ЗАТВЕРДЖЕНО
Вченою радою факультету
національної безпеки, права та
міжнародних відносин
22 грудня 2023 р., протокол №11
Голова Вченої ради
_____ Лариса СЕРГІЄНКО

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА»

для здобувачів вищої освіти освітнього ступеня «магістр»
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
теорії та історії держави і права
21 грудня 2023 р., протокол № 12

Завідувач кафедри
_____ Валерій НОНІК

Гарант освітньо-професійної програми
_____ Димитрій ГРИЦИШЕН

Розробник: д.е.н., доц., доцент кафедри теорії та історії держави і права
ДИКИЙ Анатолій

Житомир
2023– 2024 н.р.

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 навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань
25 “Воєнні науки, національна безпека, безпека державного кордону”</td><td colspan="2">нормативна</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">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 – 3</td><td>2</td><td>2</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>4</td><td>4</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи – 6</td><td rowspan="10">Освітній ступінь “магістр”</td><td>24 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>24 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>72 год.</td><td>106 год.</td></tr>
<tr><td colspan="2" rowspan="2">Вид контролю: екзамен</td></tr>
</table>

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

для денної форми навчання – 40% аудиторних занять, 60% самостійної та індивідуальної роботи;

для заочної форми навчання – 12% аудиторних занять, 88% самостійної та індивідуальної роботи

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Інформаційна безпека» є формування у здобувачів вищої освіти знань та компетенцій, спрямованих на забезпечення інформаційної безпеки в системі національної безпеки.

Завданнями вивчення навчальної дисципліни є:

– отримання фундаментальних знань щодо інформаційної безпеки держави;

– систематизація знань та уявлень щодо загроз безпеці держави в інформаційній сфері;

– ідентифікація інтересів всіх членів суспільства в інформаційній сфері

– розуміння системи забезпечення безпеки інформаційно-комунікаційних систем;

– формування уявлень щодо сучасних проявів тероризму в інформаційному просторі.

Зміст навчальної дисципліни направлений на формування загальних та спеціальних компетентностей, визначених стандартом вищої освіти зі спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»:

Загальні компетентності

ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу

ЗК 2. Здатність приймати обґрунтовані рішення

ЗК 6. Здатність вчитися і оволодівати сучасними знаннями

Спеціальні компетентності:

СК 3. Здатність використовувати понятійно-категоріальний апарат теорії національної безпеки, аналізувати та розвивати структуру системи забезпечення національної безпеки та принципи її функціонування

СК 7. Здатність інтегрувати знання та розв’язувати складні задачі національної безпеки (за окремими сферами забезпечення і видами діяльності) у широких та/або мультидисциплінарних контекстах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності

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

ПРН1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.

ПРН2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності

ПРН3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.

ПРН7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.

ПРН12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки.

ПРН17. Виявляти та прогнозувати ризики національній безпеці України з урахуванням теорій терорології та іредентизму та обґрунтовувати заходи щодо їх мінімізації для забезпечення економічної безпеки держави

3. Програма навчальної дисципліни «ІНФОРМАЦІЙНА БЕЗПЕКА»

ЗМІСТОВИЙ МОДУЛЬ 1

Тема 1. Формування інформаційної безпеки держави

1. Елементи та рівні інформаційної безпеки
2. Національне та міжнародне законодавство щодо забезпечення інформаційної безпеки держави
3. Формування комплексної системи захисту інформаційного простору України

Тема 2. Загрози безпеці держави в інформаційній сфері

1. Поняття та види загроз безпеці держави в інформаційній сфері
2. Інформаційні війни як джерело загрози національній безпеці
3. Державна політика щодо забезпечення інформаційної безпеки

Тема 3. Методи оцінки та аналізу інформаційних ризиків

1. Класифікація ризиків інформаційної безпеки
2. Методика оцінки ризиків інформаційної безпеки
3. Удосконалення системи інформаційної безпеки

