МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА

Кафедра міжнародних відносин, міжнародної інформації та безпеки

КОМПЛЕКС НАВЧАЛЬНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ

з дисципліни
«МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА»

рівень вищої освіти: другий (магістерський)
галузь знань: 29 «Міжнародні відносини»
спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітня програма: «Міжнародна інформаційна безпека»
вид дисципліни: за вибором
факультет міжнародних економічних відносин та туристичного бізнесу

Укладач: канд. юрид. наук, доц. Доценко О. М.

2020 / 2021 навчальний рік

1. НАВЧАЛЬНИЙ КОНТЕНТ (РОЗШИРЕНИЙ ПЛАН ЛЕКЦІЙ)

РОЗДІЛ 1. ЗАГАЛЬНІ ЗАСАДИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тема 1. Концепція інформаційного протиборства в міжнародних відносинах.
ЛЕКЦІЯ 1. Концепція інформаційного протиборства в міжнародних відносинах.

Час проведення – 2 год.
Навчальні питання:

1. Інформаційний чинник конфліктів у сучасних міжнародних відносинах. Роль процесів глобалізації та інформатизації у взаємодії суб'єктів міжнародних відносин. Природа та сутність міжнародного конфлікту. Суб'єкти міжнародного конфлікту. Основні функції міжнародного конфлікту. Методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах. Дезінформація та пропаганда.

2. Поняття та зміст інформаційного протиборства. Поняття інформаційного протиборства. Історичні етапи розвитку інформаційного протиборства. Фактори та умови сучасного ведення інформаційного протиборства. Мета та принципи інформаційного протиборства. Суб'єкти та об'єкти інформаційного протиборства.

3. Форми ведення інформаційного протиборства (інформаційна експансія, інформаційна агресія, інформаційна війна). Стадії інформаційного протиборства. Поняття, та ознаки інформаційної експансії. Поняття та ознаки інформаційної агресії, її види. Поняття та ознаки інформаційної війни. Засоби та методи ведення інформаційної війни. Відмінність інформаційної війни від традиційної.

Література:
Основна: 9, 13, 14, 17, 18, 19, 22, 23.
Додаткова: 1, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 22.

Тема 2. Теоретичні засади інформаційної безпеки.
ЛЕКЦІЯ 2. Теоретичні засади інформаційної безпеки.
Час проведення – 2 год.
Навчальні питання:

1. Поняття та види інформаційної безпеки. Основні підходи до визначення поняття «інформаційна безпека». Поняття міжнародної інформаціної безпеки. Групи інтересів в сфері інформаційної безпеки. Ознаки інформаційної безпеки. Класифікації інформаційної безпеки. Співвідношення понять «інформаційна безпека» та «кібербезпека».

2. Сучасні інформаційні загрози. Поняття інформаційних загроз та їх властивості. Класифікації загроз інформаційній безпеці. Інформаційна злочинність. Інформаційний тероризм. Загрози, зумовлені віртуалізацією.

3. Поняття та види інформаційної зброї. Поняття інформаційної зброї Класифікації інформаційної зброї. Ознаки інформаційної зброї.

4. Моделі системи глобальної інформаційної безпеки. Моделі A, B, C, D, E.

Література:
Основна: 1, 3, 4, 5, 6, 10, 11, 14, 15, 17, 18, 19, 21, 22, 25.
Додаткова: 3, 10, 11, 14.

Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру.

ЛЕКЦІЯ 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру.

Час проведення – 2 год.

Навчальні питання:

1. Вплив інформаційної революції на систему міжнародної безпеки. Сучасна система міжнародної безпеки. Фактори ефективності системи міжнародної безпеки. Проблема захисту інформації в системі міжнародних відносин.

2. Діяльність ООН у сфері міжнародної інформаційної безпеки. Резолюції ГА ООН «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки». Діяльність Спеціальної групи урядових експертів держав-членів ООН.

3. Роль Всесвітнього саміту з питань інформаційного суспільства у розвитку міжнародного співробітництва у сфері інформаційної безпеки. Фінальні документи першого етапу ВСІС 2003 року (Декларація принципів «Побудова інформаційного суспільства - глобальне завдання у новому тисячолітті» 2003 року. Женевський план дій 2003 року). Фінальні документи другого етапу ВСІС 2005 року. Туніська програма для інформаційного суспільства 2005 року. Туніське зобов'язання з питань інформаційного суспільства 2005 року).

4. Роль міжнародної організації кримінальної поліції (Інтерпол) у сфері міжнародної інформаційної безпеки. Операції проти кіберзлочинності Unmask (2012 року.), Strikeback (2014 року.), Aces (2015 року.), Simbabotnet (2015 року.), Singapore (2017 року). Глобальний комплекс інновацій Інтерполу. Діяльність Глобальної групи експертів з кіберзлочинності. Діяльність Центру Кіберф'южн.

Література:

Основна: 7, 12, 14, 15, 16, 17, 18, 19, 20, 21.

Додаткова: 4, 6, 10, 15, 17, 20.

Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.

ЛЕКЦІЯ 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.

