ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІМ. Ю.М. ПОТЕБНІ
ЗАПОРІЗЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ

ЗАТВЕРДЖУЮ
Директор Інженерного навчально-наукового
інституту ім. Ю.М. Потебні ЗНУ

_____ Наталя МЕТЕЛЕНКО
(підпис) (ініціали та прізвище)
«_____»_____2025 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
СУЧАСНА КРИПТОГРАФІЯ
(назва навчальної дисципліни)
підготовки _____магістра_____
(назва освітнього ступеня)
денної та заочної форм здобуття освіти

освітньо-професійна програма Інженерія програмного забезпечення
(назва)
спеціальності F2 Інженерія програмного забезпечення
(шифр, назва спеціальності)
галузі знань F Інформаційні технології
(шифр і назва)

ВИКЛАДАЧ (-ЧІ): _Скрипник Ірина Анатоліївна, кандидат фізико-математичних наук, доцент
(ПІБ, науковий ступінь, вчене звання, посада)

Обговорено та ухвалено
на засіданні кафедри електроніки, інформа-
ційних систем та
програмного забезпечення

Протокол №1 від “ ”серпня 2025 р.
Завідувач кафедри
_____Т.В. Критська
(підпис) (ініціали, прізвище)

Погоджено
Гарант освітньо-професійної програми
_____В.І. Горбенко
(підпис) (ініціали, прізвище)

2025 рік

Зв`язок з викладачем:
E-mail: sia@zsea.edu.ua , sia_zap16@gmail.com
СЕЗН ЗНУ повідомлення: *форум курсу, приватні повідомлення*
Телефон: *095-539-07-33*
Інші засоби зв'язку:

- *Microsoft Teams (студенти долучаються з особистим логіном/паролем за посиланням в інструменті Календар)*
- *Telegram (095-539-07-33)*
- *Viber (095-539-07-33)*

Кафедра: *програмного забезпечення автоматизованих систем, 9 корпус, ауд. 41а*

1. Опис навчальної дисципліни

*Курс має на **меті** вивчення теорії інформаційної безпеки комп'ютерних систем, необхідної для їх надійного і безпечного функціонування, принципів захисту інформації, що передається віддаленим користувачам, від несанкціонованого доступу, криптографічних методів захисту інформації; набуття навичок розробки криптографічних протоколів та їх реалізації.*

Зокрема, ознайомлення з методами і алгоритмами класичної криптографії, вивчення принципів інформаційної безпеки комп'ютерних систем, криптографічних методів захисту інформації, симетричних та асиметричних криптографічних систем, криптографічних протоколів, методів ідентифікації та автентифікації, генерації та перевірки цифрових підписів, генерації ключової інформації, протоколів застосування ключів та керування ними для забезпечення цілісності інформації, ознайомлення з комп'ютерними вірусами, їх типами та принципами дії.

Оволодіння знаннями та навичками в області сучасної криптографії стане основою розвинення професійних компетенцій майбутніх магістрів.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У разі успішного завершення курсу студент <u>зможе</u>:
вміти:

- *створювати криптографічні системи;*
- *застосовувати алгоритми симетричного шифрування до будь-якої інформації;*
- *застосовувати алгоритми асиметричного шифрування до будь-якої інформації;*
- *виконувати ідентифікацію та автентифікацію;*
- *генерувати криптографічні ключі;*
- *застосовувати технології розробки криптографічних протоколів;*
- *за допомогою існуючих (вбудованих) або розроблених криптографічних засобів виконувати безпечний інформаційний обмін.*

Паспорт навчальної дисципліни

Нормативні показники	денна форма здобуття освіти	заочна форма здобуття освіти
Статус дисципліни	**Вибіркова дисципліна в межах спеціальності**	
Семестр	3-й	3-й
Кількість кредитів ECTS	**4**	
Кількість годин	120	
Лекційні заняття	12 год.	6 год.
Лабораторні заняття	22 год.	6 год.
Самостійна робота	86 год.	108 год.
Консультації	Дистанційно в Microsoft Teams за розкладом в інструменті Календар: https://outlook.office365.com/	
Вид підсумкового семестрового контролю:	**залік**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=8595	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

