ЗАТВЕРДЖЕНО
Вченою радою факультету національної безпеки, права та міжнародних відносин
27 серпня 2024 р., протокол № 8
Голова Вченої ради
_____ Лариса СЕРГІЄНКО

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Аналіз даних в системі національної безпеки»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 256 «Національна безпека
(за окремими сферами забезпечення і видами діяльності)»
освітньо-професійна програма «Національна безпека
(за окремими сферами забезпечення і видами діяльності)»
факультет національної безпеки, права та міжнародних відносин
кафедра національної безпеки, публічного управління та адміністрування

Схвалено на засіданні кафедри
права та правоохоронної діяльності
26 серпня 2024 р., протокол № 8

Завідувача кафедри
_____ Іван ДРАГАН

Гарант освітньої-професійної програми
_____ Ірина СУПРУНОВА

Розробник: к.н.д.у., доцент кафедри права та правоохоронної діяльності,
Юрій КРУТІК

Житомир
2024

Робоча програма навчальної дисципліни «Аналіз даних в системі національної безпеки України» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» за освітньо-професійною програмою «Національна безпека (за окремими сферами забезпечення і видами діяльності)» затверджена Вченою радою факультету національної безпеки, права та міжнародних відносин від 27 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма</td><td>заочна форма</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань
25 «Воєнні науки, національна безпека, безпека державного кордону»</td><td colspan="2">Обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="6">Спеціальність
256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>4</td><td>4</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td>8</td><td>8</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 3;
самостійної роботи – 2,6</td><td rowspan="10">Освітній ступінь «бакалавр»</td><td>32 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>16 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>42 год.</td><td>74</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи.

для заочної форми навчання – 18 % аудиторних занять, 82 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо аналізу даних у сфері національної безпеки з використанням сучасних статистичних, інформаційно-аналітичних методів та штучного інтелекту для оцінки загроз і розробки стратегій безпеки.

Завданнями вивчення навчальної дисципліни є:

– ознайомлення здобувачів з основами аналізу даних та його роллю в системі національної безпеки;

– вивчення методів збору, перевірки та обробки інформації з офіційних і відкритих джерел (OSINT);

– опанування інструментів статистичного аналізу для оцінки ризиків і прогнозування загроз;

– використання технологій Big Data та штучного інтелекту для аналітичних задач у сфері безпеки;

– розвиток навичок застосування геоінформаційних систем (ГІС) у сфері безпеки;

– аналіз кібербезпеки, інформаційних загроз і механізмів їх виявлення;

– дослідження комплексного підходу до оцінки загроз та сценарного планування;

– вивчення методів аналізу даних у ключових сферах безпеки: державній, воєнній, економічній, продовольчій, екологічній, демографічній тощо;

– ознайомлення з міжнародним досвідом аналізу даних у сфері національної безпеки.

Зміст навчальної дисципліни спрямований на формування наступних **компетентностей** за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»:

ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК 13. Здатність виявляти можливі загрози інформаційному простору та протидіяти інформаційно-психологічним впливам шляхом використання інформаційно-комунікаційних технологій, імплементації сучасних методів інформаційної безпеки та захисту інформації

Отримані знання з навчальної дисципліни стануть складовими наступних **результатів навчання** за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»:

ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави.

ПРН 11. Вміти прогнозувати складні процеси, що відбуваються в системі національної та міжнародної безпеки і їх практичні наслідки, зокрема, явища різних сфер суспільного життя, володіти навиками професійного використання методів стратегічного планування в фаховій діяльності

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати наступні Soft skills:

– *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію; навички працювати в команді;

– *уміння виступати привселюдно*: навички, необхідні для виступів на публіці; навички проведення презентації;

– *керування часом:* уміння справлятися із завданнями вчасно;

– *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;

– *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;

– *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни
Модуль 1

ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ ДАНИХ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Тема 1. Основи аналізу даних у системі національної безпеки (ЗК 1, ПРН 11)

