МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ «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

Управління доступом в інформаційно телекомунікаційних системах

(назва навчальної дисципліни)

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

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

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

відділення *Інформаційних технологій*
(назва відділення)

Рівне – 2025 рік

Програму навчальної дисципліни *Управління доступом в інформаційно телекомунікаційних системах* розроблено на основі освітньо-професійної програми «Кібербезпека та захист інформації», спеціальності 125 Кібербезпека та захист інформації, галузі знань 12 Інформаційні технології, *затвердженої Вченою радою НУБіП України 26 квітня 2023 року, протокол № 10.*

Розробники: *Надозірний Святослав Вікторович, викладач програмування та інформаційних дисциплін.*

Програму навчальної дисципліни розглянуто і схвалено 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) (ініціали 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)

Святослав Надозірний, 2025

ВСП «РФК НУБіП України, 2025

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань, напрям підготовки, спеціальність, ступінь вищої освіти	
Ступінь вищої освіти	Фаховий молодший бакалавр
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Характеристика навчальної дисципліни	
Вид	обов’язкова
Загальна кількість годин	150
Кількість кредитів ECTS	5
Кількість змістових модулів	4
Мова викладання, навчання та оцінювання	українська
Курсовий проект (робота)	
Форма контролю	Іспит
Показники навчальної дисципліни для денної форм навчання	
Форма навчання	денна
Рік підготовки	2025-2026
Семестр	5
Аудиторні години:	96
Лекційні	36
Практичні	60
Самостійна робота	54
Кількість тижневих годин для денної форми навчання	6

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета дисципліни "Управління доступом в інформаційно телекомунікаційних системах" є формування у студентів комплексного розуміння принципів і методів забезпечення інформаційної безпеки, розвиток навичок аналізу ризиків, розробки і впровадження ефективних заходів захисту інформаційних систем в умовах сучасного цифрового середовища.

Основними **завданнями** вивчення дисципліни «*Управління доступом в інформаційно телекомунікаційних системах*» є Надати студентам знання про основні принципи, механізми та моделі управління доступом. Навчити проектувати та впроваджувати системи автентифікації та авторизації. Сформувати розуміння різних методів автентифікації та їх застосування. Ознайомити з принципами побудови та налаштування систем контролю доступу. Розвинути практичні навички адміністрування та аудиту систем управління доступом.

Як результат вивчення навчальної дисципліни здобувачі освіти повинні знати:

- Основні поняття та принципи управління доступом в ІТС
- Моделі контролю доступу (DAC, MAC, RBAC)
- Методи та механізми автентифікації користувачів
- Принципи роботи систем одноразової та багатофакторної автентифікації
- Протоколи мережевої автентифікації
- Механізми авторизації та розмежування доступу
- Методи захисту бездротових мереж
- Принципи побудови PKI та управління цифровими сертифікатами
- Стандарти та нормативні вимоги щодо управління доступом

Вміти:

- Проектувати системи управління доступом відповідно до вимог безпеки
- Налаштовувати різні механізми автентифікації користувачів
- Впроваджувати політики паролів та управляти обліковими записами
- Реалізовувати моделі контролю доступу в різних системах
- Налаштовувати та адмініструвати RBAC-системи
- Забезпечувати безпеку віддаленого та бездротового доступу
- Проводити аудит систем управління доступом
- Працювати з цифровими сертифікатами та PKI
- Впроваджувати багатофакторну автентифікацію

Очікувані результати навчання.

Після вивчення дисципліни «*Управління доступом в інформаційно телекомунікаційних системах*» у здобувачів освіти формуються такі компетентності:

Фахові:

ФК 08. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

ФК 09. Здатність здійснювати професійну діяльність та впроваджувати системи управління інформаційною та/або кібербезпекою.

ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно зі встановленої політики інформаційної та/або кібербезпеки.

Програмні результати навчання.

Після вивчення дисципліни «*Управління доступом в інформаційно телекомунікаційних системах*» здобувачів освіти повинні:

ПР 18. Знати системи виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

ПР 19. Вміти підтримувати працездатність з використанням інструментарію для моніторингу процесів в інформаційно-телекомунікаційних системах.

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. Основи управління доступом

Тема 1. Основи захисту інформації.

Поняття та задачі управління доступом. Місце управління доступом в загальній системі захисту інформації. Базові терміни та визначення: суб'єкт, об'єкт, право доступу. Структура та компоненти системи управління доступом. Основні загрози безпеці доступу.