КОМПЕТЕНТНОСТІ/ результати навчання	Методи навчання	Форми і методи оцінювання
Загальні компетентності: ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.	словесні методи (лекція, пояснення, розповідь, дискусія); - практичні методи (лабораторні заняття); наочні методи (метод ілюстрацій і метод демонстрацій); - логічні методи (аналітичний, індуктивний, дедуктивний); - проблемний виклад (частковопошуковий, дослідницький); - робота з навчально-методичною літературою (конспектування, анотування).	
Спеціальні (фахові, предметні) компетентності: СК 7. Володіння знаннями про інформаційні моделі даних, здатність створювати програм-	- словесні методи (лекція, пояснення, розповідь, дискусія); - практичні методи (лабораторні заняття); - наочні методи (метод ілю-	

не забезпечення для зберігання, видобування та опрацювання даних. СК11. Здатність застосовувати та розвивати фундаментальні та міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення, зокрема задач сучасної криптографії.	страцій і метод демонстрацій); - логічні методи (аналітичний, індуктивний, дедуктивний); - проблемний виклад (частково-пошуковий, дослідницький); - робота з навчально-методичною літературою (конспектування, анотування).	
Програмні результати навчання: РН03. Будувати і досліджувати моделі інформаційних процесів у прикладній області, зокрема сучасній криптографії. РН05. Розробляти, аналізувати, обґрунтовувати та систематизувати вимоги до програмного забезпечення. РН16. Планувати, організовувати та здійснювати тестування, верифікацію та валідацію програмного забезпечення. РН17. Збирати, аналізувати, оцінювати необхідну для розв'язання наукових і прикладних задач інформацію, використовуючи науково-технічну літературу, бази даних та інші джерела. Програмні результати, визначені закладом вищої освіти та освітньою програмою РН19. Розвивати та застосовувати фундаментальні та міждисциплінарні знання для розв'язання завдань інженерії програмного забезпечення		Методи контролю і самоконтролю: усний, письмовий, лабораторно-практичний. Контрольні заходи: теоретичне тестування за змістовим модулем, захист лабораторних робіт.

Міждисциплінарні зв'язки. Дисципліна «Сучасна криптографія» є вибірковою в межах спеціальності, передбачає використання знань та навичок, набутих з дисциплін «Професійно-орієнтована підготовка», «Програмування із застосуванням технології dotNET». Набуті при вивченні даного курсу знання необхідні студентам для здійснення безпечних інформаційних обмінів в подальшій діяльності у сфері інженерії програмного забезпечення.

3. Зміст навчальної дисципліни

Змістовий модуль 1. **Принципи побудови криптографічних систем**.

Складові комп'ютерної безпеки. Класифікація задач інформаційного обміну. Типи криптографічних перетворень. Ключові дані. Типи криптографічних алгоритмів.

Змістовий модуль 2. **Симетричні криптографічні системи**.

Алгоритми блочного шифрування. Схема Фейстеля. Побудова симетричної криптографічної системи. Стандарти симетричного блокового шифрування. DES. Стійкість DES. Стандарт шифрування ДСТУ: ГОСТ 28147-2009. Режими шифрування. Гамування. Стандарт AES: особливості та переваги. Стійкість симетричних алгоритмів.

Змістовий модуль 3. **Асиметричні криптографічні системи**.

Елементи теорії чисел. Модульна арифметика. Розширений алгоритм Евкліда. Функція Ейлера. Односторонні функції. Асиметричні алгоритми. Ключова інформація. Стандарт асиметричного шифрування RSA. Стійкість RSA.

Змістовий модуль 4. **Електронні цифрові підписи**.

Поняття цифрового підпису (ЦП). Концепція формування. Хеш-функції. SHA, MD5. Стандарти ЦП: RSA, DSA. Еліптичні криві. Скінченні поля. Поле Галуа. Алгоритм ECDSA. Стандарт ЦП ДСТУ 4045.

Змістовий модуль 5. **Криптографічні протоколи.**

Поняття криптографічного протоколу. Вимоги. Класифікації. Протоколи ключового обміну. Протоколи ідентифікації, автентифікації. Протоколи ЦП, передачі інформації. Формальний аналіз протоколів. Специфікації протоколів. BAN-логіка. Ідеалізована форма протоколів. Автоматна моделі протоколу автентифікації.

