СХІДНОЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ РАУФА АБЛЯЗОВА

RAUF ABLYAZOV UNIVERSITY EAST EUROPEAN

Кафедра права та інформаційної справи

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ ІС І ЗАХИСТ ДАНИХ

Спеціальність **В13 Бібліотечна, інформаційна та архівна справа**

Освітньо-наукова програма **Документно-інформаційна діяльність**

Освітній ступінь **магістр**

2025 рік

Робоча програма навчальної дисципліни «Основи ІС і захист даних»

для здобувачів вищої освіти освітнього ступеня магістр

спеціальності В13 «Бібліотечна, інформаційна та архівна справа»

освітньо-наукової програми «Документно-інформаційна діяльність»

Розробник:
Манькута Яна Миколаївна, к .е. н., доцент

Робоча програма розглянута та затверджена на засіданні кафедри права та інформаційної справи

Протокол від «____»_____20____ р. № _____

Завідувач кафедри _____ _____
підпис *Ініціали Прізвище*

Робоча програма схвалена на засіданні Навчально-методичної ради,
протокол № 04-2024/2025 від 17.04.2025.

1 ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Статус навчальної дисципліни	*Обов'язкова*
Шифр навчальної дисципліни (за ОПП)	*ОК 5*
Мова викладання	*українська*
Семестр(и)	*10*
Обсяг дисципліни (у кредитах ЄКТС і годинах)	*5 кредитів ЄКТС / 150 годин*
Передумови вивчення дисципліни:	Навчальні дисципліни підготовки за ОС «магістр» спеціальності В13 «Бібліотечна, інформаційна та архівна справа» ОНП «Документно-інформаційна діяльність»: ОК2. Інформаційно-аналітичні технології ОК10. Документальні публікації в електронному форматі
Анотація навчальної дисципліни:	Дисципліна «Основи ІС і захист даних» розглядає актуальні питання захисту інформації при створенні та використанні розподілених корпоративних інформаційних систем, методи і алгоритмам криптографічного захисту (функції хешування, електронного цифрового підпису, ідентифікації та аутентифікації користувачів інформаційних систем, управління криптографічними ключами).
Мета навчальної дисципліни:	Формування термінологічного фундаменту; навчання студентів правильно проводити аналіз загроз інформаційній безпеці; ознайомити з основними методами, принципами, алгоритмами захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників..
Завдання:	спрямована на формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації у сучасних інформаційних системах в умовах широкого використання сучасних інформаційних технологій.
Мета орієнтована на формування у здобувачів таких компетентностей:	ЗК 3. Вміння виявляти, ставити та вирішувати проблеми. СК 1. Здатність до формування ефективної системи управління інформаційною, бібліотечною та архівною діяльністю. СК 3. Здатність використовувати автоматизовані технології для вирішення практичних, управлінських, науково-дослідних і прогностичних завдань у професійній діяльності. СК 6. Здатність застосовувати комп'ютерні технології з метою вдосконалення професійної діяльності, розуміти принципи проєктування та функціонування автоматизованих БД, семантичного вебу, вебсервісів та соціальних медіа. СК 11. Здатність визначати специфіку предметної сфери діяльності для формулювання завдань автоматизації інформаційних процесів.
Результати навчання:	ПРН 7. Розробляти моделі предметної галузі, застосовувати принципи проектування автоматизованих БД, семантичного вебу, вебсервісів та соціальних медіа в інформаційній діяльності. ПРН 11. Застосувати законодавчі та нормативні документи, що регулюють функціонування інформаційної сфери.

	ПРН 13. Застосовувати прикладне програмне забезпечення для вирішення управлінських та/або наукових завдань на основі поєднання інтелектуальних здібностей людини з функціональними можливостями інформаційних систем.

2 ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Форма організації освітнього процесу	Кількість кредитів	Загальна кількість годин	Семестр вивчення	Обсяги за видами навчальних занять			Самостійна робота (год)	Вид індивідуального завдання	Форма підсумкового контролю (екзамен/залік)
				Лекції (год)	Практичні, семінарські (год)	Лабораторні (год)			
Денна форма навчання	5	150	10	32		32	86	Контрольна робота	екзамен
Заочна форма навчання	5	150	10	6		6	138	Контрольна робота	екзамен

3 ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

3.1 Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ПРИНЦИПИ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

ТЕМА 1. ОСНОВНІ ПОНЯТТЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Основні визначення теорії інформаційної безпеки та захисту інформації. Основні складові інформаційної безпеки. Важливість та складність проблеми інформаційної безпеки. Стандарти оцінювання і технічні специфікації.

