ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ

Декан математичного факультету ЗНУ
_____ ____С.І.Гоменюк____
(підпис) (ініціали та прізвище)
«_____» _____ 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ

підготовки _____бакалаврів_____

денної та заочної форми здобуття освіти

освітньо-професійна програма ___КІБЕРБЕЗПЕКА_____

спеціальності ___125 Кібербезпека та захист інформації_____

галузі знань ____12 Інформаційні технології_____

ВИКЛАДАЧ: Добровольський Геннадій Анатолійович, к.т.н, 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

_____О. С. Пшенична_____
(підпис) (ініціали, прізвище)

Погоджено
Гарант освітньо-професійної програми

_____Н.В. Матвіїшина_____
(підпис) (ініціали, прізвище)

2026 рік

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Біометрична аутентифікація

Зв`язок з викладачем: Добровольський Геннадій Анатолійович
E-mail: gen.dobr@gmail.com
Сезн ЗНУ повідомлення: https://moodle.znu.edu.ua/course/view.php?id=17928
Телефон (кафедра): +38-061-289-12-57
Інші засоби зв'язку: https://t.me/gen_dobr
Кафедра комп'ютерних наук, ауд. №39, 1 корпус ЗНУ

1. Опис навчальної дисципліни

Курс присвячений теоретичним основам і практичним методам побудови систем біометричної аутентифікації. Розглядаються фізіологічні та поведінкові біометричні характеристики людини, принципи вилучення та порівняння біометричних ознак, архітектура біометричних систем, методи оцінювання їх точності та надійності. Особлива увага приділяється сучасним алгоритмам обробки зображень та сигналів, методам машинного навчання в біометрії, а також питанням безпеки, етики й захисту персональних даних. Компетентності, отримані під час вивчення дисципліни «Біометрична аутентифікація», необхідні для виконання завдань виробничої практики, розроблення систем інформаційної безпеки та підготовки кваліфікаційної роботи.

Метою вивчення навчальної дисципліни «Біометрична аутентифікація» є формування у студентів знань про принципи функціонування біометричних систем, методи збору, обробки та аналізу біометричних даних, а також розвиток практичних навичок створення та оцінювання ефективності біометричних систем аутентифікації користувачів.

У результаті вивчення навчальної дисципліни «Біометрична аутентифікація» студент зможе:

- класифікувати біометричні технології за типом ознак і сферою застосування;
- пояснювати архітектуру та принципи роботи біометричних систем;
- застосовувати алгоритми вилучення та порівняння біометричних ознак із використанням сучасних інструментів (Python, OpenCV, TensorFlow);
- оцінювати ефективність біометричних систем за основними показниками (FAR, FRR, EER);
- аналізувати загрози безпеці біометричних даних та пропонувати способи їх захисту;
- дотримуватись етичних і правових норм під час розроблення та експлуатації біометричних систем.

Паспорт навчальної дисципліни

Нормативні показники	**денна форма здобуття освіти**	**заочна форма здобуття освіти**
Статус дисципліни	**Вибіркова**	
Семестр	6-й	6-й
Кількість кредитів ECTS	5	5
Кількість годин	150	150
Лекційні заняття	24 год.	6 год.
Лабораторні заняття	24 год.	8 год.
Самостійна робота	102 год.	136 год.
Консультації	Згідно розкладу: дистанційно: Google Meet: https://meet.google.com/mwp-gbkw-xhk	
Вид підсумкового семестрового контролю:	**іспит**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=17928	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	**Методи навчання**	**Форми і методи оцінювання**
Компетентності		
ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/ або кібербезпеки. ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	лекція-візуалізація, пояснення, демонстрування, дискусія, аналіз, виконання завдань практичних робіт	**Поточний контроль:** захист лабораторних та самостійних робіт, опитування, тестування **Підсумковий контроль:** тестування

СК 1 Здатність розробляти та застосовувати математичні моделі, аналізувати статистичні дані розробляти прогностичні моделі для виявлення та дослідження загроз у комп'ютерних системах.		
Результати навчання		
ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень ПРН 22 – Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки. ПРН 28 – Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.	лекція-візуалізація, пояснення, дискусія, аналіз, виконання завдань практичних робіт	**Поточний контроль:** захист лабораторних та самостійних робіт, опитування, тестування **Підсумковий контроль:** тестування

3. Зміст навчальної дисципліни

Змістовий модуль 1. Вступ до біометричної аутентифікації

Тема 1. Основи біометрії та аутентифікації

Поняття ідентифікації та аутентифікації. Різниця між біометричною та класичною аутентифікацією. Класифікація біометричних характеристик. Сфери застосування біометрії.