4. Структура навчальної дисципліни

Вид заняття /роботи	Назва теми	Кількість годин		Згідно з розкладом
		о/д.ф.	з.ф.	
Лекція 1	Тема. Складові комп'ютерної безпеки. Класифікація задач інформаційного обміну. Типи криптографічних перетворень. Принципи побудови криптографічних систем.	2	1	*щотижня*
Лекція 2	Тема. Алгоритми блочного шифрування. Схема Фейстеля. Стандарти симетричного шифрування. DES. ДСТУ: ГОСТ 28147-2009. AES	2	1	
Лекція 3	Тема. Модульна арифметика. Розширений алгоритм Евкліда. Функція Ейлера. Односторонні функції. Стандарт асиметричного шифрування RSA.	2	1	
Лекція 4	Тема. Поняття цифрового підпису (ЦП). Концепція формування ЦП. Хеш-функції. SHA, MD5. Стандарти ЦП RSA, DSA.	2	1	
Лекція 5	Тема. Еліптичні криві. Скінченні поля. Поле Галуа. Алгоритм ECDSA. Стандарт ЦП ДСТУ 4045.	2	1	
Лекція 6	Тема. Поняття криптографічного протоколу. Протоколи ключового обміну, ідентифікації, автентифікації.	2	1	

Лабораторне заняття 1	Тема. Дослідження стандартів блочного шифрування (з секретним ключем) із вбудованих бібліотек dot-NET, Python. Розміщено в СЕЗН ЗНУ.	2	1	*щотижня*
Лабораторне заняття 2	Тема. Реалізація алгоритму DES (Data Encryption Standard) засобами dotNET, Python. Розміщено в СЕЗН ЗНУ.	2	1	
Лабораторне заняття 3	Тема. Дослідження стандартів симетричного шифрування з секретним ключем із вбудованих бібліотек dotNET, Python. Розміщено в СЕЗН ЗНУ	2	1	
Лабораторне заняття 4	Тема. Реалізація алгоритму AES засобами dotNET, Python. Розміщено в СЕЗН ЗНУ	2	1	
Лабораторне заняття 5	Тема. Дослідження стандартів шифрування з відкритим ключем із вбудованих бібліотек dotNET, Python. Розміщено в СЕЗН ЗНУ.	2	1	
Лабораторне заняття 6	Тема. Реалізація алгоритму RSA засобами dotNET, Python. Розміщено в СЕЗН ЗНУ.	2	1	
Лабораторне заняття 7	Тема. Дослідження стандартів ЦП з відкритим ключем із вбудованих бібліотек dotNET, Python. Розміщено в СЕЗН ЗНУ.	2	-	
Лабораторне заняття 8	Тема. Реалізація цифрового підпису з хеш-функцією RSA засобами dotNET, Python. Розміщено в СЕЗН ЗНУ.	2	-	
Лабораторне заняття 9	Тема. Дослідження засобів ідентифікації та автентифікації із вбудованих бібліотек dotNET, Python. Розміщено в СЕЗН ЗНУ.	2	-	
Лабораторне заняття 10	Тема. Розробка протоколів ідентифікації та автентифікації засобами dotNET, Python. Розміщено в СЕЗН ЗНУ.	2	-	
Лабораторне заняття 11	Тема. Дослідження криптографічних протоколів. Розробка протоколів ключового обміну. Розміщено в СЕЗН ЗНУ.	2	-	

5. Види і зміст контрольних заходів

Поточні контрольні заходи

Обов'язкові види роботи:

Лабораторна робота *(max від 6 до 10 балів) – передбачається 5 лабораторних робіт, які студент повинен представити для захисту у вигляді комп'ютерної програми та файлу, що виконується, у СЕЗН Moodle* https://moodle.znu.edu.ua/course/view.php?id=8632*. Захист лабораторної роботи відбувається або в комп'ютерному класі або online (при умові дистанційного навчання). При оцінюванні захисту лабораторної роботи викладач враховує правильність відповіді студента на теоретичні питання, що відносяться до теми лабораторної роботи, та повноту і якість роботи відповідної програми. Вчасність виконання лабораторної роботи враховується з допомогою множника, що зменшується у діапазоні (1–0.1) з кроком 0.1 за кожен прострочений тиждень. Всі лабораторні завдання індивідуальні, тому викладач приймає лабораторну роботу у студента тільки з завданням відповідного варіанту.*

Лаб.№ 1 Дослідження стандартів шифрування з секретним ключем. Реалізація алгоритму DES (Data Encryption Standard).
Лаб.№ 2 Дослідження стандартів шифрування з секретним ключем. Реалізація алгоритму AES.
Лаб.№ 3 Дослідження стандартів шифрування з відкритим ключем. Реалізація алгоритму RSA.
Лаб.№ 4 Розробка цифрового підпису.
Лаб.№ 5 Розробка протоколів ідентифікації та автентифікації.

