БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Викладач: к.ф.-м.н., доц. Леонтьєва Вікторія Володимирівна.
Кафедра: фундаментальної та прикладної математики, 1й корп. ЗНУ, ауд. 21-б (1й поверх)
E-mail: : vleonteva15@gmail.com
Телефон: (061) 289-12-24 (кафедра), 289-41-11 (деканат)
Інші засоби зв'язку: *Moodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти		Прикладна математика. Бакалавр				
Статус дисципліни		Вибіркова				
Кредити ECTS	4	**Навч. рік**	2022-2023 2 семестр	**Рік навчання - 4**	**Тижні**	14
Кількість годин	120	**Кількість змістових модулів[1]**		**6**	**Лекційні заняття – 14 год Лабораторні заняття –14 год Самостійна робота – 92 год.**	
Вид контролю	*Екзамен*					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=15649				
Консультації: *особисті* – щотижнево за розкладом (1 год.), І корпус, ауд. 21-б (1й поверх); *дистанційні* – Zoom, за попередньою домовленістю. *Запис на консультації:* особисті повідомлення в Moodle						

ОПИС КУРСУ

Метою курсу є оволодіння знаннями та вміннями, які утворять теоретичний і практичний фундамент, необхідний для комплексного підходу до розв'язання питань інформаційної безпеки, аналізу якості систем захисту інформації й отримання навичок управління інформаційною безпекою.

Основними **завданнями** вивчення дисципліни «Безпека програм та даних» є:

- теоретичних основ проблеми зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення конфіденційної інформації, способів захисту від несанкціонованого доступу до інформації;
- набуття вмінь та практичних навичок використання методологічних, організаційних та наукових основ розробки засобів і систем збору та захисту інформації;
- набуття вмінь та навичок щодо забезпечення інформаційної безпеки процесів опрацювання, зберігання та поширення інформації в інформаційно-комунікаційних мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем і засобів здійснення погроз з боку потенційних порушників.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

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

1. Формулювати математичну постановку задачі захисту інформації.
2. Опираючись на математичні засади симетричної криптографії вибирати методи стосовно задачі, що розв'язується.
3. Розробляти програми із застосуванням методів криптографічного захисту інформації.
4. Застосовувати методи асиметричного шифрування, цифрового підпису та хешування.

---

[1] **1 змістовий модуль = 15 годин (0,5 кредита ECTS). Детальна формула розрахунку – в рекомендаціях.**

5. Застосовувати базові криптографічні протоколи
6. Дотримуватися міжнародних принципів академічної доброчесності (research conduct).
7. Писати тези наукових доповідей, грантові пропозиції і публічно презентувати їх.

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких **компетентностей**:

ЗК1 Здатність до абстрактного мислення, аналізу та синтезу
ЗК6 Здатність вчитися і оволодівати сучасними знаннями
СК1 Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування
СК3 Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем
СК6 Здатність до системного мислення, застосування методології системного аналізу для дослідження складних проблем різної природи, методів формалізації та розв'язування системних задач, що мають суперечливі цілі, невизначеності та ризики

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. Інформаційна безпека : навч. посіб. Львів : вид-во Львівської політехніки, 2019. 580 с.
2. Лісовська Ю. П. Інформаційна безпека України : навч. посіб. Київ : вид-во Кондор, 2018. 172 с.

Презентації, завдання лабораторних та самостійних робіт, методичні рекомендації до виконання лабораторних та самостійних робіт, розміщені на платформі Moodle: https://moodle.znu.edu.ua/course/view.php?id=15649 ***кожного заняття рекомендуються додаткові джерела (див. Moodle).***

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи (max 60 балів):

Лабораторні роботи – 6 робіт, виконання і захист кожної оцінюється в 4 бали. Загалом **24 балів.**

Самостійні роботи – 6 робіт, виконуються самостійно, а складання кожної оцінюється в 4 бали. Загалом **24 бали**.