Тема 4. Оцінка рівня інформаційної безпеки за національними та міжнародними стандартами

1. Оцінка рівня інформаційної безпеки інформаційних ресурсів
2. Критерії оцінки рівня інформаційної безпеки за національними стандартами
3. Критерії оцінки рівня інформаційної безпеки за міжнародними стандартами
4. Нормативно-правове забезпечення захищеності інформаційних ресурсів

Тема 5. Формування та реалізація інформаційної безпеки України

1. Інформаційна безпека як складова національної безпеки держави
2. Суб'єкти забезпечення інформаційної безпеки і захисту інформації.
3. Мета функціонування та завдання системи забезпечення інформаційної безпеки
4. Основні функції системи забезпечення інформаційної безпеки України
5. Стан та перспективи розвитку інформаційної безпеки України
6. Інформаційна політика держави

Тема 6. Протидія кібервійнам та кібертероризму

1. Протидія гібридним та асиметричним проявам кібервійн в забезпеченні національної безпеки
2. Напрями та способи використання кіберпростору у терористичних цілях
3. Сучасні стратегії протидії кібертероризму

ЗМІСТОВИЙ МОДУЛЬ 2

Тема 7. Інформаційна безпека України у сфері прав і свобод людини

1. Забезпечення захисту прав і свобод людини в інформаційній сфері
2. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина
3. Нормативно-правове забезпечення інформаційної безпеки України

Тема 8. Загрози людині та суспільству в інформаційній сфері

1. Кібергігієна та маніпулювання свідомістю
2. Реалізація маніпулятивного впливу з використанням інформаційних технологій
3. Вплив інформаційного середовища на психологічний стан особистості та мас

Тема 9. Поняття та зміст інформаційного супротиву

1. Форми інформаційної війни
2. Форми інформаційного супротиву
3. Інформація як зброя в інформаційній війні

ЗМІСТОВИЙ МОДУЛЬ 3

Тема 10. Забезпечення безпеки інформаційно-комунікаційних систем

1. Інформаційні атаки, методи їх виявлення та блокування
2. Актуальність, повнота та точність системи виявлення атак
3. Методи, засоби та технології кіберзахисту інформаційних систем
4. Основні моделі забезпечення безпеки інформаційного простору
5. Особливості реалізації комплексних систем захисту інформації

Тема 11. Організаційно-технічне забезпечення технічного захисту інформації

1. Основні організаційні та технічні заходи захисту інформації
2. Завдання та структура державної системи технічного захисту інформації
3. Контроль ефективності технічного захисту інформації

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								
Тема 1. Формування інформаційної безпеки держави	11	2	2	7	11	1	–	10
Тема 2. Загрози безпеці держави в інформаційній сфері	11	2	2	7	11	1	–	10
Тема 3. Методи оцінки та аналізу інформаційних ризиків	11	2	2	7	11	1	1	9
Тема 4. Оцінка рівня інформаційної безпеки за національними та міжнародними стандартами	11	2	2	7	11	1	–	10
Тема 5. Формування та реалізація інформаційної безпеки України	13	4	4	5	10	1	1	8
Тема 6. Протидія кібервійнам та кібертероризму	11	2	2	7	11	1	1	9
Разом за змістовий модуль 1	**68**	**34**	**34**	**40**	**65**	**6**	**3**	**56**
Змістовий модуль 2								
Тема 7. Інформаційна безпека України у сфері прав і свобод людини	10	2	2	6	11	1	–	10
Тема 8. Загрози людині та суспільству в інформаційній сфері	10	2	2	6	11	–	1	10
Тема 9. Поняття та зміст інформаційного супротиву	10	2	2	6	11	–	1	10
Разом за змістовий модуль 2	**30**	**6**	**6**	**18**	**33**	**1**	**2**	**30**
Змістовий модуль 3								
Тема 10. Забезпечення безпеки інформаційно-комунікаційних систем	11	2	2	7	11	1	–	10
Тема 11. Організаційно-технічне забезпечення технічного захисту інформації	11	2	2	7	11	–	1	10
Разом за змістовий модуль 3	**22**	**4**	**4**	**14**	**22**	**1**	**1**	**20**
ВСЬОГО	**120**	**24**	**24**	**72**	**120**	**8**	**6**	**106**

