ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

АЛГОРИТМИ ШИФРУВАННЯ ТА ЗАХИСТУ ДАНИХ

Викладач: кандидат фізико-математичних наук, доцент, Зіновєєв Ігор Валерійович
Кафедра: Загальної математики, І корпус, ауд. 21а
E-mail: zinoveev@znu.edu.ua
Телефон: (061) 289-12-54
Інші засоби зв'язку: Moodle (форум курсу, приватні повідомлення)

Освітня програма, рівень вищої освіти:		Інформаційні системи та штучний інтелект, Магістр					
Статус дисципліни:		Обов'язкова					
Кредити ECTS	3	**Навч. рік:**	2023-24 1 семестр	**Рік навчання**	1	**Тижні**	10
Кількість годин	90	**Кількість змістових модулів**	4	**Лекційні заняття – 10** **Лабораторні заняття – 20** **Самостійна робота – 60**			
Вид контролю:		Екзамен					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=14746					
Консультації: час консультація за розкладом консультацій (розміщено на стенді кафедри) Moodle (форум курсу), Zoom							

ОПИС КУРСУ

Курс є необхідною складовою частиною базової теоретичної та практичної підготовки студента, що навчається за освітньою програмою «Інформаційні системи та штучний інтелект», а також є основою для подальшого вивчення спеціальних дисциплін.

Курс «Алгоритми шифрування та захисту даних» складається з 4-х змістових модулів:

1. Основні поняття криптографії та захисту інформації. Історичний огляд криптографічних методів захисту інформації. Класичні алгоритми симетричного шифрування.;
2. Симетрична та асиметрична криптографія. Класичні алгоритми асиметричного шифрування. Алгоритми на основі мереж Фейстеля та SP-мереж.;
3. Сучасні криптографічні методи захисту інформації. Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі блокового шифрування.
4. Алгоритми захисту даних. Електронний цифровий підпис. Алгоритми та технології аутентифікації.

Основною **метою** викладання курсу є отримання компетентностей в області криптографії, криптографічного захисту даних.

Основними **завданнями** курсу є: надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації; формування у студентів категоріальних понять з основ математики симетричної та асиметричної криптографії; формування у студентів умінь обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів; стимулювання студентів до активної аналітико-пошукової роботи.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У разі успішного завершення курсу студент **зможе**:

- застосовувати на практиці набуті знання про джерела і способи дії загроз на об'єкти інформаційної безпеки ;
- використовувати фундаментальні та спеціальні знання з математики до розв'язання прикладних задач в галузі шифрування, кодування даних, захисту даних;
- володіти алгоритмами шифрування інформаційних текстів та застосовувати їх;
- працювати з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів;
- створювати засобами стандартного програмного забезпечення елементи захисту даних.

Використання новітніх програмних засобів під час виконання практичних та лабораторних завдань розвине як загальні, так і професійні компетенції слухачів.

Змістове наповнення курсу, що викладається на лекційних і лабораторних заняттях та засвоюється студентом під час самостійної роботи, забезпечує набуття **компетентностей**:
ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.
СК 4. Здатність розробляти математичні, інформаційні та комп'ютерні моделі об'єктів і процесів інформатизації.
СК 6. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки
СК 10. Здатність застосовувати методи захисту даних в інформаційних системах

Програмні результати навчання:

РН 1. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.
РН 10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації
РН 12. Розробляти та використовувати методи штучного інтелекту
РН 13. Розробляти та використовувати алгоритми шифрування та захисту даних в інформаційних системах

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, плани занять, методичні рекомендації до виконання індивідуальних та практичних завдань, групових творчих проектів розміщені на платформі Moodle:
https://moodle.znu.edu.ua/course/view.php?id=14746

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи

Теоретичний контроль (кількість балів зазначено на сторінці дисципліни в moodle) – усні (до 2 балів за один контроль) та письмові (до 5 балів за один контроль) опитування на лекціях, лабораторних заняттях, тестування – (до 5 балів за тест).