1.1. Поняття, мета та завдання аналізу даних
1.2. Роль аналітики в системі національної безпеки
1.3. Інформаційне забезпечення видів національної безпеки
1.4. Аналітичні продукти
1.5. Концепція створення єдиної інформаційної системи

Тема 2. Джерела та методи збору даних у сфері безпеки (ЗК 1, ПРН 11)

2.1. Офіційні джерела та відкриті дані (OSINT)
2.2. Соціологічні дослідження та моніторинг громадської думки
2.3. Аналітичні платформи та бази даних
2.4. Методи верифікації та перевірки достовірності даних
2.5. Етичні та правові аспекти використання закритих даних

Тема 3. Основи статистичного аналізу даних (ЗК 1, СК 13, ПРН 6, ПРН 11)

3.1. Дескриптивна статистика та візуалізація даних
3.2. Кореляційний та регресійний аналіз
3.3. Прогнозування на основі часових рядів
3.4. Ймовірнісний аналіз загроз та оцінка ризиків

Тема 4. Використання великих даних та штучного інтелекту (ЗК 1, ЗК 5, СК 13, ПРН 6, ПРН 11)

4.1. Big Data у сфері безпеки
4.2. Машинне навчання для аналізу загроз

4.3. Автоматизовані системи моніторингу та розпізнавання патернів
4.4. Аналіз соціальних мереж та цифрових слідів

Тема 5. Геоінформаційні системи (ГІС) у сфері безпеки (ЗК 1, ЗК 5, СК 13, ПРН 6, ПРН 11)
5.1. Основи геопросторового аналізу
5.2. ГІС для прогнозування кризових ситуацій
5.3. Використання супутникових знімків та дронів
5.4. Аналіз мобільності населення та міграційних процесів

Тема 6. Розвідка на основі відкритих джерел (OSINT) (ЗК 1, ЗК 5, СК 13, ПРН 6, ПРН 11)
6.1. Методи OSINT у сфері національної безпеки
6.2. Виявлення дезінформації та інформаційних загроз
6.3. Інструменти автоматизованого збору інформації
6.4. Методичні аспекти використання OSINT

Тема 7. Кібербезпека та захист інформації (ЗК 1, ЗК 5, СК 13, ПРН 6, ПРН 11)
7.1. Основи кіберзагроз та методи їх виявлення
7.2. Аналіз загроз у Dark Web
7.3. Використання штучного інтелекту у сфері кібербезпеки
7.4. Сучасні пошукові сервіси та інструменти аналізу кіберзлочинів

Тема 8. Комплексна оцінка загроз національній безпеці (ЗК 1, ПРН 11)
8.1. Інтеграція різних методів аналізу
8.2. Візуалізація даних та розробка аналітичних звітів
8.3. Сценарне планування загроз та практичне застосування результатів аналізу в ухваленні рішень
8.4. Цифрові технології та аналітичні засоби аналізу воєнних злочинів в Україні

ЗМІСТОВИЙ МОДУЛЬ 2. ПРАКТИЧНЕ ЗАСТОСУВАННЯ АНАЛІЗУ ДАНИХ У РІЗНИХ СФЕРАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Тема 9. Аналіз даних у сфері державної безпеки (ЗК 1, ЗК 5, ПРН 11)
9.1. Моніторинг політичної стабільності та державного управління
9.2. Аналіз діяльності іноземних спецслужб та гібридних загроз
9.3. Виявлення корупційних схем та фінансових махінацій
9.4. Вплив інформаційних кампаній на державну безпеку

Тема 10. Аналіз даних у воєнній безпеці (ЗК 1, ЗК 5, СК 13, ПРН 6, ПРН 11)
10.1. Оцінка воєнних загроз та обороноздатності
10.2. Використання ГІС та супутникової розвідки
10.3. Прогнозування воєнних конфліктів
10.4. Аналіз відкритих джерел для оцінки воєнних ризиків

Тема 11. Аналіз даних у сфері економічної безпеки (ЗК 1, ЗК 5, ПРН 11)
11.1. Виявлення фінансових ризиків та макроекономічних загроз