Час проведення – 4 год.

Навчальні питання:

1. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки європейських держав. Конвенція Ради Європи про кіберзлочинність 2001 року. Рішення Ради Міністрів ОБСЄ № 7/06 «Протидія використанню Інтернету в терористичних цілях» 2006 року. Діяльність ЄС у сфері забезпечення інформаційної безпеки регіону. Ініціатива «Електронна Європа» (eEurope). Діяльність Агентства ЄС з мереж і інформаційної безпеки (ENISA). Навчання Cyber Europe. Діяльність Команди реагування на надзвичайні ситуації CERT-EU. Стратегія ЄС з кібербезпеки 2013 року. Діяльність Європейського центру по боротьбі з кіберзлочинністю (ЕС3). Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС 2016 року (NIS Directive).

2. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки держав Азії та Азіатсько-Тихоокеанського регіону. Інструменти забезпечення інформаційної безпеки в рамках організації Азіатсько-Тихоокеанського економічного співробітництва (АТЕС). Результати самітів міністрів АТЕС у сфері телекомунікацій та інформації. Інструменти забезпечення інформаційної безпеки в рамках Асоціації держав Південно-Східної Азії. Регіональний форум АСЕАН з питань безпеки. Інструменти забезпечення інформаційної безпеки в рамках Шанхайської організації співробітництва (ШОС).

3. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав. Інструменти забезпечення інформаційної

безпеки в рамках Організації Американських держав. Роль Міжамериканської комісії з питань зв'язку (CITEL) у забезпеченні інформаційної безпеки.

Література:
Основна: 2, 8, 12, 14, 15, 17, 18, 19, 21, 24.
Додаткова: 2, 15, 16, 17, 18, 19, 21, 23, 24, 25.

2. ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ, ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ ТА ПОТОЧНОГО КОНТРОЛЮ ЗНАНЬ, УМІНЬ ТА НАВИЧОК ЗДОБУВАЧІВ НА ПРАКТИЧНИХ ЗАНЯТТЯХ

РОЗДІЛ 1. ЗАГАЛЬНІ ЗАСАДИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тема 1: Концепція інформаційного протиборства в міжнародних відносинах.
Практичне заняття 1: **Концепція інформаційного протиборства в міжнародних відносинах.**

Час проведення – 2 год.

Навчальні питання для розгляду на практичному занятті:
1. Інформаційний чинник конфліктів у сучасних міжнародних відносинах.
2. Поняття та зміст інформаційного протиборства.
3. Форми ведення інформаційного протиборства (інформаційна експансія, інформаційна агресія, інформаційна війна).

Питання для контролю засвоєння знань:
1) Перерахуйте основні функції міжнародного конфлікту.
2) Визначте методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах.
3) Охарактеризуйте історичні етапи розвитку інформаційного протиборства.
4) Розкрийте поняття та ознаки інформаційної експансії.
5) Розкрийте поняття та ознаки інформаційної агресії.
6) Розкрийте поняття та ознаки інформаційної війни.

Література:
Основна: 9, 13, 14, 17, 18, 19, 22, 23.
Додаткова: 1, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 22.

Самостійна робота – 18 год.

Завдання для самостійної роботи здобувачів:
1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття (4 год.).
2. Підготувати презентації доповідей з наступних тем (на вибір) (3 год.):
1) Інформаційні війни в сучасних міжнародних відносинах.
2) Відмінність інформаційної війни від традиційної.
3) Методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах.
2. Підготувати схему на тему: «Поняття та зміст інформаційного протиборства» (2 год.).

3. Ознайомитися та проаналізувати наукову статтю Литвиненко О. Інформаційна складова у сучасній гібридній війні проти України: виклики й загрози. *Українознавчий альманах.* Київ, 2016. Вип. 19. С. 172–174. URL: http://nbuv.gov.ua/UJRN/Ukralm_2016_19_42 (4 год.).

4. Підготувати есе на тему: «Інструменти інформаційного протиборства сторін в російсько-українському конфлікті» (5 год.).

Завдання для роботи на практичному занятті:

1. Усне опитування та навчальна дискусія за навчальними питаннями для розгляду на практичному занятті.
2. Захист презентацій доповідей.
3. Навчальна дискусія за науковою статтею Литвиненко О. «Інформаційна складова у сучасній гібридній війні проти України: виклики й загрози».
4. Захист есе.

Тема 2: Теоретичні засади інформаційної безпеки.

Практичне заняття 2: **Теоретичні засади інформаційної безпеки.**

Час проведення – 2 год.

Навчальні питання для розгляду на практичному занятті:

1. Поняття та види інформаційної безпеки.
2. Сучасні інформаційні загрози.
3. Поняття та види інформаційної зброї.
4. Моделі системи глобальної інформаційної безпеки.

Питання для контролю засвоєння знань:

1) Розкрийте основні підходи до визначення поняття «інформаційна безпека».
2) Охарактеризуйте види інформаційної безпеки.
3) Охарактеризуйте види загроз інформаційній безпеці.
4) Класифікуйте інформаційну зброю.
5) Охарактеризуйте моделі системи глобальної інформаційної безпеки.
6) Дайте визначення поняття «міжнародна інформаційна безпека».

