ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ

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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРБЕЗПЕКА ШТУЧНОГО ІНТЕЛЕКТУ

підготовки _____бакалаврів_____

денної та заочної форми здобуття освіти

освітньо-професійна програма ___КІБЕРБЕЗПЕКА_____

спеціальності ___125 Кібербезпека_____ _

галузі знань ____12 Інформаційні технології_____

ВИКЛАДАЧ: Добровольський Геннадій Анатолійович, к.т.н, доцент кафедри комп'ютерних наук

Обговорено та ухвалено
на засіданні кафедри комп'ютерних наук

Протокол №_1_ від "_25__" _серпня__2025 р.
Завідувач кафедри комп'ютерних наук

_____Г. М. Шило_____
(підпис) (ініціали, прізвище)

Погоджено
Гарант освітньо-професійної програми

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

2025 рік

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Кібербезпека штучного інтелекту

Зв`язок з викладачем: Добровольський Геннадій Анатолійович
E-mail: gen.dobr@gmail.com
Сезн ЗНУ повідомлення: https://moodle.znu.edu.ua/course/view.php?id=17975
Телефон (кафедра): +38-061-289-12-57
Інші засоби зв'язку: https://t.me/gen_dobr
Кафедра комп'ютерних наук, ауд. №39, 1 корпус ЗНУ

1. Опис навчальної дисципліни

Навчальна дисципліна «Кібербезпека штучного інтелекту» присвячена вивченню теоретичних засад і практичних методів забезпечення безпеки систем штучного інтелекту протягом усього їх життєвого циклу. У межах курсу розглядаються специфічні загрози та вразливості, притаманні системам машинного навчання, включно з атаками на дані, моделі та інфраструктуру, а також ризики, пов'язані з порушенням конфіденційності, цілісності й доступності. Значну увагу приділено атакам типу adversarial, підміні навчальних даних, витоку інформації з моделей, компрометації процесів навчання та розгортання, а також використанню штучного інтелекту як інструменту кіберзахисту.

У курсі аналізуються сучасні підходи до побудови стійких і надійних систем ШІ, зокрема adversarial training, диференційна приватність, federated learning, безпечні практики MLOps, а також міжнародні рекомендації та фреймворки з управління ризиками і безпекою ШІ (NIST AI Risk Management Framework, ISO/IEC 27001 у контексті ШІ, ENISA AI Threat Landscape). Розглядаються етичні, правові та соціальні аспекти безпечного використання штучного інтелекту, включно з вимогами до захисту персональних даних і відповідальністю розробників та операторів інтелектуальних систем.

Компетентності, набуті під час вивчення дисципліни «Кібербезпека штучного інтелекту», є фундаментальними для подальшого опанування спеціалізованих курсів у галузі кібербезпеки, аналізу ризиків, безпеки програмного забезпечення та інтелектуальних систем, а також для виконання завдань виробничої практики й кваліфікаційних робіт, пов'язаних із проєктуванням і впровадженням безпечних ШІ-рішень.

Метою вивчення навчальної дисципліни «Кібербезпека штучного інтелекту» є формування у студентів системного розуміння загроз і ризиків, характерних для систем штучного інтелекту, набуття знань щодо методів їх виявлення, аналізу та мінімізації, а також розвиток практичних навичок проєктування, оцінювання та експлуатації безпечних і надійних систем машинного навчання відповідно до міжнародних стандартів і кращих практик.

У результаті вивчення навчальної дисципліни «Кібербезпека штучного інтелекту» студент зможе:

- аналізувати архітектуру систем штучного інтелекту з погляду кібербезпеки;
- ідентифікувати загрози, вразливості та сценарії атак на дані, моделі й інфраструктуру ШІ;
- пояснювати механізми та наслідки adversarial-атак і атак на приватність моделей;
- застосовувати методи підвищення стійкості та надійності моделей машинного навчання;
- інтегрувати вимоги безпеки у процеси розроблення та експлуатації ШІ (secure MLOps);
- використовувати сучасні фреймворки, стандарти та рекомендації з кібербезпеки штучного інтелекту для оцінювання ризиків і прийняття обґрунтованих рішень.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Кібербезпека штучного інтелекту

