько-політологічні студії. № 40. 2022. Видавничий дім «Гельветика» С. 148-154.
11. Завгородня Ю.В. Різновиди політичних конфліктів у кіберпросторі. Актуальні проблеми політики. Одеса, 2023. Вип. 71 С.74-78
12. Завгородня Ю.В. Роль НАТО у боротьбі з кіберконфліктами. Регіональні студії. № 30. Видавничий дім «Гельветика» 2022. С.62-65.
13. Завгородня Ю.В. Трансформаційні уявлення про конфлікт в політичних процесах. Актуальні проблеми політики. Одеса, 2022. № 69. С.61-64.
14. Завгородня Ю.В. Фейки як сучасна форма політичного протиборства у кіберпросторі. Регіональні студії. № 28. 2022. Видавничий дім «Гельветика С. 67-71
15. Завгородня Ю.В. Форми впливу на політичний конфлікт: теоретичний аналіз. Актуальні проблеми політики. 2020. № 65. С. 12–17.
16. Конвенція про кіберзлочинність, ратифікована Україною від 07.09.2005, підстава - 2824-IV, URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
17. Кормич Л., Краснопольська Т. та Завгородня Ю. (2024). Цифрова трансформація та забезпечення національної безпеки. Evropsky Politicky a Pravni Diskurz, 11, 1, 29-37. (Scopus)
18. Кормич Л.І., Краснопольська Т.М., Завгородня Ю.В. Конструктивізм та деструктивність суспільних змін у Східній та Центрально-Східній Європі в усвідомленні українського соціуму. Актульні проблеми політики. №73. 2024. С. 5-15.
19. Пехник А.В., Завгородня Ю.В. Сучасні загрози кібертехнологій в політичному процесі. Актуальні проблеми політики. 2021. № 68. http://www.app.nuoua.od.ua/archive/68_2021/14.pdf
20. Постанова КМУ від 04 квітня 2023 р. № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text
21. Постанова КМУ від 08 березня 2024 р. № 276 «Про утворення Міжвідомчої робочої групи з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави» URL: https://zakon.rada.gov.ua/laws/show/276-2024-%D0%BF#Text
22. Постанова КМУ від 17 лютого 2023 р. № 142 «Про представника Державної служби спеціального зв'язку та захисту інформації в Об'єднаному центрі передових технологій з кібероборони НАТО» URL: https://zakon.rada.gov.ua/laws/show/142-2023-%D0%BF#Text
23. Постанова КМУ від 19 грудня 2023 р. № 1163-р «Про затвердження плану заходів на 2023—2024 роки з реалізації Стратегії кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text
24. Постанова КМУ від 24 березня 2023 р. № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text

25. Про основні засади забезпечення кібербезпеки України. Відомості Верховної Ради України. 2017. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#n169
26. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
27. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (втратила чинність) URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11
28. Kormych Liudmyla, Zavhorodnia Yuliia The concept of modern political confrontation in cyber space. Journal of Cybersecurity, Volume 9, Issue 1, 2023. https://doi.org/10.1093/cybsec/tyad017 (Web of Science, Scopus).
29. Zavhorodnia Yu., Povydys V., Kozminykh A., Mamontova E. Information Policy of the State in the Context of Growing Cyber Threats. Pakistan Journal of Criminology. Vol 15. No 1 January-March 2023. (111-124) (Scopus).
30. Zavhorodnia Yuliia, Features of protection of China's national interests within cybernetic space. Evropsky Politicky a Pravni Diskurz, 2021, Volume 8, Issue 6. p.37-42 (Scopus).
31. Zavhorodnya Y. Political decisions on cyber security in European countries. «KELM (Knowledge, Education, Law, Management)». № 1(53), 2023. P.129-135
32. Zavhorodnya Y. The specifics of the development of political opposition in tne cybernetic sphere. «KELM (Knowledge, Education, Law, Management)». № 7(51), 2022. P.71-79

НАВЧАЛЬНЕ ВИДАННЯ

Юлія Володимирівна Завгородня

КІБЕРЗАГРОЗИ В СУЧАСНОМУ ПОЛІТИЧНОМУ ПРОСТОРІ

МЕТОДИЧНІ ВКАЗІВКИ

метод. вказівки для підготовки до практичних занять та самостійної роботи здобувачів вищої освіти другого (магістерського) рівня

галузі знань – 05 «Соціальні та поведінкові науки»,

спеціальності – 052 «Політологія»

Електронне видання

В авторській редакції