ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
[ВПП 8]

Кредити та кількість годин: **очна форма навчання:** 5 ECTS; години: 16 лекційних, 14 семінарських, 120 самостійної роботи, залік.
заочна форма навчання: 5 ECTS; години: 8 лекційних, 8 семінарських, 134 самостійної роботи, залік.

І. Опис навчальної дисципліни

Сучасний стан розвитку держави характеризується стрімким розвитком інформаційних технологій, які використовують в усіх сферах життєдіяльності суспільства. В умовах глобалізації процес інформатизації охопив усі країни світу. Сучасні інформаційні технології інтенсивно впроваджуються у процес управління. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зросла. Неспроможність ефективного управління та невідповідність інформаційної структури новим умовам існування може призвести до втрати власного суверенітету. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення.

Отже, беззаперечним є те, що в будь-якій розвиненій країні має існувати система забезпечення інформаційної безпеки, а функції та повноваження відповідних державних органів повинні бути закріплені на законодавчому рівні. Проблема забезпечення інформаційної безпеки України знайшла відображення в законах «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Концепції національної безпеки України. Сутність інформаційної безпеки як невід'ємної складової національної безпеки України вперше була зазначена у Законі «Про основи національної безпеки України». Відповідно до законодавства України під інформаційною безпекою розуміють стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Державна політика в сфері інформаційної безпеки зосереджена на задоволенні та захисті життєво важливих інтересів та потреб громадянина, суспільства і держави в інформаційній сфері щодо: продукування, споживання, розповсюдження і розвитку національного стратегічного контенту та інформації в інтересах громадянина, суспільства і держави. функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих комп'ютерних систем, що формують інфраструктурну основу внутрішньодержавного інформаційного простору.

ІІ. Мета та завдання навчальної дисципліни

Мета – розкрити основи державної політики у сфері кібербезпеки, інформаційної безпеки, захисту інформації з обмеженим доступом в Україні та світі, та сформувати навички підготовки документів для прийняття рішень представниками органів державної влади в інформаційній сфері. Сформувати у студентів теоретичні засади та практичні основи.

Завданнями навчальної дисципліни є:

- розвинути у здобувачів здатність оцінювати результати професійної діяльності та якісно їх застосовувати на практиці;
- розвинути критичне мислення та наполегливість при виконанні поставлених завдань при роботі з інформацією;
- набути навики виявляти, ставити та вирішувати професійні задачі, розвинути вміння узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати діяльності;
- демонструвати знання та вміння застосовувати набуті навички в роботі з інформаційним середовищем на виявлення загроз життєдіяльності особи та держави.

III. Результати навчання

Опанувавши навчальну дисципліну, студенти зможуть:

- розуміти основні теоретичні поняття;
- застосовувати набуті знання у практичних ситуаціях;
- працювати із правовою та законодавчою базою;
- здійснювати пошук новинних ресурсів та вміти кооперувати до них в поставлених питаннях;
- шукати способи та технічні засоби перевірки та розуміння кіберзабезпечення;
- знати правила поводження з особистими даним та таємною інформацією;
- застосовувати на практиці методики взаємодії з інформаційним забезпеченням;
- використовувати науково-технічні засоби для досліджень;
- вивчати інформацію з метою встановлення її автентичності та вміння протистояти дезінформації;
- визначати предмет експертного дослідження міжнародного забезпечення інформаційної безпеки;
- аналізувати внутрішні та зовнішні складові процесів виявлення та протидії гібридним загрозам, їх роль та важливість в контексті захисту національної безпеки держави;
- виявляти ознаки та факти ворожого гібридного впливу, як загрози національній безпеці;
- аналізувати комплексну природу, складність, логіку і закономірності гібридних загроз;
- використовувати досвід держав-членів НАТО та інших провідних зарубіжних країн із захисту національної безпеки держави в умовах гібридних загроз;
- забезпечувати громадську стійкість та безперебійність професійної діяльності в умовах гібридних загроз.