ТЕМА 2. КЛАСИФІКАЦІЯ ПОГРОЗ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ. РІВНІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Джерела погроз безпеки інформації. Найбільш розповсюджені погрози інформаційної безпеки. Основні визначення і критерії класифікації погроз. Найбільш поширені погрози конфіденційності, цілісності, доступності. Законодавчі, правові та організаційні рівні захисту інформації.

ТЕМА 3. СЕРВІСИ ТА МЕХАНІЗМИ ПРОГРАМНОГО-ТЕХНІЧНОГО РІВНЯ ЗАХИСТУ. ІНФОРМАЦІЇ. ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Основи принципи та механізми програмно-технічного рівня захисту інформації. Сервіси програмно-технічного рівня. Захист від НСД: сервіс ідентифікації і аутентифікації користувача. Основні принципи та методи аутентифікації. Парольна аутентифікація. Аутентифікація за допомогою біометричних даних.

ТЕМА 4. УПРАВЛІННЯ ДОСТУПОМ. МІЖМЕРЕЖЕВІ ЕКРАНИ. ТЕХНІЧНІ МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Політики розмежування прав доступу. Механізми контролю за доступом. Основні моделі управління доступом. Рольове управління доступом. Протоколювання і аудит. Активний аудит. Загальний опис. Призначення та функції брандмауерів. Типи брандмауерів. Організація захисту від технічних каналів витоку інформації. Канали просочування інформації. Вимоги до НД ТЗІ.

ЗМІСТОВИЙ МОДУЛЬ 2. ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

ТЕМА 5. ОСНОВНІ ПОЛОЖЕННЯ ЩОДО ОРГАНІЗАЦІЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Базові терміни та визначення. Основні задачі забезпечення інформаційної безпеки. Джерела загроз інформаційній безпеці. Визначення інформаційних ресурсів, що підлягають захисту.

ТЕМА 6. КОНЦЕПЦІЯ ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ УСТАНОВИ

Фізичний захист інформації. Організація допуску та доступу персоналу до конфіденційної інформації. Захист конфіденційної інформації.

ТЕМА 7 СЛУЖБА ЗАХИСТУ ІНФОРМАЦІЇ УСТАНОВИ

Організаційне забезпечення безпеки інформації обмеженого доступу. Організація та функції служби захисту інформації установи. Організація контролю за безпекою інформації.

ТЕМА 8. СУТНІСТЬ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ І ПРИНЦИПИ ЇЇ ОРГАНІЗАЦІЇ

Методологічні та концептуальні засади комплексної системи захисту інформації. Проведення робіт зі створення КСЗІ. Методологічні та концептуальні засади комплексної системи захисту інформації. Етапи створення КСЗІ. Правові підстави для створення КСЗІ. Призначення та структура Плану захисту інформації в ІС. Зміст Плану захисту інформації в ІТС.

ЗМІСТОВИЙ МОДУЛЬ 3 БЕЗПЕКА І ЗАХИСТ ДАНИХ ТА ПРОГРАМ

ТЕМА 9. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ АВТЕНТИЧНОСТІ ТА ЦІЛІСНОСТІ ДАНИХ

Функції хешування та електронний цифровий підпис. Основні властивості хеш-функцій. Функція хешування SHA, MD5. Однонаправлені хеш-функції на основі симетричних блокових алгоритмів. Ключові і безключові функції хешування.

ТЕМА 10. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

Основні властивості цифрового підпису. Алгоритм цифрового підпису RSA. Алгоритм цифрового підпису Ель Гамаля. Алгоритм цифрового підпису DSA.

3.2 Тематика і зміст лекцій

№	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1.	Тема 1. Основні поняття захисту інформації в інформаційних системах	4	
2.	Тема 2. Класифікація погроз інформації в інформаційних системах. Рівні забезпечення безпеки інформації	4	1
3.	Тема 3. Сервіси та механізми програмного-технічного рівня захисту. інформації. Ідентифікації та аутентифікації користувачів інформаційних систем	4	1
4.	Тема 4. Управління доступом. Міжмережеві екрани. Технічні методи і засоби захисту інформації	2	1
5.	Тема 5. Основні положення щодо організації системи захисту інформації	4	1
6.	Тема 6. Концепція побудови системи безпеки установи	4	
7.	Тема 7 Служба захисту інформації установи	4	1
8.	Тема 8. Сутність комплексної системи захисту інформації і принципи її організації	2	
9.	Тема 9. Механізми забезпечення автентичності та цілісності даних	2	1
10.	Тема 10. Електронний цифровий підпис	2	
Усього годин		**32**	**6**