11.2. Моніторинг тіньової економіки та нелегальних фінансових операцій
11.3. Аналіз санкційної політики та її наслідків
11.4. Методи оцінки економічної стійкості держави

Тема 12. Аналіз даних у сфері інформаційної безпеки (ЗК 1, ЗК 5, СК 13, ПРН 6, ПРН 11)

12.1. Виявлення інформаційних атак та пропагандистських кампаній
12.2. Аналіз кіберзагроз та зламів
12.3. Використання AI у боротьбі з дезінформацією
12.4. Захист критичної інформаційної інфраструктури

Тема 13. Аналіз даних у сфері екологічної безпеки (ЗК 1, ЗК 5, СК 13, ПРН 6, ПРН 11)

13.1. Оцінка впливу екологічних катастроф
13.2. Аналіз забруднення довкілля та його наслідків
13.3. Використання супутникових знімків у моніторингу екологічних загроз
13.4. Виявлення нелегального використання природних ресурсів

Тема 14. Аналіз даних у сфері демографічної безпеки (ЗК 1, ЗК 5, ПРН 11)

14.1. Динаміка народжуваності та смертності
14.2. Дослідження тенденцій міграції
14.3. Демографічні кризи та їх наслідки
14.4. Політика держави у сфері демографічної безпеки

Тема 15. Аналіз даних у сфері продовольчої безпеки (ЗК 1, ЗК 5, ПРН 11)

15.1.Аналіз ризиків продовольчої безпеки
15.2. Економічна доступність продовольства
15.3. Аналіз якості та безпечності харчових продуктів
15.4. Вплив воєнних конфліктів на глобальну продовольчу безпеку

Тема 16. Ризик-орієнтований підхід аналізу даних в сфері національної безпеки (ЗК 1, ЗК 5, ПРН 11)

16.1. Сутність ризик-орієнтованого підходу
16.2. Структура і рівні ризик-орієнтованого підходу
16.3. Виявлення, оцінювання та визначення ризиків
16.4. Управління ризиками в сфері національної безпеки
16.5. Міжнародний досвід застосування ризик-орієнтованого підходу в безпековій сфері

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	практичні	самостійна робота	усього	лекції	практичні	самостійна робота
ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ ДАНИХ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ								
Тема 1. Основи аналізу даних у системі національної безпеки	5	2	1	2	5	1	–	4
Тема 2. Джерела та методи збору даних у сфері безпеки	5	2	1	2	5	1	–	4
Тема 3. Основи статистичного аналізу даних	5	2	1	2	6	1	–	5
Тема 4. Використання великих даних та штучного інтелекту	5	2	1	2	6	1	–	5
Тема 5. Геоінформаційні системи (ГІС) у сфері безпеки	5	2	1	2	6	1	–	5
Тема 6. Розвідка на основі відкритих джерел (OSINT)	5	2	1	2	6	1	–	5
Тема 7. Кібербезпека та захист інформації	6	2	1	3	6	1	–	5
Тема 8. Комплексна оцінка загроз національній безпеці	6	2	1	3	5	1	–	4
Разом за змістовим модулем 1	**42**	**16**	**8**	**18**	**45**	**8**	–	**37**
Змістовий модуль 2. ПРАКТИЧНЕ ЗАСТОСУВАННЯ АНАЛІЗУ ДАНИХ У РІЗНИХ СФЕРАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ								
Тема 9. Аналіз даних у сфері державної безпеки	6	2	1	3	6	1	–	5
Тема 10. Аналіз даних у воєнній безпеці	6	2	1	3	6	1	–	5
Тема 11. Аналіз даних у сфері економічної безпеки	6	2	1	3	5	–	1	4
Тема 12. Аналіз даних у сфері інформаційної безпеки	6	2	1	3	5	–	1	4
Тема 13. Аналіз даних у сфері екологічної безпеки	6	2	1	3	5	–	1	4
Тема 14. Аналіз даних у сфері демографічної безпеки	6	2	1	3	5	–	1	4
Тема 15. Аналіз даних у сфері продовольчої безпеки	6	2	1	3	6	–	1	5
Тема 16. Ризик-орієнтований підхід аналізу даних в сфері національної безпеки	6	2	1	3	7	–	1	6
Разом за змістовим модулем 2	**48**	**16**	**8**	**24**	**45**	**2**	**6**	**37**
РАЗОМ	**90**	**32**	**16**	**42**	**90**	**10**	**6**	**74**