Література:

Основна: 1, 3, 4, 5, 6, 10, 11, 14, 15, 17, 18, 19, 21, 22, 25.
Додаткова: 3, 10, 11, 14.

Самостійна робота – 14 год.

Завдання для самостійної роботи здобувачів:

1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття (4 год.).
2. Підготувати презентації доповідей з наступних тем (на вибір) (3 год.):

1) Класифікації інформаційної зброї.
2) Інформаційна злочинність у сучасному світі.

3. Підготувати схему на тему: «Класифікації інформаційної безпеки» (2 год.).
3. Підготувати есе на тему (на вибір) (5 год.):

1) «Співвідношення понять «інформаційна безпека» та «кібербезпека».
2) «Співвідношення понять «інформаційна безпека» та «міжнародна інформаційна безпека».

Завдання для роботи на практичному занятті:

1. Усне опитування та навчальна дискусія за навчальними питаннями для розгляду на практичному занятті.
2. Виконання тестових завдань за навчальними питаннями для розгляду на практичному занятті.
3. Захист презентацій.
4. Захист есе.

Тема 3: Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру.

Практичне заняття 3: **Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру.**

Час проведення – 2 год.

Навчальні питання для розгляду на практичному занятті:

1. Вплив інформаційної революції на систему міжнародної безпеки.
2. Діяльність ООН у сфері міжнародної інформаційної безпеки.
3. Роль Всесвітнього саміту з питань інформаційного суспільства у розвитку міжнародного співробітництва у сфері інформаційної безпеки.
4. Роль міжнародної організації кримінальної поліції (Інтерпол) у сфері міжнародної інформаційної безпеки.

Питання для контролю засвоєння знань:

1) Назвіть фактори ефективності системи міжнародної безпеки.
2) Принципи сучасної системи міжнародної безпеки.
3) У чому полягає значення Резолюції ГА ООН A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» 1998 року.
4) Охарактеризуйте проблематику міжнародної інформаційної безпеки в підсумкових документах ВСІС Женевського етапу 2003 року.
5) Охарактеризуйте проблематику міжнародної інформаційної безпеки в підсумкових документах ВСІС Туніського етапу 2005 року.
6) Визначте роль Спеціальної групи урядових експертів держав-членів ООН у забезпеченні міжнародної інформаційної безпеки.

Література:

Основна: 7, 12, 14, 15, 16, 17, 18, 19, 20, 21.

Додаткова: 4, 6, 10, 15, 17, 20.

Самостійна робота – 14 год.

Завдання для самостійної роботи здобувачів:

1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття (4 год.).
2. Підготувати презентації доповідей з наступних тем (на вибір) (3 год.):
1) Операції Інтерполу проти кіберзлочинності.
2) Роль Міжнародного Союзу Електрозв'язку у забезпеченні міжнародної інформаційної безпеки.
3. Підготувати схему на тему: «Резолюції ГА ООН «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» (2 год.).

3. Підготувати есе на тему: «Криза сучасної системи безпеки: у пошуках нового міжнародного порядку» (5 год.).

Завдання для роботи на практичному занятті:

1. Усне опитування та навчальна дискусія за навчальними питаннями для розгляду на практичному занятті.
2. Виконання тестових завдань за навчальними питаннями для розгляду на практичному занятті.
3. Захист презентацій.
4. Захист есе.

Тема 4: Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.

Практичне заняття 4: **Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.**

Час проведення – 4 год.

Навчальні питання для розгляду на практичному занятті:

1. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки європейських держав.
2. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки держав Азії та Азіатсько-Тихоокеанського регіону.
3. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав.

Питання для контролю засвоєння знань:

1) Назвіть основні нормативно-правові інструменти забезпечення інформаційної безпеки держав Азії та Азіатсько-Тихоокеанського регіону.
2) Назвіть основні інституційні інструменти забезпечення інформаційної безпеки держав Європи.
3) Що таке ініціатива «Електронна Європа»?
4) Охарактеризуйте результати щорічних самітів міністрів АТЕС у сфері телекомунікацій та інформації.
5) Визначте ключові завдання Програмного документу ENISA на 2020–2022 роки.
6) Охарактеризуйте основні положення Багатосторонньої міжамериканської стратегії щодо боротьби із загрозами кібербезпеці 2004 року.

Література:

Основна: 2, 8, 12, 14, 15, 17, 18, 19, 21, 24.

Додаткова: 2, 15, 16, 17, 18, 19, 21, 23, 24, 25.

Самостійна робота – 24 год.

Завдання для самостійної роботи здобувачів:

1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття (4 год.).
2. Підготувати презентації доповідей з наступних тем (на вибір – перші чотири на перші дві години заняття, другі чотири – на другі дві години заняття) (6 год.):
   1) Роль Європолу у сфері забезпечення інформаційної безпеки регіону.
   2) Діяльність Команди реагування на надзвичайні ситуації CERT-EU.