Програмними результатами навчання, згідно з освітньо-професійною програмою «Національна безпека (за окремими сферами забезпечення і видами діяльності)» для другого (магістерського) рівня вищої освіти, є:

ПРН-1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки держави.
ПРН-3. Ухвалювати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), зокрема в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.
ПРН-8. Забезпечувати принцип гендерної рівності під час здійснення професійної діяльності.
ПРН-9. Синтезувати спектр заходів та підходів, що можуть бути використані для вирішення проблем, пов’язаних із викликами глобальній, європейській та регіональній безпеці.
ПРН-17. Комплексно використовувати комунікативні можливості у різних сферах національної безпеки та розуміти особливості провадження кризового менеджменту у сфері управління національною безпекою.
ПРН-18. Демонструвати розуміння комплексної природи, складності, логіки і закономірності гібридних загроз.
ПРН-19. Виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії.
ПРН-20. Використовувати сучасні технології для прийняття рішень в боротьбі із гібридними загрозами.
ПРН-21. Застосовувати спеціалізовані знання у ефективній протидії гібридним впливам у сфері національної безпеки.

IV. Програма навчальної дисципліни (структура дисципліни)

№	Тема дисципліни	Вид навчального	Самостійна робота	Обов’язкове читання	Контрольні заходи

		заняття			
1	Державне управління в умовах розвитку інформаційного суспільства	Лекція (2 год.) Практична (2 год.)	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 1, 2, 3	Бесіда з викладачем. Робота із теоретичними завданнями.
2	Поняття та структура безпеки особи, суспільства, держави в інформаційній сфері	Лекція (2 год.) Практична (2 год.) ***Заочна форма*** Лекція 1 год.	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 1, 4, 5, 6, 7.	Робота в парах. Обговорення теоретичних питань.
3	Концептуальні засади забезпечення кібербезпеки в Україні та світі	Лекція (2 год.) Практична (2 год.) ***Заочна форма*** Лекція 1 год. Практична 1 год.	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 1. Допоміжна література: 3-6.	Робота в групі, розв'язання практичних завдань.
4	Концептуальні засади забезпечення інформаційної безпеки в Україні та світі	Лекція (2 год.) Практична (2 год.) ***Заочна форма*** Практична 1 год.	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 8. Допоміжна література: 7-9.	Робота в парах. Обговорення теоретичних питань
5	Проміжний модульний контроль для очної форми навчання	Практична (2 год.)	Повторення матеріалу (8 год.) ***Заочна форма*** 10 год.	Основна література: 1-8, лекційні матеріали. Допоміжна література: 1-9.	Тест 1

6	Концептуальні засади захисту інформації з обмеженим доступом в Україні та світі	Лекція (2 год.) Практична (2 год.)	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 8-12. Допоміжна література: 9-12.	Робота в парах. Обговорення теоретичних питань
7	Повноваження суб'єктів національної системи кібербезпеки України	Лекція (2 год.) Практична (2 год.) ***Заочна форма*** Лекція 2 год. Практична 2 год.	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: додаток проекту по стратегії кібербезпеки. 13	Робота в групі, розв'язання практичних завдань.
8	Захист національних електронних інформаційних ресурсів	Лекція (2 год.) Практична (2 год.) ***Заочна форма*** Лекція 2 год.	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 1, 2, 5 Допоміжна література: 3, 7, 8	Робота в групі, розв'язання практичних завдань.
9	Імплементація положень Конвенції про кіберзлочинність в Україні	Лекція (2 год.) Практична (2 год.)	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 5, 7, 9 Допоміжна література: 5, 8, 9.	Робота в групі, розв'язання практичних завдань.
10	Критична інформаційна інфраструктура	Лекція (2 год.) Практична (2 год.) ***Заочна форма*** Лекція 2 год. Практична 2 год.	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 1-6 Допоміжна література: 8, 9, 10	Усне опитування, захист презентацій та індивідуальних завдань.

11	Загрози при роботі онлайн та методи їх уникнення	Лекція (2 год.) Практична (2 год.)	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 3, 5, 6 Допоміжна література: 8, 9, 12	Робота в групі, розв'язання практичних завдань.
12	Закордонний та вітчизняний досвід боротьби з фейками та дезінформацією	Лекція (2 год.) Практична (2 год.)	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 8, 9, 11 Допоміжна література: 3, 5, 8	Робота в групі, розв'язання практичних завдань.
13	Соціальні мережі і особиста безпека. Інформаційна грамотність	Лекція (2 год.) ***Заочна форма*** Практична 2 год.	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 1-9 Допоміжна література: 5-8	Обговорення теоретичних питань, розв'язання завдань.
14	Державна таємниця. Захист службової інформації та іншої інформації з обмеженим доступом.	Лекція (2 год.) Практична (4 год.)	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (8 год.) ***Заочна форма*** 10 год.	Основна література: 5, 6, 8 Допоміжна література: 1, 3, 5	Робота в групі, розв'язання практичних завдань.
15	Розвиток технологій штучного інтелекту та його вплив на державну політику в інформаційній сфері	Лекція (2 год.) Практична (2 год.)	Опрацювати рекомендовану літературу. Законспектувати основні терміни та поняття по темі (4 год.) ***Заочна форма*** 10 год.	Основна література: 5, 6, 8 Допоміжна література: 8, 9, 10	Обговорення теоретичних питань, розв'язання завдань.

