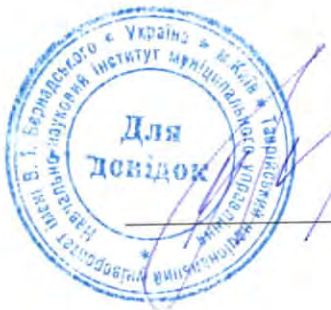
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. І. ВЕРНАДСЬКОГО
Навчально-науковий інститут муніципального управління
та міського господарства
Кафедра комп'ютерних та інформаційних технологій



ЗАТВЕРДЖУЮ

Директор інституту

_____Володимир КИСЕЛЬОВ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КРИПТОЛОГІЇ ТА ЗАХИСТ ІНФОРМАЦІЇ

першого (бакалаврського) рівня вищої освіти

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 122 «Комп'ютерні науки»

Освітньо–професійна програма: «Комп'ютерні науки»

Форма здобуття освіти: очна (денна)

КИЇВ 2025

УКЛАДАЧ силабусу д.т.н., професор, професор кафедри комп'ютерних та інформаційних технологій

_____ Олександр СЄЛЮКОВ

(підпис)

Розглянуто та схвалено на засіданні кафедри комп'ютерних та інформаційних технологій

Протокол № 1 від 26.08.2025

Завідувач кафедри _____ Олександр ГУЙДА

(підпис)

Гарант освітньо-професійної програми «Комп'ютерні науки»

к.т.н., доцент _____ Сергій ЛІСОВЕЦЬ

(підпис)

1. **Загальна інформація про навчальну дисципліну**	
1.Назва навчальної дисципліни, код в ОПП	**Основи криптології та захист інформації** Код ОК 1.2.13
2.Статус навчальної дисципліни	Навчальна дисципліна професійної підготовки
3.Рік навчання, семестр у якому викладається дисципліна	4 рік навчання 7 та 8 семестри
4.Обсяг навчальної дисципліни (кількість кредитів, загальна кількість годин (аудиторних за видами занять, самостійної роботи здобувача вищої освіти)	6 кредитів загальна кількість годин: 180 аудиторних: 64 лекцій: 32 год практичні: 32 год самостійна робота: 116 год
5.Вид підсумкового (семестрового) контролю	Залік 7 семестр, екзамен 8 семестр
6.Інформація про консультації	Згідно затвердженого графіка консультацій
7.Мова викладання	українська
8.Прізвище, ім’я, по батькові викладача (науковий ступінь, вчене звання, посада)	Д.т.н, проф. Олександр СЄЛЮКОВ
9.Контактна інформація викладача	seliukov.oleksandr@tnu.edu.ua
10.Посилання на силабус на вебсайті Університету	https://tnu.edu.ua/_kafedra-kompyuternix-ta-informacijnix-texnologij_/
2. Опис навчальної дисципліни	
Анотація дисципліни	Дисципліна «Основи криптології та захисту інформації» спрямована на формування у здобувачів вищої освіти спеціальності F3 Комп’ютерні науки системних теоретичних знань і практичних уявлень про принципи криптології та сучасні методи захисту інформації в комп’ютерних системах і мережах. У межах дисципліни розглядаються базові поняття криптографії та криптоаналізу, симетричні й асиметричні криптографічні алгоритми, хеш-функції та механізми забезпечення цілісності й автентичності даних, а також основи побудови систем інформаційної безпеки. Особливу увагу приділено криптографічним протоколам, інфраструктурі відкритих ключів, захисту інформації в комп’ютерних мережах і веб-системах, а також сучасним і перспективним напрямам розвитку криптології. Дисципліна забезпечує підґрунтя для подальшого вивчення спеціалізованих курсів з інформаційної безпеки та застосування криптографічних методів у професійній діяльності

