МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ЦІДРОЗДІЛ «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»
Циклова комісія *програмування та інформаційних дисциплін*

ЗАТВЕРДЖУЮ
Заступник директора з навчальної роботи
29 серпня 2025 р.
Людмила БАЛДИЧ

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Системи моніторингу загроз та атак

освітньо-професійна програма — *Кібербезпека та захист інформацій*
(назва освітньо-професійної програми)

галузь знань — *12 Інформаційні технології*
(шифр і назва напряму підготовки)

спеціальність — *125 Кібербезпека та захист інформацій*
(шифр і назва спеціальності)

відділення — *Інформаційних технологій*
(назва відділення)

Рівне – 2025 рік

Програму навчальної дисципліни *Системи моніторингу загроз та атак* розроблено на основі освітньо-професійної програми «Кібербезпека та захист інформацій » для здобувачів освіти освітньо-професійного ступеня «Фаховий молодший бакалавр» галузі знань *12 Інформаційні технології*, спеціальності *125 Кібербезпека та захист інформацій*, затвердженої Вченою радою НУБіП України від 26.04.2023 №10

Розробник: Черняк Вадим Андрійович, викладач програмування та інформаційних дисциплін, спеціаліст.

Програма навчальної дисципліни затверджена на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від *29 серпня* 2025 року № *1*

Голова циклової комісії *програмування та інформаційних дисциплін*

29 серпня 2025 року _____ *Павло СТРИК*
(підпис) (ім'я та прізвище)

Погоджено методичною радою ВСП «РФК НУБіП України»

Протокол від *29 серпня* 2025 року № *1*

29 серпня 2025 року Голова _____ *Людмила БАЛДИЧ*
(підпис) (ім'я та прізвище)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань, напрям підготовки, спеціальність, освітньо-професійний ступінь		
Освітньо-професійний ступінь	Фаховий молодший бакалавр	
Галузь знань	12 Інформаційні технології	
Спеціальність	125 Кібербезпека та захист інформацій	
Характеристика навчальної дисципліни		
Вид	вибіркова	
Загальна кількість годин	90	
Кількість кредитів ECTS	3	
Кількість змістових модулів	2	
Мова викладання, навчання та оцінювання	українська	
Форма контролю	залік	
Показники навчальної дисципліни для денної та заочної форм навчання		
Форма навчання	денна	
Рік підготовки, навчальний рік	IV, 2025-2026	
Семестр	8	
Аудиторні години:	44	
лекційні	14	
практичні	30	
семінарські	-	
Самостійна робота	46	
Кількість тижневих годин для денної форми навчання	2,5	

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Системи моніторингу загроз та атак»** є формування у здобувачів освіти знань, умінь і практичних навичок щодо організації, налаштування, експлуатації та вдосконалення систем моніторингу безпеки, спрямованих на виявлення, аналіз і реагування на загрози та кібератаки в інформаційно-телекомунікаційних системах.

У процесі навчання студенти повинні оволодіти сучасними підходами, методами та інструментами моніторингу подій інформаційної безпеки, засобами збору, оброблення й аналізу даних про інциденти, а також навчитись приймати рішення щодо запобігання, виявлення та усунення наслідків кібератак.

Основними завданнями вивчення дисципліни є формування у здобувачів освіти знань і практичних компетентностей щодо:

- розуміння принципів побудови та функціонування систем моніторингу загроз та атак у сфері інформаційної та кібербезпеки;
- знання нормативно-правової бази України, міжнародних стандартів і регламентів, що регулюють діяльність із моніторингу, виявлення та реагування на інциденти безпеки;
- застосування методів аналізу інформаційних потоків, виявлення аномальної активності, оцінювання рівня загроз та уразливостей інформаційних систем;
- використання програмних та програмно-апаратних засобів моніторингу, зокрема SIEM-систем, IDS/IPS, аналізаторів мережевого трафіку;
- здійснення збору, оброблення та інтерпретації інформації про події безпеки для ухвалення управлінських рішень у сфері інформаційної та кібербезпеки;
- формування навичок реагування на інциденти, забезпечення неперервності функціонування інформаційних систем та відновлення їх після реалізації загроз чи атак;
- використання сучасних методів ризик-аналізу та забезпечення безперервного удосконалення процесів моніторингу загроз відповідно до політики інформаційної безпеки організації.