Частина лабораторних та самостійних робіт передбачає представлення їх на занятті. Якщо студент відмовляється представляти доповідь або матеріали, він отримує кількість балів меншу на 1 бал.

Поточні контрольні роботи – 2 тести по 6 балів кожен (проводяться на базі Moodle). Загалом **12 балів**.

Підсумкові контрольні заходи:

Залік складається з 3 запитань: 2 теоретичних та 1 практичного. Методичне забезпечення іспиту: Moodle: https://moodle.znu.edu.ua/course/view.php?id=15649. Оцінювання: теоретичні запитання по 20 балів, практичне завдання – 20 балів. Загалом **40 балів**.

Контрольний захід		**Термін виконання**	**% від загальної оцінки**
Поточний контроль (max 60%)			
Змістовий модуль 1	Лабораторна робота №1	1-2 тиждень	4%
	Самостійна робота №1	2 тиждень	4%
	тестове завдання контрольної роботи №1	6 тиждень	2%
Змістовий модуль 2	Лабораторна робота №2	3-4 тиждень	4%
	Самостійна робота №2	4 тиждень	4%
	тестове завдання контрольної роботи №1	6 тиждень	2%
Змістовий модуль 3	Лабораторна робота №3	5-6 тиждень	4%
	Самостійна робота №3	6 тиждень	4%
	тестове завдання контрольної роботи №1	6 тиждень	2%
Змістовий модуль 4	Лабораторна робота №4	7-8 тиждень	4%
	Самостійна робота №4	8 тиждень	4%
	тестове завдання контрольної роботи №2	12 тиждень	2%
Змістовий модуль 5	Лабораторна робота №5	9-10 тиждень	4%
	Самостійна робота №5	10 тиждень	4%
	тестове завдання контрольної роботи №2	12 тиждень	2%
Змістовий модуль 6	Лабораторна робота №6	11-12 тиждень	4%
	Самостійна робота №6	13-14 тиждень	4%
	тестове завдання контрольної роботи №2	14 тиждень	2%
Підсумковий контроль (max 40%)			
Два теоретичних завдання заліку		За розкладом	20%
Практичне завдання заліку		За розкладом	20%
Разом			**100%**

Критерії оцінювання:

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 змістового модулю	Зміст і контрольний захід	Кількість балів
Змістовий модуль 1. *Основні напрямки розвитку інформаційної безпеки*			
Тиждень 1 Лекція	Передумови та основні напрямки розвитку інформаційної безпеки	Загальні відомості. Ризики, їх класифікація. Способи порушення інформаційної безпеки. Організаційне забезпечення інформаційної безпеки.	
Тиждень 1-2 Лабораторна робота	Лабораторна робота №1 Шифри Полібія, Цезаря, Тритемія.	Шифрування та дешифрування на основі квадрату Полібія. Шифрування та дешифрування на основі шифру Цезаря. Шифрування та дешифрування на основі таблиці Тритемія. Опитування на парі. Захист лабораторної роботи. Представлення звіту з лабораторної роботи та доповіді. Звіт з лабораторної роботи та доповідь завантажуються в Moodle.	4
Тиждень 2 Самостійна робота студента	Самостійна робота студента №1. Передумови та основні напрямки розвитку інформаційної безпеки	Загальні відомості. Ризики, їх класифікація. Способи порушення інформаційної безпеки. Організаційне забезпечення інформаційної безпеки. Підготовка доповіді та презентації. Захист самостійної роботи	4
Змістовий модуль 2. *Основні методи захисту інформаційних систем*			
Тиждень 3. Лекція	Методи захисту інформаційних систем. Основні методи шифрування. Потокові та блокові криптографічні алгоритми	Методи захисту інформаційних систем. Загальні поняття та визначення. Принципи створення криптографічних алгоритмів. Модель захищеної комп'ютерної системи. Криптографічні примітиви. Класифікація методів шифрування. Потокові криптографічні алгоритми: шифр Цезаря, шифр «алфавітне додавання», шифр Полібія, шифр «модульна арифметика», шифр «подвійний квадрат». Блокові криптографічні алгоритми: шифр «жезл», шифр стандартної перестановки, шифр вертикальної перестановки, шифри з використанням комбінованих перестановок, шифри – трафарети, квадрат та прямокутник Кардано.	
Тиждень 3-4 Лабораторна робота	Лабораторна робота №2 Шифри Віженера	Шифрування та дешифрування на основі 1-го шифру Віженера. Шифрування та дешифрування на основі 2-го шифру Віженера (шифру з автоключем). Шифрування та дешифрування на основі 3-го шифру Віженера (шифру з періодичним ключем). Опитування на парі. Захист лабораторної роботи. Представлення звіту з лабораторної роботи та доповіді. Звіт з лабораторної роботи та доповідь завантажуються в Moodle.	4