	фахівців з комп'ютерних наук.
Мета, завдання та цілі вивчення дисципліни	**Мета** дисципліни Метою вивчення дисципліни «Основи криптології та захисту інформації» є формування у здобувачів вищої освіти спеціальності F3 Комп'ютерні науки системних знань про теоретичні засади криптології та практичні підходи до захисту інформації в комп'ютерних системах і мережах, а також розвиток умінь застосовувати криптографічні методи й засоби для забезпечення конфіденційності, цілісності та автентичності інформації. **Завдання дисципліни** Завданнями вивчення дисципліни є: – ознайомлення з базовими поняттями, термінами та історією розвитку криптології; – вивчення принципів побудови симетричних та асиметричних криптографічних алгоритмів; – формування уявлень про криптографічні хеш-функції та механізми забезпечення цілісності й автентичності даних; – засвоєння основ криптографічних протоколів і принципів функціонування інфраструктури відкритих ключів; – аналіз загроз інформаційній безпеці та методів захисту інформації в комп'ютерних системах і мережах; – формування навичок використання криптографічних засобів у процесі розроблення та експлуатації програмного забезпечення. **Цілі вивчення дисципліни** У результаті вивчення дисципліни здобувачі вищої освіти повинні: – розуміти роль криптології та захисту інформації у сучасних комп'ютерних науках; – знати основні криптографічні алгоритми, протоколи та механізми захисту інформації; – вміти обґрунтовувати вибір криптографічних методів залежно від вимог до безпеки інформації; – застосовувати базові криптографічні засоби для захисту даних у комп'ютерних системах і мережах; – оцінювати потенційні загрози та ризики інформаційній безпеці й пропонувати відповідні заходи захисту.
Пререквізити	Теорія інформації та кодування
Постреквізити	Підготовка до атестації

Формат проведення дисципліни	Змішаний; У разі роботи в дистанційному режимі використовується корпоративне середовище Google Classroom; Лекції та практичні у дистанційному режимі будуть вестися через Google Meet; поточна комунікація з викладачем здійснюється ч корпоративну пошту.

3. Програмні результати навчання відповідно до освітньо-професійної програми:

Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів комп'ютерних наук, інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК8. Здатність генерувати нові ідеї (креативність).

ЗК10. Здатність бути критичним і самокритичним.

ЗК11. Здатність приймати обґрунтовані рішення.

ЗК16. Здатність розробляти й управляти проектами.

Фахові компетентності:

ФК3. Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.

ФК8. Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об'єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління.

ФК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Програмні результати навчання:

ПРН1.Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.

ПРН3.Використовувати знання закономірностей випадкових явищ, їх властивостей та операцій над ними, моделей випадкових процесів та сучасних

програмних середовищ для розв'язування задач статистичної обробки даних і побудови прогнозних моделей.

ПРН5.Проектувати, розробляти та аналізувати алгоритми розв'язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислюваних функцій.

ПРН13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення

ПРН15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

4. Тематика та зміст навчальної дисципліни

Номер та назва розділу, теми, перелік основних питань	**Вид навчального заняття**	**Форми і методи контролю знань**	**Кількість годин** Лекція/ практичне заняття
МОДУЛЬ 1. ТЕОРЕТИЧНІ ОСНОВИ КРИПТОЛОГІЇ ТА КРИПТОГРАФІЧНІ МЕТОДИ			
Тема 1.1. Криптологія як наука. Основні поняття та історія розвитку. Криптологія в системі інформаційної безпеки. Криптографія і криптоаналіз. Об'єкти та завдання криптології. Історичні етапи розвитку криптографії. Класичні криптосистеми та їх обмеження. Роль криптографії у сучасних комп'ютерних науках	Лекція/ практичне заняття	Виконання практичних робіт по темі	4/4
Тема 1.2. Симетричні криптографічні алгоритми. Поняття симетричного шифрування. Потокові та блочні шифри. Основні режими роботи блочних шифрів. Криптостійкість симетричних алгоритмів. Приклади сучасних симетричних алгоритмів. Переваги та недоліки симетричного шифрування		Виконання практичних робіт по темі	4/4

