ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
Декан математичного факультету
(підпис) С.І. Гоменюк
(ініціали та прізвище)
«01» вересня 2025 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

підготовки бакалаврів

денної та заочної форми здобуття освіти

освітньо-професійна програма «Комп’ютерні науки»

спеціальності 122 Комп’ютерні науки

галузі знань 12 Інформаційні технології

ВИКЛАДАЧ: Решевська Катерина Сергіївна, к.т.н., доцент, доцент кафедри комп’ютерних наук

Обговорено та ухвалено
на засіданні кафедри комп’ютерних наук

Протокол №1 від «25» серпня 2025 р.
Завідувач кафедри комп’ютерних наук
_____Г. М. Шило

Погоджено
Гарант освітньо-професійної програми
_____Н. В. Матвіїшина

2025 рік

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Технології захисту інформації

Зв`язок з викладачем: Решевська Катерина Сергіївна
E-mail: reshka82zp@gmail.com
Сезн ЗНУ повідомлення: https://moodle.znu.edu.ua/course/view.php?id=4202
Телефон (кафедра): 289-12-57
Кафедра комп'ютерних наук, ауд. №39, 1 корпус ЗНУ

1. Опис навчальної дисципліни

Опанування технологій захисту інформації є ключовою складовою професійної підготовки фахівців у галузі комп'ютерних наук, оскільки в умовах цифровізації та зростання обсягів даних питання забезпечення конфіденційності, цілісності й доступності інформації набувають особливої актуальності.

Метою вивчення навчальної дисципліни «Технології захисту інформації» є є формування у студентів знань з методів, засобів і принципів захисту інформації в сучасному інформаційному середовищі.

Основними **завданнями** вивчення дисципліни «Технології захисту інформації» є:

- ознайомлення з основними поняттями і термінами;
- вивчення загроз інформаційній безпеці;
- розгляд сучасних криптографічних протоколів;
- оволодіння методами шифрування даних та схемою підписання електронно-цифрового підпису.

Дисципліна «Технології захисту інформації» вивчається у 6-му семестрі. Необхідними для вивчення дисципліни «Технології захисту інформації» є знання, уміння і навички, засвоєні при вивченні дисциплін «Комп'ютерні мережі», «Операційні системи», «Бази даних та інформаційні системи». Дисципліна «Технології захисту інформації» може служити підготовчою базою для вивчення дисципліни «Проєктування програмних систем», для виконання кваліфікаційної роботи бакалавра.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Технології захисту інформації

Паспорт навчальної дисципліни

Нормативні показники	**денна форма здобуття освіти**	**заочна форма здобуття освіти**
1	***2***	***3***
Статус дисципліни	**Обов'язкова**	
Семестр	6-й	6-й
Кількість кредитів ECTS	4	4
Кількість годин	120 год.	120 год.
Лекційні заняття	24 год.	6 год.
Лабораторні заняття	24 год.	6 год.
Самостійна робота	72 год.	108 год.
Консультації	За розкладом; дистанційно	
Вид підсумкового семестрового контролю:	**екзамен**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=4202	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	**Методи навчання**	**Форми і методи оцінювання**
Компетентності		
Здатність до абстрактного мислення, аналізу та синтезу	лекція-візуалізація, пояснення, демонстрація, виконання завдань лабораторних робіт, метод-мікрофон	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Здатність застосовувати знання у практичних ситуаціях	лекція-візуалізація, кейс-метод пояснення, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Знання та розуміння предметної області та розуміння професійної діяльності	лекція-візуалізація, пояснення, демонстрування, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Здатність вчитися і оволодівати сучасними знаннями	лекція-візуалізація, пояснення,	**Поточний контроль**: захист лабораторних робіт,

Компетентності/ результати навчання	Методи навчання	Форми і методи оцінювання
	демонстрування, виконання завдань лабораторних робіт, аналіз	опитування, тестування **Підсумковий контроль:** тестування
Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури	лекція-візуалізація, пояснення, демонстрування, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Програмні результати навчання		
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	лекція-візуалізація, пояснення, демонстрування, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв’язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об’єктів інформатизації.	лекція-візуалізація, пояснення, демонстрування, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних	лекція-візуалізація, пояснення, демонстрування, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування

3. Зміст навчальної дисципліни

Змістовий модуль 1. Основи теорії захисту інформації

Вступ до курсу «Технології захисту інформації». Поняття захисту інформації та інформаційної безпеки. Основні цілі захисту інформації:

конфіденційність, цілісність і доступність. Аутентифікація та авторизація як механізми контролю доступу до інформаційних ресурсів. Організаційні, програмні та технічні заходи захисту інформації. Основні технології захисту інформації: шифрування, файрволи, антивірусні та антималware засоби, системи виявлення та запобігання вторгненням, аудит і журналювання подій.

Забезпечення цілісності даних у процесах зберігання та передавання інформації. Хешування як механізм контролю цілісності даних. Властивості криптографічних хеш-функцій та їх застосування. Основні алгоритми хешування: контрольні суми, MD5, SHA та їх характеристики. Хешування файлів, цифрових носіїв і паролів. Додавання солі та розтягнення ключа як методи підвищення стійкості хешування. Коди автентифікації повідомлень HMAC та їх використання для забезпечення цілісності й автентичності даних.

Змістовий модуль 2. Криптографічні алгоритми. Симетричні криптоалгоритми

Вступ до криптографії та криптології як науки про створення і злам секретних кодів. Поняття криптографії та її роль у забезпеченні конфіденційності інформації. Шифрування як процес перетворення відкритого тексту у зашифрований та дешифрування як зворотний процес. Поняття відкритого тексту, криптограми та криптографічного ключа. Роль ключа в забезпеченні безпеки криптографічних алгоритмів. Історичний розвиток криптографії та приклади класичних методів шифрування: скитала, шифр Цезаря, шифр Віженера, машина Enigma. Алгоритм і шифр як основа криптографічних перетворень. Основні методи створення криптограм: транспозиція, заміна та схема одноразових шифроблокнотів. Принцип сучасної криптографії, що базується на відкритості алгоритмів і секретності ключів. Керування криптографічними ключами як критичний елемент безпеки криптосистем. Класифікація алгоритмів шифрування за способом використання ключів. Симетричне шифрування з використанням спільного секретного ключа та його особливості. Асиметричне шифрування з використанням відкритого і закритого ключів та його переваги і недоліки. Процес симетричного шифрування та проблеми масштабування керування ключами. Типи криптографічних перетворень: блокові та потокові шифри. Блокові шифри та їх принцип роботи з даними фіксованої довжини. Потокові шифри та їх особливості шифрування бітів або байтів у реальному часі. Комбінування блокових і потокових методів у складних криптографічних системах. Основні симетричні алгоритми шифрування: DES, 3DES, IDEA та AES. Особливості алгоритму 3DES і підвищення стійкості за рахунок багаторазового шифрування. Алгоритм IDEA та його застосування в системах PGP і GPG. Алгоритм AES як сучасний стандарт шифрування та його використання для захисту інформації високого рівня.

Змістовий модуль 3. Асиметричні алгоритми шифрування

Поняття асиметричної криптографії та її місце в системі захисту інформації. Проблема розподілу ключів у класичній криптографії та шляхи її розв'язання. Протокол обміну ключами Діффі–Хеллмана, його принцип роботи та роль у формуванні спільного секретного ключа через незахищений канал зв'язку. Історія розвитку криптографії з відкритим ключем та внесок Вітфілда Діффі, Мартіна Хеллмана і Ральфа Меркла. Поняття пари ключів: відкритого та закритого, і принцип неможливості відновлення закритого ключа з відкритого. Вразливості алгоритму Діффі–Хеллмана та атака «людина посередині», необхідність використання механізмів аутентифікації. Алгоритм RSA як перший практичний асиметричний алгоритм шифрування, його математична основа та застосування для шифрування і цифрового підпису. Керування криптографічними ключами: створення, обмін, зберігання, використання та заміна ключів. Поняття довжини ключа та простору ключів, їх вплив на стійкість криптосистем. Порівняння симетричних і асиметричних методів шифрування за ефективністю, швидкодією та сферою застосування. Комбіноване використання асиметричної криптографії для обміну ключами та симетричної криптографії для захисту великих обсягів даних. Практичні застосування асиметричних алгоритмів у протоколах SSL/TLS, SSH, IKE, PGP та технологіях VPN і IPsec.