Практичний контроль (кількість балів зазначено на сторінці дисципліни в moodle) – розв'язання практичних завдань, завдань самостійної роботи (до 5 балів за один контроль), письмові контрольні роботи (до 5 балів за один контроль, двічі на семестр), тестування – (до 5 балів за тест).

Реферат – оволодіння матеріалом, що виноситься на самостійну роботу (до 3 балів за один реферат, двічі на семестр).

Підсумкові контрольні заходи:

Індивідуальне дослідницьке завдання, проект (ІДЗ, можливо виконання у групі з двох, трьох студентів).

ІДЗ видається за один – два місяці до завершення теоретичного навчання поточного семестру. Термін виконання не менше одного місяця. Виконане ІДЗ, на передостанньому тижні теоретичного навчання поточного семестру подається викладачеві у вигляді оформленої пояснювальної записки (постановка задачі, побудова та обґрунтування адекватності обраної математичної моделі, криптосистеми, обґрунтування методу розв'язання поставленої задачі, розв'язок задачі, інтерпретація отриманих результатів, рекомендації до застосування).

На останньому тижні проводиться публічний захист у групі (до 20 балів).

Формат захисту ІДЗ проекту: презентація, тривалістю до 10 хвилин та відповідь на задані присутніми питання (до 5 хвилин).

Детальні вимоги та практичні рекомендації до виконання ІДЗ на сторінці курсу у Moodle та на поточних консультаціях.

Результати ІДЗ можуть стати основою для доповідей на студентських науково-практичних конференціях.

Залікове тестове завдання (до 20 балів)– проводиться у системі Moodle або MyTestXPro із використанням (за необхідністю) розроблених програмних продуктів, та спеціального програмного забезпечення. Критерії оцінювання та вимоги до тесту наведено в інструкції до тесту та поточній консультації.

Контрольний захід		**Термін виконання**	**% від загальної оцінки**
Поточний контроль (max 60%)			**60**
Змістовий модуль 1	Теоретичний контроль. Тест за змістовим модулем.	Тиждень 1-2	**4**
	Лабораторні завдання	Тиждень 1-2	**8**
Змістовий модуль 2	Теоретичний контроль. Тест за змістовим модулем.	Тиждень 3-5 Тиждень 5	**6**
	Лабораторні завдання	Тиждень 3-5	**12**
Змістовий модуль 3	Теоретичний контроль. Тест за змістовим модулем.	Тиждень 6-8 Тиждень 8	**6**
	Лабораторні завдання	Тиждень 5-8	**12**
Змістовий модуль 4	Теоретичний контроль. Тест за змістовим модулем.	Тиждень 9-10	**4**
	Лабораторні завдання	Тиждень 9-10	**8**
Підсумковий контроль (max 40%)			
Екзаменаційний тест за курс			**20**
Захист індивідуального дослідницького завдання або групового проекту		Тиждень 10	**20**
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)		

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

Тиждень і вид заняття	**Тема заняття**	**Контрольне завдання**	**Кількість балів**
Змістовий модуль 1. Основні поняття криптографії та захисту інформації. Історичний огляд криптографічних методів захисту інформації. Класичні алгоритми симетричного шифрування.			
Тиждень 1 Лекція 1	Основні поняття криптографії та захисту інформації. Історія криптографії. Криптографія та захист даних. Поняття та види шифрів. Вимоги до шифрів – принцип Керхгоффа. Шифрувальні машини. Ідеальний шифр і класи стійкості шифрів. Шифри заміни. Шифри переставляння. Шифри гамування.	Фронтальне опитування (усне, письмове, тестування)	**2**
Тиждень 1 Лабораторна робота 1	Класичні алгоритми симетричного та асиметричного шифрування. Шифр Цезаря. Квадрати Полібія. Шифри заміни.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	**4**
Тиждень 2 Лабораторна робота2	Класичні алгоритми симетричного та асиметричного шифрування. Шифр Кардано. Шифри переставляння.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	**4**
		Тест за змістовим модулем	**2**