5. Теми практичних занять

№ з/п	Назва теми	К-ть годин	
		денна форма	заочна форма
1	2	3	4
ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ ДАНИХ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ			
1	**Тема 1.** Основи аналізу даних у системі національної безпеки	1	–
2	**Тема 2.** Джерела та методи збору даних у сфері безпеки	1	–
3	**Тема 3.** Основи статистичного аналізу даних	1	–
4	**Тема 4.** Використання великих даних та штучного інтелекту	1	–
5	**Тема 5.** Геоінформаційні системи (ГІС) у сфері безпеки	1	–
6	**Тема 6.** Розвідка на основі відкритих джерел (OSINT)	1	–
7	**Тема 7.** Кібербезпека та захист інформації	1	–
8	**Тема 8.** Комплексна оцінка загроз національній безпеці	1	–
Разом за змістовим модулем 1		**8**	**–**
ЗМІСТОВИЙ МОДУЛЬ 2. ПРАКТИЧНЕ ЗАСТОСУВАННЯ АНАЛІЗУ ДАНИХ У РІЗНИХ СФЕРАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ			
9	**Тема 9.** Аналіз даних у сфері державної безпеки	1	–
10	**Тема 10.** Аналіз даних у воєнній безпеці	1	–
11	**Тема 11.** Аналіз даних у сфері економічної безпеки	1	1
12	**Тема 12.** Аналіз даних у сфері інформаційної безпеки	1	1
13	**Тема 13.** Аналіз даних у сфері екологічної безпеки	1	1
14	**Тема 14.** Аналіз даних у сфері демографічної безпеки	1	1
15	**Тема 15.** Аналіз даних у сфері продовольчої безпеки	1	1
16	**Тема 16.** Ризик-орієнтований підхід аналізу даних в сфері національної безпеки	1	1
Разом за змістовим модулем 2		**8**	**6**
РАЗОМ		**16**	**6**

6. Завдання для самостійної роботи

№ з/п	Назва теми	К-ть годин	
		денна форма	заочна форма
1	2	3	4
ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ ДАНИХ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ			
1	**Тема 1.** Основи аналізу даних у системі національної безпеки 1.2. Роль аналітики в системі національної безпеки	2	4
2	**Тема 2.** Джерела та методи збору даних у сфері безпеки 2.5. Етичні та правові аспекти використання закритих даних	2	4
3	**Тема 3.** Основи статистичного аналізу даних 3.3. Прогнозування на основі часових рядів	2	5
4	**Тема 4.** Використання великих даних та штучного інтелекту 4.4. Аналіз соціальних мереж та цифрових слідів	2	5
5	**Тема 5.** Геоінформаційні системи (ГІС) у сфері безпеки 5.4. Аналіз мобільності населення та міграційних процесів	2	5
6	**Тема 6.** Розвідка на основі відкритих джерел (OSINT)	2	5