16	Підсумковий модуль	Практична 2 год.	Повторення матеріалу (4 год.) ***Заочна форма*** 14 год.	Основна література: 1-6 Допоміжна література: 6-10	Написання тестових завдань

V. Порядок оцінювання результатів навчання (з урахуванням можливості проведення контрольних заходів за допомогою дистанційних технологій)

Результати навчання	**Контрольні заходи**	**Вимоги до виду контролю**	**Оцінювання**
Розуміти основні теоретичні поняття, застосовувати набуті практичні навички із дослідження теоретичних ресурсів та положень, їх правильному використанні в службовій діяльності, спрямуванні на сприяння найбільш успішному здійсненню конституційних положень про захист інтересів держави, законних інтересів громадян та інформаційної безпеки.	Обговорення теоретичних питань, робота в парах, розв'язання практичних завдань. Захист презентацій та індивідуальних завдань.	Розгорнутість та ґрунтовність суджень. Критичне мислення та логічно побудований підхід до змодельованих ситуацій. Вивчення законодавчої бази та аналіз додаткових джерел, згідно з наданим матеріалом	42 бали (14*3б.=42) ***Заочна форма*** 20 балів (4*5б.=20)
Продемонструвати вміння чітко занотовувати та оформлювати набуту на лекційних заняттях інформацію у вигляді заздалегідь підготовленої конспектів. Додаткова робота на самостійне опрацювання.	Проміжна контрольна робота (тест)	Тест складається з 20 питань. Правильну відповідь оцінюємо в 1 бал. Відповідь на розгорнуте питання оцінюємо в 8 балів. Студент повинен уміти дати особисту оцінку інформації, висунутих тез грамотною аргументацією, а також здатність дійти збалансованої подачі інформації	28 балів
Студент повинен уміти використовувати науково-технічні засоби для досліджень, вивчати інформацію з метою встановлення її автентичності та вміння протистояти дезінформації, а також	Підсумкова контрольна робота	Тест складається з 30 питань. Правильна відповідь оцінюємо в 1 бал.	30 балів ***Заочна форма*** 80 балів

визначати предмет експертного дослідження міжнародного забезпечення інформаційної безпеки.			

Орієнтовний перелік питань для підготовки підсумкового контролю

1. Правове регулювання діяльності соцмереж та інших технологічних компаній в Україні (
2. Facebook, Google, Microsoft, Amazon.)
3. Повноваження Міністерства оборони та Генерального штабу ЗСУ у сфері кібербезпеки:
4. Система кібербезпеки банківських установ сформована на підставі нормативно правових актів Нацбанку України. ЗУ «Про банки і банківську діяльність»
5. Особливості правового статусу банківської таємниці в Україні;
6. Дотримання режиму захисту персональних даних соціальними мережами та іншими великими технологічними компаніями в Україні;
7. Особливості охорони класифікованої інформації в європейському союзі та США;
8. Перспективи правового регулювання режиму комерційної таємниці в Україні з урахуванням зарубіжного досвіду.
9. Аналіз проекту нової стратегії кібербезпеки звернути увагу на коментарі
10. Повноваження Міноборони та генштабу України, щодо кіберзахисту в умовах надзвичайного та воєнного стану
11. Повноваження департаменту кіберполіції з питань кіберзлочинів (зокрема міжнародного співробітництва)
12. Повноваження СБУ щодо розслідування кіберзлочинів (чинне та перспективне законодавство) дивитися інформацію про департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки
13. Проект стратегії кібербезпеки
14. Аналіз положення про здійснення контролю за дотримання банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг
15. Структура національних електронних інформаційних ресурсів (дивитися національний реєстр ресурсів)
16. Правова основа та особливості використання, захисту платформи «дія» в Україні
17. Сфери економіки та промисловості України в яких функціонують об’єкти критичної інфраструктури;
18. Критерії віднесення інформаційно-телекомунікаційних систем до об’єктів критичної інформаційної інфраструктури;
19. Повноваження мін цифри щодо цифрової грамотності, кібергігієни, медіа грамотності;
20. Повноваження міжгалузевої ради з питань цифрового розвитку цифрових трансформації і цифровізації;
21. Висновки міжнародних організацій (ООН, ОБСЄ та ін.) а також зарубіжних країн стосовно впливу пандемії на виникнення підвищення загроз при роботі в інтернеті