Тест змістового модулю *передбачає відповіді на запитання у СЕЗН Moodle* https://moodle.znu.edu.ua/course/view.php?id=8632 з матеріалу змістового модуля *максимальним балом 10.*

Підсумкові контрольні заходи:

Тест з дисципліни у *СЕЗН Moodle* https://moodle.znu.edu.ua/course/view.php?id=8632
Передбачає відповідь на 30 запитань вибраних випадковим чином із банку питань множинного типу. Всі питання відповідають тематиці курсу. За необхідності після тесту може проводитися додаткове опитування. Максимальна кількість балів – 40.

Контрольний захід		**Термін виконання**	**% від загальної оцінки**
Поточний контроль (max 60%)			
Змістовий модуль 1 (розділ 1)	*Лабораторна робота №1*	*1-2 тиждень*	**8**
Змістовий модуль 2 (розділ 2)	*Лабораторна робота №2*	*3-4 тиждень*	**8**
Змістовий модуль 3 (розділ 3)	*Лабораторна робота №3* *Тест*	*5-6 тиждень* *7 тиждень*	**8** **10**
Змістовий модуль 4 (розділ 4)	*Лабораторна робота №4*	*7-8 тиждень*	**8**
Змістовий модуль 5 (розділ 5)	*Лабораторна робота №5*	*9-10 тиждень*	**8**
	Тест		**10**
Підсумковий контроль (max 40%)			
Тест у СЕЗН Moodle		Залік	**40**
Разом			**100%**

Шкала оцінювання: 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

Основна:

1. Козіна Г. Л. Криптографія від історії до сучасних стандартів : навч. посібник. Запоріжжя : НУ «Запорізька політехніка», 2020. 192 с.
2. Інформаційна безпека : навч. посібник / Ю. Я. Бобало та ін. Львів : Видавництво Львівської політехніки, 2019. 580 с.
3. Євсеєв С. П., Мілов О. В., Король О. Г. Лабораторний практикум з основ криптографічного захисту : навч. посіб. Харків : ХНЕУ ім. С. Кузнеця, 2020. 222 с.
4. Полторак В. П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
5. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption Paperback. Kindle Edition, 2017. 313 p.
6. Klima R. E., Klima R., Sigmon N. P., Sigmon N.. Cryptology: Classical and Modern (2nd ed.). New York : Chapman and Hall/CRC, 2018. 496 p. DOI:https://doi.org/10.1201/9781315170664
7. Steinberg J., Beaver K., Winkler I., Coombs T. Cybersecurity All-in-One For Dummies. New York: Wiley, 2022. 700 p.

Додаткова:

1. Вербівський Д., Якимчук Б. Криптологія : опорний коспект лекцій. Житомир : Вид-во ЖДУ ім. Івана Франка, 2023. 173 с.
2. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
3. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Чинний від 2015–07–01] Вид. офіц. Київ : Мінекономрозвитку України, 2015. (Інформація та документація)
4. Полторак В. П., Савчук О. В. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Вибрані розділи : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 385с.

Інформаційні ресурси в Інтернеті

1. Платформа підвищення кваліфікації з кібербезпеки. URL: https://www.rangeforce.com.

2. Портал безкоштовних програм електронного навчання в галузі криптографії та криптоаналізу The CrypTool Portal. URL: http://www.cryptool.org/en.
3. Сайт повної та безкоштовної реалізації стандарту GNU Privacy Guard OpenPGP. URL: http://www.gnupg.org GnuPG.
4. Сайт розробника алгоритму і програми PGP. URL: http://www.pgpi.com.
5. Український ресурс з безпеки. URL: http://kiev-security.org.ua.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[1]