Згідно з вимогами освітньо-професійної програми студенти повинні:

Знати:

- види загроз інформації в комп’ютерних системах та мережах;
- основні протоколи безпеки;
- принципи функціонування систем захисту;
- основні програмні і апаратні засоби захисту інформації в комп’ютерних системах
та мережах;
- засоби організації розмежування доступу комп’ютерних мережах.

Вміти:

- виконати аналіз безпеки комп'ютерної системи або мережі та усунути можливі
шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконати адміністрування прав доступу до комп´ютерної системи та мережі з метою перешкоди призначення невиправданих привілеїв;
- перевірити надійність захисту інформації та стійкості його
щодо хакерських атак шляхом моделювання загроз;
- підібрати тип та структуру локальної комп’ютерної мережі;
- підібрати комплекс необхідних апаратно-програмних засобів для захисту комп’ютерної системи та мережі.

Очікувані результати навчання.

Після вивчення дисципліни «Системи моніторингу загроз та атак» у здобувачів освіти формуються такі **компетентності:**

Загальні:

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК05. Здатність здійснювати пошук, оброблення та аналіз інформації з різних джерел для прийняття професійних рішень.

Фахові:

ФК02. Здатність використовувати інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки.

ФК08. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

ФК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно зі встановленої політики інформаційної та/або кібербезпеки.

Програмні результати навчання.

ПР02. Знати національні та міжнародні стандарти, регулюючі акти виявлення, ідентифікації, аналізу та реагування на інциденти в сфері інформаційної безпеки та/або кібербезпеки.

ПР11. Вміти забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнівних програмних впливів та кібератак.

ПР18. Знати системи виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

ПР19. Вміти підтримувати працездатність із використанням інструментарію для моніторингу процесів в інформаційно-телекомунікаційних системах.

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. Моніторинг мережевої безпеки

Тема 1. Основні поняття та призначення моніторингу. Рівні та складові систем моніторингу.

Поняття моніторингу, його роль у виявленні загроз. Основні елементи системи моніторингу та їх взаємодія.

Створення систем спостереження за станом комп'ютерної мережі чи пристроїв. Приклади практичних схем моніторингу.

Тема 2. Моніторинг у різних сферах діяльності. Види систем моніторингу.

Застосування моніторингу в енергетиці, транспорті, сільському господарстві, IT. Основні типи систем моніторингу.

Тема 3. Завдання та принципи організації моніторингу.

Головні функції систем моніторингу. Основні етапи побудови та організації роботи моніторингової системи.

Тема 4. Датчики як основне джерело інформації для моніторингу.

Призначення датчиків, види сигналів, способи передачі даних у системи моніторингу.

Принципи дії найпоширеніших датчиків. Приклади використання у системах контролю стану обладнання чи безпеки.

Змістовий модуль 2. Практичне застосування систем моніторингу загроз та атак

Тема 5. Організація системи моніторингу загроз та атак на підприємстві.

Виявлення загрози і спроби атак. Основні кроки створення простої системи кібермоніторингу.

Приклади систем моніторингу для захисту технологічних процесів і даних підприємств АПК.

Тема 6. Системи моніторингу мереж і виявлення атак. Популярні програми для моніторингу.

Основи роботи з системами IDS, сканерами мереж та SIEM-програмами (HP Operations Manager, ManageEngine, SolarWinds, WhatsUp Gold тощо).

Тема 7. Кібергігієна — основа безпечної роботи в інформаційному середовищі.

Прості правила захисту від кіберзагроз. Користування паролями, антивірусами, оновленнями.

Тема 8. Системи виявлення вторгнень (IDS): призначення і принципи роботи.

Як працюють IDS-системи, які типи вторгнень вони фіксують, приклади програмних рішень.