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

Тиждень і вид заняття	**Тема заняття**	**Контрольне завдання**	**Кількість балів**
Змістовий модуль 2. Симетрична та асиметрична криптографія. Класичні алгоритми асиметричного шифрування. Алгоритми на основі мереж Фейстеля та SP-мереж.			
Тиждень 3 Лекція 2	Симетрична та асиметрична криптографія. Класичні алгоритми симетричного та асиметричного шифрування. Шифри заміни. Шифри переставляння. Шифри гамування.	Фронтальне опитування (усне, письмове, тестування).	2
Тиждень 3 Лабораторна робота 3	Класичні алгоритми симетричного та асиметричного шифрування. Шифри гамування.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4
Тиждень 4 Лабораторна робота 4	Класичні алгоритми симетричного та асиметричного шифрування. Мережа Фейстеля.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4
Тиждень 5 Лекція 3	Сучасні криптографічні методи захисту інформації, основні види та їх реалізація. Мережа Фейстеля. Шифри на основі мережі Фейстеля. Американський шифр DES. Шифри на основі SP-мережі.	Фронтальне опитування (усне, письмове, тестування).	2
Тиждень 5 Лабораторна робота 5	Класичні алгоритми симетричного та асиметричного шифрування. Шифри на основі SP-мережі.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4
		Тест за змістовим модулем	3
Змістовий модуль 3. Сучасні криптографічні методи захисту інформації. Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі блокового шифрування.			
Тиждень 6 Лабораторна робота 6	Блокове шифрування. ДСТУ 28147-89.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4

Тиждень і вид заняття	**Тема заняття**	**Контрольне завдання**	**Кількість балів**
Тиждень 7 Лекція 4	Блокове шифрування. Основні принципи роботи блокових шифрів. Сучасні криптосистеми на основі блокового шифрування (ДСТУ 28147-89, DES, AES, Rijndael, ДСТУ 7624:2014 «Калина»). Складені шифри	Фронтальне опитування (усне, письмове, тестування)	2
Тиждень 7 Лабораторна робота 7	Блокове шифрування. AES. Американський шифр DES.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4
Тиждень 8 Лабораторна робота 8	Блокове шифрування. ДСТУ 7624:2014 «Калина».	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4
		Тест за змістовим модулем	3
Змістовий модуль 4. Алгоритми захисту даних. Електронний цифровий підпис. Алгоритми та технології аутентифікації.			
Тиждень 9 Лекція 5	Алгоритми захисту даних. Електронний цифровий підпис (ЦП). Стандарти ЦП. Цифровий підпис RSA. Алгоритми та технології аутентифікації Системи захисту Діффі-Хеллмана. Криптосистема Ель–Гамаля.	Фронтальне опитування (усне, письмове, тестування)	2
Тиждень 9 Лабораторна робота 9	Алгоритми захисту даних. Електронний цифровий підпис (ЦП). Цифровий підпис RSA	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4
Тиждень 10 Лабораторна робота 10	Алгоритми та технології аутентифікації Системи захисту Діффі-Хеллмана. Алгоритми та технології аутентифікації Криптосистема Ель–Гамаля.	Згідно плану заняття, захист л.р., перевірка , оволодіння теоретичним матеріалом, практичними вміннями та навичками	4

Тиждень і вид заняття	Тема заняття	Контрольне завдання	Кількість балів
		Тест за змістовим модулем	2
Тиждень 10 Захист ІДЗ	Підсумковий контроль	Захист ІДЗ. Доповідь. Презентація.	20
Тиждень 11	Підсумковий контроль Екзамен	Тестування (проводиться у системі Moodle або MyTestXPro)	20
Всього			**100**

ОСНОВНІ ДЖЕРЕЛА

1. 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.
2. Інформаційна безпека : навч. посібник / Ю. Я. Бобало та ін. Львів : Видавництво Львівської політехніки, 2019. 580 с.
3. Козіна Г. Л. Криптографія від історії до сучасних стандартів : навч. посібник. Запоріжжя : НУ «Запорізька політехніка», 2020. 192 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.