5. Теми практичних занять

№ з/п	Назва теми	К-ть годин	
		Д.ф.	З.ф.
1	Тема 1. Формування інформаційної безпеки держави	2	–
2	Тема 2. Загрози безпеці держави в інформаційній сфері	2	–
3	Тема 3. Методи оцінки та аналізу інформаційних ризиків	2	1
4	Тема 4. Оцінка рівня інформаційної безпеки за національними та міжнародними стандартами	2	–
5	Тема 5. Формування та реалізація інформаційної безпеки України	4	1
6	Тема 6. Протидія кібервійнам та кібертероризму	2	1
7	Тема 7. Інформаційна безпека України у сфері прав і свобод людини	2	10
8	Тема 8. Загрози людині та суспільству в інформаційній сфері	2	10
9	Тема 9. Поняття та зміст інформаційного супротиву	2	10
10	Тема 10. Забезпечення безпеки інформаційно-комунікаційних систем	2	10
11	Тема 11. Організаційно-технічне забезпечення технічного захисту інформації	2	10
РАЗОМ		**24**	**6**

6. Завдання для самостійної роботи

№ з/п	Назва теми	К-ть годин	
		Д.ф.	З.ф.
1	Тема 1. Формування інформаційної безпеки держави 2. Національне та міжнародне законодавство щодо забезпечення інформаційної безпеки держави	7	10
2	Тема 2. Загрози безпеці держави в інформаційній сфері 2. Інформаційні війни як джерело загрози національній безпеці	7	10
3	Тема 3. Методи оцінки та аналізу інформаційних ризиків 1. Класифікація ризиків інформаційної безпеки	7	9
4	Тема 4. Оцінка рівня інформаційної безпеки за національними та міжнародними стандартами 4. Нормативно-правове забезпечення захищеності інформаційних ресурсів	7	10
5	Тема 5. Формування та реалізація інформаційної безпеки України 5. Стан та перспективи розвитку інформаційної безпеки України 6. Інформаційна політика держави	5	8
6	Тема 6. Протидія кібервійнам та кібертероризму 2. Напрями та способи використання кіберпростору у терористичних цілях	7	9
7	Тема 7. Інформаційна безпека України у сфері прав і свобод людини 3. Нормативно-правове забезпечення інформаційної безпеки України	6	10
8	Тема 8. Загрози людині та суспільству в інформаційній сфері 2. Реалізація маніпулятивного впливу з використанням інформаційних технологій	6	10
9	Тема 9. Поняття та зміст інформаційного супротиву 3. Інформація як зброя в інформаційній війні	6	10
10	Тема 10. Забезпечення безпеки інформаційно-комунікаційних систем 1. Інформаційні атаки, методи їх виявлення та блокування	7	10
11	Тема 11. Організаційно-технічне забезпечення технічного захисту інформації 1. Основні організаційні та технічні заходи захисту інформації	7	10
Разом:		**72**	**106**

7. Індивідуальні завдання

Під час опанування блоку самостійної роботи студенти мають виконати індивідуальні науково-дослідні проекти у вигляді рефератів на такі теми:

1. Актуальні проблеми інформаційної безпеки в Україні і шляхи їх розв’язання
2. Інформація як предмет злочину: здійснити аналіз структури інформаційних ресурсів
3. Проблеми захисту персональних даних в Україні
4. Стан, тенденції та проблеми захисту інформації в інформаційних системах України
5. Інформаційна війна: суть, методи та засоби ведення, стан в Україні
6. Правові аспекти і законодавче забезпечення захисту інформації в Україні:
7. Класифікація загрози інформації і каналів витоку сучасних інформаційних систем і мереж:
8. Європейська конвенція з кіберзлочинів і завдання щодо забезпечення інформаційної безпеки в Україні
9. Характеристика основних видів національної безпеки України
10. Основи державної інформаційної політики у сфері захисту інформації

