ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Економічний факультет
Силабус навчальної дисципліни

ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Викладач: *доктор фіз.-мат. Наук, професор, Козін Ігор Вікторович*
Кафедра: *економічної кібернетики, 5-й корпус ЗНУ, ауд.113*
E-mail: ainc@ukrpost.net
Телефон:
Інші засоби зв'язку:

Освітня програма, рівень вищої освіти		Економічна кібернетика бакалавр				
Статус дисципліни		Вибіркова				
Кредити ECTS 3		**Навч. рік**	2021-22	**Рік навчання**	**Тижні**	16
Кількість годин 90		**Кількість змістових модулів[1] 4**		**4-й**	**Лекційні заняття – 32 Лабораторні заняття – 16 Самостійна робота – 42**	
Вид контролю	*Залік*					
Посилання на курс в Moodle^		https://moodle.znu.edu.ua/course/view.php?id=3632				
Консультації: ***2 год на тиждень за розкладом***		*кількість на тиждень, тривалість, формат (за розкладом, за домовленістю, особисто чи дистанційно)*				

ОПИС КУРСУ

Мета курсу.
Мета курсу - познайомити студентів з основами сучасної теорії і практики забезпечення безпеки інформації у великих інформаційних системах, познайомитися з основними моделями безпеки даних, що існують стандартами і перспективами/

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У разі успішного завершення курсу студент зможе:

- вибирати методологію і розробляти методику побудови моделі безпеки фінансової організації;
- розробляти необхідну інформативну базу по забезпеченню безпеки даних;
- робити якісну і кількісну оцінку політики безпеки;
- використовувати методи і прийоми математичного моделювання, розробляти власні найпростіші механізми захисту інформації;
- оцінювати внутрішні і зовнішні погрози інформації.

.

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, плани семінарських занять, методичні рекомендації до виконання індивідуальних завдань розміщені на платформі Moodle:
https://moodle.znu.edu.ua/course/view.php?id=3632

[1] **1 змістовий модуль = 15 годин (0,5 кредита ECTS)**

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи:

Поточний контроль здійснюється у вигляді лабораторних робіт за темами та вигляді коротких тестувань (10 питань). Передбачено 8 лабораторних робіт, кожна з яких оцінюється в 6 балів та 2 тестових завдання по 6 балів. Тестування проводяться в системі Moodle.

Підсумкові контрольні заходи:

Підсумковий семестровий контроль складається з двох частин

1. *Індивідуальне завдання за темами з заданого переліку тем. Максимальна оцінка – 20 балів*
2. *Підсумковий тест (Moodle) або опитування – Максимальна оцінка – 20 балів*

Контрольний захід			**Термін виконання**	**% від загальної оцінки**
Поточний контроль (max 60%)				
розділ 1	*Змістовий модуль 1*	*Лабораторні роботи 1-2*	За розкладом занять	12
	Змістовий модуль 2	*Лабораторні роботи 3-4 Тестування*	За розкладом занять	18
розділ 2	*Змістовий модуль 3*	*Лабораторні роботи 5-6*	За розкладом занять	12
	Змістовий модуль 4	*Лабораторні роботи 7-8 Тестування*	За розкладом занять	18
Підсумковий контроль (max 40%)				
Індівідуальне завдання				20
Підсумковий тест або/та опитування				**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**	**Контрольний захід**	**Кількість балів**
		Змістовий модуль 1	
Тиждень 1-2 Лекція 1-2	Історія побудови платіжних систем	Лабораторна робота 1	6