Тема 2. Теоретичні основи управління доступом

Формальні моделі розмежування доступу. Матриця доступу та її представлення. Монітор безпеки та його функції. Основні принципи автентифікації та авторизації. Політики та процедури управління доступом.

Змістовий модуль 2. Механізми автентифікації

Тема 3. Базові механізми автентифікації.

Парольні системи та їх характеристики. Методи зберігання та передачі паролів. Політики управління паролями. Токени та смарт-карти. Інфраструктура відкритих ключів (PKI). Цифрові сертифікати та їх життєвий цикл.

Тема 4. Сучасні методи автентифікації.

Біометричні методи автентифікації. Характеристики біометричних систем. Двофакторна автентифікація. Багатофакторна автентифікація. Стандарти та протоколи автентифікації. Безпека та надійність різних методів автентифікації.

Змістовий модуль 3. Авторизація та контроль доступу

Тема 5. Класичні моделі контролю доступу.

Дискреційне управління доступом (DAC). Списки контролю доступу (ACL). Мандатне управління доступом (MAC). Рівні безпеки та мітки доступу. Реалізація моделей в сучасних ОС. Переваги та недоліки різних моделей.

Тема 6. Рольове управління.

Концепція рольового управління доступом. Ієрархія ролей та наслідування прав. Статичне та динамічне призначення ролей. Адміністрування RBAC-систем. Типові сценарії застосування RBAC.

Змістовий модуль 4. Безпека мережевого доступу

Тема 7. Протоколи та сервіси мережевого доступу.

Протокол Kerberos. Служба каталогів LDAP. Active Directory та групові політики. Протоколи OAuth та OpenID Connect. VPN-технології та їх реалізація. Безпека віддаленого доступу.

Тема 8. Безпека бездротових мереж.

Стандарти безпеки Wi-Fi мереж. Методи автентифікації в Wi-Fi. Протокол WPA3 та його особливості. Типові атаки на бездротові мережі. Методи захисту та моніторингу Wi-Fi мереж.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин			
	денна форма			
	усього	у тому числі		
		лекції	практ.	с.р.
1	2	3	4	5
Змістовий модуль 1. Основи управління доступом				
Тема 1. Основи захисту інформації	20	4	10	6
Тема 2. Теоретичні основи управління доступом.	17	4	6	7
Разом за змістовим модулем 1	37	8	16	13
Змістовий модуль 2. Механізми автентифікації.				
Тема 3. Базові механізми автентифікації.	21	6	8	7
Тема 4. Сучасні методи автентифікації .	17	4	6	7
Разом за змістовим модулем 2	38	10	14	14
Змістовий модуль 3. Управління інформаційною безпекою.				
Тема 5. Класичні моделі контролю доступу.	23	6	10	7
Тема 6. Рольове управління.	17	4	6	7
Разом за змістовим модулем 3	40	10	16	14
Змістовий модуль 4. Безпека мережевого доступу.				
Тема 7. Протоколи та сервіси мережевого доступу.	23	6	10	7
Тема 8. Безпека бездротових мереж.	12	2	4	6
Разом за змістовим модулем 4	35	8	14	13
Всього годин	120	36	50	24
Підготовка до екзамену	30			
Всього годин	150			

5. ТЕМИ ЛЕКЦІЙНИХ, ПРАКТИЧНИХ ЗАНЯТЬ ТА ЗМІСТ САМОСТІЙНОГО ВИВЧЕННЯ

№ теми	№ заняття	Вид навчальної діяльності	Назва теми	Кількість годин
Змістовий модуль 1. Основи управління доступом				**37**
1.	**Тема 1. Основи захисту інформації**			**20**
	1	Лекція 1	Вступ до управління доступом, базові поняття та термінологія	2
	2	Лекція 2	Компоненти систем управління доступом та загрози безпеці	2
		Самостійна робота	Ознайомлення з компонентами в розрізі існуючих вразливостей	6
	3	Практична робота 1	Аналіз вразливостей системи управління доступом	2
	4	Практична робота 2	Оцінка ризиків безпеки доступу	2
	5	Практична робота 3	Розробка політики управління доступом	2
	6	Практична робота 4	Документування механізмів контролю доступу	2
	7	Практична робота 5	Планування системи управління доступом	2
2	**Тема 2. Теоретичні основи управління доступом**			**17**
	8	Лекція 3	Формальні моделі та матриця доступу	2
	9	Лекція 4	Принципи автентифікації та авторизації	2
		Самостійна робота	Дослідження екзотичних форм аутентифікації і доступу	7
	10	Практична робота 6	Побудова та аналіз матриці доступу	2
	11	Практична робота 7	Моделювання монітору безпеки	2
	12	Практична робота 8	Реалізація базових механізмів контролю	2
Змістовий модуль 2. Механізми аутентифікації				**38**
6	**Тема 3. Базові механізми аутентифікації**			**21**
	13	Лекція 5	Парольні системи та політики	2
	14	Лекція 6	Токени та смарт-карти	2
	15	Лекція 7	Інфраструктура відкритих ключів	2
		Самостійна робота	Вивчення історичних аспектів порушення парольних політик	7
	16	Практична робота 9	Налаштування парольних політик в ОС Windows	2
	17	Практична робота 10	Налаштування парольних політик в Linux	2
	18	Практична робота 11	Робота з апаратними токенами	2
	19	Практична робота 12	Управління цифровими сертифікатами	2
7	**Тема 4. Сучасні методи автентифікації**			**17**