11. Інформаційні системи та технології як об’єкти інформаційної безпеки
12. Роль і місце інформаційної безпеки в загальній системі національної безпеки держави
13. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення
14. Інформаційні системи та технології як об’єкти інформаційної безпеки
15. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права
16. Інформаційна безпека в глобальній мережі Інтернет
17. Особливості розвитку глобальної мережі Інтернет в Україні й інформаційна безпека
18. Безпека інформації в комп’ютерних системах
19. Інформація як знаряддя вчинення злочину
20. Боротьба з комп’ютерними правопорушеннями: проблеми і шляхи їх розв’язання
21. Інформаційна боротьба, інформаційна війна й інформаційна зброя: підготовка, ведення і застосування
22. Психологічна війна: підготовка, ведення
23. Інформаційна війна як форма ведення інформаційного протиборства
24. Кіберзагрози для України в інформаційному просторі
25. Механізми запобігання і протидії кіберзлочинності США
26. Механізми запобігання і протидії кіберзлочинності ЄС
27. Загроза міжнародного інформаційного тероризму
28. Система суб’єктів національної системи кібербезпеки щодо протидії кібертероризму
29. Кібертероризм як елемент та глобальна зброя гібридної війни
30. Забезпечення кібербезпеки України від загроз кібертероризму

Результати науково-дослідного проекту перезентуються серед здобувачів вищої освіти

Оцінка за індивідуальний науково-дослідний проект є обов’язковим компонентом підсумкової оцінки з навчального курсу.

8. Методи навчання

Результат навчання	Методи навчання
1	2
ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки	Вербальні (лекція, пояснення); наочні (спостереження, ілюстрація, демонстрація); практичні (різні види вправ та завдань, практики); дискусійний метод; метод активного навчання (проведення ділових ігор, мозковий штурм, командна робота); ситуаційний метод
ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності	Вербальні (лекція, пояснення); наочні (спостереження, ілюстрація, демонстрація); практичні (різні види вправ та завдань, практики); дискусійний метод; метод активного навчання (проведення ділових ігор, мозковий штурм, командна робота); ситуаційний метод.

1	2
ПРН 3. Приймати обґрунтовані рішен-ня з питань забезпечення національної безпеки держави (за сферами забезпе-чення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог	Вербальні (лекція, пояснення); наочні (спостереження, ілюстрація, демонстрація); практичні (різні види вправ та завдань, практики); дискусійний метод; метод активного навчання (проведення ділових ігор, мозковий штурм, командна робота); ситуаційний метод.
ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища	Вербальні (лекція, пояснення); наочні (спостереження, ілюстрація, демонстрація); практичні (різні види вправ та завдань, практики); дискусійний метод; метод активного навчання (проведення ділових ігор, мозковий штурм, командна робота); ситуаційний метод.
ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки	Вербальні (лекція, пояснення); наочні (спостереження, ілюстрація, демонстрація); практичні (різні види вправ та завдань, практики); дискусійний метод; метод активного навчання (проведення ділових ігор, мозковий штурм, командна робота); ситуаційний метод.
ПРН 17. Виявляти та прогнозувати ризики національній безпеці України з урахуванням теорій терорології та іредентизму та обґрунтовувати заходи щодо їх мінімізації для забезпечення економічної безпеки держави	Вербальні (лекція, пояснення); наочні (спостереження, ілюстрація, демонстрація); практичні (різні види вправ та завдань, практики); дискусійний метод; метод активного навчання (проведення ділових ігор, мозковий штурм, командна робота); ситуаційний метод.

9. Методи контролю

В основу системи оцінювання навчальної дисципліни покладено поточний та модульний контроль результатів навчання і принцип накопичення зароблених здобувачем вищої освіти балів.