Лабораторна робота 1	Захист інформації в комплексі "GBANK"		
		Змістовий модуль 1	
Тиждень 3-4 Лекція 3-4 Лабораторна робота 2	Правові засади побудови платіжних систем Захист бази даних Microsoft Access та її об'єктів на рівні користувача	Лабораторна робота 2	6
		Змістовий модуль 2	
Тиждень 5-6 Лекція 5-6 Лабораторна робота 3	Місце платіжних систем у загальному плані захисту інформації Коди, що виявляють та виправляють помилки	Лабораторна робота 3	6
		Змістовий модуль 2	
Тиждень 7-8 Лекція 7-8 Лабораторна робота 4	Основні види атак на інформацію. Моделювання атак.	Тестування Лабораторна робота 4	12
		Змістовий модуль 5	
Тиждень 9-10 Лекція 9-10 Лабораторна робота 5	Основні методи захисту інформації в інформаційних системах. Ідентифікація та аудентифікація користувача. Протоколи захисту. Побудова та аналіз систем протоколювання	Лабораторна робота 5	6
		Змістовий модуль 3	
Тиждень 11-12 Лекція 11-12 Лабораторна робота 6	Розподіл прав доступу. Контроль цілосності інформації. Контрольні розряди, контрольні суми. Цифровий електронний підпис.	Лабораторна робота 6	6
		Змістовий модуль 4	
Тиждень 13-14 Лекція 13-14 Лабораторна робота 7	Шифрування інформації. Резервне копіювання.	Лабораторна робота 7	6
		Змістовий модуль 4	
Тиждень 15-16 Лекція 15-16	Моделі політики безпеки. Модель Бела	Тестування Лабораторна робота 8	12

Лабораторна робота 8	Лападулла.		

ОСНОВНІ ДЖЕРЕЛА

Основна:

1. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2016. – 636 с. Допоміжна література
2. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці : Видавничий дім "РОДОВІД", 2014. – 428 с.
3. Корченко А. О. Банківська безпека. / А. О. Корченко, Л. М. Скачек, В. О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.

Додаткова:

1. Комп'ютерна злочинність і інформаційна безпека / А. П. Леонов ; за заг. ред. А. П. Леонова. - Мінськ : АРІЛ, 2000. - 552 с.
2. Системы поддержки принятия решений: учебное пособие / Уринцов А. И, Дик В. В - М. : МЭСИ, 2008. – 230 с.
3. Галатенко В.А. Основы информационной безопасности. М.: Изд-во ИНТУИТ.ру, 2005. - 208 с
4. Задірака В. К., Олексюк О. С. Методи захисту фінансової інформації. Київ: Вища школа, 2009. 460 с.
5. Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12.
6. Закон України «Про захист інформації в автоматизованих системах». URL: https://zakon.rada.gov.ua/laws/show/2594-15.
7. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12.
8. Закон України «Про науково-технічну інформацію». URL: https://zakon.rada.gov.ua/laws/show/848-19.
9. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. Київ: Держстандарт України, 1998.
10. Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2014. — 240 p. — ISBN 9780128008126.
11. Stewart, James Michael. CISSP® : Certified Information Systems Security Professional Study Guide : [англ.] / James Michael Stewart, Mike Chapple, Darril Gibson. — Seventh Edition. — Canada : John Wiley & Sons, Inc., 2015. — 1023 p. — ISBN 978-1-119-04271-6.
12. Moore, Robert. Cybercrime : Investigating High Technology Computer Crime : [англ.]. — 2nd ed. — Boston : Anderson Publ., 2011. — 318 p. — ISBN 9781437755824.
13. Phishing attacks and countermeasures / Ramzan, Zulfikar // Handbook of Information and Communication Security : [англ.] / Peter Stavroulakis, Mark Stamp. — L. : Springer Science & Business Media, 2010. — 867 p. — ISBN 978-3-642-04117-4.
14. Johnson, John. The Evolution of British Sigint : 1653–1939 : [англ.]. — Her Majesty's Stationary Office, 1998. — 58 p.
15. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Москва: Книжный мир, 2009. 352 с.
16. Кузнецов О. О., Євсеєв С. П., Король О. Г. Захист інформації в інформаційних системах. Методи традиційної криптографії. Харків : Вид. ХНЕУ, 2010. 316 с.
17. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації. Чернівці: Видавничий дом «Родовід», 2014. 428 с.
18. Столлингс Вильям. Криптография и защита сетей: принципы и практика. 2-е изд. Москва: Издательский дом «Вильямс», 2008. 672 с.