Номер та назва розділу, теми, перелік основних питань	Вид навчального заняття	Форми і методи контролю знань	Кількість годин Лекція/ практичне заняття
Тема 1.3. Асиметричні криптографічні алгоритми та криптографія з відкритим ключем. Принципи асиметричного шифрування. Генерація ключових пар. Основні асиметричні алгоритми. Обмін ключами. Порівняльний аналіз симетричних та асиметричних методів. Області застосування		Виконання практичних робіт по темі	4/4
Тема 1.4. Хеш-функції та криптографічні перетворення цілісності. Криптографічні хеш-функції та їх властивості. Контроль цілісності інформації. Колізії та стійкість до атак. Криптографічні коди автентифікації повідомлень. Використання хеш-функцій у сучасних інформаційних системах		Виконання практичних робіт по темі Тестове опитування	4/4
МОДУЛЬ 2. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ			
Тема 2.1. Основи захисту інформації та моделі безпеки. Поняття інформаційної безпеки. Загрози, вразливості та ризики. Основні моделі безпеки. Принципи побудови систем захисту інформації. Політика безпеки інформаційних систем	Лекція/ практичне заняття	Виконання практичних робіт по темі	4/4
Тема 2.2. Криптографічні протоколи та інфраструктура відкритих ключів. Криптографічні протоколи та їх призначення. Протоколи автентифікації та захищеного обміну даними. Інфраструктура відкритих ключів. Цифрові сертифікати. Центри сертифікації та управління ключами		Виконання практичних робіт по темі	4/4
Тема 2.3. Захист інформації в комп'ютерних мережах і веб-системах. Криптографічні засоби захисту мережних з'єднань. Захист передавання даних у мережах. Основи безпеки веб-додатків. Атаки на мережеві та веб-системи та методи їх протидії		Виконання практичних робіт по темі	4/4

Номер та назва розділу, теми, перелік основних питань	Вид навчального заняття	Форми і методи контролю знань	Кількість годин Лекція/ практичне заняття
Тема 2.4. Прикладні аспекти та сучасні напрями криптології і захисту інформації. Застосування криптографії в операційних системах і прикладному програмному забезпеченні. Захист даних у хмарних технологіях. Основи квантової криптографії. Перспективи розвитку криптології та інформаційної безпеки		Виконання практичних робіт по темі Тестове опитування	4/4

5. Інформація про індивідуальне завдання

У межах вивчення дисципліни передбачено виконання індивідуальних завдань, які реалізуються у формі практичних робіт та контрольних тестових завдань за тематичними модулями курсу. Індивідуальні завдання спрямовані на закріплення теоретичних положень криптології та формування практичних умінь застосування методів і засобів захисту інформації.

Самостійна робота здобувачів вищої освіти має на меті поглиблене опрацювання навчального матеріалу, опанування рекомендованих джерел, а також розвиток навичок пошуку, критичного аналізу та узагальнення інформації з питань криптографії й інформаційної безпеки. Особлива увага приділяється розумінню принципів функціонування криптографічних алгоритмів і механізмів захисту даних.

Під час виконання практичних робіт здобувачі застосовують набуті теоретичні знання для розв’язання типових і прикладних завдань у сфері захисту інформації, зокрема пов’язаних із шифруванням даних, контролем цілісності, автентифікацією та безпечним обміном інформацією в комп’ютерних системах і мережах. Завдання орієнтовані на формування базових практичних навичок, необхідних для подальшої професійної діяльності у галузі комп’ютерних наук.

Оцінювання результатів самостійної роботи здійснюється в процесі поточного контролю шляхом перевірки виконаних практичних робіт, проведення тестування та аналізу рівня засвоєння навчального матеріалу. Кожне індивідуальне завдання оцінюється відповідно до встановленої бальної шкали, а отримані результати враховуються під час формування підсумкової оцінки з дисципліни.

Для здобувачів заочної форми навчання індивідуальні завдання формуються з урахуванням варіантності та специфіки дисципліни, що забезпечує індивідуальний підхід до їх виконання. Детальні відомості щодо змісту завдань, вимог до оформлення, порядку виконання та захисту подаються у методичних рекомендаціях до вивчення курсу.

6. Технічне обладнання та програмне забезпечення

Для забезпечення навчального процесу з дисципліни «Основи криптології та захисту інформації» використовуються технічні засоби та програмне забезпечення, необхідні для проведення лекційних, практичних занять і виконання індивідуальних завдань.