Поточний контроль – це оцінювання засвоєння здобувачем вищої освіти навчального матеріалу під час проведення аудиторних занять, при виконанні індивідуальної і самостійної роботи.

Контроль виконання індивідуальних завдань – демонстрація та захист індивідуального завдання.

Контроль виконання самостійної роботи студентами здійснюється на практичних заняттях дисципліни.

Модульний контроль – це оцінювання якості засвоєння навчального матеріалу змістових модулів.

Підсумковий (семестровий) контроль (екзамен):

1. Накопичення рейтингових балів в межах дисципліни проводиться в балах, які у підсумку переводяться у національну шкалу та шкалу ЄКТС.

2. Загальна кількість балів на останньому занятті з навчальної дисципліни оприлюднюється здобувачам вищої освіти та виставляється в відомість обліку успішності академічних груп.

3. У випадку погодження здобувача вищої освіти з оцінкою поточної успішності, вона вважається остаточною, враховується як результат семестрового контролю і вноситься у залікову книжку.

4. У разі незгоди здобувача вищої освіти з результатами поточної успішності, оцінка з дисципліни виставляється за результатами дистанційного складання екзамену. До тестування допускаються здобувачі, які отримали 50 і більше балів.

5. У разі, якщо студент отримав від 0 до 59 балів, то в відомість за національною шкалою виставляється оцінка «незадовільно» («F» та «FX» відповідно до шкали ЄКТС).

Способи перевірки досягнення програмних результатів навчання

В ході вивчення дисципліни досягнення програмних результатів навчання контролюється шляхом застосуванням наступних видів контролю:

Результат навчання	Методи контролю
1	2
ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки	Поточний контроль (оцінювання роботи під час аудиторних занять; усне опитування на заняттях, виконання практичних завдань; поточне тестування; самостійні роботи). Контроль виконання індивідуальних завдань. Контроль виконання самостійної роботи студентами. Модульний контроль (модульна контрольна робота). Підсумковий контроль (екзамен).
ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності	Поточний контроль (оцінювання роботи під час аудиторних занять; усне опитування на заняттях, виконання практичних завдань; поточне тестування; самостійні роботи). Контроль виконання індивідуальних завдань. Контроль виконання самостійної роботи студентами. Модульний контроль (модульна контрольна робота). Підсумковий контроль (екзамен).
ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог	Поточний контроль (оцінювання роботи під час аудиторних занять; усне опитування на заняттях, виконання практичних завдань; поточне тестування; самостійні роботи). Контроль виконання індивідуальних завдань. Контроль виконання самостійної роботи студентами. Модульний контроль (модульна контрольна робота). Підсумковий контроль (екзамен).
ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища	Поточний контроль (оцінювання роботи під час аудиторних занять; усне опитування на заняттях, виконання практичних завдань; поточне тестування; самостійні роботи). Контроль виконання індивідуальних завдань. Контроль виконання самостійної роботи студентами. Модульний контроль (модульна контрольна робота). Підсумковий контроль (екзамен).

1	2
ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки	Поточний контроль (оцінювання роботи під час аудиторних занять; усне опитування на заняттях, виконання практичних завдань; поточне тестування; самостійні роботи). Контроль виконання індивідуальних завдань. Контроль виконання самостійної роботи студентами. Модульний контроль (модульна контрольна робота). Підсумковий контроль (екзамен).
ПРН 17. Виявляти та прогнозувати ризики національній безпеці України з урахуванням теорій терорології та іредентизму та обґрунтовувати заходи щодо їх мінімізації для забезпечення економічної безпеки держави	Поточний контроль (оцінювання роботи під час аудиторних занять; усне опитування на заняттях, виконання практичних завдань; поточне тестування; самостійні роботи). Контроль виконання індивідуальних завдань. Контроль виконання самостійної роботи студентами. Модульний контроль (модульна контрольна робота). Підсумковий контроль (екзамен).