	6.2. Виявлення дезінформації та інформаційних загроз		
7	**Тема 7.** Кібербезпека та захист інформації 7.3. Використання штучного інтелекту у сфері кібербезпеки	3	5
8	**Тема 8.** Комплексна оцінка загроз національній безпеці 8.2. Візуалізація даних та розробка аналітичних звітів	3	4
Разом за змістовим модулем 1		**18**	**37**
ЗМІСТОВИЙ МОДУЛЬ 2. ПРАКТИЧНЕ ЗАСТОСУВАННЯ АНАЛІЗУ ДАНИХ У РІЗНИХ СФЕРАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ			
9	**Тема 9.** Аналіз даних у сфері державної безпеки 9.4. Вплив інформаційних кампаній на державну безпеку	3	5
10	**Тема 10.** Аналіз даних у воєнній безпеці 10.3. Прогнозування воєнних конфліктів	3	5
11	**Тема 11.** Аналіз даних у сфері економічної безпеки 11.4. Методи оцінки економічної стійкості держави	3	4
12	**Тема 12.** Аналіз даних у сфері інформаційної безпеки 12.1. Виявлення інформаційних атак та пропагандистських кампаній	3	4
13	**Тема 13.** Аналіз даних у сфері екологічної безпеки 13.1. Оцінка впливу екологічних катастроф	3	4
14	**Тема 14.** Аналіз даних у сфері демографічної безпеки 14.1. Динаміка народжуваності та смертності	3	4
15	**Тема 15.** Аналіз даних у сфері продовольчої безпеки 15.3. Аналіз якості та безпечності харчових продуктів	3	5
16	**Тема 16.** Ризик-орієнтований підхід аналізу даних в сфері національної безпеки 16.5. Міжнародний досвід застосування ризик-орієнтованого підходу в безпековій сфері	3	6
Разом за змістовим модулем 2		**24**	**37**
РАЗОМ		**42**	**74**

7. Індивідуальні самостійні завдання

Індивідуальна робота здобувачів вищої освіти з навчальної дисципліни «Аналіз даних в системі національної безпеки України» включає виконання завдань:

Завдання 1. Проведіть аналіз основних напрямів застосування аналітичних даних для оцінки загроз у сфері національної безпеки у формі аналітичного звіту.

Структура роботи має включати наступні складові:

- визначення поняття аналізу даних у сфері безпеки;
- основні завдання аналітики у сфері національної безпеки;
- види аналітичних продуктів у сфері безпеки;
- практичні приклади застосування аналізу даних для прогнозування загроз.

Завдання 2. Проаналізуйте підходи до організації інформаційних систем у різних державах (наприклад, США, ЄС, Китай, Україна) у формі аналітичного звіту

Структура роботи має включати наступні складові:

- огляд основних інформаційних систем у сфері національної безпеки;
- способи інтеграції аналітичних даних у державні рішення;

– переваги та недоліки різних підходів.

Завдання 3. Використовуючи відкриті дані, створіть презентацію на одну з тем (на вибір: загрози економічній, інформаційній або воєнній безпеці).

Завдання 4. Використовуючи OSINT-методи, зберіть дані про актуальні загрози національній безпеці.

Джерела: Моніторинг новинних сайтів, аналітичних платформ, соціальних мереж.

Завдання 5. Використовуючи статистичні методи, спрогнозуйте ймовірність соціальних заворушень у країні (на основі історичних даних), використовуючи методи кореляційного аналізу, регресійного аналізу, часових рядів.

Завдання 6. Проаналізуйте випадки кібератак на державні установи, використовуючи OSINT-дані та офіційні звіти.

Результати аналізу подайте у формі звіту або презентації

Завдання 7. Проведіть аналіз інформаційних кампаній у соцмережах, спрямованих на дестабілізацію держави, використовуючи методи NLP (аналіз текстів), кластеризації даних, OSINT.

Результати аналізу подайте у формі аналітичного звіту із візуалізацією даних.

Завдання 8. Дослідіть вплив воєнних дій на сільськогосподарське виробництво та продовольчі ланцюги.

Результати аналізу подайте у формі звіту або презентації

8. Методи навчання

Під час викладання навчальної дисципліни використовуються методи навчання, що сприяють досягненню відповідних програмних результатів.

Результат навчання	Методи навчання
ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання, практичних завдань); – Ситуаційний метод; – Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)
ПРН 11. Вміти прогнозувати складні процеси, що відбуваються в системі національної та міжнародної безпеки і їх практичні наслідки, зокрема, явища різних сфер суспільного життя, володіти навиками професійного використання методів стратегічного планування в фаховій діяльності	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; – Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)

9. Методи контролю

Перевірка досягнення програмних результатів навчання здійснюється з використанням наступних методів.