Технічне обладнання включає персональні комп'ютери або ноутбуки з доступом до локальної мережі та мережі Інтернет, мультимедійне обладнання для демонстрації навчальних матеріалів під час лекційних занять, а також засоби візуалізації для представлення схем, алгоритмів і прикладів криптографічних перетворень.

Програмне забезпечення передбачає використання операційних систем загального призначення, середовищ програмування та інструментів розроблення, що застосовуються у підготовці фахівців з комп'ютерних наук. У навчальному процесі можуть використовуватися програмні засоби для реалізації та тестування криптографічних алгоритмів, інструменти для роботи з хеш-функціями, цифровими підписами та сертифікатами, а також засоби аналізу та захисту інформації в комп'ютерних системах і мережах.

Для організації змішаного та дистанційного навчання, проведення онлайн-занять, консультацій і захисту практичних робіт використовуються сервіси Google Meet, які забезпечують синхронну комунікацію між викладачем і здобувачами вищої освіти. Для підтримки навчального процесу, розміщення навчально-методичних матеріалів, індивідуальних завдань, тестових опитувань, а також для зворотного зв'язку та оцінювання результатів навчання застосовується платформа Google Classroom.

Використання зазначених технічних засобів і програмного забезпечення забезпечує доступність навчального контенту, ефективну взаємодію учасників освітнього процесу та створює умови для формування практичних навичок у сфері криптології та захисту інформації.

7. Політика дисципліни.

Політика дисципліни «Основи криптології та захисту інформації» ґрунтується на принципах академічної доброчесності, відповідальності та дотримання встановлених правил організації освітнього процесу.

Політика щодо академічної доброчесності передбачає самостійне виконання всіх видів навчальної діяльності. Використання несанкціонованих матеріалів, сторонньої допомоги або відтворення чужих результатів під час тестування, виконання практичних робіт і підсумкового контролю не допускається. Будь-які прояви порушення академічної доброчесності розглядаються відповідно до чинних нормативних документів закладу вищої освіти та тягнуть за собою застосування визначених заходів академічної відповідальності.

Питання перезарахування результатів навчання у разі академічної мобільності, а також порядок повторного проходження контролю чи відпрацювання пропущених занять регулюються внутрішніми положеннями Таврійського національного університету імені В. І. Вернадського та здійснюються за умови наявності підтвердних документів і погодження з викладачем.

Політика щодо дотримання термінів виконання завдань передбачає своєчасне подання всіх форм навчальної роботи. Завдання, подані із запізненням без обґрунтованих причин, оцінюються з пониженням максимально можливого балу. Повторне проходження тестування або інших форм контролю допускається лише у разі наявності поважних причин, підтверджених відповідними документами.

Політика щодо відвідування занять базується на розумінні активної участі здобувачів в освітньому процесі як важливої умови досягнення запланованих результатів навчання. У разі виникнення об’єктивних обставин, що унеможливлюють очну присутність, допускається використання дистанційних форм навчання за погодженням із викладачем. Дотримання зазначених правил сприяє ефективному опануванню змісту дисципліни та формуванню професійної відповідальності майбутніх фахівців з комп’ютерних наук.

8. Система оцінювання та вимоги

І семестр

У першому семестрі підсумкова оцінка з дисципліни формується на основі результатів поточної навчальної діяльності здобувача вищої освіти. Максимальна кількість балів, яку можна отримати за семестр, становить 100 балів.

Поточний контроль здійснюється шляхом виконання практичних робіт за темами модуля 1 та підсумкового тестового завдання. За виконання практичних робіт за темами 1.1–1.4 здобувач може отримати по 20 балів за кожну роботу. За результатами тестового завдання за модулем 1 нараховується до 20 балів.

Підсумковий контроль у першому семестрі проводиться у формі заліку. Оцінка за залік визначається як сума балів, отриманих за всі види навчальної діяльності протягом семестру. Результати поточного контролю доводяться до відома здобувачів вищої освіти в установленому порядку.