ДОДАТКОВІ ДЖЕРЕЛА

1. Вербівський Д., Якимчук Б. Криптологія : опорний коспект лекцій. Житомир : Вид-во ЖДУ ім. Івана Франка, 2023. 173 с.
2. Глинчук Л. Я. Криптологія : навч.-метод. посіб. Луцьк : Вежа-Друк, 2014. 164 с.
3. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: Теорія. Практика. Застосування. Харків : Форт, 2013. 880 с.
4. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
5. 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)
6. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Прикладна криптологія» : для студентів техн. спец. / А. Д. Кожухівський та ін. Київ : Державний університет телекомунікацій, 2020. 109 с. URL: https://dut.edu.ua/uploads/l_2167_57004775.pdf

7. 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. Законодавство України. Офіційний сайт парламенту України. URL: http://zakon.rada.gov.ua.
2. Платформа підвищення кваліфікації з кібербезпеки. URL: https://www.rangeforce.com.
3. Портал безкоштовних програм електронного навчання в галузі криптографії та криптоаналізу The CrypTool Portal. URL: http://www.cryptool.org/en.
4. Сайт Національної академії внутрішніх справ України. URL: http://www.naiau.kiev.ua.
5. Сайт повної та безкоштовної реалізації стандарту GNU Privacy Guard OpenPGP. URL: http://www.gnupg.org GnuPG.
6. Сайт розробника алгоритму і програми PGP. URL: http://www.pgpi.com.
7. Український ресурс з безпеки. URL: http://kiev-security.org.ua.
8. Центр комп'ютерної безпеки м. Київ. URL: https://infocity.kiev.ua.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ

Відвідування занять. Регуляція пропусків.
Відвідування занять обов'язкове.
Завдання мають бути виконанні в зазначені терміни.
Пропуски занять, незалежно від причини підлягають відпрацюванню у години консультацій.
За умови систематичних пропусків може бути застосована процедура повторного вивчення дисципліни (див. посилання на Положення у додатку до силабусу).

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).

Використання комп'ютерів/телефонів на занятті
Під час занять персональні електронні пристрої (телефони, ПК) можна використовувати лише за умови виробничої необхідності (за погодженням з викладачем). Мобільні телефони повинні бути переведені на беззвучний режим. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо.

Комунікація
Очікується, що студенти перевірятимуть свою електронну пошту і сторінку дисципліни в Moodle та реагуватимуть своєчасно. Всі робочі оголошення можуть надсилатися через старосту, на електронну на пошту та розміщуватимуться в Moodle. Будь ласка, перевіряйте повідомлення вчасно. *Ел. пошта має бути підписана справжнім ім'ям і прізвищем*.

ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2023-2024 рр.

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ 2023-2024 н. р. доступний за адресою: https://tinyurl.com/yckze4jd.

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ. Студенти і викладачі Запорізького національного університету несуть персональну відповідальність за дотримання принципів академічної доброчесності, затверджених **Кодексом академічної доброчесності ЗНУ:** https://tinyurl.com/ya6yk4ad. Декларація академічної доброчесності здобувача вищої освіти (додається в обов'язковому порядку до письмових кваліфікаційних робіт, виконаних здобувачем, та засвідчується особистим підписом): https://tinyurl.com/y6wzzlu3.

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.

НЕФОРМАЛЬНА ОСВІТА. Порядок зарахування результатів навчання, підтверджених сертифікатами, свідоцтвами, іншими документами, здобутими поза основним місцем навчання, регулюється Положенням про порядок визнання результатів навчання, отриманих у неформальній освіті: https://tinyurl.com/y8gbt4xs.

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: **Борисов Костянтин Борисович**
Електронна адреса: uv@znu.edu.ua Гаряча лінія: Тел. (061) 228-75-50

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.

ЕЛЕКТРОННЕ 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