Результат навчання	Методи контролю
ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання практичних робіт, залік
ПРН 11. Вміти прогнозувати складні процеси, що відбуваються в системі національної та міжнародної безпеки і їх практичні наслідки, зокрема, явища різних сфер суспільного життя, володіти навиками професійного використання методів стратегічного планування в фаховій діяльності	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання практичних робіт, залік

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний та підсумковий контроль.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни. Підсумковий контроль проводиться у формі заліку. Процедура складання заліку визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань поточного контролю	100	100
Підсумкова семестрова оцінка	**100**	**100**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	80	80
Виконання та захист індивідуальних самостійних завдань	20	20
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**): 1. Підготовка наукових статей, тез доповідей наукових конференцій	до 20	до 20
Разом за виконання завдань поточного контролю	**100**	**100**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти[1]	Кількість балів за семестр	
	денна форма	заочна форма
Виступи на заняттях	20	20
Участь у дискусії, обговорення питань	20	20
Виконання тестових завдань	15	15
Виконання практичних та ситуаційних завдань, вправ	25	25
Разом за виконання завдань під час навчальних занять	**80**	**80**

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів під час навчальних занять може використовуватися 100-бальна шкала оцінювання щодо кожного окремо виду робіт. Розрахунок загальної кількості балів, які здобувач може набрати за результатами роботи під час навчальних занять протягом семестру, проводиться за формулою:

$$Р_{НЗ} = \sum(Р_i \times ВК_i) \times К_{НЗ}, \quad (1)$$

де $Р_{НЗ}$ – загальна кількість балів, набраних здобувачем за виконання завдань під час навчальних занять за семестр;

$Р_i$ – кількість набраних здобувачем балів за семестр за виконання і-го виду робіт під час навчальних занять (за 100-бальною шкалою);

$ВК_i$ – ваговий коефіцієнт за виконання і-го виду робіт під час навчальних занять. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, яка передбачена за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання усіх видів робіт під час навчальних занять за семестр;

$К_{НЗ}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що передбачена за виконання завдань під час навчальних занять за семестр,

на 100 балів.

Якщо здобувач вищої освіти набрав за поточний контроль 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F		0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1	2	3
1.	Аналіз даних	Data Analysis
2.	Аналітичні продукти	Analytical Products
3.	Аномалія в даних	Data Anomaly
4.	Автоматизовані системи моніторингу	Automated Monitoring Systems
5.	Великі дані	Big Data
6.	База даних	Database
7.	Верифікація даних	Data Verification
8.	Візуалізація даних	Data Visualization
9.	Військова розвідка	Military Intelligence
10.	Геоінформаційні системи	Geoinformation Systems
11.	Гібридна війна	Hybrid Warfare
12.	Глобальна безпека	Global Security
13.	Демографічна безпека	Demographic Security
14.	Джерела даних	Data Sources
15.	Дезінформація	Disinformation
16.	Економічна безпека	Economic Security
17.	Екологічна безпека	Environmental Security
18.	Етичні аспекти аналізу даних	Ethical Aspects of Data Analysis
19.	Захист інформації	Information Protection
20.	Збір розвідданих	Intelligence Collection
21.	Інформаційна безпека	Information Security
22.	Інформаційне забезпечення	Information Assurance
23.	Інформаційні війни	Information Warfare
24.	Кібербезпека	Cybersecurity
25.	Класифікація загроз	Threat Classification
26.	Кореляційний аналіз	Correlation Analysis
27.	Машинне навчання	Machine Learning
28.	Моніторинг громадської думки	Public Opinion Monitoring
29.	Оцінка ризиків	Risk Assessment
30.	Розвідка на основі відкритих джерел	Open Source Intelligence
31.	Прогнозування загроз	Threat Forecasting
32.	Політична безпека	Political Security
33.	Розвідувальна аналітика	Intelligence Analytics
34.	Ризик-орієнтований підхід	Risk-based approach
35.	Соціальна безпека	Social security
36.	Супутникова розвідка	Satellite intelligence
37.	Сценарне планування	Scenario planning
38.	Тіньова економіка	Shadow economy
39.	Технологічна безпека	Technological security
40.	Фінансування тероризму	Terrorist financing
41.	Фундаментальний аналіз	Fundamental analysis
42.	Цифрові сліди	Digital footprints
43.	Штучний інтелект	Artificial intelligence