3.3 Тематика лабораторних робіт

№ з/п	Назва теми заняття	Обсяг у годинах	
		Денна форма	Заочна форма
1	№ 1. Розробка плану захисту інформації в автоматизованій системі.	4	1
2	№ 2. Класифікація інформації, що обробляється в ІС.	4	
3	№ 3. Опис компонентів АС та технології обробки інформації.	4	1
4	№ 4. Аналіз ризиків та загроз для інформації в ІС.	4	1
5	№ 5. Формування політики безпеки інформації в ІС.	4	1
6	№ 6. Аналіз і користування системою документів з забезпечення захисту інформації в ІС.	4	1
7	№ 7. Розробка календарного плану робіт з захисту інформації в ІС.	4	
8	№ 8. Створення цифрового підпису.	4	1
Усього годин		**32**	**6**

3.3 Самостійна робота здобувача (СРЗ)

№ з/п	Назва теми заняття	Обсяг у годинах	
		Денна форма	Заочна форма
1	Нормативно-правова база України у сфері ОЗЗІ.	8	12
2	Державна таємниця і конфіденційна інформація, що є власністю держави.	8	12
3	Звід відомостей, що становлять державну таємницю.	8	12

4	Види об’єктів захисту. Основні напрямки організаційного захисту інформації на підприємстві.	8	12
5	Розголошення інформації, яка захищається. Способи запобігання розголошення інформації, яка захищається.	8	12
6	Комерційна таємниця та порядок її визначення. Організація робіт з інформацією, яка є комерційною таємницею.	8	12
7	Організація внутрішньооб’єктного режиму на підприємстві. Організація охорони об’єктів підприємства. Організація інженерно-технічної безпеки.	8	12
8	Організація інформаційно-аналітичної роботи. Етапи виконання інформаційно-аналітичних досліджень виробничих ситуацій. Методи виконання аналітичних досліджень.	6	12
9	Організація роботи з персоналом підприємства Підбір та підготовка кадрів. Перевірка персоналу на благонадійність. Укладання контрактів та домовленостей про секретність. Особливості звільнення співробітників, які володіють конфіденційною інформацією.	6	10
10	Загальні вимоги до розробки технічного завдання на створення КСЗІ в ІТС.	6	12
11	Механізми забезпечення конфіденційності. Сервіс криптографічного захисту даних.	6	10
12	Механізми забезпечення автентичності та цілісності даних	6	10
	Усього годин	**86**	**138**

3.5 Індивідуальні завдання (ІЗ)

Здобувачі денної форми навчання виконують ІЗ у таких формах:

1) Написання реферату. Обсяг реферату має бути в межах 15-20 сторінок стандартного формату А4 у друкованому вигляді. Структура реферату: титульний аркуш; зміст; вступ; 2-3 пункти; висновки; список літератури.

Вимоги до оформлення реферату: текст розміщується на аркуші, обмеженому полями: зліва 25 мм, справа 10 мм; зверху та знизу - по 20 мм. На сторінці розміщується не більше ніж 28-30 рядків по 57-60 знаків у кожному (комп’ютерний набір - шрифт Times New Roman, 14 кегль, міжрядковий інтервал 1,5).тему реферату здобувач освіти обирає із запропонованого кафедрою переліку.

3) *Виконання індивідуального практичного завдання, які включені у* «Методичні вказівки до вивчення дисципліни «Основи ІС і захист даних»».

2) Підготовка і написання тез з тематики курсу з наступним опублікуванням.

Здобувачі *заочної форми* навчання виконують ІЗ у формі контрольної роботи відповідно до «Методичних вказівок до вивчення дисципліни «Основи ІС і захист даних»».

3.6 Форми поточного, проміжного та підсумкового контролю

Контрольні заходи з перевірки успішності засвоєння навчального матеріалу з освітньої компоненти включають: поточний контроль, виконання індивідуальних завдань, підсумковий контроль.

Поточний контроль має на меті перевірку виконання завдань як аудиторної, так і самостійної роботи здобувачів освіти та може проводитися в таких формах:

- захист звітів з виконання лабораторних робіт;
- усне, письмове опитування на аудиторних заняттях;

– перевірка виконання завдань СРЗ.

Контроль виконання ІЗ здійснюється у формі публічного захисту рефератів, перевірки виконання індивідуальних практичних завдань, контрольної роботи.

Формою підсумкового контролю є екзамен.

Семестровий екзамен – вид підсумкового контролю засвоєння здобувачами освіти теоретичного та практичного матеріалу за освітньою компонентою за семестр, що проводиться в період екзаменаційної сесії.