VI. Рекомендована література

Основна

1. Державне управління в умовах розвитку інформаційного суспільства : навч. посіб. /Н.В. Грицяк, Л.В. Литвинова. К.: Вид-во К.І.С., 2015. 108 с.
2. Марущак А. І. Методи правового регулювання безпеки особи, суспільства, держави в інформаційній сфері. Вісник Національної академії правових наук України. 2019. № 3. С. 75-89.
3. Державна інформаційна політика в Україні в умовах розвитку інформаційного суспільства : навч.-метод. матеріали / Т. В. Федорів, М.Т. Солоха ; упоряд. Н. В. Ясько. К. : НАДУ, 2013. 36 с.
4. Марущак А.І. Інформаційне право: доступ до інформації: Навчальний посібник. К.: КНТ, 2007. 532 с.

5. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності: Навчальний посібник. К.: Видавничий дім «Скіф», КНТ, 2008. 344 с.
6. Марущак А. І. Інформаційне право України : підручник. К.: «Дакор», 2011. 456 с.
7. Zoreslava Brzhevska, Nadiia Dovzhenko, Halyna Haidur, Andriy Anosov, Критерії моніторингу достовірності інформації в інформаційному просторі. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка": Том 1 № 5 (2019): Кібербезпека: освіта, наука, техніка
8. Закон України «Про Суспільне телебачення і радіомовлення України»
9. Закон України «Про державну таємницю»
10. Закон України «Про захист персональних даних»
11. Закон України «Про основні засади забезпечення кібербезпеки в Україні»
12. Цивільний кодекс України

Допоміжна

1. Ігор Розкладай. ЯК УКРАЇНА ПРОТИДІЄ ІНФОРМАЦІЙНІЙ АГРЕСІЇ РОСІЇ, 2018 https://cedem.org.ua/articles/yak-ukrayina-protydiye-informatsijnij-agresiyi-rosiyi/
2. Рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", уведене в дію Указом Президента України від 15 травня 2017 року № 133
3. Марущак А.І., Петров С.Г. Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецзв'язку України). Інформація і право. 2020. № 2. С. 77-84.
4. Марущак А.І. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. Безпека інформації. 2019. Том 25. № 1. С. 13-17. URL:
5. http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13665.
6. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року №96/2016.
7. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017.
8. Марущак А.І. Правові основи захисту інформації з обмеженим доступом: Курс лекцій. К.: КНТ, 2007. 208 с.
9. Попова Н. О. Поняття комерційної таємниці як об'єкта права інтелектуальної власності в законодавстві України / Н. О. Попова // Форум права. - 2014. - № 2. - С. 364–368.
10. Марущак А. І. Охорона банківської таємниці : навч. посібник. Л: Янтар, 2013. 262 с.
11. Katherine E. Bliss and J. Stephen Morrison, The Risks of Misinformation and Vaccine Hesitancy within the Covid-19 Crisis, Center for Strategic & International Studies, commentary, September 4, 2020, at https://www.csis.org/analysis/risks-misinformation-and-vaccine-hesitancy-within-covid-19-crisis;
12. Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305.
13. Keir Giles The Next Phase of Russian Information Warfare. Riga : NATO Strategic Communications Centre of Excellence, 2017 . 16 p.
14. Sweijs, T., & Zilincik, S. (2019). Cross Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p.
15. World Health Organization, Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation, joint statement by WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFRC, September 23, 2020, at https://www.who.int/news-room/detail/23-09-2020-managing-the-covid-19-infodemicpromoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation

VII. Інформаційні ресурси в Інтернет

Офіційний сайт МВС України - http://mvs.gov.ua

Офіційний сайт Міністерства юстиції України - http://www.minjust.gov.ua/

Національний координаційний центр кібербезпеки. https://www.rnbo.gov.ua/ua/Diialnist/4658.html

Глосарій гібридних загроз URL: https://warn-erasmus.eu/ua/glossary/

Електронний ресурс: Європейський центр з протидії гібридним загрозам Hybrid CoE URL: https://www.hybridcoe.fi/

Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond, European View 2020, Martens Center for European Studies, Vol. 19(1) 62–70.