Паспорт навчальної дисципліни

Нормативні показники	**денна форма здобуття освіти**	**заочна форма здобуття освіти**
Статус дисципліни	**Вибіркова**	
Семестр	6-й	6-й
Кількість кредитів ECTS	5	5
Кількість годин	150	150
Лекційні заняття	24 год.	6 год.
Лабораторні заняття	24 год.	8 год.
Самостійна робота	102 год.	136 год.
Консультації	Згідно розкладу: дистанційно: Google Meet: https://meet.google.com/mwp-gbkw-xhk	
Вид підсумкового семестрового контролю:	**іспит**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=17975	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	**Методи навчання**	**Форми і методи оцінювання**
Компетентності		
ФК 1 Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК 2 Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/ або кібербезпеки. ФК 12 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	лекція-візуалізація, пояснення, демонстрування, дискусія, аналіз, виконання завдань практичних робіт	**Поточний контроль:** захист лабораторних та самостійних робіт, опитування, тестування **Підсумковий контроль:** тестування

Результати навчання		
ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПРН 12 Розробляти моделі загроз та порушника ПРН 29 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	лекція-візуалізація, пояснення, дискусія, аналіз, виконання завдань практичних робіт	**Поточний контроль:** захист лабораторних та самостійних робіт, опитування, тестування **Підсумковий контроль:** тестування

3. Зміст навчальної дисципліни

Змістовий модуль 1. Теоретичні основи кібербезпеки штучного інтелекту
Тема 1. Теоретичні основи кібербезпеки штучного інтелекту
Базові поняття кібербезпеки у контексті систем штучного інтелекту, їх місце в сучасному інформаційному просторі, відмінності від класичних інформаційно-телекомунікаційних систем. Архітектура систем ШІ, життєвий цикл моделей машинного навчання та точки виникнення ризиків безпеки.

Змістовий модуль 2. Дані як критичний актив систем штучного інтелекту
Тема 2. Дані як критичний актив систем штучного інтелекту
Загрози та вразливості, пов’язані з навчальними, валідаційними й експлуатаційними даними. Атаки на цілісність і достовірність даних, підміна та отруєння вибірок, проблеми конфіденційності, методи захисту даних і забезпечення приватності.

Змістовий модуль 3. Атаки на моделі машинного навчання
Тема 3. Атаки на моделі машинного навчання
Аналіз атак, спрямованих безпосередньо на моделі ШІ. Adversarial-атаки, інверсія моделей, membership inference та витік параметрів. Наслідки таких атак для безпеки та надійності інтелектуальних систем.

Змістовий модуль 4. Методи забезпечення стійкості та надійності моделей
Тема 4. Методи забезпечення стійкості та надійності моделей
Підходи до підвищення стійкості моделей до зловмисних впливів, adversarial training, регуляризація, детектування аномалій та оцінювання стійкості. Вплив захисних методів на якість і продуктивність моделей.

Змістовий модуль 5. Безпека інфраструктури та MLOps
Тема 5. Безпека інфраструктури та MLOps

Захист обчислювальної інфраструктури, середовищ навчання і розгортання моделей, безпечні практики MLOps. Ризики хмарних сервісів, контроль доступу до моделей, моніторинг, аудит та логування подій безпеки.

Змістовий модуль 6. Штучний інтелект як інструмент кіберзахисту
Тема 6. Штучний інтелект як інструмент кіберзахисту
Застосування методів машинного навчання для виявлення атак, аналізу аномалій та реагування на інциденти кібербезпеки. Переваги й обмеження використання ШІ в системах захисту та питання довіри до автоматизованих рішень.

Змістовий модуль 7. Управління ризиками та відповідність стандартам у сфері безпеки ШІ
Тема 7. Управління ризиками та відповідність стандартам у сфері безпеки ШІ
Підходи до ідентифікації, аналізу та оцінювання ризиків систем штучного інтелекту. Міжнародні стандарти й фреймворки, що регламентують безпеку та надійність ШІ, їх застосування в організаційній практиці.

Змістовий модуль 8. Етичні, правові та соціальні аспекти кібербезпеки штучного інтелекту
Тема 8. *Етичні, правові та соціальні аспекти кібербезпеки штучного інтелекту*
Модуль присвячений питанням відповідального та безпечного використання ШІ, захисту прав і свобод людини, обробки персональних даних та відповідальності розробників і операторів систем. Аналізуються сучасні регуляторні ініціативи та їх вплив на проєктування й експлуатацію інтелектуальних систем.