Як IPS-системи блокують загрози в реальному часі. Відмінність між IDS і IPS, практичне використання.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Назви змістових модулів і тем	Кількість годин			
		денна форма			
		всього	лекційні	практичні	самостійне вивчення
Змістовий модуль 1 Моніторинг мережевої безпеки					
Тема 1	Вступ. Основні поняття та призначення моніторингу. Рівні та складові систем моніторингу	10	2	2	6
Тема 2	Моніторинг у різних сферах діяльності. Види систем моніторингу	12	2	4	6
Тема 3	Завдання та принципи організації моніторингу.	10	-	4	6
Тема 4	Датчики як основне джерело інформації для моніторингу	12	2	4	6
Разом за змістовим модулем 1		**44**	**6**	**14**	**24**
Змістовий модуль 2. . Практичне застосування систем моніторингу загроз та атак					
Тема 5	Організація системи моніторингу загроз та атак на підприємстві	12	2	4	6
Тема 6	Системи моніторингу мереж і виявлення атак. Популярні програми для моніторингу	10	2	4	4
Тема 7	Кібергігієна — основа безпечної роботи в інформаційному середовищі	12	2	4	6
Тема 8	Системи виявлення вторгнень (IDS): призначення і принципи роботи	12	2	4	6
Разом за змістовим модулем 2		**46**	**8**	**16**	**22**
Всього годин		**90**	**14**	**30**	**46**

5. ТЕМИ ЛЕКЦІЙНИХ, ПРАКТИЧНИХ ЗАНЯТЬ ТА ЗМІСТ САМОСТІЙНОГО ВИВЧЕННЯ

№ теми	№ занят-тя	Вид навчальної діяльності	Назва теми	Кількість годин
IIIV семестр				**90** 34/10/76
Змістовий модуль 1. . Моніторинг мережевої безпеки				**44**
1	***Вступ. Основні поняття та призначення моніторингу. Рівні та складові систем моніторингу***			**10**
	1	лекція 1	Поняття моніторингу, його роль у виявленні загроз. Основні елементи системи моніторингу та їх взаємодія	2
		самостійне вивчення	Створення систем спостереження за станом комп'ютерної мережі чи пристроїв. Приклади практичних схем моніторингу	6
	2	Практична робота 1	Розробка та налаштування системи моніторингу мережевого середовища для виявлення інцидентів безпеки	2
2	***Моніторинг у різних сферах діяльності. Види систем моніторингу***			**12**
	3	лекція 2	Застосування моніторингу в енергетиці, транспорті, сільському господарстві, ІТ	2
		самостійне вивчення	Основні типи систем моніторингу	6
	4	Практична робота 2	Моніторинг, його види та основні напрямки застосування у різних сферах діяльності (енергетиці, транспорті, сільському господарстві, ІТ)	2
	5	Практична робота 3	Складові елементи та принципи функціонування систем моніторингу	2
3	***Завдання та принципи організації моніторингу***			**10**
		самостійне вивчення	Головні функції систем моніторингу.	2
	6	практична робота 4	Порядок реєстрації авторського права на комп'ютерну програму. Підготовка та заповнення основних документів для подання заявки.	2
		самостійне вивчення	Основні етапи побудови та організації роботи моніторингової системи	4
	7	Практична робота 5	Особливості вільного використання програм у навчальних, наукових і службових цілях.	2
4	***Датчики як основне джерело інформації для моніторингу***			**12**
	8	лекція 3	Призначення датчиків, види сигналів, способи передачі даних у системи моніторингу	2
		самостійне вивчення	Принципи дії найпоширеніших датчиків.	2
	9	практична робота6	Датчики як основне джерело інформації для моніторингу	2
		самостійне вивчення	Приклади використання у системах контролю стану обладнання чи безпеки	4
	10	практична робота 7	Призначення датчиків, види сигналів, способи передачі даних у системи моніторингу	2