Cederberg A. How can Societies Be Defended against Hybrid Threats? / A. Cederberg, P. Eronen // STRATEGIC SECURITY ANALYSIS SEPTEMBER, 2015. – No 9. URL : http://www.defenddemocracy.org/content/uploads/documents/GCSP_Strategic_Security_ Analysis_-_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf.

Chambers J. Countering gray-zone hybrid threats. Analysis of Russia's 'New Generation Warfare' and Implications for the US Army / J. Chambers. – October 18, 2016. URL : https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.

Countering hybrid threats: EU-NATO cooperation. – March, 2017. URL : http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017) 599315_EN.pdf.

Countering Hybrid Warfare Project: Understanding Hybrid Warfare a Multinational Capability Development Campaign project URL : https://www.gov.uk/ government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Davis J.R. Jr. Continued evolution of hybrid threats. The Russian Hybrid Threat Construct and the Need for Innovation URL : http://www.ileridunya.com/ wp-content/uploads/2016/02/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf.

Defence Budgets and Cooperation in Europe: Developments, Trends and Drivers URL: http://www.iai.it/sites/default/files/pma_report.pdf

Department of Defense: Report on Strategic Communication. URL: http://www.au.af.mil/au/awc/awcgate/dod/dod_report_strategic_communication_11feb10.pdf.

Joint communication to the European Parliament and the Council. Joint framework on countering hybrid threats. A European Union response 2016 URL : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

Kofman M. A Closer Look at Russia's 'Hybrid War / M. Kofman, M. Rojansky // Kennan Cable (Kennan Institute at the Woodrow Wilson Center, April 2015). – № 7, April 2015. URL : https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY %20KOFMAN.pdf.

Michael Rühle, Clare Roberts (2021). Enlarging NATO's toolbox to counter hybrid threats, 19 March, URL : https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybridthreats/index.html

Pomerantsev P. Why we're post-fact? URL: https://granta.com/why-were-post-fact/

Security and defense: Significant progress to enhance Europe's resilience against hybrid threats – more work ahead European Commission. – Press release, Brussels, 19 July 2017. URL : http://europa.eu/rapid/press-release_IP-17-2064_en.htm.

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.

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.

VIII. Політики курсу

Відвідування занять є обов'язковим.

Дотримання термінів виконання завдань

Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Складання пропущених контрольних заходів відбувається із дозволу деканату за наявності поважних причин (наприклад, лист тимчасової непрацездатності, довідка ЛКК).

Особливості вивчення навчальної дисципліни за допомогою технологій дистанційного навчання.

Відповідно до Положення про дистанційне навчання в Національному університеті "Острозька академія" (URL: https://www.oa.edu.ua/publik_information/polojennia_dystanc_navchannia.pdf), у разі продовження карантинних заходів, заняття та консультації проводитимуться з використанням системи Google Meet (кодове слово: marushchak) що надає можливість двостороннього зв'язку між студентами та викладачем. З цією ж метою використовуватиметься корпоративна пошта НаУ ОА. Тестові форми контролю студенти зможуть проходити в інформаційній системі Moodle, де також розміщені необхідні ресурси з курсу

Політика доброчесності

Прослуховуючи цей курс, Ви погодились виконувати положення Кодексу академічної доброчесності.

Окреслимо його основні складові:

Складати всі проміжні та фінальні завдання самостійно без допомоги сторонніх осіб.

Надавати для оцінювання лише результати власної роботи.

Не вдаватися до кроків, що можуть нечесно покращити ваші результати чи погіршити/покращити результати інших студентів.

Не публікувати відповіді на питання, що використовуються в рамках курсу для оцінювання знань студентів.

Курс підготовлено за рекомендаціями проєкту ERASMUS+ «Академічна протидія гібридним загрозам–WARN» Erasmus+ Capacity Building Project WARN 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-J

Co-funded by the Erasmus+ Programme of the European Union

WARN