3) Діяльність Агентства ЄС з мереж і інформаційної безпеки (ENISA).
4) Діяльність Європейського центру по боротьбі з кіберзлочинністю (EC3).
5) Роль НАТО у сфері забезпечення міжнародної інформаційної безпеки.
6) Стратегічний план дій Робочої групи з питань телекомунікацій та інформації на 2016–2020 роки (SAP 2016–2020).
7) Регіональний форум АСЕАН з питань безпеки.
8) Роль Міжамериканської комісії з питань зв'язку (CITEL) у забезпеченні інформаційної безпеки.

3. Ознайомитися та проаналізувати Закон про кібербезпеку ЄС (Регламент 2019/881) https://eur-lex.europa.eu/eli/reg/2019/881/oj та скласти план-конспект основних його положень (4 год.).

4. Підготувати схему на тему: «Результати Самітів міністрів АТЕС у сфері телекомунікацій та інформації за 1996–2020 роки» (2 год.).

5. Ознайомитися та проаналізувати Стратегію розвитку ШОС до 2025 року від 10.11.2017 року http://infoshos.ru/ru/?id=137 та скласти план-конспект основних її положень (4 год.).

6. Поділитися на дві групи та підготувати питання здобувачам іншої групи за всіма темами курсу для колоквіуму (4 год.).

Завдання для роботи на практичному занятті:

1. Усне опитування та навчальна дискусія за навчальними питаннями для розгляду на практичному занятті.
2. Виконання тестових завдань за навчальними питаннями для розгляду на практичному занятті.
3. Захист презентацій.
4. Навчальна дискусія за Законом про кібербезпеку ЄС (Регламент 2019/881).
5. Навчальна дискусія за Стратегією розвитку ШОС до 2025 року від 10.11.2017 роук.
6. Колоквіум за питаннями, що були підготовлені групами здобувачів за всіма темами курсу.

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ПІДГОТОВКИ ММ-ПРЕЗЕНТАЦІЙ ДОПОВІДЕЙ (з використанням Microsoft PowerPoint)

Мультимедійна презентація – інструмент, що дозволяє передавати інформацію у візуалізованому, схематичному вигляді, що підвищує її цінність.

Загальні вимоги: наявність титульного слайду, на якому зазначаються: тема доповіді, ПІБ здобувача, навчальна група та факультет; дотримання єдиного стилю оформлення усіх слайдів; дотримання прийнятих правил орфографії, пунктуації, скорочень і правил оформлення тексту (відсутність точки в заголовках і т. д.); перелік використаних джерел (на останньому слайді); не менше 15 слайдів.

Вимоги до дизайну: використання корпоративного шаблону факультету (наявність на всіх слайдах назви, логотипу та електронної адреси факультету МЕВ та ТБ); використання не більше трьох кольорів на одному слайді (один для фону, другий для заголовків, третій для тексту); при виборі кольору тексту та заливки діаграм дотримуватись правила 3-х кольорів – використовувати три основні кольори та їх відтінки; уникати зміни фону слайдів (у виключних випадках, використовувати комфортні тони).

Вимоги до вмісту слайдів: на слайді бажано подавати: одне ключове поняття; 7–8 рядків тексту; одну діаграму з аналітичним коментарем; одну схему SmartArt; зміст презентації має відповідати меті та завданням доповіді; розташування інформації на слайді – переважно горизонтальне, зверху вниз по головній діагоналі; найбільш важлива

інформація має розташовуватися в центрі екрану; якщо на слайді картинка – напис розміщується під нею.

Вимоги до тексту: стислість і лаконічність викладу, максимальна інформативність тексту; для подання текстового матеріалу використовувати шрифт з розміром – 20 пт, мінімально і лише у виключних випадках – 14 пт; використовувати шрифти без зарубок і не більше 1–2-х варіантів шрифтів; довжина рядка не більше 36 знаків; відстань між рядками рекомендована усередині абзацу 1,5, а між –абзаців – 2 інтервали; форматувати текст по ширині, не допускати «рваних» країв тексту; підкреслення використовується лише в гіперпосиланнях.

Вимоги до візуального і анімаційного ряду: матеріал має бути структурований, у тому числі в схемах та організаційних діаграмах; матеріал за потреби підкріплювати доречними графічними зображеннями та відео-фрагментами; цифрові дані краще представляти у вигляді таблиць та діаграм, витриманих у стриманих кольорах; давати посилання на мультимедійний зміст і хмарні дані через функцію гіперпосилання; якість зображення (контраст зображення по відношенню до фону; відсутність «зайвих» деталей на фотографії або картинці, яскравість і контрастність зображення); якість музичного ряду (ненав'язливість музики, відсутність сторонніх шумів); ефекти анімації застосовувати для акцентування уваги на визначених моментах, поетапного виведення вмісту слайду на екран, для демонстрації руху або послідовності дій.

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО НАПИСАННЯ ЕСЕ

Есе – самостійна творча письмова робота, ознакою якої є особистісний характер сприймання проблеми та її осмислення, невеликий обсяг, вільна композиція, невимушеність та емоційність викладу.

