ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ПІДПРИЄМНИЦТВА ТА ФІНАНСІВ
Силабус навчальної дисципліни

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Викладач: *доктор економічних наук, доцент Клопов Іван Олександрович*
Кафедра: *інформаційних технологій, підприємництва та фінансів,*
Корпус 10, ауд. 416
E-mail: *klopov@znu.edu.ua*
Телефон:
Інші засоби зв'язку: *Moodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти:		Інформаційна економіка Бакалавр					
Статус дисципліни:		Обов'язкова					
Кредити ECTS	5	**Навч. рік:**	2022-23	**Рік навчання**	1	**Тижні**	14
Кількість годин	150	**Кількість змістових модулів**	8	**Лекційні заняття** – 32 **Лабораторні заняття** – 32 **Самостійна робота** – 86			
Вид контролю:		Залік					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=14454					
Консультації: *особисті – вівторок, четвер, з 11:00 до 13:00, корпус 11, ауд. 416;* *дистанційні – Zoom, за попередньою домовленістю*							

ОПИС КУРСУ

Метою *вивчення навчальної дисципліни «Інформаційна безпека та захист інформації» є формування знань і навичок, необхідних для формалізованого опису, синтезу й аналізу, криптографічних систем.*

Основні ***завдання*** *вивчення дисципліни «Інформаційна безпека та захист інформації» полягають в тому, щоб ознайомити студентів з основами математичних теорій, на яких ґрунтуються криптографія та криптоаналіз, і навчити їх практичному застосуванню цих основ для розв'язання конкретних задач криптографії та криптоаналізу; ознайомити з сучасними криптографічними алгоритмами й протоколами, відомими підходами до аналізу криптосистем та тенденціями розвитку криптографії та криптоаналізу, навчити методам синтезу й аналізу криптосистем.*

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У разі успішного завершення курсу студент зможе:

- розуміти принципи економічної науки, особливості функціонування економічних систем.
- застосовувати аналітичний та методичний інструментарій для обґрунтування пропозицій та прийняття управлінських рішень різними економічними агентами (індивідуумами, домогосподарствами, підприємствами та органами державної влади).
- пояснювати моделі соціально-економічних явищ з погляду фундаментальних принципів і знань на основі розуміння основних напрямів розвитку економічної науки.
- застосовувати відповідні економіко-математичні методи та моделі для вирішення економічних задач.

– проводити аналіз функціонування та розвитку суб'єктів господарювання, визначати функціональні сфери, розраховувати відповідні показники які характеризують результативність їх діяльності.

– ідентифікувати джерела та розуміти методологію визначення і методи отримання соціально-економічних даних, збирати та аналізувати необхідну інформацію, розраховувати економічні та соціальні показники.

– виконувати міждисциплінарний аналіз соціально- економічних явищ і проблем в однієї або декількох професійних сферах з врахуванням ризиків та можливих соціально-економічних наслідків.

Загальні компетентності:

ЗК4. Здатність застосовувати знання у практичних ситуаціях.

ЗК8. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові, предметні) компетентності

СК2. Здатність здійснювати професійну діяльність у відповідності з чинними нормативними та правовими актами.

СК7. Здатність застосовувати комп'ютерні технології та програмне забезпечення з обробки даних для вирішення економічних завдань, аналізу інформації та підготовки аналітичних звітів.

СК14. Здатність поглиблено аналізувати проблеми і явища в одній або декількох професійних сферах з врахуванням економічних ризиків та можливих соціально-економічних наслідків.

СК 15. Розуміння принципів, функцій і домінант інформаційної економіки як особливої та самостійної парадигми світового економічного світогляду.

СК 18. Навички використання пакетів прикладних програм, прикладного комп'ютерного програмного забезпечення, спеціалізованих цифрових сервісів для вирішення задач аналізу і синтезу соціально-економічних, математичних, інформаційних та інших складних систем.

Програмні результати навчання:

ПРН4. Розуміти принципи економічної науки, особливості функціонування економічних систем.

ПРН5. Застосовувати аналітичний та методичний інструментарій для обґрунтування пропозицій та прийняття управлінських рішень різними економічними агентами (індивідуумами, домогосподарствами, підприємствами та органами державної влади).

ПРН7. Пояснювати моделі соціально-економічних явищ з погляду фундаментальних принципів і знань на основі розуміння основних напрямів розвитку економічної науки.

ПРН8. Застосовувати відповідні економіко-математичні методи та моделі для вирішення економічних задач.

ПРН10. Проводити аналіз функціонування та розвитку суб'єктів господарювання, визначати функціональні сфери, розраховувати відповідні показники які характеризують результативність їх діяльності.

ПРН13. Ідентифікувати джерела та розуміти методологію визначення і методи отримання соціально-економічних даних, збирати та аналізувати необхідну інформацію, розраховувати економічні та соціальні показники.