4. Структура навчальної дисципліни

Вид заняття /роботи	**Назва теми**	**Кількість годин, о/д. ф.**	**Згідно з розкладом**
1	***2***	***3***	***4***
Лекція	Вступ до навчальної дисципліни. Поняття кібербезпеки штучного інтелекту. Місце систем ШІ в сучасному інформаційному просторі. Основні виклики та загрози безпеці інтелектуальних систем.	2	тиждень 1
Лабораторна робота	ЛР1. Аналіз архітектури системи штучного інтелекту та визначення потенційних загроз. Дослідження життєвого циклу моделі машинного навчання з погляду кібербезпеки. Ідентифікація активів, загроз і вразливостей.	2	тиждень 1
Самостійна робота	Ознайомлення з програмою курсу, термінологією та базовими поняттями кібербезпеки штучного інтелекту. Опрацювання рекомендованих джерел щодо архітектури систем ШІ та їх життєвого циклу.	8	тиждень 1
Лекція	Архітектура систем штучного інтелекту та життєвий цикл моделей машинного навчання.	2	тиждень 2

	Аналіз точок виникнення ризиків безпеки на етапах збирання даних, навчання, тестування та експлуатації.		
Лабораторна робота	ЛР2. Дослідження атак на навчальні дані. Моделювання сценаріїв отруєння даних та підміни вибірок. Аналіз впливу порушення цілісності даних на результати навчання моделей.	2	тиждень 2
Самостійна робота	Самостійне вивчення матеріалів з аналізу загроз і вразливостей систем штучного інтелекту. Підготовка до лабораторної роботи з ідентифікації активів і побудови первинної моделі загроз.	8	тиждень 2
Лекція	Дані як критичний актив систем ШІ. Загрози конфіденційності, цілісності та доступності даних. Отруєння навчальних вибірок і підміна джерел даних.	2	тиждень 3
Лабораторна робота	ЛР2. (продовження) Дослідження … навчання моделей.	2	тиждень 3
Самостійна робота	Опрацювання наукових публікацій і звітів щодо атак на дані машинного навчання. Аналіз прикладів отруєння даних та підміни навчальних вибірок. Підготовка до лабораторної роботи.	9	тиждень 3
Лекція	Проблеми приватності в системах штучного інтелекту. Витоки інформації з навчальних і експлуатаційних даних. Основні підходи до захисту даних у системах ШІ.	2	тиждень 4
Лабораторна робота	ЛР3. Аналіз ризиків конфіденційності даних у системах штучного інтелекту. Дослідження витоків інформації та оцінювання загроз порушення приватності при роботі з навчальними наборами даних.	2	тиждень 4
Самостійна робота	Вивчення питань конфіденційності та приватності даних у системах ШІ. Ознайомлення з підходами до захисту персональних даних і забезпечення приватності в машинному навчанні.	9	тиждень 4
Лекція	Атаки на моделі машинного навчання. Adversarial-атаки на етапах навчання та використання моделей. Наслідки атак для надійності й безпеки інтелектуальних систем.	2	тиждень 5
Лабораторна робота	ЛР4. Моделювання атак на моделі машинного навчання. Генерація adversarial-прикладів та оцінювання їх впливу на точність і стабільність моделей.	2	тиждень 5
Самостійна робота	Самостійне опрацювання матеріалів з adversarial-атак на моделі машинного навчання. Аналіз прикладів атак і їх впливу на якість та	8	тиждень 5