12. Рекомендована література

Основна література

1. Білявська Ю., Микитенко Н., Шестак Я. Кібербезпека та захист інформації під час пандемії COVID-19. *THE INTERNATIONAL SCIENTIFIC-PRACTICAL JOURNAL "COMMODITIES AND MARKETS"*. 2021. Т. 37, № 7. С. 34–46. URL: https://doi.org/10.31617/tr.knute.2021(37)03.

2. Криза правоохоронної системи України: монографія / За загальною редакцією В.В. Євдокимова, Д.О. Грицишена. - Житомир: Видавничий дім "Бук-друк, 2023. 584 с.

3. Мартинюк С. Характеристика принципів функціонування osint у сфері національної безпеки. *Juridical scientific and electronic journal*. 2021. No. 9. P. 332–334. URL: https://doi.org/10.32782/2524-0374/2021-9/82.

4. Марченко О. Кібербезпека та захист інформації: аналіз впливу ризиків та загроз із використанням сучасних ефективних стратегій захисту кіберпростору. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2023. № 3. С. 50–59. URL: https://doi.org/10.32782/it/2023-3-6.

5. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України ; навчальний посібник / Куреєва О.С., Крутік Ю.В., Махлай О.М., Треус А.С. / за загальною редакцією кандидата психологчних наук О.С. Куреєвої. Хмельницький: Видавництво НАДПСУ, 2022. 400 с.

6. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. – Київ: «ВАІТЕ», 2024. 444 с.

7. Споришев К. Геоінформаційні системи в державному управлінні діяльністю сил безпеки України. *"Scientific Notes of Taurida V.I. Vernadsky University", series "Public Administration"*. 2024. № 1. С. 196–200. URL: https://doi.org/10.32782/tnu-2663-6468/2024.1/34.

Допоміжна література

1. Копиця О., Узлов Д. Методи визначення категорій кіберінцидентів та оцінки ризиків інформаційної безпеки. *Computer Science and Cybersecurity*. 2023. No. 2. P. 33–42. URL: https://doi.org/10.26565/2519-2310-2023-2-04.

2. Кушнір О. К., Чаплінський В. Р. Статистичні методи аналізу великих даних. Modern Economics. 2023. № 39(2023). С. 75-81. DOI: https://doi.org/10.31521/modecon.V39(2023)-11.

3. Панченко О. А., Гнатенко В. С. Економічна кібербезпека в державній системі національної безпеки. *Public management*. 2021. Т. 27, № 2. С. 29–44. URL: https://doi.org/10.32689/2617-2224-2021-2(27)-3.

4. Прощаєв В.В. Принципи розвідувальної діяльності за законодавством країн пострадянського простору: порівняльний аналіз. Науковий вісник публічного та приватного права. Випуск 1, том 1, 2019. С. 96-10

5. Руснак Ю., Стужук Ю. Стратегічне інформаційне управління в системі безпеки та оборони: інтеграція та оптимізація. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*. 2024. Т. 94, № 1. С. 86–96. URL: https://doi.org/10.32453/3.v94i1.1584.

6. Таченко І., Коробейнікова Т., Захарченко С. Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки. *InterConf*. 2021. С. 417–432. URL: https://doi.org/10.51582/interconf.7-8.11.2021.042.

13. Інформаційні ресурси в Інтернеті

1. Інформаційна безпека. URL: https://apps.prometheus.org.ua/learning/course/course-v1:Internews+INFOS101+UA_2021_T3/home

2. OSINT — розвідка з відкритих джерел та інформаційна безпека URL: https://apps.prometheus.org.ua/learning/course/course-v1:Prometheus+OSINT101+2024_T3/home

3. Інформаційна гігієна під час війни: URL: https://apps.prometheus.org.ua/learning/course/course-v1:Prometheus+IHWAR101+2022_T2/home