19. Поповский В. В., Персиков А. В. Защита информации в телекоммуникационных системах: учебн.: в 2 т. Харьков: ООО «Компания СМИТ», 2006. Т. 1. 292 с.
20. Вербіцький О. В. Вступ до криптології. Львів: Наук.-техн. літ., 1998. 248 с.
21. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. Санкт-Питербург: Питер, 2008. 272 с.
22. Бабаш А. В., Шанкин Г. П. История криптографии. Часть I. Москва: Гелиос АРВ, 2002.
23. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. Москва: ДМК, 2000. 448 с.
24. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва: Единая Европа, 1994.

Інформаційні джерела:

1. Виды и классификация атак на информационные системы https://igorosa.com/vidy-i-klassifikaciya-atak-na-informacionnye-sistemy/
2. ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. management [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341 1 6
3. ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber =46414
4. ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=464 13
5. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. – Режим доступа к ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11423
6. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanoviz-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii
7. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. – Режим доступа к ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11425
8. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Электронный ресурс]. – Режим доступа к ресурсу: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr13335-4-2005.
9. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. – Режим доступа к ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11427. 16. ISO/IEC 27001:2013
10. Information technology – Security techniques – Information security management systems – Requirements. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=545 34.

11. ISO/IEC 27002:2013 – Information technology -- Security techniques – Code of practice for information security controls. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber =54533 1 7
12. ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/search.htm?qt=ISO%2FIEC+27006%3A2015+&so rt=rel&type=simple&published=on.
13. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). [Электронный ресурс]. – Режим доступа к ресурсу: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf
14. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Электронный ресурс]. – Режим доступа к ресурсу: http://s-byte.com/useful/27002.pdf
15. Безпека інформаційних систем [Электронный ресурс]. – Режим доступа к ресурсу: https://naurok.com.ua/test/bezpeka-informaciynih-sistem-219481.html
16. Методи захисту інформації: види загроз і засоби захисту, класи безпеки [Электронный ресурс]. – Режим доступа к ресурсу: http://guverina.org.ua/news/uk/bezopasnost-metodi-zahistu-informacii-vidi-zagroz-i-zasobi-zahistu-klasi-bezpeki/
17. Європейські стандарти захисту інформації в Україні [Электронный ресурс]. – Режим доступа к ресурсу: https://nt.ua/blog/isms
18. Про засади інформаційної безпеки України: проект Закону № 4949 від 28.05.2014 р. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[2]

Відвідування занять. Регуляція пропусків.
Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Студенти, які за певних обставин не можуть відвідувати практичні 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 UniCheck. 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

[2] *Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, реактивів тощо. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!*

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.
Під час виконання заходів контролю (тестів, 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 розміщуються викладачем на форумі курсу. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити студентів подаються викладачем впродовж тижня, або на чергові консультації.
Якщо за технічних причин доступ до Moodle є неможливим, або ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу ainc@ukrpost.net. У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Економічний факультет
Силабус навчальної дисципліни

ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2020-2021 рр.

ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ 2020-2021 н. р. *(посилання на сторінку сайту ЗНУ)*

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/ycyfws9v. 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 (061)228-15-84 (щоденно з 9 до 21).

ЗАПОБІГАННЯ КОРУПЦІЇ. Уповноважена особа з питань запобігання та виявлення корупції (Воронков В. В., 1 корп., 29 каб., тел. +38 (061) 289-14-18).

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 17.00; субота з 09.00 до 15.00.

ЕЛЕКТРОННЕ ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE): https://moodle.znu.edu.ua
Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресами:
· для студентів ЗНУ - moodle.znu@gmail.com, Савченко Тетяна Володимирівна
· для студентів Інженерного інституту ЗНУ - alexvask54@gmail.com, Василенко Олексій Володимирович
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