Змістовий модуль 2. Архітектура та показники ефективності біометричних систем

Тема 2. Архітектура біометричних систем і критерії якості

Вимоги до біометричних систем: універсальність, унікальність, стабільність, вимірюваність, прийнятність. Архітектура біометричної системи: сенсор, модуль обробки, база шаблонів, модуль прийняття рішення. Показники ефективності: FAR, FRR, EER, ROC-криві.

Робота з відкритими наборами біометричних даних (LFW, CASIA, FVC).

Змістовий модуль 3. Фізіологічні біометричні ознаки
Тема 3. Фізіологічні методи біометричної аутентифікації
Відбитки пальців, райдужна оболонка, сітківка, геометрія руки, розпізнавання обличчя. Принципи зчитування даних. Методи вилучення ознак. Джерела похибок. Порівняння фізіологічних методів за точністю, надійністю та стійкістю до атак.

Змістовий модуль 4. Поведінкові біометричні ознаки
Тема 4. Поведінкові методи біометричної аутентифікації
Голос, динаміка підпису, клавіатурний ритм, хода. Особливості та стабільність поведінкових ознак. Методи аналізу часових рядів і спектральних характеристик. Порівняння з фізіологічними методами.

Змістовий модуль 5. Попередня обробка біометричних даних
Тема 5. Обробка біометричних сигналів і зображень
Фільтрація шумів, нормалізація, вирівнювання освітлення, підвищення контрасту. Сегментація та виділення ROI. Перетворення Фур'є, Sobel, Canny. Морфологічна обробка. Обробка та візуалізація зображень за допомогою OpenCV і NumPy.

Змістовий модуль 6. Вилучення ознак і побудова біометричних шаблонів
Тема 6. Методи вилучення ознак та моделі представлення даних
LBP, HOG, Gabor-фільтри, PCA, SIFT, SURF. Формування вектора ознак і шаблону користувача. Застосування нейронних мереж (CNN, FaceNet, DeepFace) для біометрії.

Змістовий модуль 7. Порівняння шаблонів та оцінювання ефективності

Тема 7. Порівняння біометричних шаблонів і прийняття рішень
Метрики схожості: евклідова, косинусна, Manhattan, Mahalanobis. Порогові рішення. Алгоритми класифікації: k-NN, SVM, Decision Trees.

Тема 8. *Оцінювання якості біометричних систем*
Автоматизація адміністрування з Ansible. Приклад сценарію автоматизації адміністрування.

Змістовий модуль 8. Безпека, правові аспекти та сучасні застосування

Тема 9. *Безпека біометричних систем*
Автоматизація адміністрування з Ansible. Приклад сценарію автоматизації адміністрування.

Тема 10. *Етичні, правові аспекти та сучасні тенденції*
Захист персональних даних і GDPR. Приватність і зберігання біометричних шаблонів.
Інтеграція біометрії у прикладні системи (банкінг, мобільні пристрої, контроль доступу).
Хмарні сервіси та API (AWS Rekognition, Microsoft Face API).
Сучасні напрями: 3D-біометрія, багатомодальні системи, IoT, Smart City, deep learning.