	20	Лекція 8	Біометричні методи автентифікації	2
	21	Лекція 9	Багатофакторна автентифікація	2
		Самостійна робота	Ознайомлення з існуючими рішеннями на ринку для аутентифікації з допомогою біометрії	7
	22	Практична робота 13	Налаштування біометричного сканера	2
	23	Практична робота 14	Інтеграція TOTP автентифікації	2
	24	Практична робота 15	Налаштування SMS/Email автентифікації	2
Змістовий модуль 3. Авторизація та контроль доступу				**40**
12	**Тема 5. Класичні моделі контролю доступу**			**23**
	25	Лекція 10	Дискреційне управління доступом	2
	26	Лекція 11	Мандатне управління доступом	2
	27	Лекція 12	Реалізація моделей в сучасних ОС	2
		Самостійна робота	Ознайомлення з компонентами в розрізі існуючих вразливостей	7
	28	Практична робота 16	Налаштування ACL у файловій системі Windows	2
	29	Практична робота 17	Налаштування прав доступу в Linux	2
	30	Практична робота 18	Конфігурація SELinux	2
	31	Практична робота 19	Реалізація мандатної моделі	2
	32	Практична робота 20	Аудит системи контролю доступу	2
13		**Тема 6. Рольове управління**		**17**
	33	Лекція 13	Концепція RBAC та ієрархія ролей	2
	34	Лекція 14	Адміністрування RBAC-систем	2
		Самостійна робота	Побудова власного практичного рішення на базі RBAC	7
	35	Практична робота 21	Проектування ієрархії ролей	2
	36	Практична робота 22	Налаштування RBAC в системі	2
	37	Практична робота 23	Адміністрування рольових політик	2
Змістовий модуль 4. Безпека мережевого доступу				**35**
14		**Тема 7. Протоколи та сервіси мережевого доступу**		**23**
	38	Лекція 15	Протокол Kerberos та LDAP	2
	39	Лекція 16	Active Directory та групові політики	2
	40	Лекція 17	VPN-технології	2
		Самостійна робота	Ознайомлення з існуючими продуктами на ринку для організації захищеного зв’язку	7
	41	Практична робота 24	Налаштування Kerberos-автентифікації	2

	42	Практична робота 25	Конфігурація LDAP-сервера	2
	43	Практична робота 26	Управління групами в Active Directory	2
	44	Практична робота 27	Налаштування VPN-сервера	2
	45	Практична робота 28	Конфігурація клієнтського VPN-доступу	2
15		**Тема 8. Безпека бездротових мереж**		**12**
	46	Лекція 18	Захист Wi-Fi мереж	2
		Самостійна робота	Дослідження наявних бездротових мереж на предмет захищеності	6
	47	Практична робота 29	Налаштування WPA3 безпеки	2
	48	Практична робота 30	Моніторинг та аудит Wi-Fi мережі	2
			Всього	**120**
			Підготовка до екзамену	**30**
			Всього	**150**