Здобувач вищої освіти, який не виконав усі передбачені програмою практичні роботи або не набрав мінімально допустиму кількість балів, до складання заліку не допускається та зобов'язаний ліквідувати академічну заборгованість відповідно до чинних правил університету.

II семестр

У другому семестрі оцінювання результатів навчання здійснюється на основі поєднання поточного контролю та семестрового екзамену. Загальна кількість балів за семестр становить 100, з яких до 60 балів припадає на поточну навчальну діяльність і до 40 балів – на екзаменаційний контроль.

Поточний контроль у межах модуля 2 передбачає виконання практичних робіт за темами 2.1–2.4, кожна з яких оцінюється у 10 балів, а також тестове завдання за модулем 2, максимальна оцінка за яке становить 20 балів. Поточний контроль спрямований на перевірку рівня засвоєння теоретичних положень дисципліни та сформованості практичних навичок застосування криптографічних методів і засобів захисту інформації.

Семестровий контроль проводиться у формі екзамену, за результатами якого здобувач може отримати до 40 балів. Екзамен дозволяє комплексно оцінити рівень знань, умінь і здатність застосовувати навчальний матеріал у типових професійних ситуаціях.

Підсумкова оцінка за другий семестр визначається шляхом додавання балів поточного контролю та екзаменаційної оцінки. Здобувачі вищої освіти, які не набрали мінімально необхідної кількості балів за результатами поточної роботи або мають невиконані завдання, до складання екзамену не допускаються та проходять процедуру ліквідації академічної заборгованості у встановленому порядку. Повторне складання екзамену з метою підвищення позитивної оцінки не передбачене.

8.1 Шкала та схема формування підсумкової оцінки

Тема	Вид роботи	Кількість балів
Ісеместр		
Модуль 1		
Тема 1.1.	Практична робота 1	20
Тема 1.2.	Практична робота 2	20
Тема 1.3.	Практична робота 3	20
Тема 1.4.	Практична робота 4	20
Модуль 1	Тестове завдання	20
Підсумковий контроль - залік		
	Загальна кількість балів	**100**
II семестр		
Модуль 2		
Тема 2.1.	Практична робота 5	10
Тема 2.2.	Практична робота 6	10
Тема 2.3.	Практична робота 7	10
Тема 2.4.	Практична робота 8	10
Модуль 2	Тестове завдання	20
Підсумковий контроль		
	Екзамен	40
	Загальна кількість балів	**100**

Загальна система оцінювання курсу	**I семестр** У першому семестрі підсумкова оцінка з дисципліни формується на основі результатів поточного контролю. Вона є сумою балів, отриманих за виконання практичних робіт за темами модуля 1 та тестового опитування за відповідним модулем. Кожен вид навчальної діяльності має визначену вагу в загальній структурі оцінювання, що забезпечує об’єктивну перевірку рівня засвоєння

	навчального матеріалу. Оцінювання результатів навчання здійснюється за 100-бальною шкалою. Підсумкова оцінка за семестр визначається як сума балів за всі види робіт та відповідає критеріям переведення у шкалу ECTS і національну шкалу оцінювання згідно з установленою таблицею відповідності. **II семестр** У другому семестрі підсумкова оцінка з дисципліни формується з урахуванням результатів поточного контролю та підсумкового контролю у формі екзамену. Вона є сумою балів за виконання практичних робіт за темами модуля 2, тестового опитування за модулем та результатів екзаменаційного контролю, кожен з яких має визначену вагу в загальній системі оцінювання. Оцінювання здійснюється за 100-бальною шкалою з подальшим переведенням результатів у шкалу ECTS та національну шкалу відповідно до затвердженої таблиці оцінювання. Такий підхід забезпечує комплексну оцінку рівня теоретичної підготовки та практичної готовності здобувачів вищої освіти з дисципліни.
Розрахункова графічна-робота	В рамках курсу не передбачено виконання РГР.
Лабораторні та практичні роботи	**Критерії оцінювання практичних робіт:** Під час оцінювання практичних робіт враховуються такі складові: – рівень підготовленості здобувача вищої освіти до практичного заняття та розуміння теоретичних положень теми; – самостійність виконання завдань і дотримання принципів академічної доброчесності; – повнота та коректність виконання поставлених завдань, логічність отриманих результатів; – дотримання встановлених термінів подання практичних робіт.