4. Структура навчальної дисципліни

Вид заняття /роботи	Назва теми	Кількість годин о/д. ф.	Згідно з розкладом
1	***2***	***3***	***4***
Лекція	Вступ. Предмет і завдання адміністрування ІС. Архітектура сучасних ІС.	2	тиждень 1
Лабораторна робота	ЛР1. Ознайомлення з видами біометричних характеристик (обличчя, відбитки, голос)	2	тиждень 1
Самостійна робота	Опрацювання базових понять біометрії. Порівняння класичної та біометричної аутентифікації	8	тиждень 1
Лекція	Класифікація біометричних методів та сфери їх застосування	2	тиждень 2
Лабораторна робота	ЛР2. Аналіз зображень відбитків пальців. Вилучення ключових точок	2	тиждень 2
Самостійна робота	Аналіз вимог до біометричних систем. Огляд сфер застосування біометрії	8	тиждень 2
Лекція	Архітектура біометричних систем аутентифікації	2	тиждень 3
Лабораторна робота	ЛР3. Аналіз голосових даних. Побудова ознак для ідентифікації мовця	2	тиждень 3
Самостійна робота	Вивчення архітектури біометричних систем. Ознайомлення з відкритими біометричними датасетами (LFW, CASIA, FVC)	9	тиждень 3
Лекція	Показники ефективності біометричних систем (FAR, FRR, EER, ROC)	2	тиждень 4
Лабораторна робота	ЛР4. Реалізація попередньої обробки зображень обличчя за допомогою OpenCV	2	тиждень 4
Самостійна робота	Опрацювання показників ефективності FAR, FRR, EER, ROC. Аналіз прикладів оцінювання систем	9	тиждень 4
Лекція	Фізіологічні біометричні ознаки: принципи та методи	2	тиждень 5
Лабораторна робота	ЛР5. Використання HOG та LBP для побудови шаблонів обличчя	2	тиждень 5
Самостійна робота	Самостійне вивчення фізіологічних біометричних методів (відбитки, обличчя, райдужка). Порівняльний аналіз	8	тиждень 5
Лекція	Поведінкові біометричні ознаки та аналіз поведінки користувачів	2	тиждень 6
Лабораторна робота	ЛР6. Обчислення метрик схожості (евклідова, косинусна) між шаблонами облич	2	тиждень 6
Самостійна робота	Опрацювання поведінкових біометричних ознак (голос, підпис, клавіатурний ритм)	8	тиждень 6
Лекція	Попередня обробка біометричних сигналів і зображень	2	тиждень 7

Лабораторна робота	ЛР7. Побудова ROC- та DET-кривих для оцінювання системи розпізнавання	2	тиждень 7
Самостійна робота	Вивчення методів попередньої обробки біометричних зображень і сигналів	9	тиждень 7
Лекція	Методи вилучення ознак і побудова біометричних шаблонів	2	тиждень 8
Лабораторна робота	ЛР8. Виявлення підроблених зображень (spoof detection)	2	тиждень 8
Самостійна робота	Самостійне опрацювання методів вилучення ознак (LBP, HOG, Gabor, PCA). Огляд CNN у біометрії	9	тиждень 8
Лекція	Порівняння біометричних шаблонів і алгоритми класифікації	2	тиждень 9
Лабораторна робота	ЛР9. Реалізація базових методів захисту шаблонів користувачів	2	тиждень 9
Самостійна робота	Вивчення методів порівняння шаблонів і алгоритмів класифікації (k-NN, SVM)	8	тиждень 9
Лекція	Оцінювання якості та тестування біометричних систем	2	тиждень 10
Лабораторна робота	ЛР10. Розробка простої системи FaceID на Python (OpenCV, dlib)	2	тиждень 10
Самостійна робота	Аналіз методології тестування біометричних систем. Побудова та інтерпретація ROC/DET-кривих	8	тиждень 10
Лекція	Безпека біометричних систем: загрози, атаки, захист	2	тиждень 11
Лабораторна робота	ЛР11. Комбінування розпізнавання обличчя і голосу для підвищення точності	2	тиждень 11
Самостійна робота	Самостійне вивчення атак на біометричні системи та методів захисту (PAD, template protection)	9	тиждень 11
Лекція	Правові аспекти та сучасні тенденції розвитку біометрії	2	тиждень 12
Лабораторна робота	ЛР12. Аналіз моделей глибокого навчання для біометрії (FaceNet, DeepFace)	2	тиждень 12
Самостійна робота	Опрацювання правових та етичних аспектів. Підготовка до підсумкового контролю	9	тиждень 12

Методичні рекомендації до практичних та самостійних занять розміщено СЕЗН ЗНУ Moodle на сторінці дисципліни.

