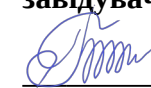


Затверджено
завідувач кафедри КІ



Ігор БУЧЕНКО

“ 31 ” серпня 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ »

Лектор курсу			Давиденко Анатолій Миколайович, д.т.н., проф., професор кафедри комп'ютерної інженерії		Контактна інформація лектора	E-mail: davidenkoan@gmail.com Тел.: 067 250 5314 код курсу в системі Google Classroom – a754t3au https://classroom.google.com/c/ODg2MTQ1MjY4NTM1?cjc=a754t3au	
Галузь знань			F «Інформаційні технології»		Рівень вищої освіти	магістр	
Спеціальність			F7 Комп'ютерна інженерія		Семестр	10	
Освітня програма			Комп'ютерні системи та технології		Тип дисципліни	Обов'язкова. Цикл дисциплін професійної підготовки	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка Курсова робота
			2	60	18	-	18

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	1. Математичні методи моделювання та оптимізації процесів 2. Технології штучного інтелекту 3. Дослідження та проектування комп'ютерних систем та мереж 4. Перспективні комп'ютерні системи та мережі 5. Адміністрування комп'ютерних систем
--	---

Освітні компоненти для яких є базовою	1. Науково-дослідна практика 2. Переддипломна практика 3. Кваліфікаційна робота
Мета курсу:	Вивчення принципів організації, побудови, проектування та функціонування комп'ютерних систем, схемотехнічних вузлів і пристроїв обчислювальної техніки.

Компетентності відповідно до освітньої програми	
Soft- skills / Загальні компетентності (ЗК)	Hard-skills / Спеціальні компетентності (СК)
ЗК7. Здатність приймати обґрунтовані рішення.	СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення. СК2. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизованого проектування. СК8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу. СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів.

Програмні результати навчання (РН)
РН4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань. РН6. Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення. РН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем. РН9. Планувати і виконувати наукові і прикладні дослідження з інформаційних технологій та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми; складати пропозиції щодо фінансування досліджень та/або проектів.

РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Теоретичні основи та управління доступом Рекомендовані джерела: [1, 6, 7]			
Заняття 1.1. Вступ до захисту даних. Основні поняття (CIA), класифікація загроз та вразливостей.	Лекція 1 2 год.		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.2. Аналіз вразливостей та оцінка ризиків комп'ютерної системи.	Практична робота 1 2 год.	4 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 1.3. Ідентифікація, аутентифікація та авторизація (AAA). Багатофакторна аутентифікація (MFA).	Лекція 2 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.4. Налаштування політик паролів та багатофакторної аутентифікації.	Практична робота 2 2 год.	4 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 1.5. Моделі розмежування доступу (дискретна, рольова - RBAC) в операційних системах.	Лекція 3 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.6. Налаштування прав доступу до файлів та ресурсів (ACL) у Windows/Linux.	Практична робота 3 2 год.	4 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 2. Криптографічні технології захисту даних. Рекомендовані джерела: [2, 6, 7]			
Заняття 2.1. Симетричні (AES) та асиметричні (RSA, ECC) криптографічні алгоритми.	Лекція 4 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.2. Використання утиліт шифрування файлів та дисків.	Практична робота 4	4 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь. Розгляд і оцінювання виконаних лабораторних робіт.

	2 год		
Заняття 2.3. Хеш-функції, цифрові підписи та Інфраструктура відкритих ключів (PKI).	Лекція 5 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.4. Генерація та використання ключів SSH/GPG, перевірка контрольних сум та підписання файлів.	Практична робота 5 2 год	4 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь. Розгляд і оцінювання виконаних лабораторних робіт.
Тема 3. Безпека мереж та баз даних Рекомендовані джерела: [3, 4, 6, 7]			

Заняття 3.1. Безпека мережевих передач. Базові принципи VPN, TLS/SSL та фаєрволів.	Лекція 6 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 3.2. Налаштування базового міжмережевого екрана (UFW / iptables) або простого VPN.	Практична робота 6 2 год.	4 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь. Розгляд і оцінювання виконаних лабораторних робіт.
Заняття 3.3. Захист баз даних: шифрування даних (At-Rest / In-Transit) та аудит подій безпеки.	Лекція 7 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 3.4. Шифрування чутливих даних у СУБД та аналіз логів подій безпеки.	Практична робота 7 2 год.	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь. Розгляд і оцінювання виконаних лабораторних робіт.