Змістовий модуль 4. Керування відкритими ключами інфраструктура відкритих ключів (PKI)

Поняття керування відкритими ключами в асиметричній криптографії та його роль у безпечному обміні даними в Інтернеті. Сертифікати SSL/TLS як цифрові посвідчення автентичності веб-сайтів та їх структура: відкритий ключ, центр сертифікації, період дії, алгоритм підпису. Центри сертифікації (CA) та їх роль у перевірці ідентичності і видачі сертифікатів, приклади комерційних та безкоштовних CA. Інфраструктура відкритих ключів (PKI): компоненти, процес створення, зберігання, розповсюдження та відкликання сертифікатів; база даних сертифікатів; сховище сертифікатів; роль кореневого CA. Класи сертифікатів PKI та рівні довіри. Топології PKI: однокоренева, ієрархічна, перехресна, гібридна. Оперативна сумісність PKI із протоколами SSL/TLS, IPsec, S/MIME, EAP-TLS та каталогами LDAP/X.500. Реєстрація, аутентифікація і відкликання сертифікатів: сертифікати самопідписані, CRL та OCSP. Практичне застосування PKI на підприємстві: аутентифікація, захист мережного та веб-трафіку, контроль доступу, підписання коду, шифрування файлів, двофакторна аутентифікація. Виклики безпеки при використанні PKI та SSL/TLS: шифрування трафіку, перевірка сертифікатів, моніторинг мережі, захист від шкідливих програм і витоків даних.

Змістовий модуль 5. Безпека ОС Windows

Поняття безпеки операційної системи Windows та її роль у захисті даних і контролі доступу користувачів. Еволюція ОС Windows від MS-DOS до сучасних версій Windows 10/11, зокрема розвиток графічного інтерфейсу користувача, багатопроцесності та підтримки 64-розрядних систем. Архітектура Windows: рівень апаратної абстракції (HAL), ядро, драйвери пристроїв, режим користувача та режим ядра, ізоляція процесів та захист адресного простору. Вразливості ОС та загрози безпеки: шкідливе ПЗ, несанкціонований доступ, помилки драйверів та програм. Засоби захисту Windows: Windows Defender, брандмауер, контроль служб, налаштування прав доступу, шифрування даних, політики безпеки, складні паролі та обмеження прав адміністратора. Механізми контролю доступу та автентифікації користувачів: облікові записи, групи, Active Directory, управління політиками безпеки та журналювання подій. Оновлення та патчі як важливий елемент захисту ОС від відомих уразливостей. Практичне застосування безпекових механізмів на підприємстві: захист робочих станцій та серверів, контроль доступу до ресурсів, шифрування даних на дисках, захист мережного трафіку, підвищення стійкості до шкідливого ПЗ та витоків конфіденційної інформації. Виклики безпеки при використанні Windows: складність конфігурації, своєчасне оновлення, взаємодія з корпоративними мережами, захист від фішингу та експлойтів, контроль привілейованих користувачів та адміністраторів.

Змістовий модуль 6. Комплексна безпека інформаційних ресурсів: мережеві, хмарні та фізичні аспекти

Хмарна безпека та її роль у захисті даних, застосунків і інфраструктури в середовищі хмарних обчислень. Основи віртуалізації: віртуальні машини, контейнери та віртуальні робочі столи як базові компоненти хмарних сервісів. Модель спільної відповідальності між постачальником хмарних послуг і клієнтом, залежно від типу хмарного розгортання та сервісної моделі.

Поняття контролю доступу та його роль у захисті фізичних, інформаційних і мережних ресурсів організації. Фізичні засоби контролю доступу: охорона, периметральні бар’єри, замки, смарт-картки, відеоспостереження, системи виявлення вторгнень і mantrap-системи. Логічні засоби контролю доступу: паролі, шифрування, біометрія, списки контролю доступу, брандмауери, маршрутизатори та системи виявлення вторгнень.