ПРН17. Виконувати міждисциплінарний аналіз соціально- економічних явищ і проблем в однієї або декількох професійних сферах з врахуванням ризиків та можливих соціально-економічних наслідків.

ПРН 19. Використовувати інформаційні та комунікаційні технології для вирішення соціально-економічних завдань, підготовки та представлення аналітичних звітів.

ПРН 25. Проводити системний аналіз реальних об'єктів інформатизації, обґрунтовувати вибір інформаційних і комунікаційних технологій для комп'ютерної реалізації їх інформаційних моделей з врахуванням ризиків інформаційної безпеки та кібербезпеки.

ПРН 30. Застосовувати міждисциплінарні методи дослідження на стику економіки, менеджменту, математики, інформатики та інших наук і відповідні прикладні інформаційні та комунікаційні системи й технології для вирішення завдань інформатизації управлінської діяльності економічних систем.

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

1. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник. Черкаси: ЧДТУ, 2018. 223 с.
2. Технології захисту інформації: підручник для студ. / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
3. Al Sweigart Cracking Codes with Python. An Introduction to Building and Breaking Ciphers. Al Sweigart, 2018. 416 p.
4. Матеріали лекцій дисципліни «Інформаційна безпека та захист інформації» (платформа Moodle в Системі електронного забезпечення навчання ЗНУ).
5. Тестові завдання до лекційного матеріалу дисципліни «Інформаційна безпека та захист інформації» (платформа Moodle в Системі електронного забезпечення навчання ЗНУ).
6. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Інформаційна безпека та захист інформації» (платформа Moodle в Системі електронного забезпечення навчання ЗНУ).

КОНТРОЛЬНІ ЗАХОДИ

Поточні контрольні заходи.

На змістовні модулі передбачено два види контрольних заходів:

- *контрольний захід, що діагностує рівень засвоєння теоретичних знань (усне опитування та тестування);*
- *контрольний захід, що діагностує рівень сформованості вмінь і навичок (ситуаційне або аналітичне завдання).*

Бали за кожен змістовий модуль усього, теоретичне і практичне завдання, становлять 1-4 модуль по 7 балів, 5-8 модуль по 8 балів , що у сумі складає 60 балів.

Підсумкові контрольні заходи:

На підсумковий семестровий контроль також передбачено 2 контрольні заходи (теоретичне і практичне завдання), вага кожного завдання складає 20 балів, загальна кількість за підсумковий семестровий контроль складає 40 балів.

Додаткові види роботи (бальна система стимулювання активності студентів) *- це система додаткових балів, яку введено з метою заохочування студентів до планомірної, систематичної роботи з опанування теоретичним матеріалом і поглибленого оволодіння ними практичними навичками, які передбачено цим курсом. Ці додаткові бали можуть стати вирішальними для отримання більш високої оцінки за весь курс! Тому, НАПОЛЕГЛИВО РЕКОМЕНДУЄМО студентові скористатися цією нагодою СУТТЄВО підвищити свій загальний бал, отриманий після виконання всіх обов`язкових видів контрольних заходів!*

Позааудиторна навчальна активність *як один з видів врахування програмних результатів вивчення цієї дисципліни студентом у формі самоосвіти (неформальна або інформальна) та підтвердження їх відповідним документом (диплом, сертифікат, свідоцтво тощо). Якщо програмні результати, отримані під час вивчення конкретного змістового модуля, зі знаннями й уміннями, одержаними під час позанавчальної самоосвіти (онлайн-курси, розміщені на відкритих навчальних платформах, воркшопи, вебінари, майстер-класи, тренінги тощо) відповідають вимогам робочої програми навчальної дисципліни, то студент звільняється від виконання поточних контролів з цього змістового модуля, а результати зараховуються йому «автоматом» з максимальною бальною оцінкою відповідно до критеріїв оцінювання. У випадку, коли програмні результати частково відповідають вимогам (неповні, схожі, але зі спорідненої галузі знань тощо), викладач має право або звільнити студента від складання окремих поточних контролів у межах цього змістового модуля, або при їх складанні оцінити за максимальним балом.*

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

№ змістового модуля	Види поточних контрольних заходів	Зміст поточного контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
1	Тест 1	Питання для підготовки: Поняття інформаційної безпеки комп'ютерних систем. Апаратно-програмні засоби захисту інформації. Основні елементи політики безпеки інформаційних систем.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	**3**
	Лабораторна робота 1	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 1	**2**			**7**
2	Тест 2	Питання для підготовки: Класифікація методів криптографічного захисту інформації. Шифрування інформації методами підстановок та перестановок. Шифрування інформації методами гамування та аналітичних перетворень.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	**3**