Відвідування занять. Регуляція пропусків.
Теоретико-практичний характер курсу передбачає обов'язкове відвідування лекцій і лабораторних занять. Студенти, які за певних обставин не можуть відвідувати заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущенні завдання мають бути відпрацьовані на найближчій консультації впродовж тижня після пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання шляхом виконання індивідуального письмового завдання.
Студенти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Політика академічної доброчесності
Усі письмові роботи, що виконуються слухачами під час проходження курсу, перевіряються на наявність плагіату за допомогою спеціалізованого програмного забезпечення. Відповідно до чинних правових норм, плагіатом вважатиметься: копіювання чужої наукової роботи чи декількох робіт та оприлюднення результату під своїм іменем; створення суміші власного та запозиченого тексту без належного цитування джерел; рерайт (перефразування чужої праці без згадування оригінального автора). Будь-яка ідея, думка чи речення, ілюстрація чи фото, яке ви запозичуєте, має супроводжуватися посиланням на першоджерело. Приклади оформлення цитувань див. на Moode: https://moodle.znu.edu.ua/mod/resource/view.php?id=103857
Виконавці індивідуальних дослідницьких завдань обов'язково додають до текстів своїх робіт власноруч підписану Декларацію академічної доброчесності (див. посилання у Додатку до силабусу).
Роботи, у яких виявлено ознаки плагіату, до розгляду не приймаються і відхиляються без права перескладання. Якщо ви не впевнені, чи підпадають зроблені вами запозичення під визначення плагіату, будь ласка, проконсультуйтеся з викладачем.
Висока академічна культура та європейські стандарти якості освіти, яких дотримуються у ЗНУ, вимагають від дослідників відповідального ставлення до вибору джерел. Посилання на такі ресурси, як Wikipedia, бази даних рефератів та письмових робіт (Studopedia.org та подібні) є неприпустимим. Рекомендовані бази даних для пошуку джерел:
Електронні ресурси Національної бібліотеки ім. Вернадського: http://www.nbuv.gov.ua
Цифрова повнотекстова база даних англомовної наукової періодики JSTOR: https://www.jstor.org/

Використання комп'ютерів/телефонів на занятті
Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). Будь ласка, не забувайте активувати режим «без звуку» до початку заняття.

[1] **Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, і т.д. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!**

Під час виконання заходів контролю (термінологічних диктантів, контрольних робіт, іспитів) використання гаджетів заборонено. У разі порушення цієї заборони роботу буде анульовано без права перескладання.

Комунікація
Базовою платформою для комунікації викладача зі студентами є Moodle.
Важливі повідомлення загального характеру – зокрема, оголошення про терміни подання контрольних робіт, коди доступу до сесій у Microsoft Teams та ін. – регулярно розміщуються викладачем на форумі курсу та в календарі Microsoft Teams. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити студентів подаються викладачем впродовж трьох робочих днів. Для оперативного отримання повідомлень про оцінки та нову інформацію, розміщену на сторінці курсу у Moodle, будь ласка, переконайтеся, що адреса електронної пошти, зазначена у вашому профайлі на Moodle, є актуальною, та регулярно перевіряйте папку «Спам». Якщо за технічних причин доступ до Moodle є неможливим, або ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу sia@zsea.edu.ua. У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ 2024-2025 н. р. доступний за адресою: https://tinyurl.com/yckze4jd.

НАВЧАЛЬНИЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) 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 ЗНУ: https://tinyurl.com/y9tve4lk.

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в 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. Порядок повторного вивчення визначається Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: https://tinyurl.com/y9pkmmp5. Підстави та процедури відрахування студентів, у тому числі за невиконання навчального плану, регламентуються Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ: https://tinyurl.com/ycds57la.

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://tinyurl.com/57wha734. 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://tinyurl.com/yd6bq6p9; Положення про призначення та виплату соціальних стипендій у ЗНУ: https://tinyurl.com/y9r5dpwh.

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога **Марті Ірини Вадимівни** (061) 228-15-84, (099) 253-78-73 (щоденно з 9 до 21).

УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КОРУПЦІЇ Запорізького національного університету: **Банах Віктор Аркадійович**

Електронна адреса:
Гаряча лінія: Тел.

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. Якщо вам потрібна спеціалізована допомога, будь ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://tinyurl.com/ydhcsagx.

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 (MOODLE): https://moodle.znu.edu.ua
Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресою: moodle.znu@znu.edu.ua.
У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.
Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте 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/
ЦЕНТР НІМЕЦЬКОЇ МОВИ, ПАРТНЕР ГЕТЕ-ІНСТИТУТУ: https://www.znu.edu.ua/ukr/edu/ocznu/nim
ШКОЛА КОНФУЦІЯ (ВИВЧЕННЯ КИТАЙСЬКОЇ МОВИ): http://sites.znu.edu.ua/confucius