10. Розподіл балів

Оцінювання досягнень здобувачів за дисципліною за кількісним критерієм здійснюється за 100-бальною шкалою та шкалою ЄКТС (A, B, C, D, E, FX, F).
Бали розподілені за темами дисципліни наступним чином:

Критерії оцінювання														НДП	Сума
Змістовий модуль 1							Змістовий модуль 2				Змістовий модуль 3				
Т1	Т2	Т3	Т4	Т5	Т6	МКР	Т7	Т8	Т9	МКР	Т10	Т11	МКР	5	100
7	7	7	7	7	7	5	7	7	7	5	7	7	5		

Шкала оцінювання

За шкалою	Екзамен	Бали
A	Відмінно	90-100
B	Добре	82-89
C		74-81
D	Задовільно	64-73
E		60-63
FX	Незадовільно	35-59
F		0-34

11. Рекомендована література

Основна література

1. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / Під. ред. В.М. Богуша. К.: Видавництво Ліра-К, 2020. 554 с.

2. Буйницька О.П. Інформаційні технології та технічні засоби навчання. К.: Центр навчальної літератури. 2019. 240 с.

3. Бурячок В.Л., Киричок Р В., Складанний П.М. Основи інформаційної та кібернетичної безпеки / Навчальний посібник. К., 2018. 320 с.

4. Величко О.М., Гордієнко Т.Б. Інтелектуальні інформаційні системи: структура і застосування: підручник. К.: Олді+, 2022. 728 с.

5. Гуржій А. М., Возненко Л.І., Поворознюк Н.І., Самсонов В.В. Основи інформаційних технологій : навчальний посібник для здобувачів професійної (професійно-технічної) освіти. К.: Літера ЛТД, 2023. 288 с.

6. Дикий А.П. Формування інформаційно-комунікаційної системи запобігання та протидії економічній злочинності. Наукові перспективи. 2021. № 11 (17). С. 486–499.

7. Дикий А.П., Наумчук К.М., Тростенюк Т.М. Аналіз сучасних загроз інформаційній безпеці держави. Економічний простір: збірник наукових праць. 2021. №176. С. 155-158.

8. Дикий А. П. Інформаційно-комунікаційне забезпечення функціонування правоохоронної системи. Криза правоохоронної системи України : колективна монографія. Житомир : Бук-друк. 2023. 584 с. С. 496-577.

9. Дикий А. П. Державна політика запобігання та протидії економічній злочинності в системі гарантування економічної безпеки України : монографія. Житомир : Бук-Друк. 2023. 428 с.

10. Дикий А. П., Дика О. С., Наумчук К. М., Тростенюк Т. М. Понятійно-категоріальний апарат інформаційної безпеки України в забезпеченні національної безпеки. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2022. Вип. 4. С. 23–31. URL: https:// journals.ksauniv.ks.ua/index.php/public/issue/view/17.

11. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці держави. Економічний простір. 2021. № 176. С. 155–158. URL: http://www.prostir.pdaba.dp.ua/index.php/journal/article/view/1044.

12. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Особливості державного управління інформаційною безпекою в умовах воєнного стану. Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XXV Міжнародної науково-практичної конференції / за ред. І. В. Жукової, Є. О. Романенка. Рига (Латвія) : ВАДНД, 07 жовтня 2022 р. 487 с. С. 41–46. URL: http://perspectives.pp.ua/public/site/conferency/conf-25.pdf.

13. Дикий А.П. Формування інформаційно-комунікаційної системи запобігання та протидії економічній злочинності. Наукові перспективи. 2021. № 11 (17). С. 486–499. URL: http://perspectives.pp.ua/index.php/np/article/ view/3646/3666.

14. Dykyi A., Dyka O., Naumchuk K. Analysis of current threats to the information security of the state. Socioworld. Social research & behavioral sciences journal. 2021. Vol. 6. Is. 04 (02). PP. 130–138. URL: https://doi.org/ 10.5281/zenodo.5810442.