		Комбіновані методи. Концепція криптосистем з відкритим ключем.		
	Лабораторна робота 2	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 2	**2**			**4**
3	Тест 3	Питання для підготовки: Класифікація методів криптографічного захисту інформації. Шифрування інформації методами підстановок та перестановок. Шифрування інформації методами гамування та аналітичних перетворень. Комбіновані методи. Концепція криптосистем з відкритим ключем.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	**3**
	Лабораторна робота 3	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 3	**2**			**7**
4	Тест 4	Питання для підготовки: Проблема аутентифікації даних та електронний цифровий підпис. Хеш-функція та особливості її використання. Алгоритм шифрування електронного цифрового підпису RSA.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,3 бали.	**3**
	Лабораторна робота 4	Вимоги до виконання та оформлення: Лабораторна робота у	Кожне завдання лабораторної роботи за змістовим модулем	**4**

		вигляді файлу завантажена на сайт системи Moodle ЗНУ.	оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	
Усього за ЗМ 4	**2**			**7**
5	Тест 5	Питання для підготовки: Методи захисту програм від копіювання. Методи захисту компакт-дисків від копіювання. Комп'ютерна графологія.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,4 бали.	**4**
	Лабораторна робота 5	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 5	**2**			**8**
6	Тест 6	Питання для підготовки: Класифікація програм з потенційно небезпечними наслідками. Міжмережеві екрани.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,4 бали.	**4**
	Лабораторна робота 6	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 6	**2**			**8**
7	Тест 7	Питання для підготовки: Моделі комп'ютерних атак та етапи їх реалізації. Безпека систем електронної комерції. Безпека електронних	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь	**4**

		платіжних систем.	оцінюється у 0,4 бали.	
	Лабораторна робота 7	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 7	**2**			**8**
8	Тест 8	Питання для підготовки: Безпека інформаційних ресурсів у ІКСМ. Організація технічного захисту інформації. Методика і критерії оцінки захищеності інформації. Захист інформації на базі ISO/IEC.	Тестові питання оцінюються: правильно/ неправильно. Кількість питань – 10. Правильна відповідь оцінюється у 0,4 бали.	**4**
	Лабораторна робота 8	Вимоги до виконання та оформлення: Лабораторна робота у вигляді файлу завантажена на сайт системи Moodle ЗНУ.	Кожне завдання лабораторної роботи за змістовим модулем оцінюється від 1 до 4 балів з урахуванням відповідей на запитання при захисті роботи. Загальна максимальна сума балів визначається кількістю завдань в роботі.	**4**
Усього за ЗМ 8	**2**			**8**
Усього за змістові модулі	**16**			**60**

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)		

ОСНОВНІ ДЖЕРЕЛА

Основна:

1. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник. Черкаси: ЧДТУ, 2018. 223 с.
2. Технології захисту інформації: підручник для студ. / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
3. Al Sweigart Cracking Codes with Python. An Introduction to Building and Breaking Ciphers. Al Sweigart, 2018. 416 p.

Додаткова:

1. Лужецький В. А. Інформаційна безпека : навчальний посібник. Вінниця : УНІВЕРСУМ-Вінниця. 2019. 240 с.
2. Лужецький В. А. Захист персональних даних : навчальний посібник. Вінниця : УНІВЕРСУМ-Вінниця, 2017. 248 с.
3. Грайворонський М. В. Безпека інформаційно-комунікаційних систем. Київ : Вид.група BUV, 2019. 608 с.
4. Лісовська Ю. П. Інформаційна безпека України : навчальний посібник для студентів вищих навчальних закладів. Київ : Кондор, 2020. 170 с.
5. Sean Smith The Internet of Risky Things: Trusting the Devices That Surround Us 1st Edition. O'Reilly Media. 2017. 240 p.

Інформаційні ресурси:

1. Закон України «Про інформацію» : за станом на 1 січня 2013 р. / Верховна Рада України. Офіц. вид. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : за станом на 1 січня 2013 р. / Верховна Рада України. Офіц. вид. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0
3. Портал безпека [Електронний ресурс]. URL : www.bezpeka.com
4. Національна бібліотека України імені В. І. Вернадського. URL: http://www.nbuv.gov.ua/

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ

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 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.orgma 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 (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 CiscoWebex та ін. – регулярно розміщуються викладачем на форумі курсу. 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 технічнихпричин доступ до Moodleє неможливим, або ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу klopov@znu.edu.ua. У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ПІДПРИЄМНИЦТВА ТА ФІНАНСІВ
Силабус навчальної дисципліни

ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2022-2023

ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ: *http://sites.znu.edu.ua/navchalnyj_viddil/1635.ukr.html*

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.

ОСВІТНІЙ 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.

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

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога (061)228-15-84 (щоденно з 9 до 21).

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.