ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Викладач: *Горелікова Тетяна Олексіївна*
Кафедра: *комп'ютерних наук, І корпус, ауд. 39*
E-mail: *horelikova.t@znu.edu.ua*
Телефон: *(061) 289-12-57*
Інші засоби зв'язку: M*oodle (форум курсу, приватні повідомлення)*

Освітня програма, рівень вищої освіти:		Кібербезпека та захист інформації Бакалавр					
Статус дисципліни:		Обов'язкова					
Кредити ECTS	6	**Навч. рік:**	2026-2027 1 семестр	**Рік навчання**	4	**Тижні**	16
Кількість годин	180	**Кількість змістових модулів**	3	**Лекційні заняття** – 32 год **Лабораторні заняття** – 32 год **Самостійна робота** – 116 год			
Вид контролю:		Іспит					
Посилання на курс в Moodle		https://moodle.znu.edu.ua/course/view.php?id=18584					
Консультації: особисті щотижнево за розкладом (1 год.), дистанційні – Zoom, за попередньою домовленістю Запис на консультації: особисті повідомлення в Moodle							

ОПИС КУРСУ

Навчальна дисципліна присвячена захисту інформації від її несанкціонованого отримання через технічні канали. У курсі розглядаються види загроз і технічних каналів витоку інформації, методи та технічні засоби протидії, пошукові заходи, інструментальний контроль захищеності об'єктів і принципи побудови комплексної системи захисту інформації. Курс зосереджений на технічному захисті інформації на рівні об'єкта, обладнання, інформаційних ліній та технічних засобів. При цьому курс не передбачає поглибленого вивчення фізики процесів, а зосереджується на практичному виборі методів і засобів захисту, їх перевірці та комплексному застосуванні.

Програмні результати навчання	
ПРН1	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки
ПРН2	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки
ПРН3	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
ПРН4	Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах

ПРН5	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки
ПРН6	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)
ПРН7	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту
ПРН8	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем
ПРН9	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах
ПРН10	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки
ПРН11	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно-телекомунікаційних системах, ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів
ПРН12	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки
ПРН13	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів
ПРН14	Вирішувати задачі забезпечення безперервності бізнес- процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами

ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, презентаційні та відео матеріали, завдання та методичні рекомендації до практичних занять і самостійної роботи, методичне забезпечення поточного і підсумкового контролю, основна та додаткова література розміщені на платформі Moodle.

РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ

Поточні контрольні заходи

Основними контрольними заходами є завдання практичних занять, завдання самостійних робіт й тести, які виконуються після опанування відповідної теми курсу. Всі поточні контрольні заходи та методичні рекомендації до їх виконання розташовані на платформі Moodle.

Підсумкові контрольні заходи

Індивідуальне завдання. *Аналіз загроз технічним каналам витоку інформації та розроблення комплексу заходів технічного захисту для заданого об'єкта інформаційної діяльності (перелік об'єктів та варіантів наведено в завданні). 20 балів. Завдання, вихідні дані та перелік варіантів робіт наведено в завданні на платформі Moodle.*

Підсумковий контроль (іспит). *Виконання практичних завдань екзаменаційного білету – 20 балів (проводиться письмово в аудиторії або онлайн на платформі Moodle).*

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Змістовий модуль 1. Основи систем технічного захисту інформації та загрози технічними каналами		
Тиждень 1 Лекція 1	Теоретичні основи, поняття та термінологія систем технічного захисту інформації.	–
Тиждень 1 Практичне заняття 1	Визначення інформації, об'єктів та можливих напрямів її технічного захисту.	*Практичне завдання №1.* Класифікація об'єктів інформаційної діяльності та визначення вимог до їх захисту. (*max 3 бали*)
Тиждень 2 Лекція 2	Інформація як об'єкт технічного захисту. Види інформації, характеристики інформації, що підлягає захисту, та основні властивості захищеної інформації.	–
Тиждень 2 Практичне заняття 2	Класифікація інформації та визначення її критичності для об'єкта захисту.	*Практичне завдання №2.* Визначення інформації, що підлягає захисту. (*max 3 бали*)
Тиждень 3 Лекція 3	Основні види загроз, джерела загроз та формування технічних каналів витоку інформації.	–
Тиждень 3 Практичне заняття 3	Виявлення можливих каналів витоку інформації на заданому об'єкті.	*Практичне завдання №3.* Аналіз технічних каналів витоку інформації. (*max 3 бали*)
Тиждень 4 Лекція 4	Демаскувальні ознаки та побічні інформаційні прояви.	–
Тиждень 4 Практичне заняття 4	Визначення можливих інформаційних проявів та оцінювання їх небезпечності.	*Практичне завдання №4.* Виявлення демаскувальних ознак. (*max 3 бали*)
Тиждень 5 Лекція 5	Модель загроз технічному захисту інформації.	–
Тиждень 5 Практичне заняття 5	Формування моделі порушника та визначення пріоритетних загроз для заданого об'єкта.	*Практичне завдання №5.* Побудова моделі загроз. (*max 3 бали*)
Тиждень 6 Лекція 6	Основні етапи організації захисту, визначення вразливостей та вибір заходів протидії загрозам.	–
Тиждень 6 Практичне заняття 6	Аналіз захищеності об'єкта та формування переліку першочергових заходів захисту	*Практичне завдання №6.* Оцінювання захищеності об'єкта. (*max 3 бали*)