№ теми	№ занят-тя	Вид навчальної діяльності	Назва теми	Кількість годин
Змістовий модуль 2. Практичне застосування систем моніторингу загроз та атак				**46**
5	***Організація системи моніторингу загроз та атак на підприємстві***			**12**
	11	лекція 4	Виявлення загрози і спроби атак. Основні кроки створення простої системи кібермоніторингу	2
		самостійне вивчення	Приклади систем моніторингу для захисту технологічних процесів і даних підприємств АПК	6
	12	практична робота 8	Організація системи моніторингу загроз та атак на підприємстві. Виявлення загрози і спроби атак	2
	13	практична робота 9	Основні кроки створення простої системи кібермоніторингу. Приклади систем моніторингу для захисту технологічних процесів і даних підприємств АПК	2
6	***Системи моніторингу мереж і виявлення атак. Популярні програми для моніторингу***			**10**
	14	лекція 5	Основи роботи з системами IDS, сканерами мереж	2
		самостійне вивчення	SIEM-програмами (HP Operations Manager, ManageEngine, SolarWinds, WhatsUp Gold)	4
	15	практична робота10	Принципи побудови систем моніторингу мереж, способами виявлення атак та інструментами для аналізу мережевої активності	2
	16	практична робота11	Принципи функціонування систем IDS, SIEM та мережевих сканерів визначення їх призначення, роль у виявленні атак і зборі даних про інциденти інформаційної безпеки	2
7	***Кібергігієна — основа безпечної роботи в інформаційному середовищі***			**12**
	17	лекція 6	Прості правила захисту від кіберзагроз.	2
		самостійне вивчення	Користування паролями, антивірусами, оновленнями	6
	18	практична робота 12	Кібергігієна — основа безпечної роботи в інформаційному середовищі	2
	19	практична робота 13	Ефективні способи захисту персональних даних та пристроїв, правила користуватися паролями, антивірусами й системними оновленнями для запобігання кіберзагрозам	2
8	***Системи виявлення вторгнень (IDS): призначення і принципи роботи***			**12**
	20	Лекція 7	Як працюють IDS-системи, які типи вторгнень вони фіксують, приклади програмних рішень	2
		самостійне вивчення	Як IPS-системи блокують загрози в реальному часі. Відмінність між IDS і IPS, практичне використання	6
	21	практична робота 14	Системи виявлення вторгнень (IDS): призначення, принципи роботи та типи вторгнень	2
	22	практична робота 15	Системи запобігання вторгненням (IPS): робота в реальному часі. Відмінності між IDS і IPS	2
			Всього	**90**

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуально-консультативна робота виконується за графіком у таких формах: індивідуальні заняття, консультації, перевірка виконання курсової роботи та індивідуальних завдань і захист результатів їх виконання тощо.

Формами організації індивідуально-консультативної роботи є:

а) консультації з теоретичного матеріалу:

- інтерактивне спілкування (питання-відповідь);
- групові (розгляд типових завдань);
- диспути (обговорення вирішення типових питань);

б) індивідуальні та групові консультації з освоєння практичного матеріалу;

в) індивідуальна здача та захист виконаних курсових робіт для комплексної оцінки ступеня оволодіння програмним матеріалом.

7. ПЕРЕЛІК ПИТАНЬ НА ЗАЛІК

1. Предмет і завдання навчальної дисципліни «Системи моніторингу загроз та атак».
2. Поняття ліцензування у сфері інформаційної безпеки.
3. Поняття сертифікації у сфері інформаційної безпеки.
4. Мета і завдання ліцензування засобів захисту інформації.
5. Основні етапи процесу ліцензування програмного забезпечення.
6. Законодавча база України у сфері ліцензування діяльності з технічного захисту інформації.
7. Роль Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ) у сфері ліцензування.
8. Види ліцензій на програмні продукти.
9. Поняття авторського права на програмне забезпечення.
10. Майнові та немайнові права автора програмного продукту.
11. Види авторських договорів у сфері розроблення програмного забезпечення.
12. Умови передачі майнових прав на програмне забезпечення.
13. Поняття легального та неліцензованого програмного забезпечення.
14. Ознаки, що визначають ліцензійне програмне забезпечення.
15. Програми ліцензування і засоби перевірки легальності використання ПЗ.
16. Поняття і роль сертифікації у забезпеченні інформаційної безпеки.
17. Основні етапи проведення сертифікації засобів захисту інформації.
18. Види сертифікації в Україні.
19. Суб’єкти процесу сертифікації та їх повноваження.
20. Нормативна база України щодо сертифікації засобів захисту інформації.
21. Технічні регламенти та їх роль у сертифікації інформаційних систем.
22. Поняття «сертифікат відповідності» та «декларація про відповідність».
23. Вимоги до документації, що подається на сертифікацію.
24. Порядок оформлення сертифіката відповідності.