Фізичний захист інформаційних систем: огорожі, бар’єри, вимоги до їх конструкції та обслуговування як першого рівня безпеки. Біометричні системи аутентифікації, їх переваги, обмеження, критерії вибору та типи помилок (помилкове відхилення і помилкове схвалення).

4. Структура навчальної дисципліни

Вид заняття /роботи	Назва теми	Кількість годин		Згідно з розкладом
		о/д. ф.	з.ф.	
Лекція 1	Основні положення теорії захисту інформації. Засоби захисту інформації. Безпека ОС Windows. Криптографія. Хешування даних.	2	0,5	тиждень 1
Лабораторне заняття 1	Хешування. Знайомство з бібліотекою OpenSSL	2	0,5	тиждень 1
Лекція 2	Симетричні криптосистеми.	2	0,5	тиждень 2
Лабораторне заняття 2	Симетричне шифрування засобами OpenSSL.	2	0,5	тиждень 2
Лекція 3	Криптографія з відкритим ключем	4	1	тиждень 3, 4
Лабораторне заняття 3	Шифрування із відкритим ключем засобами OpenSSL	4	1	тиждень 3,4
Лекція 4	Електронно-цифровий підпис. Алгоритми і засоби реалізації	4	1	тиждень 5,6
Лабораторне заняття 4	Електронний цифровий підпис	4	1	тиждень 5,6
Лекція 5	Електронно-цифровий підпис. Алгоритми і засоби реалізації	4	1	тиждень 7,8
Лабораторне заняття 5	Електронний цифровий підпис	4	1	тиждень 7,8
Самостійна робота	Дослідження використання хешування, симетричних та асиметричних алгоритмів у криптографічних протоколах і службах безпеки	36	54	тиждень 1-8
Лекція 6	Безпека ОС Windows	4	1	тиждень 9,10
Лабораторне заняття 6	Моніторинг і керування системними ресурсами в Windows	4	1	тиждень 9, 10
Лекція 7	Комплексна безпека інформаційних ресурсів: мережеві, хмарні та фізичні аспекти	4	1	тиждень 11, 12
Лабораторне заняття 7	Класифікація сповіщень у середовищі Windows та Unix/Linux	4	1	тиждень 11, 12
Самостійна робота	Забезпечення інформаційної безпеки в середовищі хмарних сервісів	36	54	тиждень 9-12

5. Види і зміст контрольних заходів

Вид заняття /роботи	Вид контрольного заходу	Зміст контрольного заходу	Критерії оцінювання та термін виконання	Усього балів
Поточний контроль				
Лабораторна робота №1	Захист лабораторної роботи №1	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=4202), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –1	4
Лабораторна робота №2	Захист лабораторної роботи №2	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=4202), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –1	4
Лабораторна робота №3	Захист лабораторної роботи №3	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=4202), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –1	4
Лабораторна робота №4	Захист лабораторної роботи №4	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=4202), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –1	4
Лабораторна робота №5	Захист лабораторної роботи №5	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=4202), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –1	4
Самостійна робота	Тестування	Тестові завдання в Тестах 1,2		
Поточний контроль	Тест 1	Відповіді на 10 тестових питань (https://moodle.znu.edu.ua/course/view.php?id=4202)	10 питань по 1 балу	10
Поточний контроль	Тест 2	Відповіді на 10 тестових питань (https://moodle.znu.edu.ua/course/view.php?id=4202)	10 питань по 0,5 балів	5
Лабораторна робота №6	Захист лабораторної роботи №6	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=4202), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –4; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –1	5
Лабораторна робота №7	Захист лабораторної роботи №7	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=4202), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –4; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –1	5
Самостійна робота	Тестування	Тестові завдання В тестах 3,4,5,6		
Поточний контроль	Тест 3	Відповіді на 10 тестових завдання (https://moodle.znu.edu.ua/cour	10 питань по 0,5 бала	5