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Тиждень 6 Самостійна робота	Аналіз загроз та каналів витоку інформації	*Самостійна робота №1.* Розроблення моделі загроз для заданого об'єкта та визначення основних технічних каналів витоку інформації. (*max 2 бали*)
Тиждень 6	Основи систем технічного захисту інформації, загрози, канали витоку, модель порушника та оцінювання захищеності.	*Тест №1.* (*max 2 бали*)
Змістовий модуль 2. Методи та засоби технічного захисту інформації		
Тиждень 7 Лекція 7	Методи запобігання витоку інформації технічними каналами.	–
Тиждень 7 Практичне заняття 7	Визначення відповідного методу захисту для заданої ситуації безпеки.	*Практичне завдання №7.* Вибір методу протидії технічному витоку інформації. (*max 3 бали*)
Тиждень 8 Лекція 8	Захист інформації від побічних електромагнітних випромінювань і наведень.	–
Тиждень 8 Практичне заняття 8	Визначення доцільних заходів та засобів захисту інформаційної апаратури від електромагнітних проявів.	*Практичне завдання №8.* Вибір технічних заходів захисту від електромагнітних проявів. (*max 3 бали*)
Тиждень 9 Лекція 9	Захист інформаційних і телекомунікаційних ліній від технічного витоку інформації.	–
Тиждень 9 Практичне заняття 9	Вибір способів захисту та формування схеми захисту заданої інформаційної лінії від технічного витоку.	*Практичне завдання №9.* Проєктування захисту інформаційної лінії від технічного витоку. (*max 3 бали*)
Тиждень 10 Лекція 10	Акустичний та віброакустичний захист інформації.	–
Тиждень 10 Практичне заняття 10	Вибір заходів захисту приміщення відповідно до норм акустичного та віброакустичного захисту.	*Практичне завдання №10.* Формування комплексу акустичного та віброакустичного захисту. (*max 3 бали*)
Тиждень 11 Лекція 11	Екранування, фільтрація та інші технічні засоби захисту інформації.	–
Тиждень 11 Практичне заняття 11	Формування набору технічних засобів для реалізації визначених способів захисту.	*Практичне завдання №11.* Підбір та обґрунтування комплексу технічних засобів захисту. (*max 3 бали*)

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Тиждень 11 Самостійна робота	Розроблення комплексу методів та засобів технічного захисту інформації.	*Самостійна робота №2.* Обґрунтування вибору методів і технічних засобів для забезпечення захисту заданого об'єкта. (*max 2 бали*)
Тиждень 11	Методи захисту, захист від електромагнітних проявів, захист інформаційних ліній, акустичний захист, екранування та фільтрація.	*Тест №2.* (*max 2 бали*)
Змістовий модуль 3. Пошукові заходи, інструментальний контроль та побудова комплексної системи захисту інформації		
Тиждень 12 Лекція 12	Організація пошукових заходів на об'єктах інформаційної діяльності.	–
Тиждень 12 Практичне заняття 12	Визначення послідовності пошукових заходів, зон обстеження та порядку фіксації результатів.	*Практичне завдання №12.* Розроблення плану пошукового обстеження об'єкта. (*max 3 бали*)
Тиждень 13 Лекція 13	Засоби та методи виявлення технічних засобів збору інформації.	–
Тиждень 13 Практичне заняття 13	Визначення відповідних засобів пошуку залежно від умов об'єкта та завдань обстеження.	*Практичне завдання №13.* Вибір засобів для проведення пошукового обстеження. (*max 3 бали*)
Тиждень 14 Лекція 14	Інструментальний контроль технічної захищеності об'єкта.	–
Тиждень 14 Практичне заняття 14	Аналіз результатів контролю, визначення відхилень та формування висновків щодо стану захищеності.	*Практичне завдання №14.* Опрацювання та інтерпретація результатів інструментального контролю. (*max 3 бали*)
Тиждень 15 Лекція 15	Побудова комплексної системи технічного захисту інформації.	–
Тиждень 15 Практичне заняття 15	Об'єднання окремих технічних заходів у взаємопов'язану систему захисту заданого об'єкта.	*Практичне завдання №15.* Розроблення структури комплексної системи захисту інформації. (*max 3 бали*)
Тиждень 16 Лекція 16	Оцінювання стану та вдосконалення комплексної системи захисту інформації.	–
Тиждень 16 Практичне заняття 16	Узагальнення результатів пошукового обстеження, та оцінювання реалізованої системи.	*Практичне завдання №16.* Комплексне оцінювання результатів захисту об'єкта інформаційної діяльності. (*max 3 бали*)