25. Права та обов’язки заявника при проведенні сертифікації.
26. Відмінності між обов’язковою та добровільною сертифікацією.
27. Особливості сертифікації засобів технічного захисту інформації.
28. Поняття технічних каналів витоку інформації.
29. Сертифікація засобів криптографічного захисту інформації.
30. Порядок проведення експертизи засобів криптографічного захисту.
31. Особливості сертифікації програмних засобів захисту інформації.
32. Вимоги до програмних засобів захисту при сертифікації.
33. Роль акредитованих лабораторій у процесі сертифікації.
34. Структура сертифікаційного випробування.
35. Поняття «експертний висновок» у процесі сертифікації.
36. Контроль за дотриманням вимог після отримання сертифіката відповідності.
37. Підстави для анулювання сертифіката відповідності.
38. Взаємозв’язок між ліцензуванням і сертифікацією засобів захисту інформації.
39. Роль стандартів ДСТУ та ISO/IEC у сертифікації засобів захисту інформації.
40. Міжнародна система сертифікації Common Criteria (ISO/IEC 15408).
41. Поняття рівня довіри до засобів захисту інформації (EAL).
42. Міжнародна практика сертифікації програмного забезпечення.
43. Відповідальність за порушення законодавства у сфері ліцензування і сертифікації.
44. Захист авторських прав на програмні продукти в Україні.
45. Відмінність між відкритими та закритими моделями програмного забезпечення (Open Source, Freeware, Shareware).
46. Сутність концепції відкритого коду (Open Source License).
47. Особливості використання вільного програмного забезпечення у сфері інформаційної безпеки.
48. Етапи життєвого циклу програмного забезпечення та його якість.
49. Вимоги до забезпечення якості програмних засобів протягом життєвого циклу.
50. Значення ліцензування і сертифікації у побудові комплексної системи захисту інформації.

8. МЕТОДИ НАВЧАННЯ

У процесі вивчення дисципліни «Системи моніторингу загроз та атак» використовуються різноманітні методи навчання, серед яких: пояснення та розповідь викладача, евристична бесіда, проблемно-орієнтовані лекції, демонстрація та ілюстрація матеріалу, навчальні дискусії й диспути, проведення мозкових штурмів, робота студентів у малих групах, застосування кейс-методу, самостійне виконання практичних завдань, розв’язування ситуаційних задач і виконання тренувальних вправ.

9. КОНТРОЛЬ РЕЗУЛЬТАТІВ НАВЧАННЯ

9.1. Форми та засоби поточного і підсумкового контролю

Контроль знань студентів здійснюється за модульно-рейтинговою системою.

Засобами діагностики та методами демонстрування результатів навчання здобувачів освіти з дисципліни є:

- індивідуальне опитування, фронтальне опитування;
- модульні контрольні робот у формі тестування;
- презентація дослідження за темою курсової роботи;
- звіти з виконання практичних робіт;
- комплексна контрольна робота;
- залік
- екзамен.

Зміст курсу дисципліни «Системи моніторингу загроз та атак» поділений на 2 змістових модулів. Кожний модуль включає в себе лекції, практичні заняття та самостійну роботу студентів і завершуються рейтинговим контролем рівня засвоєння знань програмного матеріалу відповідної частини курсу.

У змістовий модуль 1 (ЗМ1) входять теми 1-4, у змістовий модуль 2 (ЗМ2) – теми 5-8.

Після завершення відповідно змістового модуля проводяться ***модульні контрольні роботи*** **(МК)**. До модульної контрольної роботи допускаються студенти, які опрацювали весь обсяг теоретичного матеріалу в т. ч і матеріал самостійно, виконали практичні (практичні, графічні, розрахункові) роботи, відпрацювали семінарські заняття.

Рейтингову кількість балів студента формують бали, отримані за модульні контрольні роботи, які проводяться у формі тестування, та середній рейтинг виконання практичних (практичні, графічні, розрахункові) робіт і відпрацювання семінарських занять.