Вид заняття /роботи	Вид контрольного заходу	Зміст контрольного заходу	Критерії оцінювання та термін виконання	Усього балів
		se/view.php?id=4202)		
Поточний контроль	Тест 4	Відповіді на 10 тестових завдання (https://moodle.znu.edu.ua/course/view.php?id=4202)	10 питань по 0,3 бала	3
Поточний контроль	Тест 5	Відповіді на 10 тестових завдання (https://moodle.znu.edu.ua/course/view.php?id=4202)	10 питань по 0,3 бала	3
Поточний контроль	Тест 6	Відповіді на 10 тестових завдання (https://moodle.znu.edu.ua/course/view.php?id=4202)	10 питань по 0,4 бала	4
Усього за поточний контроль				**60**
Підсумковий контроль				
Форма підсумкового контролю	**Вид підсумкового контрольного заходу**	**Зміст підсумкового контрольного заходу**	**Критерії оцінювання**	**Усього балів**
Екзамен	Питання тесту	30 питань (https://moodle.znu.edu.ua/course/view.php?id=4202)	Одне теоретичне питання №1-20 -1 бал, одне теоретичне питання №20-30 – 2 бали	**40**
Усього за підсумковий контроль				**40**

Шкала оцінювання ЗНУ: національна та ECTS

За шкалою ***ECTS***	**За шкалою університету**	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

6. Основні навчальні ресурси

Рекомендована література

1. Жуковицький І. В., Остапець Д. О. Захист інформації в комп'ютерних мережах / за ред. І. В. Жуковицького ; Укр. держ. ун-т науки і технологій. Дніпро : УДУНТ, 2024. 146 с.

2. Зубок В. Ю., Мохор В. В. Кібербезпека топології Internet : монографія. Київ : ІПМЕ ім. Г. Є. Пухова, 2022. 191 с.

3. Основи технологій захисту інформації. Завдання до практичних занять : навч. посіб. / уклад.: В. В. Демчинський, М. В. Грайворонський, О. В. Кіреєнко. Київ : КПІ ім. Ігоря Сікорського, 2022. 107 с.

4. Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 135 с.

5. Терейковський І. А., Корченко А. О. Інтелектуалізовані методи захисту інформації: нейронні мережі в захисті інформації : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 176 с.

6. Терейковський І. А., Корченко О. Г., Погорелов В. В. Методи розпізнавання кібератак: розпізнавання комп'ютерних вірусів : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 127 с.

7. Benson V., Mcalaney J. Emerging Cyber Threats and Cognitive Vulnerabilities. London : Academic Press, 2020. 252 p.

8. Trends in Data Protection and Encryption Technologies / V. Mulder, A. Mermoud, V. Lenders, B. Tellenbach (eds.). Cham : Springer, 2023. 262 p.

9. Zheng Z. Modern Cryptography: A Classical Introduction to Informational and Mathematical Principle. Vol. 1. Singapore : Springer, 2022. 359 p.

10. Zheng Z., Tian K., Liu F. Modern Cryptography : A Classical Introduction to Informational and Mathematical Principle. Vol. 2. Singapore : Springer, 2023. 191 p.

Інформаційні ресурси

1. Онлайн платформа Networking Academy: URL: https://skillsforall.com/course/networking-basics?courseLang=en-US
2. Каталог нормативних документів, який містить українські стандарти. URL: https://csm.kiev.ua/nd/nd.php?b=1&l=32442&utm_source=chatgpt.com.
3. Стандарти для локальних/міських мереж (Networking) у міжнародній системі стандартів – класифікація по ISO/IEC/IEEE URL: https://www.iso.org/ics/35.110/x/

7. Регуляції і політики курсу

Відвідування занять. Регуляція пропусків.
Відвідування усіх занять є обов'язковим. Студенти зобов'язані дотримуватися усіх строків, визначених для виконання усіх видів робіт, передбачених даною дисципліною. Пропуски та запізнення на заняття є недопустимими.