Тиждень і вид заняття	Тема змістового модулю	Зміст і контрольний захід	Кількість балів
Тиждень 4 Самостійна робота студента	Самостійна робота студента №2. Методи захисту інформаційних систем. Основні методи шифрування. Потокові та блокові криптографічні алгоритми	Підготовка доповіді та презентації. Захист самостійної роботи.	4
Змістовий модуль 3. *Криптосистеми та їх використання в інформаційній безпеці*			
Тиждень 5 Лекція	Складові симетричні, асиметричні та гібридні криптосистеми	Складові симетричні криптосистеми: багатоалфавітна криптосистема Віжинера, багаторівнева криптосистема DES, багаторівнева криптосистема ГОСТ 28147-89, новий стандарт симетричного шифрування. Асиметричні та гібридні криптосистеми: криптосистема RSA, алгоритм шифрування Ель Гамаля, порівняльний аналіз асиметричних криптосистем, комбіновані криптосистеми, розповсюдження ключів.	
Тиждень 5-6 Лабораторна робота	Лабораторна робота №3. Шифри Кардано і Арджeнті.	Шифрування та дешифрування на основі поворотної решітки. Шифрування та дешифрування на основі шифру Арджeнті. Опитування на парі. Захист лабораторної роботи. Представлення звіту з лабораторної роботи та доповіді. Звіт з лабораторної роботи та доповідь завантажуються в Moodle.	4
Тиждень 6 Самостійна робота студента	Самостійна робота №3. Складові симетричні, асиметричні та гібридні криптосистеми	Підготовка доповіді та презентації. Захист самостійної роботи.	4
Тиждень 6 Контрольна робота	Контрольна робота №1	Тестування в Moodle. Перевіряється on-line.	6
Змістовий модуль 4. *Інформаційна безпека на державному рівні: практика України*			
Тиждень 7 Лекція	Забезпечення інформаційної безпеки на державному рівні: практика України.	Визначення інформаційної безпеки, об’єкти, суб’єкти, основні складові. Система забезпечення інформаційної безпеки. Загрози інформаційній безпеці України у контексті діяльності Держспецзв'язку.	
Тиждень 7-8 Лабораторна робота	Лабораторна робота №4. Шифри з варіацією розміру «вікна шифрування» і Вернама	Шифрування та дешифрування з варіацією розміру «вікна» шифрування. Шифрування та дешифрування на основі шифру Вернама. Опитування на парі. Захист лабораторної роботи. Представлення звіту з лабораторної роботи та доповіді. Звіт з лабораторної роботи та доповідь завантажуються в Moodle.	4