6. ПЕРЕЛІК ПИТАНЬ НА ЕКЗАМЕН

1. Визначення та цілі управління доступом в ІТС
2. Місце управління доступом в загальній системі захисту інформації
3. Основні компоненти системи управління доступом
4. Класифікація методів управління доступом
5. Суб'єкти та об'єкти доступу: визначення та характеристики
6. Основні загрози безпеці доступу в ІТС
7. Політика безпеки: визначення та складові
8. Механізми реалізації політики безпеки
9. Поняття та функції монітора безпеки
10. Матриця доступу: концепція та реалізація
11. Визначення та види автентифікації
12. Фактори автентифікації та їх характеристики
13. Парольні системи: принципи роботи та вимоги
14. Методи зберігання паролів
15. 15. Методи передачі паролів у мережі
16. 16. Політики управління паролями
17. 17. Види та характеристики токенів
18. 18. Принципи роботи смарт-карт
19. Інфраструктура відкритих ключів (PKI)
20. 20. Цифрові сертифікати та їх структура
21. 21. Центри сертифікації та їх функції
22. 22. Життєвий цикл цифрового сертифіката
23. 23. Біометричні характеристики та їх властивості
24. 24. Типи біометричних систем
25. 25. Методи біометричної ідентифікації
26. 26. Точність та надійність біометричних систем
27. 27. Принципи двофакторної автентифікації
28. 28. Методи реалізації двофакторної автентифікації
29. 29. Багатофакторна автентифікація: переваги та недоліки
30. Стандарти автентифікації
31. 31. Дискреційне управління доступом: принципи

32. 32. Реалізація DAC в операційних системах
    33. Списки контролю доступу (ACL)
    34. Переваги та недоліки DAC
    35. Мандатне управління доступом: принципи
    36. Рівні безпеки в MAC
    37. Правила мандатної політики безпеки
    38. Реалізація MAC в сучасних ОС
    39. Порівняння DAC та MAC
    40. Концепція рольового управління доступом
    41. Компоненти RBAC-моделі
    42. Ієрархія ролей в RBAC
    43. Статичне розподілення ролей
    44. Динамічне розподілення ролей
    45. Адміністрування RBAC-систем
    46. Переваги та недоліки RBAC
    47. Атрибутне управління доступом (ABAC)
    48. Політики та правила в ABAC
    49. Порівняння RBAC та ABAC
    50. Гібридні моделі управління доступом
33. 51. Протокол Kerberos: принципи роботи
    52. Компоненти системи Kerberos
    53. Процес автентифікації в Kerberos
    54. Квитки та ключі в Kerberos
    55. Служба каталогів LDAP
    56. Структура каталогу LDAP
    57. Операції в LDAP
    58. Active Directory: компоненти та функції
    59. Групові політики в Active Directory
    60. Управління користувачами в Active Directory
    61. Протокол OAuth: принципи роботи
    62. Ролі в OAuth
    63. Типи грантів OAuth
    64. OpenID Connect: особливості та переваги
    65. VPN: призначення та типи
    66. Протоколи тунелювання VPN
    67. Методи шифрування у VPN
    68. Безпека віддаленого доступу
    69. Стандарти безпеки Wi-Fi
    70. Протокол WPA2: механізми захисту
    71. Протокол WPA3: нові функції безпеки
    72. Методи автентифікації в Wi-Fi мережах
    73. Управління ключами в Wi-Fi мережах
    74. Типові атаки на Wi-Fi мережі
    75. Методи захисту від атак на Wi-Fi
    76. Моніторинг безпеки Wi-Fi мереж
    77. Аудит безпеки систем управління доступом
    78. Методи тестування механізмів автентифікації
    79. Інструменти аналізу безпеки доступу
    80. Документування систем управління доступом

7. МЕТОДИ НАВЧАННЯ

Під час вивчення дисципліни «Управління доступом в інформаційно телекомунікаційних системах» у навчальному процесі застосовуються такі методи навчання: розповідь, бесіда, проблемні лекції, пояснення, демонстрація, ілюстрація, навчальна дискусія, диспут, мозкові атаки, робота в малих групах, кейс-метод, самостійне виконання практичних завдань, розв'язування задач, виконання вправ.

8. КОНТРОЛЬ РЕЗУЛЬТАТІВ НАВЧАННЯ

8.1. Форми та засоби поточного і підсумкового контролю

Контроль знань здобувачів освіти здійснюється за модульно-рейтинговою системою.

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

- індивідуальне опитування, фронтальне опитування;
- поточне тестування;
- підсумкове тестування з кожного змістовного модуля;
- директорська контрольна робота;
- залік;
- екзамен.

Зміст курсу дисципліни «Комплексні системи захисту інформації» поділений на 2 змістових модулів. Кожний модуль включає в себе лекції, лабораторні заняття та самостійну роботу здобувачів освіти і завершуються рейтинговим контролем рівня засвоєння знань програмного матеріалу відповідної частини курсу.