	У першому семестрі кожна практична робота за темами модуля 1 оцінюється максимально у 20 балів. У другому семестрі кожна практична робота за темами модуля 2 оцінюється максимально у 10 балів.
Тест	Тестові завдання проводяться після завершення вивчення кожного модуля з метою перевірки рівня засвоєння теоретичного матеріалу, ключових понять і принципів криптології та захисту інформації. Оцінювання тестування здійснюється з урахуванням правильності та повноти відповідей. Максимальна кількість балів за тестове завдання за кожним модулем становить 20 балів.
Екзамен	У першому семестрі підсумковий контроль проводиться у формі заліку та визначається сумою балів, набраних за всі види навчальної діяльності протягом семестру. У другому семестрі підсумковий контроль здійснюється у формі екзамену. Екзамен спрямований на комплексну перевірку теоретичних знань і здатності застосовувати їх для розв'язання типових завдань у сфері криптології та захисту інформації. Максимальна оцінка за екзамен становить 40 балів. Підсумкова оцінка з дисципліни формується відповідно до встановленої системи оцінювання та переводиться у шкалу ECTS і національну шкалу згідно з чинними нормативними вимогами.
Умови допуску до підсумкового контролю	Позитивна оцінка за всіма обов'язковими видами робіт (тести та практичні роботи). Допуск до екзамену 40 балів за поточний контроль

5. Рекомендовані джерела інформації

Назва теми	Рекомендовані джерела інформації до теми (основна література; допоміжна література;

	інформаційні ресурси в мережі Інтернет)
Модуль 1. Теоретичні основи криптології та захисту інформації	
Тема 1.1. Криптологія як наука. Осн поняття та історія розвитку	Основна література: 2, 8, Додаткова література: 3, Інформаційні ресурси в Інтернеті: 1, 2,
Тема 1.2. Симетричні криптограф алгоритми	Основна література: 2, 1, Додаткова література: 3, Інформаційні ресурси в Інтернеті: 5, 6,
Тема 1.3. Асиметричні криптограф алгоритми та криптографія з відкри ключем	Основна література: 2, 1, Додаткова література: 1, Інформаційні ресурси в Інтернеті: 3, 5,
Тема 1.4. Хеш-функції та криптограф механізми забезпечення цілісності	Основна література: 2, 1, Додаткова література: 6, Інформаційні ресурси в Інтернеті: 5, 11,
Модуль 2. Захист інформації в комп'ютерних системах та мережах	
Тема 2.1. Основи інформаційної безпек моделі захисту інформації	Основна література: 1, 7, Додаткова література: 3, Інформаційні ресурси в Інтернеті: 1, 10
Тема 2.2. Криптографічні протоколи інфраструктура відкритих ключів	Основна література: 1, 2, Додаткова література: 1, Інформаційні ресурси в Інтернеті: 3, 5,
Тема 2.3. Захист інформації комп'ютерних мережах і веб-системах	Основна література: 1, 5, Додаткова література: 2, 4, Інформаційні ресурси в Інтернеті: 4, 6 14
Тема 2.4. Управління та аудит сис інформаційної безпеки	Основна література: 4, 6, Додаткова література: 1, 7, Інформаційні ресурси в Інтернеті: 8, 12

Основна література

1. Бобало Ю.Я., Горбатий І.В., Кіселичник М.Д. *Інформаційна безпека: навч. посібник*. Львів: Видавництво Львівської політехніки, 2019. – 580 с.

2. Щур Н.О., Покотило О.А. *Основи криптології: навч. посібник*. Житомир: Житомирська політехніка, 2021. – 120 с

3. Герман, М. Л. Політика та стратегія державного регулювання інформаційної безпеки. Львів: Видавництво Львівського національного університету, 2017. 275 с.

4. Гончаров, П. А. Менеджмент інформаційної безпеки: Основи та практичні аспекти. Львів: Видавництво ЛНУ ім. Івана Франка, 2020. 230 с.