Мета есе полягає в розвитку навичок самостійного творчого мислення й письмового послідовного викладу власних думок.

Есе дозволяє авторові навчитися чітко й грамотно формулювати думки, структурувати інформацію, використовувати основні категорії аналізу, виділяти причиново-наслідкові зв'язки, ілюструвати поняття відповідними прикладами, аргументувати свої висновки; володіти науковим стилем мовлення.

Есе виражає індивідуальні враження й міркування автора з конкретного приводу або предмета й не претендує на вичерпне трактування. Відносно обсягу й функції межує, з одного боку, з науковою статтею й літературним нарисом (з яким есе нерідко плутають), з іншого боку – з філософським трактатом. Есеїстичному стилю властиві образність, рухливість асоціацій, нерідко антитиповість мислення, орієнтування на інтимну відвертість і розмовну інтонацію.

Види есе:

1) **Вільне** – невеликий обсяг (7–10 речень); вільна форма і стиль викладу; довільна структура; обов'язкова вимога – наявність позиції автора.

2) **Формальне** – дотримання структури тексту; наявність відповідних компонентів (тези, аргументи, приклади, оцінювальні судження, висновки); обґрунтування (аргументування) тези.

Види формального есе:

- інформаційне (есе-розповідь, есе-визначення, есе-опис);
- критичне;
- есе-дослідження (порівняльне есе, есе-протиставлення, есе причини-наслідку, есе-аналіз).

Вимоги до формального есе:

1. Обсяг – 2–3 сторінки тексту (200–300 слів).
2. Есе повинно сприйматися як цілісний твір, ідея якого зрозуміла й чітка.
3. Кожен абзац есе розкриває одну думку.

4. Необхідно писати стисло і ясно. Есе не повинно містити нічого зайвого, має нести лише інформацію, необхідну для розкриття ідеї есе, власної позиції автора.

5. Есе має відрізнятися чіткою композиційною побудовою, бути логічним за структурою. В есе, як і в будь-якому творі, повинна простежуватися внутрішня логіка, що визначається, з одного боку, авторським підходом до обговорюваного питання, а з іншого – самим питанням. Необхідно уникати різких стрибків від однієї ідеї до іншої, думка має розкриватися послідовно.

6. Есе повинно засвідчити, що його автор знає й осмислено застосовує теоретичні поняття, терміни, узагальнення, ідеї.

7. Есе має містити переконливе аргументування порушеної проблеми.

Есе повинне містити: чіткий виклад суті поставленої проблеми, включати самостійно проведений аналіз цієї проблеми з використанням концепцій і аналітичного інструментарію, розглянутого в рамках дисципліни, висновки, що узагальнюють авторську позицію з поставленої проблеми.

Структура есе:

Есе складається з таких частин – вступ, основна частина, висновок.

Вступ – обґрунтування вибору теми есе (1–2 абзаци). На цьому етапі дуже важливо правильно сформулювати тезу, яку Ви розкриєте в основній частині. У вступі фокусується увага на проблематиці есе, ставляться ключові питання. Не зайвим буде вказівка на актуальність (значимість для сучасного суспільства) проблеми есе. На цьому етапі дуже важливо правильно сформулювати питання, на які ви збираєтеся знайти відповідь у ході свого дослідження. При роботі над вступом можуть допомогти відповіді на наступні питання: «Чи потрібно давати визначення термінам, що пролунали в темі есе?», «Чому тема, яку я розкриваю, є важливою в даний момент?», «Які поняття будуть залучені в мої міркування?», «Чи можу я розділити тему на трохи більше дрібних підтем?» і т. д. Використовуйте «пастки» для залучення уваги, такі як: цитата, вірш, питання, роздуми, незвичайні факти, ідей або смішні історії. Немає необхідності висловлювати в першій пропозиції основну думку. Уникайте таких фраз, як «Це есе про…» або «Я збираюся говорити про…».

Основна частина – теоретичні основи обраної проблеми й виклад основного питання (3–5 абзаців). Ця частина припускає розвиток аргументації й аналізу, а також обґрунтування їх, виходячи з наявних даних, інших аргументів і позицій. Тут мало погодитися або не погодитися з чиєюсь думкою, необхідно продовжити або доповнити її. Аргументи повинні бути послідовними. Кожна думка має підкріплюватися доказами. У процесі побудови есе необхідно пам'ятати, що один абзац повинен містити тільки одне твердження й відповідний доказ. Виражайте свої думки зрозуміло. Підкріплюйте основні ідеї фактами, роздумами, ідеями, яскравими описами, цитатами або іншою інформацією чи матеріалами. Один зі способів визначення основних пунктів есе та логічності висвітлення теми в цілому – використання підзаголовків для позначення в головній частині ключових моментів аргументованого викладення.

Висновок – узагальнення й аргументовані висновки до теми, які підсумовують есе або ще раз вносять пояснення, підкріплюють зміст і значення викладеного в основній частині (1–2 абзаци). Продемонструйте вашу позицію щодо порушеної проблеми. Методи, що рекомендують для складання висновка: повторення, ілюстрація, цитата. Висновок може містити такий дуже важливий, що доповнює есе, елемент як вказівка на застосування дослідження, на розвиток взаємозв’язків з іншими проблемами.