Тема 4. Відмовостійкість, резервне копіювання та аудит Рекомендовані джерела: [5, 6, 7]			
Заняття 4.1. Резервне копіювання (Backup): стратегії, правила (3-2-1) та незмінні сховища (Immutable).	Лекція 8 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 4.2. Створення та тестування плану резервного копіювання даних.	Практична робота 8 2 год	2 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь. Розгляд і оцінювання виконаних лабораторних робіт.
Заняття 4.3. Захист від сучасних загроз (Ransomware) та організаційні заходи безпеки.	Лекція 9 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 4.4. Розробка регламенту безпеки та комплексний міні-	Практична	4 бали	Усне опитування, виконання завдань на практичне

проект захисту робочої станції.	робота 9 2 год.		застосування знань і вмінь. Розгляд і оцінювання виконаних лабораторних робіт.
---------------------------------	--------------------	--	--

Самостійна робота			
Тема 1. Дослідження біометричних методів аутентифікації та їх вразливостей.	8 год.	5 балів	Огляд сучасних технологій ідентифікації за відбитками пальців, обличчям чи сітківкою ока та аналізують способи їх обходу (наприклад, підроблені відбитки або атаки за допомогою згенерованих фото).
Тема 2. Аналіз принципів роботи та наслідків атак програм-вимагачів (Ransomware).	8 год.	5 балів	Механізми проникнення шифрувальників у корпоративні мережі, алгоритми шифрування файлів та методи вимагання викупу. На основі реальних кейсів розробляються рекомендації щодо мінімізації збитків та ефективного реагування на такі інциденти.
Тема 3. Розробка інструкції з налаштування безпечного середовища для віддаленої роботи.	8 год.	5 балів	Створення практичний посібника із захисту домашнього або мобільного робочого місця співробітника компанії. Інструкція охоплює налаштування надійного VPN-з'єднання, шифрування локального диска, використання багатофакторної аутентифікації та правил безпечного поводження з електронною поштою.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ	
●	Мультимедійний проектор;
●	Комп'ютерний клас для проведення практичних занять

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Chapple M., Seidl D. CompTIA Security+ Study Guide: Exam SY0-701. 9th ed. Sybex, 2023. URL: <https://www.wiley.com/en-us/comptia-security-study-guide-with-over-500-practice-test-questions-exam-sy0-701-9th-edition-p-9781394211425> (дата звернення: 01.10.2026).
2. Aumasson J.-P. Serious Cryptography: A Practical Introduction to Modern Encryption. 2nd ed. No Starch Press, 2024. URL: <https://nostarch.com/serious-cryptography-2nd-edition> (дата звернення: 01.10.2026).
3. Andress J. Foundations of Cybersecurity: A Straightforward Introduction. 2nd ed. No Starch Press, 2026. URL: <https://nostarch.com/foundations-cybersecurity-2e> (дата звернення: 01.10.2026).
4. Захист інформації в комп'ютерних системах і кібербезпека, (Частина 1). Навчальний посібник / Лахно В.А., Гусев Б.С., Касаткін Д.Ю., Хорольська К.В. // – Київ: Редакційно видавничий відділ НУБіП України, 2023. – 301 с.
5. Meeuwisse R. Cybersecurity for Beginners. 2nd ed. Cyber Security Body of Knowledge, 2023. URL: <https://globalcybersecuritynetwork.com/resource/cybersecurity-for-beginners-by-raef-meeuwisse/> (дата звернення: 01.10.2026).
6. National Institute of Standards and Technology (NIST). (2023). NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.
7. OWASP Foundation. (2023). OWASP Top Ten: The Ten Most Critical Web Application Security Risks.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій, лабораторних і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за

завдання 0 балів.

- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є виконання всіх практичних робіт і виконання самостійних завдань, які передбачені структурою освітньої компоненти «Дослідження і проектування комп'ютерних систем і мереж».

Якщо студента не допущено до складання заліку, як такого, що не виконав індивідуальний план, йому надається час до перескладання для виконання всіх вимог допуску. Студент має право на два перескладання. При повторному перескладанні екзамену його у студента може приймати комісія, яка створюється директором ННІТ. Оцінка комісії є остаточною. У випадку отримання студентом 0 балів (неприйнятно), що тягне відрахування за невиконання навчального плану.

Оцінювання студентів здійснюється за накопичувальною 100-бальною системою і складається із двох основних оцінкових блоків і розподіляється в певних пропорціях 60 (бали напрацьовані під час вивчення дисципліни – Поточний контроль), 40 (підсумкове оцінювання - Екзамен):

Форми контролю	Види навчальної роботи	Оцінювання
Поточний контроль	● Виконання практичних робіт	40 балів
	● Самостійна робота	20 балів
Підсумкове оцінювання	Екзамен проходить у письмовій формі.	40 балів

Додаткова оцінка

Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:

- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні	5 балів
- Стаття в іноземному рецензованому виданні	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка /запис в екзаменаційній відомості
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	Достатній Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (В)
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та	Достатній Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (С)

	поясненні прийнятих рішень, в межах дисципліни, що вивчається.		
67-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	Середній Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-66	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	Середній Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену/заліку.	Незадовільний Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) В залікову книжку не представляється