Форма проведення семестрового екзамену – електронне тестування. При проведенні підсумкового контролю у формі електронного тестування використовується набір тестових завдань, які містяться в бібліотеці електронних курсів системи дистанційного навчання СУРА для перевірки знань здобувачі освіти.

3.7 Методи викладання, навчання

Лекції (проблемні лекції, лекції-демонстрації з використанням мультимедійного обладнання).

Лабораторні роботи (виконання, оформлення звіту та захист).

Самостійне навчання (опрацювання підручників, посібників, наукових публікацій; виконання завдань самостійної роботи, індивідуальні завдання).

4 КРИТЕРІЇ І ПОРЯДОК ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Кожний вид поточної навчальної роботи здобувача оцінюються за 5-бальною шкалою.

Критерії оцінювання роботи здобувачів на семінарських, практичних, лабораторних заняттях, виконання завдань СРС:

Оцінка	Критерії оцінювання навчальних досягнень
5 балів	Оцінюється робота здобувача, який у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко та всебічно розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу, вільно послуговується науковою термінологією, розв'язує задачі стандартним або оригінальним способом, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки. Може аргументовано обрати раціональний спосіб виконання завдання й оцінити результати власної практичної діяльності; виконує завдання, не передбачені навчальною програмою; вільно використовує знання для розв'язання поставлених перед ним завдань.
4 бали	Оцінюється робота здобувача, який достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову літературу, розв'язує задачі стандартним способом, послуговується науковою термінологією. Але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки. За зразком самостійно виконує практичні завдання, передбачені програмою; має стійкі навички виконання завдання.
3 бали	Оцінюється робота здобувача, який відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні знання окремих положень, записує основні формули, рівняння, закони. Не здатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки. Планує та виконує частину завдання за допомогою викладача.
2 бали	Оцінюється робота здобувача, який не володіє навчальним матеріалом у достатньому обсязі, проте фрагментарно, поверхово (без аргументації та обґрунтування) викладає окремі питання навчальної дисципліни, не розкриває

Оцінка	Критерії оцінювання навчальних досягнень
	зміст теоретичних питань і практичних завдань. Виконує лише елементи завдання, потребує постійної допомоги викладача.
1 бал	Оцінюється робота здобувача, який не в змозі викласти зміст більшості питань теми та курсу, володіє навчальним матеріалом на рівні розпізнавання явищ, допускає істотні помилки, відповідає на запитання, що потребують однослівної відповіді. Виконує лише елементи завдання, потребує постійної допомоги викладача.
0 балів	Оцінюється робота здобувача, який не володіє навчальним матеріалом та не в змозі його висвітлити, не розуміє змісту теоретичних питань та практичних завдань.

Критерії оцінювання виконання ІЗ для дисциплін, вивчення яких завершується екзаменом:

Оцінка	Критерії оцінювання
10 балів	Оцінюється робота студента, який у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко та всебічно розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу, вільно послуговується науковою термінологією, розв'язує задачі стандартним або оригінальним способом, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки. Може аргументовано обрати раціональний спосіб виконання завдання й оцінити результати власної практичної діяльності; виконує завдання, не передбачені навчальною програмою; вільно використовує знання для розв'язання поставлених перед ним завдань.
8-9 балів	Оцінюється робота студента, який достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову літературу, розв'язує задачі стандартним способом, послуговується науковою термінологією. Але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки. За зразком самостійно виконує практичні завдання, передбачені програмою; має стійкі навички виконання завдання.
7 балів	Оцінюється робота студента, який відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні знання окремих положень, записує основні формули, рівняння, закони. Не здатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки. Планує та виконує частину завдання за допомогою викладача.
6 балів	Оцінюється робота студента, який не володіє навчальним матеріалом у достатньому обсязі, проте фрагментарно, поверхово (без аргументації та обґрунтування) викладає окремі питання навчальної дисципліни, не розкриває зміст теоретичних питань і практичних завдань. Виконує лише елементи завдання, потребує постійної допомоги викладача.
5 балів	Оцінюється робота студента, який не в змозі викласти зміст більшості питань теми та курсу, володіє навчальним матеріалом на рівні розпізнавання явищ, допускає істотні помилки, відповідає на запитання, що потребують однослівної відповіді. Виконує лише елементи завдання, потребує постійної допомоги викладача.
< 5 балів	Оцінюється робота студента, який не володіє навчальним матеріалом та не в змозі його висвітлити, не розуміє змісту теоретичних питань та практичних завдань.

Згідно з діючою в університеті системою комплексної діагностики знань здобувачів, з метою стимулювання планомірної та систематичної навчальної роботи, оцінка знань здобувачів здійснюється за 100-бальною системою.