При оцінюванні есе в центрі уваги знаходиться: здібність розуміти, оцінювати та встановлювати зв’язки між ключовими моментами проблем та запитань; уміння диференціювати протилежні підходи та моделі, застосовуючи їх до емпіричного матеріалу або дискусії з принципових питань; здібність критично та незалежно оцінити наявні дані, точку зору, позицію, аргументи; здатність до застосування аналітичних підходів, моделей тощо.

3. ЗАВДАННЯ ДЛЯ ПІДСУМКОГОВО КОНТРОЛЮ ЗНАНЬ, УМІНЬ ТА НАВИЧОК ЗДОБУВАЧІВ, ЗАЛІКОВИХ РОБІТ

Перелік питань до заліку

Заліковий білет містить 40 тестових завдань.

Питання для підготовки:

1. Роль процесів глобалізації та інформатизації у взаємодії суб'єктів міжнародних відносин.
2. Поняття та сутність міжнародного конфлікту.
3. Основні функції міжнародного конфлікту.
4. Методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах.
5. Поняття та зміст інформаційного протиборства.
6. Історичні етапи розвитку інформаційного протиборства.
7. Фактори та умови сучасного ведення інформаційного протиборства.
8. Мета та принципи інформаційного протиборства.
9. Стадії інформаційного протиборства.
10. Поняття, та ознаки інформаційної експансії.
11. Поняття та ознаки інформаційної агресії, її види.
12. Поняття та ознаки інформаційної війни.
13. Основні підходи до визначення поняття «інформаційна безпека».
14. Поняття «міжнародна інформаційна безпека».
15. Класифікації інформаційної безпеки.
16. Поняття інформаційних загроз та їх властивості.
17. Класифікації загроз інформаційній безпеці.
18. Інформаційна злочинність та інформаційний тероризм.
19. Поняття та ознаки інформаційної зброї.
20. Класифікації інформаційної зброї.
21. Моделі системи глобальної інформаційної безпеки.
22. Фактори ефективності системи міжнародної безпеки.
23. Резолюції ГА ООН «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки».
24. Діяльність Спеціальної групи урядових експертів держав-членів ООН в сфері міжнародної інформаційної безпеки.
25. Роль Всесвітнього саміту з питань інформаційного суспільства у розвитку міжнародного співробітництва у сфері інформаційної безпеки.
26. Роль міжнародної організації кримінальної поліції (Інтерпол) у сфері міжнародної інформаційної безпеки.
27. Конвенція Ради Європи про кіберзлочинність 2001 року.
28. Ініціатива «Електронна Європа» (eEurope).
29. Діяльність Агентства ЄС з мереж і інформаційної безпеки (ENISA).
30. Навчання Cyber Europe.
31. Діяльність Команди реагування на надзвичайні ситуації CERT-EU.
32. Діяльність Європейського центру по боротьбі з кіберзлочинністю (ЕС3).
33. Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС 2016 року (NIS Directive).
34. Інструменти забезпечення інформаційної безпеки в рамках АТЕС.
35. Результати самітів міністрів АТЕС у сфері телекомунікацій та інформації.
36. Інструменти забезпечення інформаційної безпеки в рамках АСЕАН.
37. Регіональний форум АСЕАН з питань безпеки.
38. Інструменти забезпечення інформаційної безпеки в рамках ШОС.
39. Інструменти забезпечення інформаційної безпеки в рамках ОАД.
40. Роль Міжамериканської комісії з питань зв'язку (CITEL) у сфері інформаційної безпеки.

Приклад залікового білету

Харківський національний університет імені В. Н. Каразіна
Факультет міжнародних економічних відносин та туристичного бізнесу

Галузь знань: 29 «Міжнародні відносини»
Спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітня програма: «Міжнародна інформаційна безпека»
Семестр: 3
Форма навчання: денна
Рівень вищої освіти: другий (магістерський)
Навчальна дисципліна: «Міжнародна інформаційна безпека»

ЗАЛІКОВИЙ БІЛЕТ № 1

1. Дати відповідь на тестові завдання (Додаток 1).

Затверджено на засіданні кафедри міжнародних відносин,
міжнародної інформації та безпеки
протокол № 1 від “26” серпня 2020 р.