Тиждень і вид заняття	Тема змістового модулю	Зміст і контрольний захід	Кількість балів
Тиждень 8 Самостійна робота студента	Самостійна робота студента №4. Забезпечення інформаційної безпеки на державному рівні: практика України	Визначення інформаційної безпеки, об'єкти, суб'єкти, основні складові. Система забезпечення інформаційної безпеки. Загрози інформаційній безпеці України у контексті діяльності Держспецзв'язку. Підготовка доповіді та презентації. Захист самостійної роботи.	4
Змістовий модуль 5. *Інформаційна безпека на державному рівні та криптографічні методи захисту*			
Тиждень 9. Лекція	Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту).	Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Криптографічний захист інформації. Науково-технічна діяльність.	
Тиждень 9-10 Лабораторна робота	Лабораторна робота № 5. Мережа Фейстеля.	Шифрування та дешифрування на основі мережі Фейстеля. Особливості застосування. Опитування на парі. Захист лабораторної роботи. Представлення звіту з лабораторної роботи та доповіді. Звіт з лабораторної роботи та доповідь завантажуються в Moodle.	4
Тиждень 10 Самостійна робота студента	Самостійна робота №5. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту)	Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Криптографічний захист інформації. Науково-технічна діяльність. Підготовка доповіді та презентації. Захист самостійної роботи.	4
Змістовий модуль 6. *Інформаційна безпека на державному рівні та технічні методи захисту*			
Тиждень 11 Лекція	Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту)	Технічний захист інформації в Україні, основні аспекти. Побудова і організаційна структура системи ТЗІ в Україні.	
Тиждень 11-12. Лабораторна робота	Лабораторна робота №6. Алгоритм RSA	Асиметрична криптосистема RSA та її використання. Алгоритм формування відкритого і секретного ключів. Опитування на парі. Захист лабораторної роботи. Представлення звіту з лабораторної роботи та доповіді. Звіт з лабораторної роботи та доповідь завантажуються в Moodle.	4
Тиждень 13,14 Самостійна робота студента	Самостійна робота №6. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту)	Технічний захист інформації в Україні, основні аспекти. Побудова і організаційна структура системи ТЗІ в Україні. Підготовка доповіді та презентації. Захист самостійної роботи.	4
Тиждень 14 Контрольна робота	Контрольна робота №2	Тестування в Moodle. Перевіряється on-line.	6

ОСНОВНІ ДЖЕРЕЛА

Книги:

1. Бобало Ю. Я., Горбатий І. В., Кіселичник М. Д. та ін. Інформаційна безпека : навч. посіб. Львів : вид-во Львівської політехніки, 2019. 580 с.
2. Лісовська Ю. П. Інформаційна безпека України : навч. посіб. Київ : вид-во Кондор, 2018. 172 с.
3. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
4. Лубко Д. В., Шаров С. В. Методи та системи штучного інтелекту : навч. посіб. Мелітополь : ФОП Однорог Т. В., 2019. 264 с.
5. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації : навч. посіб. Одеса : Фенікс, 2015. 264 с.
6. Голев Д. В. Методика оцінки інформаційної захищеності телекомунікацій : навч. посіб. Одеса : Одес. нац. акад. зв'язку ім. О. С. Попова, 2013. 218 с.
7. Захарченко М. В., Кононович В. Г., Кільдішев В. Й., Голев Д. В. Інформаційна безпека. Захист інформації у комп'ютерах та комп'ютерних мережах : навч. посіб. Одеса : Одес. нац. акад. зв'язку ім. О. С. Попова, 2011. 166 с.
8. Захарченко М. В., Голев Д. В., Русляченко О. Ю., Бєлова Ю. В. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. Одеса : Одес. нац. акад. зв'язку ім. О. С. Попова, 2012. 187 с.
9. Гороховський О. І. Інтелектуальні системи. Вінниця : Вінниц. нац. техн. університет, 2010. 193 с.
10. Кузнецов О. О., Євсеєв С. П., Король О. Г. Захист інформації в інформаційних системах. Методи традиційної криптографії. Харків : Вид. ХНЕУ, 2010. 316 с.
11. Браіловський М. М., Лазарєв Г. П., Хорошко В. О. Захист інформації у банківській діяльності. Київ : ТОВ «ПоліграфКонсалтинг», 2010. 216 с.
12. Бабак В. П. Теоретичні основи захисту інформації: підручник. Київ : Книжкове вид-во НАУ, 2008. 752 с.
13. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи. Київ : Видавничий дім «СофтПрес», 2005. 316 с.
14. Вербіцький О. В. Вступ до криптології. Львів : ВНТЛ, 1998. 248 с.
15. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ : Видавнича група BHV, 2009. 608 с.
16. Кузнецов О. О., Євсеєв С. П., Король О. Г. Захист інформації в інформаційних системах. Харків : Вид. ХНЕУ, 2011. 510 с.
17. Скобелєв В. Г. Основи захисту інформації : навч. посіб. Донецьк : ДонНТУ, 2006. 173 с.