Підсумкова оцінка виставляється на підставі суми накопичених балів здобувачем, отриманих у ході поточного, рубіжного контролів, виконання ІЗ, складання екзамену (підсумковий контроль).

Схема розподілу балів:

50 балів (поточний, рубіжний контроль)	10 балів (контроль виконання індивідуальних завдань)	40 балів (підсумковий контроль)

Мінімальний пороговий рівень з кожного виду контролю:

30 балів (поточний, рубіжний контроль)	5 балів (контроль виконання індивідуальних завдань)	25 балів (підсумковий контроль)

Підсумкова семестрова оцінка за 100-бальною шкалою переводиться у національну шкалу відповідно до таблиці:

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проєкту (роботи)	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

5 ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засобами оцінювання та методами демонстрування результатів навчання з вивчення навчальної дисципліни «Основи ІС і захист даних» є:

- тести;
- реферат;
- усні, письмові відповіді при проведенні контрольних заходів (рубіжний контроль);
- доповіді і виступи на аудиторних заняттях;
- усні відповіді під час проведення опитування на заняттях;
- звіти з виконання завдань СРЗ;
- звіти з виконання лабораторних робіт;
- звіти з виконання індивідуальних практичних завдань;
- презентації результатів виконаних завдань та досліджень.

6 ІНСТРУМЕНТИ, ОБЛАДНАННЯ, ПРОГРАМНЕ І МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Електронні ресурси: конспект лекцій, електронна бібліотека навчальної літератури, презентації окремих тем, банк тестів, методичні вказівки до вивчення дисципліни для здобувачів.

7 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Базова література:

1. Остапов С. Е., Жихаревич В.В., Добровольський Ю.Г. Сучасні методи та засоби захисту інформації. Чернівці: ЧНУ, 2021. 72 с.. 288 с. URL: https://archer.chnu.edu.ua/bitstream/handle/123456789/2831/%D0%A1%D1%83%D1%87%D0%B0%D1%81%D0%BD%D1%96%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%97%D0%86_%D0%90%D1%81%D0%BF.pdf?sequence=1&isAllowed=yf.

2. Концептуальні основи захисту інформаційного суверенітету України : монографія / О. В. Задерейко, О. В. Троянський, Р. І. Чанишев, А. І. Дика. Одеса : Фенікс, 2022. 220 с. URL: https://doi.org/10.32837/11300.22733.

3. Методологія інформаційних систем та баз даних: теоретичний і практичний підходи : навч. посібник / уклад. Ю.О. Ушенко, М.Л. Ковальчук, М.С. Гавриляк, А.Л. Негрич. Чернівці : Чернівецький нац. ун-т ім. Ю. Федьковича, 2021. 240 с. URL: https://archer.chnu.edu.ua/bitstream/handle/123456789/4106/%D0%A3%D1%88%D0%B5%D0%BD%D0%BA%D0%BE_%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC.pdf?sequence=1&isAllowed=y.

4. Захист інформації в комп'ютерних системах : підручник для студ. спец. 123 «комп'ютерна інженерія» / уклад. О. М. Гапак, С. І. Балога; рец. : М. І. Глебена. Ужгород : ПП "АУТДОР-ШАРК, 2021. 184 с. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/36506.

5. Інформаційна безпека : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. Ю.Я. Бобала, І.В. Горбатого. Львів : Львівська політехніка, 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf.

Основна література:

6. Хлапонін Ю. І. Комплексні системи захисту інформації : конспект лекцій. Київ: КНУБА, 2022. 84 с.. URL: https://repositary.knuba.edu.ua/server/api/core/bitstreams/6b05fa85-b573-4300-ad40-45b63e198ffa/content.

7. Кібербезпека та інформаційні технології : монографія. Х. : ТОВ «ДІСА ПЛЮС», 2020. 380 с. URL: https://kbpz.kntu.kr.ua/file/content/6633/2020-kiberbezpeka-ta-informatsiini-tekhnolohii-monohrafiia-.pdf.

8. Сучасні інформаційні технології в кібербезпеці : монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. ; за ред. В. К. Ободяка, І. В. Шелехова. Суми : Сумський державний університет, 2021. 348 с.. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/82619/3/Obodiak_kiberbezpeka.pdf.

9. Дудикевич, В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навч. пос. Вінниця : ВНТУ, 2018. 316 с. URL: https://pdf.lib.vntu.edu.ua/books/IRVC/Dudikevich_2018_316.pdf.

10. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018 446 с. URL: https://pdf.lib.vntu.edu.ua/books/2021/Zolotar_2018_446.pdf.

Нормативні джерела:

ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.

5. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

6. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

7. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

10. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

11. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

12. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

13. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.