5. Види і зміст контрольних заходів

Вид заняття/ роботи	Вид контрольного заходу	Зміст контрольного заходу*	Критерії оцінювання та термін виконання*	Усього балів
Поточний контроль				
Практичне заняття №1 - 12	Лабораторна робота 1 - 12	Розміщено в СЕЗН ЗНУ	Повний захист кожного виконаного завдання оцінюється в 5 балів, тільки зданий звіт - 4 бала	60
Усього за поточний контроль				**60**
Підсумковий контроль				
Залік	Теоретичне завдання	Розміщено в СЕЗН ЗНУ	40 тестових питань (вибір правильної відповіді з декількох можливих) - по 0.5 бала	**40**
Усього за підсумковий контроль				**40**

Шкала оцінювання ЗНУ: національна та ECTS

1 За шкалою **1 ECTS**	**2 За шкалою університету**	2 За національною шкалою	
		3 Екзамен	4 Залік
A	90 – 100 (відмінно)	1 5 (відмінно)	2 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. Jain A.K., Ross A., Nandakumar K. Introduction to Biometrics. 2nd ed. New York : Springer, 2016. − 428 p. ISBN 978-0-387-77326-1.
2. Jain A.K., Flynn P., Ross A. Handbook of Biometrics. New York : Springer, 2007. − 802 p. ISBN 978-0-387-71041-9.
3. Das R. The Science of Biometrics: Security Technology for Identity Verification. 1st ed. London : Routledge, 2019. − 314 p. ISBN 978-1-4987-6124-6.
4. Fairhurst M. Biometrics: A Very Short Introduction. Oxford : Oxford University Press, 2023. − 144 p. ISBN 978-0-19-880910-4.
5. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами. 2-ге вид., доп. Львів : ЛьвДУВС, 2015. − 492 с. ISBN 978-617-511-169-7.
6. Бікерей О. І. Біометрична аутентифікація. Київ : НТУ Укр : [вид-во], 2024.

Додаткова

1. Alrawili R., AlQahtani A. A. S., Khan M. K. Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion. / R. Alrawili, A. A. S. AlQahtani, M. K. Khan. − 2023. − URL: https://arxiv.org/abs/2311.13416 .
2. Zhang J. et al. A Survey of Behavioral Biometric Authentication on Smartphones. J. Zhang. − 2023. − URL: https://dl.acm.org/doi/10.1145/3650215.3650342 .
3. Лунгол О. М. Біометричні технології в системах автентифікації: використання та перспективи. − Наука і техніка сьогодні. − 2024. − № 5(33). − С. 731-741. − URL: https://perspectives.pp.ua/index.php/nts/article/download/11822/11882 .

Електронні ресурси

1. Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion − R. Alrawili, A. A. S. AlQahtani, M. K. Khan. arXiv, 2024. Повний текст доступний онлайн.
2. A ZKP-based anonymous biometric authentication scheme for the E-health systems − X. Mao et al. PLoS One, 2025. Open access.
3. Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey − M. Abuhamad, A. Abusnaina, D. Nyang, D. Mohaisen. arXiv, 2020.
4. A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems − A. Sundararajan, A. I. Sarwat, A. Pons. arXiv, 2019.
5. Biometrics Recognition Using Deep Learning: A Survey − S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, D. Zhang. arXiv, 2019.
6. Multiple biometric authentication for online banking system based on multiple fuzzy approach − N. M. Anwar et al. Scientific Reports, 2025. Open access article.
7. Biometric Authentication Systems: A Survey − D. R. Tripathi, D. K. Nishad. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2020.
8. Biometrics-Based Authentication: Advancements and Real-World Implementations − Special Issue of Sensors (MDPI).
9. Analysis of biometric access control systems − H. El Bouhissi et al., CSIT Journal, 2025.
10. Do They Understand What They Are Using? − Assessing Perception and Usage of Biometrics − L. Mecke, A. Saad, S. Prange, U. Gruenefeld, F. Alt. arXiv, 2024.

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)

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ 2025-2026 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: 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. 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