Інформаційні ресурси

1. Електронні ресурси з математики. *Бібліотека TWIRPX*. URL : https://www.twirpx.com/files/#files_mathematics.
2. Електронні ресурси з інформатики та обчислювальної техніки. *Бібліотека TWIRPX*. URL : https://www.twirpx.com/files/#files_informatics.
3. Наукові ресурси. *Національна бібліотека України імені В. І. Вернадського*. URL : http://www.nbuv.gov.ua/node/1539.
4. Mathematics. *UMass Boston Open Courseware*. URL : http://ocw.umb.edu/mathematics.html.
5. Science, Maths & Technology. *Learning Space. The Open University*. URL : https://www.open.edu/openlearn/science-maths-technology.

6. Maths Resources Index. *The Economics Network*. URL : https://www.economicsnetwork.ac.uk/subjects/mathsforeconomists.
7. Maplesoft Media Releases. *Mathematics-based software & services for education, engineering, and research*. URL : https://www.maplesoft.com/company/news/releases/2021/2021-03-10-maple-2021-provides-even-more-tools-to-help-students-learn-math.aspx.
8. Ієрархічний рубрикатор інтелектуальних систем. *RAAI.* URL : http://www.raai.org/.
9. Хмарна інфраструктура E-cloud з КСЗІ. *GIGACLOUD.UA*. URL : https://cutt.ly/33fDk0j.
10. Загальні критерії. *ISOFTS*. URL : http://www.isofts.kiev.ua/c/.../get_file.
11. Законодавча та нормативна база України в області ТЗІ и КЗІ. *BEZPEKA.COM.* URL : http://www.bezpeka.com/ru/lib /lawua.html.
12. Концепція технічного захисту інформації в Україні. *Офіційний вебпортал парламенту України*. URL : http://zakon1.rada.gov.ua/cgibin/laws /main.cgi?nreg=1126-97-%EF.
13. Украинский ресурс по безопасности. *KIEV-SECURITY.ORG.UA.* URL : http://kiev-security.org.ua.
14. ISO/IEC 7498-2:1989 – Information processing systems – Open Systems Interconnection – Basic Reference Model. *Security Architecture*. URL : http://www.iso.org/iso/catalogue_detail. htm? csnumber=14256.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[2]

Відвідування занять. Регуляція пропусків.
Відвідування занять обов'язкове, оскільки курс зорієнтовано на максимальну практику використання методики розв'язання питань інформаційної безпеки програм та даних, аналізу якості систем захисту інформації й управління інформаційною безпекою. Очікується, що і викладач, і студенти в аудиторії постійно застосовують методики розв'язання питань інформаційної безпеки та різні методи захисту інформації. Будь ласка, беріть участь у дискусіях, навіть якщо соромитеся чи не впевнені у своїх знаннях!
Завдання мають бути виконанні перед заняттями. Пропуски можливі лише з поважної причини. Відпрацювання пропущених занять має бути регулярним за домовленістю з викладачем у години консультацій. Накопичення відпрацювань неприпустиме! 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
Будь ласка, вимкніть на беззвучний режим свої мобільні телефони та не користуйтеся ними під час занять. Мобільні телефони відволікають викладача та ваших колег. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Електронні пристрої можна використовувати лише за умови виробничої необхідності в них (за погодженням з викладачем).

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*. Адреси типу user123@gmail.com не приймаються!

[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!*

ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2022-2023 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