Тиждень і вид заняття	**Тема заняття**	**Контрольні заходи, кількість балів**
Тиждень 16 Самостійна робота	Проведення комплексного аналізу результатів щодо вдосконалення системи захисту.	*Самостійна робота №3.* Комплексне обстеження об'єкта та розроблення пропозицій щодо вдосконалення захисту. (*max 2 бали*)
Тиждень 16	Контроль знань з пошукових заходів, інструментального контролю та комплексної системи захисту інформації.	*Тест №3.* (*max 2 бали*)

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)		

СПИСОК ДЖЕРЕЛ

Основна література

1. Богуш В. М., Бровко В. Д., Кобус О. С., Козюра В. Д. Технічний захист інформації. Навчальний посібник. – Київ: Ліра-К, 2023. – 508 с..
2. Богуш В. М., Бровко В. Д., Кобус О. С., Козюра В. Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навчальний посібник. – Київ: Ліра-К, 2023. – 484 с.
3. Іванченко С. О., Гавриленко О. В., Липський О. А., Шевцов А. С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. – Київ: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.

Інформаційні ресурси та нормативно-правове забезпечення

4. Про внесення змін до Закону України "Про інформацію" № 2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, № 32,ст. 313.
5. Закон України "Про захист персональних даних" № 2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481.
6. Закон України "Про критичну інфраструктуру" № 2684-IX від 18.10.2022.
7. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
8. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
9. НД ТЗІ 1.6-005-2013. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.
10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
11. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційнотелекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005.
12. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99.
13. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.1999.
14. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07.
15. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011.

РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ[1]

Відвідування занять. Регуляція пропусків.
Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Аспіранти, 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 шляхом виконання індивідуального письмового завдання. Аспіранти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до сесії не допускаються.

Політика академічної доброчесності
Усі письмові роботи, що виконуються аспірантами 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 автора оригінального тексту). Будь-яка ідея, думка чи речення, ілюстрація чи фото, яке ви запозичуєте, має супроводжуватися посиланням на першоджерело. Приклади оформлення цитувань див. на платформі Moodle: https://cutt.ly/1I4Q8Me.
Виконавці індивідуальних завдань обов'язково додають до текстів своїх робіт власноруч підписану Декларацію академічної доброчесності (див. посилання у Додатку до силабусу).
Роботи, в 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 в 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; *наукометрична база Scopus: https://www.scopus.com; наукометрична база Web of Science: https://apps.webofknowledge.com*

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.

Комунікація
Базовою платформою для комунікації викладача з аспірантами є платформа Moodle. Важливі повідомлення загального характеру регулярно розміщуються викладачем на форумі курсу. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити аспірантів подаються викладачем впродовж трьох робочих днів. Для оперативного отримання повідомлень про оцінки та нову інформацію, розміщену на платформі Moodle, будь ласка, переконайтеся, що адреса електронної пошти, зазначена у вашому профайлі на Moodle, є актуальною, та регулярно перевіряйте папку «Спам». Якщо за технічних причин доступ до Moodle є неможливим або ваше питання потребує термінового розгляду, направте електронного листа на пошту або у зазначені меседжери викладача. У листі обов'язково вкажіть ваше прізвище, ім'я та курс.

[1] Тут зазначається все, що важливо для курсу: наприклад, умови допуску до лабораторій, реактивів і т.д. Викладач сам вирішує, що треба знати студенту для успішного проходження курсу!

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Силабус навчальної дисципліни

ДОДАТОК ДО СИЛАБУСУ ЗНУ

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ. Аспіранти 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 аспірантами 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 аспіранту 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 аспірантів, 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 аспірантів ЗНУ - moodle.znu@gmail.com, Савченко Тетяна Володимирівна
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.