Завідувач кафедри _____ Л. В. Новікова

Екзаменатор _____ О. М. Доценко

4. РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна література

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за ред. проф. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.
2. Гапаєва О. Міжнародна інформаційна безпека – ключовий напрям діяльності шанхайської організації співробітництва: 2006–2017 рр. *Східноєвропейський історичний вісник.* 2017. Вип. 4. С. 155–163.
3. Грицун О. О. Поняття міжнародної інформаційної безпеки: порівняльно-правовий аспект. *Науковий вісник Ужгородського національного університету.* Серія ПРАВО. 2015. Випуск 31. Том 3. С. 123–127. URL: http://www.visnyk-juris.uzhnu.uz.ua/file/No.31/part_3/33.pdf (дата звернення: 20.08.2020).
4. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об’єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 2 (18). С.16–22.
5. Зозуля О. С. Інформаційна зброя як геополітичний чинник та інструмент силової політики. *Державне управління: теорія та практика.* 2013. № 2. С. 82–89. URL: http://nbuv.gov.ua/UJRN/Dutp_2013_2_12 (дата звернення: 20.08.2020).
6. Інформаційна безпека (соціально-правові аспекти) / В. Остроухов, В. Петрик, М. Присяжнюк та ін. ; за ред. Є.Д. Скулиша. К. : КНТ, 2010. 776 с.
7. Карпов О. Н. Можливості використання баз даних Міжнародної організації кримінальної поліції – Інтерпол у протидії тероризму. *Питання інформаційної безпеки.* 2009. № 21. С. 301–306.

8. Кириченко І. О. Співробітництво організації американських держав та Сполучених Штатів Америки у сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин.* 2010. Випуск 93 (Частина І). С. 160–164.

9. Король А. Інформаційні технології в системі міжнародних відносин: проблема впровадження. *Мультиверсум. Філософський альманах.* 2015. Випуск 3–4 (141–142). С. 59–67.

10. Лапінська Є. І. Інформаційна безпека: поняття, види та ознаки. *Порівняльно-аналітичне право.* 2018. № 6. С. 262–266.

11. Левченко О. В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2014. № 2. С. 142–146 URL: http://nbuv.gov.ua/UJRN/sitsbo_2014_2_25 (дата звернення: 20.08.2020).

12. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. *Актуальні проблеми міжнародних відносин.* 2011. Випуск 102 (Частина І). С. 160–164

13. Макаренко Є. Інформаційне протиборство у сучасних міжнародних відносинах. *Міжнародні відносини. Серія «Політичні науки».* 2017. № 17. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3316/2995 (дата звернення: 20.08.2020).

14. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матер. III Міжнар. наук.-практ. конф. (м. Дніпро, 15 бер. 2019 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2019. 365 с. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/science/publish/np2d5.pdf (дата звернення: 20.08.2020).

15. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та Українські реалії. *Young Scientist.* 2019. № 12.1 (76.1). С. 55–60.

16. Терещук В. І. Міжнародні комунікації у безпековому дискурсі ООН: наявні і потенційні виклики. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3874/3534 (дата звернення: 10.05.2020).

17. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємництво, господарство і право. 2017. № 10. С. 182– 186. URL: http://pgp-journal.kiev.ua/archive/2017/10/38.pdf (дата звернення: 20.08.2020).

18. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України: дис. … докт. юрид. наук: 12.00.07 / ДВНЗ «Ужгородський національний університет. Ужгород, 2019. 487 с.

19. Толубко В. Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія. Київ : НАОУ, 2003. 320 с.

20. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. Міжнародні відносини. Серія «Політичні науки». 2018. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140 (дата звернення: 20.08.2020).

21. Широкова-Мурараш О. Г., Акчурін Ю. Р. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-праовий аспект. Інформація і право. 2011. № 1(1). С. 76–81. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/38938/14-Shirokova.pdf?sequence=1 (дата звернення: 20.08.2020).

22. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd ed. Syngress, 2014. 240 p.

23. Giacomello G. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. 1st ed. Bloomsbury Academic, 2014. 256 p.

24. Overview of Cybersecurity Status in ASEAN and the EU. Sociedade Portuguesa de Inovação (SPI), 2018. 87 p. URL: https://ec.europa.eu/research/participants/documents/downloadPublic/VndWdmIxY WFBQUVNaTc4Y25aWkxISVpLSXRPQjBiK0lHakYrMlNIa3JOZGhkaWRNUnR

ZbTVBPT0=/attachment/VFEyQTQ4M3ptUWNCZ0ErcVdweUc2Mnlzc0hRQ2gwV Wg= (Last Accessed: 20.08.2020).

25. What is the Difference between Cyber Security and Information Security? *Computer Science Degree Hub.* URL: https://www.computersciencedegreehub.com/faq/what-is-the-difference-between-cyber-security-and-information-security/ (Last Accessed: 20.08.2019).

Допоміжна література

1. Близнюк А. Гібридна війна XXI століття. Пропаганда як основна складова у політичних, соціальних та етнічних протистояннях. *Інтермарум: історія, політика, культура.* 2015. Вип. 2. С. 390–399.

2. Бойко С. Проблематика международной информационной безопасности на площадках ШОС и БРИКС. *Международная жизнь* : веб-сайт. 23.01.2019. URL: https://interaffairs.ru/news/show/21480 (дата звернення: 20.08.2020).

3. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. … канд. політ. наук: 23.00.04 / Дипломатична академія України при МЗС України; Чорноморський національний університет імені Петра Могили. Київ, 2018. 210 с.

4. Коломієць О. В. Особливості системи міжнародної безпеки в умовах глобалізації : автореф. дис. ... д-ра політ. наук : 23.00.04 / Нац. ун.-т «Одеська юридична академія». Одеса, 2015. 36 с.