Політика академічної доброчесності
Кожний студент зобов'язаний дотримуватися принципів академічної доброчесності. Письмові завдання з використанням часткових або повнотекстових запозичень з інших робіт без зазначення авторства – це *плагіат*. Використання будь-якої інформації (текст, фото, ілюстрації тощо) мають бути правильно процитовані з посиланням на автора! Якщо ви не впевнені, що таке плагіат, фабрикація, фальсифікація, порадьтеся з викладачем. До студентів, у роботах яких буде виявлено списування, плагіат чи інші прояви недоброчесної поведінки можуть бути застосовані різні дисциплінарні заходи (див. посилання на Кодекс академічної доброчесності ЗНУ в додатку до силабусу). Неприпустиме складання роботи, виконаної іншою особою.

Використання комп'ютерів/телефонів на занятті
Використання мобільних телефонів, ноутбуків та інших гаджетів під час лекційних та лабораторних занять дозволяється виключно у навчальних цілях (з активованим режимом «без звуку»).

Комунікація
Комунікація викладача зі студентами здійснюється безпосередньо на заняттях та додатково за допомогою месенджерів (наприклад, Telegram), електронної пошти і в СЕЗН Moodle (форум курсу, приватні повідомлення)

Визнання результатів неформальної та інформальної освіти
Здобувачі освіти мають право на визнання результатів навчання, отриманих поза межами формальної освітньої програми (неформальна та інформальна освіта). Результати можуть бути зараховані як виконання окремих тем, розділів, видів навчальних занять, завдань самостійної роботи, за умови їх відповідності програмним результатам навчання.
Успішне проходження курсів на онлайн платформах (наприклад, Prometheus, Coursera, edX, Udemy тощо), зміст яких корелює з тематикою дисципліни та вказаних в електронному курсі дисципліни в СЕЗН ЗНУ на платформі Moodle, може бути зараховано згідно з правилами визначеними в Положенні ЗНУ Про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти (https://surl.li/gachqj).

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ НА 2025-2026 н.р. доступний за адресою: https://surl.li/vlweoj

НАВЧАННЯ ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів Запорізького національного університету: https://surl.li/wdzjrl

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН. Наявність академічної заборгованості до 6 навчальних дисциплін (у тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Процедура повторного вивчення визначається Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: https://surl.lu/hfjbya

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ: https://surl.li/qgacqa
Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до:
Положення про порядок призначення і виплати академічних стипендій у ЗНУ: https://surl.li/unwzzm
Положення про призначення та виплату соціальних стипендій у ЗНУ: https://surl.lu/xkxmuz

ПСИХОЛОГІЧНА ДОПОМОГА. Кабінет практичного психолога **Марті Ірини Вадимівни –** навч. корп. №4, каб. №235 (понеділок, середа, четвер 9.00-11.00, 13.00-15.00), навч. корп. №9 (ІННІ) каб.57 (п'ятниця 9.00-11.00, 13.00-15.00), гуртожиток №6 (вул. Добролюбова, 19, середа 9.00-11.00, 13.00-15.00). Попередній запис за тел.: 228-76-48, (099) 253-78-73 щоденно з 9 до 15.

УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КОРУПЦІЇ Запорізького національного університету: **Банах Віктор Аркадійович**
Електронна адреса: v_banakh@znu.edu.ua

Гаряча лінія: тел. (061) 227-12-76, факс 227-12-88

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Спеціалізована допомога: (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://surl.li/ivcwih

РЕСУРСИ ДЛЯ НАВЧАННЯ

НАУКОВА БІБЛІОТЕКА: http://library.znu.edu.ua. Графік роботи абонементів: понеділок-п`ятниця з 08.00 до 16.00; вихідні дні: субота і неділя.

СИСТЕМА ЕЛЕКТРОННОГО ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ ЗАПОРІЗЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ (СЕЗН ЗНУ): https://moodle.znu.edu.ua.
Посилання для відновлення паролю: https://moodle.znu.edu.ua/mod/page/view.php?id=133015.

ЦЕНТР ІНТЕНСИВНОГО ВИВЧЕННЯ ІНОЗЕМНИХ МОВ: http://sites.znu.edu.ua/child-advance/