У змістовий модуль 1 (ЗМ1) входять теми 1-2, у змістовий модуль 2 (ЗМ2) - теми 3-4, у змістовий модуль 3 (ЗМ3) - теми 5-6, у змістовий модуль 4 (ЗМ4) - теми 7-8.

Після завершення відповідного змістового модуля проводяться ***модульні контрольні роботи*** **(МК).** До модульної контрольної роботи допускаються здобувачі освіти, які опрацювали весь обсяг теоретичного матеріалу в т.ч. і матеріал самостійно, виконали практичні роботи.

Рейтингову кількість балів здобувачів освіти формують бали, отримані за модульні контрольні роботи, які проводяться у формі тестування, та середній рейтинг виконання лабораторних робіт.

Участь здобувачів освіти в контрольних заходах обов'язкова. МК проводиться у письмовій тестовій формі, тестові завдання обов'язково включають матеріал, який передбачено до самостійного опрацювання здобувачами освіти. 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) здобувач освіти отримує як середнє арифметичне балів змістових модулів з усіх тем п'яти змістових модулів.

Оцінка навчальної успішності здобувачів освіти здійснюється під час семестрового оцінювання у формі заліку та екзамену, які передбачають два усних запитання та вирішення практичного завдання.

8.2. Критерії оцінювання результатів навчання

Критерії оцінювання модульної контрольної роботи, директорської контрольної роботи, усних і письмових відповідей на питання, виконання практичних (лабораторних 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.

8.3. Оцінювання за формами контролю

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 5, (екзамен)	**Разом,%**
25	25	25	25	100%

8.4. Шкала оцінювання

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
85-89	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

9. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. Витяг з навчального плану
2. Навчальна (типова) програма
3. Робоча навчальна програма
4. Плани занять
5. Конспект лекцій з дисципліни
6. Завдання для обов'язкової контрольної роботи
7. Інструкційно-методичні матеріали до лабораторних занять
8. Інструкційно-методичні матеріали до самостійної роботи
9. Питання до заліків з модулів
10. Контрольні тестові завдання до заліків з модулів
11. Навчальний посібник
12. Роздавальний матеріал
13. Презентації до тем

10. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ
Основна література:

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2020. – 624 с.
2. Корченко О.Г., Терейковський І.А. Захист інформації в комп'ютерних системах. – К.: НАУ, 2020. – 376 с.
3. Бурячок В.Л., Толубко В.Б. Інформаційна та кібербезпека: соціотехнічний аспект. – К.: ДУТ, 2021. – 288 с.
4. Дудикевич В.Б., Опірський І.Р. Захист інформації в інформаційних системах. – Львів: Видавництво Львівської політехніки, 2019. – 376 с.
5. Юдін О.К., Бучик С.С. Захист інформації в мережах передачі даних. – К.: НАУ, 2021. – 440 с.

Додаткова література:

1. Богуш В.М., Юдін О.К. Основи інформаційної безпеки держави. – К.: МК-Прес, 2019.
2. Гулак Г.М., Гринь А.К. Основи криптографічного захисту інформації. – К.: НАУ, 2020.
3. Хорошко В.О., Чекатков А.А. Методи й засоби захисту інформації. – К.:

Юніор, 2019.

Інтернет-ресурси:

1. Державна служба спеціального зв'язку та захисту інформації України https://cip.gov.ua/ua
2. CERT-UA (Computer Emergency Response Team of Ukraine) https://cert.gov.ua/
3. Українська команда реагування на комп'ютерні надзвичайні події https://cert.gov.ua/articles
4. Портал технічної підтримки Microsoft Ukraine https://docs.microsoft.com/uk-ua/security/
5. Національний банк стандартів України http://uas.org.ua/ua/

Міжнародні ресурси:

1. NIST Computer Security Resource Center https://csrc.nist.gov/
2. OWASP (Open Web Application Security Project) https://owasp.org/
3. IEEE Security & Privacy https://www.computer.org/security-and-privacy
4. Red Hat Security Blog https://www.redhat.com/en/blog/channel/security
5. Microsoft Security Documentation https://docs.microsoft.com/en-us/security/

Нормативні документи:

1. НД ТЗІ 1.1-002-99: Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу
2. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
3. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

Онлайн-курси та навчальні матеріали:

1. Prometheus: курси з кібербезпеки https://prometheus.org.ua/
2. Coursera: Information Security https://www.coursera.org/
3. Security Awareness Training Platform https://www.securingthehuman.org/
4. Cisco Network Academy: Cybersecurity https://www.netacad.com/
5. CompTIA Security+ Training https://www.comptia.org/training/