5. Король А. М. Інформаційні чинники демократизації політичної культури у системі міжнародних відносин : дис. … канд. політ. наук: 23.00.03 / Нац. пед. ун-т. ім. М. П. Драгоманова. Київ, 2016. 203 с.

6. Любохинець Л. С., Поплавська О. В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. *Науково-виробничий журнал «Бізнес-навігатор».* 2017. Випуск 4-1 (43). С. 93–97.

7. Почепцов Г. Г. Сучасні інформаційні війни. Київ: Києво-Могилянська академія, 2015. 498 с.

8. Рижук О. М. Поняття інформаційних та гібридних війн в умовах глобалізації. *Освіта регіону. Політологія. Психологія. Комунікації.* 2016. № 3. С. 84–88. URL: https://social-science.uu.edu.ua/article/1389 (дата звернення: 20.08.2020).

9. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. Вісник Книжкової палати. 2013. Вип. 1. С. 40–43.

10. Сербіна К. Ю. Необхідність реформування безпекового простору у контексті протидії новим викликам безпеці (на прикладі діяльності організації американських держав). *Актуальні проблеми міжнародних відносин.* 2012. Випуск 107 (Частина ІІ). С. 151–161.

11. Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення концепту. *Держава та право.* 2014. № 8. С. 18–22.

12. Соснін О. В., Воронкова В. Г., Постол О. Є. Сучасні міжнародні системи та глобальний розвиток (соціально-політичні, соціально-економічні, соціально-антропологічні виміри) : навч. посіб. Київ, 2015. 556 с.

13. Чекаленко Л. Про поняття «гібридна війна». Журнал «Віче». 2015. № 5. С. 41–42. URL: http://nbuv.gov.ua/UJRN/viche_2015_5_21 (дата звернення: 20.08.2020).

14. Щепанівський В. Г. Інформаційна безпека як складова сучасного образу України. *Актуальні проблеми міжнародних відносин.* 2011. Випуск 102 (Частина І). С. 219-228.

15. Яцишин М. Ю. Роль міжнародних організацій у протидії кіберзлочинності. Українське право. 15.12.2019. URL: https://ukrainepravo.com/international_law/public_international_law/rolmizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/ (дата звернення: 20.08.2020).

16. About APEC. *Asia-Pacific Economic Cooperation* : веб-сайт. URL: https://www.apec.org/About-Us/About-APEC (Last Accessed: 20.08.2020).
17. About CSIRTs Network. *CIRTsNEtwork* : web-site. URL: https://csirtsnetwork.eu/ (Last Accessed: 20.08.2020).
18. About ENISA. *ENISA* : web-site. URL: https://www.enisa.europa.eu/about-enisa (Last Accessed: 20.08.2020).
19. About Us. *CERT-EU.* URL: https://cert.europa.eu/cert/plainedition/en/cert_about.html (Last Accessed: 20.08.2020).
20. Collins A. Contemporary Security Studies. 3rd ed. United Kingdom: Oxford University Press, 2013. 478 p.
21. Cyber Europe 2020. URL: https://www.enisa.europa.eu/topics/cyberexercises/cyber-europe-programme/cyber-europe-2020/ (Last Accessed: 20.08.2020).
22. Deutsch M., Coleman P. T., Marcus E. C. The handbook of conflict resolution: theory and practice. 3rd. ed. San Francisco : John Wiley & Sons, 2014. 1264 p.
23. European Cybercrime Centre - EC3. Combating crime in a digital age. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Last Accessed: 20.08.2020).
24. The Shanghai Cooperation Organisation. *The Shanghai Cooperation Organisation* : веб-сайт. URL: http://eng.sectsco.org/about_sco/ (Last Accessed:20.08.2020).
25. Who we are. *OAS* : веб-сайт. URL: http://www.oas.org/en/about/who_we_are.asp (Last Accessed: 20.08.2020).

Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Верховна Рада України – www.zakon1.rada.gov.ua.
2. Міністерство закордонних справ – http://mfa.gov.ua/ua
3. Міністерство юстиції – https://minjust.gov.ua/ua
4. Конституційний Суд України – http://www.ccu.gov.ua/uk/index
5. Організація Об'єднаних Націй – http://www.un.org/
6. Європейський суд з прав людини – http://echr.coe.int/
7. Європейський союз – http://eeas.europa.eu/
8. Організація з безпеки та співробітництва в Європі – http://www.osce.org/
9. Рада Європи – http://www.coe.int/web/portal/home
10. Управління Верховного комісара ООН з прав людини – http://www.ohchr.org/
11. Національна парламентська Бібліотека України – http://www.nplu.org/
12. Національна бібліотека України імені В. І. Вернадського – www.nbuv.gov.ua
13. Київська центральна міська публічна бібліотека імені Лесі Українки – http://lucl.lucl.kiev.ua
14. Центральна наукова бібліотека Харківського національного університету імені В. Н. Каразіна – http://www.univer.kharkov.ua
15. Харківська державна наукова бібліотека ім. В. Г. Короленка – http://korolenko.kharkov.com