Участь студентів в контрольних заходах обов'язкова. МК проводиться у письмовій тестовій формі, тестові завдання обов’язково включають матеріал, який передбачено до самостійного опрацювання студентами. Студент, який не виконав вимоги щодо самостійної роботи чи будь якого іншого виду навчальної діяльності, не допускається до складання МК і даний модуль йому не зараховується.

Семестрові бали (семестровий рейтинг) студент отримує як середнє арифметичне балів змістових модулів з усіх тем п’ятьох змістових модулів:

Оцінка навчальної успішності студентів здійснюється під час семестрового оцінювання у формі екзамену, який передбачає виконання тестових завдань та вирішення практичного завдання.

9.2. Критерії оцінювання результатів начиння

Критерії оцінювання модульної контрольної роботи, директорської контрольної роботи, усних і письмових відповідей на питання, виконання практичних занять доповідей на семінарських заняттях, (виконання курсових робіт) – від 0 до 50 балів:

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – **48-50 балів**;
- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів**;
- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів**;
- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів**;
- питання розкрите фрагментарно, наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів**;
- відповідь неповна, наявні суттєві помилки при викладі та проведенні розрахунків **– 30-33 балів**;
- відповідь має значні помилки елементарного рівня – **1-30 бали**;
- відсутність відповіді на питання – **0 балів**.

Оцінювання за формами контролю

Шкала оцінювання

	Заліковий модуль 1	**Заліковий модуль 2**	**Разом**
%	50	50	100
Мінімум	0	0	0
Максимум	50	50	50

Відсоток формування компетентностей та набуття програмних результатів навчання	**Рейтинг за п'ятдесятибальною шкалою**	**Оцінка за п'ятибальною шкалою**	**Запис у заліковій книжці студента та відомості**
96-100	48, 49, 50	5	відмінно
90-95	45, 46, 47	5	відмінно
84-89	42, 43, 44	4	добре
75-83	38, 39, 40, 41	4	добре
67-74	34, 35, 36, 37	3	задовільно
60-66	30, 31, 32, 33	3	задовільно
менше 60	0-29	2	незадовільно

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. Витяг з навчального плану
2. Програма навчальної дисципліни
3. Плани занять

4. Конспект лекцій з дисципліни
5. Питання до модульних контрольних робіт
6. Питання до заліку
7. Залікові білети
8. Навчальний посібник
9. Роздавальний матеріал
10. Презентації до тем

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. **Гнатюк С. О.** Кібербезпека та захист інформації: навч. посібник. – Київ: НАУ, 2020. – 368 с.
2. **Клименко В. О., Сєдін В. І., Шелест А. С.** Основи кібербезпеки: навч. посібник. – Харків: ХНУРЕ, 2019. – 256 с.
3. **Гайда М. І., Короленко В. В.** Інформаційна безпека: концепції, технології, управління ризиками: навч. посібник. – Львів: ЛНУ ім. І. Франка, 2021. – 312 с.
4. **Пархоменко О. М., Літвінов С. В.** Системи моніторингу інформаційної безпеки: навч. посібник. – Київ: КНУ ім. Т. Шевченка, 2020. – 228 с.
5. **Костюк В. І., Мельник О. С.** Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посібник. – Київ: НАУ, 2018. – 294 с.
6. **Рибальченко О. В.** Системи виявлення та запобігання вторгненням: навч. посібник. – Харків: ХНУРЕ, 2020. – 210 с.
7. **Ахрамович В. М., Чегренець В. М., Котенко А. М.** Ліцензування, атестація та сертифікація у сфері безпеки об’єктів інформаційної діяльності: навч. посібник. – Київ: ДУТ, 2018. – 412 с.
8. **Козловський І. М., Руденко С. В.** Кіберзагрози та системи їх моніторингу: навч. посібник. – Львів: ЛДУ БЖД, 2021. – 198 с.
9. **Литвиненко І. М., Дубовий Ю. С.** Моніторинг інформаційних систем: методи, засоби, технології: навч. посібник. – Київ: КПІ ім. Ігоря Сікорського, 2019. – 276 с.
10. **Городиський В. І.** Управління інцидентами інформаційної безпеки: навч. посібник. – Київ: НАУ, 2022. – 254 с.