5. Данилов, В. С. Інформаційна безпека в умовах сучасних загроз. Львів: Видавництво Львівської політехніки, 2018. 256 с.

6. Зубарєв, В. В. Організація системи захисту інформації: Теорія і практика. Київ: Видавництво НТУУ «КПІ», 2020. 300 с.

7. Кавун С. В. Інформаційна безпека. Навчальний посібник. Харків: Вид. ХНЕУ, 2020. 352 с.

8. Козлов, О. А. Теоретичні аспекти інформаційної безпеки. Одеса: Астропринт, 2016. 290 с.

9. Крючков, С. В. Державне регулювання у сфері інформаційної безпеки України: Проблеми та рішення. Київ: Центр учбової літератури, 2021. 220 с.

10. Кудрявцев, Ю. І. Основи інформаційної безпеки: Теорія та практика. Київ: Техніка, 2017. 320 с.

Додаткова література

1. Лебедєв, А. С. Управління системами інформаційної безпеки. Київ: Видавничий дім «КНТ», 2022. 270 с.

2. Петренко, В. О. Інформаційна безпека України: Виклики та відповіді. Одеса: ОНУ ім. І. І. Мечникова, 2022. 240 с.

3. Романенко, О. В. Методологія та практика забезпечення інформаційної безпеки. Київ: Видавництво Національного університету «Київська політехніка», 2021. 250 с.

4. Семенов, М. І. Інформаційні загрози та їх класифікація. Харків: Національний технічний університет Харківського політехнічного інституту, 2019. 180 с.

5. Сергієнко, В. О. Підходи до забезпечення інформаційної безпеки в умовах воєнного стану. Харків: Видавництво ХНУРЕ, 2023. 260 с.

6. Тимошенко, І. В. Принципи та методи забезпечення інформаційної безпеки. Дніпро: Дніпровський національний університет імені Олеся Гончара, 2019. 245 с.

7. Черненко, А. В. Теоретичні та практичні аспекти менеджменту інформаційної безпеки. Київ: Видавництво «Міжнародні відносини», 2022. 300 с.

8. Шевченко, І. М. Аудит систем інформаційної безпеки. Київ: Видавництво «Юрінком Інтер», 2018. 210 с.

Інформаційні ресурси в Інтернеті

1. Національний центр кібербезпеки України. Теоретичні аспекти інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://ncc.gov.ua/

2. Інститут інформаційної безпеки. Теоретичні основи інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://iis.org.ua/theory-information-security

3. Міністерство цифрової трансформації України. Захист інформаційних систем [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/

4. Ukrainian Cyber Security Group. Поняття інформаційних загроз [Електронний ресурс]. – Режим доступу: https://ucsg.org.ua/

5. Центр моніторингу та захисту інформації. Підходи до забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://cmpi.gov.ua/

6. Методи забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://it-ukraine.org.ua/methods-information-security

7. CyberSecurity in Ukraine. Державне регулювання в умовах воєнного стану [Електронний ресурс]. – Режим доступу: https://cybersecurity.com.ua/

8. Аудит і безпека інформації. Основи аудиту систем інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://auditinfosec.com.ua/

9. Інститут безпеки та захисту інформації. Організація системи захисту інформації [Електронний ресурс]. – Режим доступу: https://ibzi.org.ua/

10. Кібербезпека України. Принципи і методи забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://cybersecurity.gov.ua/

11. Центр інформаційної безпеки. Поняття інформаційних загроз [Електронний ресурс]. – Режим доступу: https://cib.org.ua/

12. Управління інформаційною безпекою в Україні. Управління та менеджмент систем інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://info-security.ua/

13. Безпека даних та інформації. Підходи та засоби захисту інформації [Електронний ресурс]. – Режим доступу: https://datasecurity.com.ua/

14. Безпека інформаційних систем в Україні. Принципи забезпечення безпеки [Електронний ресурс]. – Режим доступу: https://securitysys.org.ua/

15. Проблеми та рішення в інформаційній безпеці. Менеджмент і аудит систем інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://info-problems.com.ua/