15. Ortynskyi , V., Pavlov, S., Pronina , O., Dykyi, A., & Kyrych, I. (2023). Achievements and prospects of digitization of public administration spheres in Ukraine: Logros y perspectivas de la digitalización de las esferas de la administración pública en Ucrania. Cuestiones Políticas, 41(79), 663-680. https://doi.org/10.46398/cuestpol.4179.44

16. Палеха Ю. І., Палеха О.Ю., Горбань Ю.І. Інформаційна культура: навч. посібн. / за заг. ред. проф. Палехи Ю.І. К.: Видавництво Ліра-К, 2020. 400 с.

17. Покотилова В.І., Фомішина В.М., Лугінін О.Є. Використання інформаційних технологій в теорії прийняття рішень. Навч. посіб. К.: Гельветика, 2019. 240 с.

18. Протидія фінансуванню тероризму в системі управління національною безпекою України: монографія / За загальною редакцією В.В. Євдокимова, Д.О. Грицишена. – Житомир: Видавничий дім "Бук-Друк", 2023. 232 с.

19. Ратушняк Т.В., Ніжегородцев В.О., Гладченко О.В. Інформаційні системи і технології: практикум : навчальний посібник. Ірпінь : Університет ДФС України, 2022. 180 с.

Додаткова література:

1. Інформаційні технології : навчальний посібник / О.І. Зачек, В.В. Сеник, Т.В. Магеровська та ін.; за ред. О.І. Зачека. Львів : Львівський державний університет внутрішніх справ, 2022. 432 с.

2. Кулешник Я. Ф., Магеровська Т. В., Зачек О. І. Застосування хмарних технологій в інформаційному забезпеченні діяльності Національної поліції: методичні вказівки. Львів : ЛьвДУВС, 2021. 64 с.

3. Сеник В.В. Основи технологій захисту інформації в комп'ютерних системах : навчально-методичний посібник / В.В. Сеник, Т.В. Рудий, С.В. Сеник, Т.В. Магеровська. Львів : ЛьвДУВС. 2019. 192 с.

4. Теоретико-методологічні засади інформатизації освіти та практична реалізація інформаційно-комунікаційних технологій в освітній сфері України : монографія / наук. ред. В. Ю. Биков, С. Г. Литвинова, В. І. Луговий. К.: ЦП Компринт, 2019. 214 с.

Нормативна база

1. Конституція України від 28.06.2006 р. (із змінами).

2. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV

3. Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг: Постанова Кабінету Міністрів України від 07.11.2018 р. № 992.

4. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ МВС України від 03.08.2017 р. № 676.

5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР (із змінами).

6. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII.

7. Про Концепцію Національної програми інформатизації. Закон України; Концепція від 04.02.1998 № 75/98-ВР

8. Про національну безпеку України. Закон України від 21.06.2018 № 2469-VIII

9. Про Раду національної безпеки і оборони України. Закон України від 05.03.1998 № 183/98-ВР

10. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України". Указ Президента України; Стратегія від 14.09.2020 № 392/2020

11. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року. Розпорядження Кабінету Міністрів України; Стратегія від 10.07.2019 № 526-р

12. Інформаційні ресурси

http://www.niss.gov.ua/
https://cyberpolice.gov.ua/
https://cip.gov-ua/ua
https://cert.gov.ua/
https://ssu.gov.ua/

Рекомендовані курси

Prometheus. Безпека в інтернеті під час війни: практичний курс. URL: https://prometheus.org.ua/course/course-v1:MINZMIN+ISWT101+2023_T2

Prometheus. Цифрова безпека на персональному рівні. URL: https://prometheus.org.ua/course/course-v1:Prometheus+DSPL101+2023_T1

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

Дія.Освіта. Персональна кібергігієна. URL: https://osvita.diia.gov.ua/simulators/personal-cyberhygiene-simulator

Дія.Освіта. Дата аналітик. SQL та Power BI. URL: https://osvita.diia.gov.ua/simulators/data-analyst-sql-and-power-bi-simulator