	надійність моделей.		
Лекція	Атаки на приватність і конфіденційність моделей. Інверсія моделей, membership inference, витік параметрів і знань. Оцінювання ризиків таких атак.	2	тиждень 6
Лабораторна робота	ЛР5. Дослідження атак на приватність моделей. Аналіз membership inference та інверсії моделей. Оцінювання ризиків витоку інформації з параметрів моделей.	2	тиждень 6
Самостійна робота	Вивчення атак на приватність моделей, зокрема membership inference та інверсії моделей. Підготовка аналітичних нотаток щодо ризиків витоку інформації.	8	тиждень 6
Лекція	Методи забезпечення стійкості моделей машинного навчання. Adversarial training, регуляризація, детектування аномалій. Компроміс між безпекою та якістю моделей.	2	тиждень 7
Лабораторна робота	ЛР6. Реалізація та аналіз методів підвищення стійкості моделей. Застосування adversarial training та простих методів детектування аномалій. Порівняльна оцінка ефективності захисних підходів.	2	тиждень 7
Самостійна робота	Опрацювання методів підвищення стійкості моделей машинного навчання. Аналіз переваг і обмежень adversarial training та інших захисних підходів.	9	тиждень 7
Лекція	Забезпечення безпеки інфраструктури систем ШІ. Захист середовищ навчання та розгортання моделей. Основи безпечних практик MLOps.	2	тиждень 8
Лабораторна робота	ЛР6. (продовження) Реалізація та аналіз методів … ефективності захисних підходів.	2	тиждень 8
Самостійна робота	Самостійне вивчення питань безпеки інфраструктури та процесів MLOps. Аналіз ризиків хмарних середовищ і практик безпечного розгортання моделей.	9	тиждень 8
Лекція	Контроль доступу, моніторинг і аудит у системах штучного інтелекту. Логування подій безпеки та виявлення інцидентів у середовищах ШІ.	2	тиждень 9
Лабораторна робота	ЛР7. Аналіз безпеки інфраструктури та MLOps-пайплайнів. Дослідження механізмів контролю доступу, моніторингу та логування у середовищах розгортання моделей ШІ.	2	тиждень 9
Самостійна робота	Опрацювання матеріалів щодо моніторингу, аудиту та реагування на інциденти у системах штучного інтелекту. Підготовка до лабораторної роботи з аналізу інфраструктури ШІ.	8	тиждень 9
Лекція	Використання штучного інтелекту в системах кіберзахисту. Виявлення атак і аномалій за	2	тиждень 10

	допомогою методів машинного навчання. Переваги та обмеження таких підходів.		
Лабораторна робота	ЛР7. (продовження) Аналіз безпеки і ... у середовищах розгортання моделей ШІ.	2	тиждень 10
Самостійна робота	Вивчення застосування штучного інтелекту в системах кіберзахисту. Аналіз сучасних рішень і досліджень у сфері виявлення атак за допомогою машинного навчання.	8	тиждень 10
Лекція	Управління ризиками безпеки штучного інтелекту. Ідентифікація загроз, аналіз і оцінювання ризиків. Огляд міжнародних стандартів і фреймворків з безпеки ШІ.	2	тиждень 11
Лабораторна робота	ЛР8. Оцінювання ризиків і відповідності системи штучного інтелекту вимогам стандартів і рекомендацій з безпеки. Побудова спрощеної моделі загроз і формування звіту з рекомендаціями щодо підвищення рівня кібербезпеки ШІ-системи.	2	тиждень 11
Самостійна робота	Опрацювання міжнародних стандартів і фреймворків з безпеки штучного інтелекту. Підготовка індивідуального аналітичного завдання з оцінювання ризиків ШІ-системи.	9	тиждень 11
Лекція	Етичні та правові аспекти кібербезпеки штучного інтелекту. Відповідальність розробників і операторів систем ШІ. Узагальнення матеріалу курсу та підготовка до підсумкового контролю.	2	тиждень 12
Лабораторна робота	ЛР8. (продовження) Оцінювання ризиків і … підвищення рівня кібербезпеки ШІ-системи.	2	тиждень 12
Самостійна робота	Узагальнення та систематизація матеріалу курсу. Підготовка до підсумкового контролю, оформлення та подання звітів з лабораторних робіт і самостійних завдань.	9	тиждень 12

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

5. Види і зміст контрольних заходів

Вид заняття/ роботи	Вид контрольного заходу	Зміст контрольного заходу*	Критерії оцінювання та термін виконання*	Усього балів
Поточний контроль				
Практичне заняття №1 - 12	Лабораторна робота 1 - 12	Розміщено в СЕЗН ЗНУ	Повний захист кожного виконаного завдання оцінюється в 5 балів, тільки зданий звіт - 3 бала	60
Усього за поточний контроль				**60**
Підсумковий контроль				
Залік	Теоретичне завдання	Розміщено в СЕЗН ЗНУ	40 тестових питань (вибір правильної відповіді з декількох можливих) - по 0.5 бала	**40**
Усього за підсумковий контроль				**40**

Шкала оцінювання ЗНУ: національна та ECTS

1 За шкалою **1 ECTS**	**2 За шкалою університету**	2 За національною шкалою	
		3 Екзамен	4 Залік
A	90 – 100 (відмінно)	1 5 (відмінно)	2 Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов’язковим повторним курсом)		

6. Основні навчальні ресурси

Рекомендована література

Основна

1. Ю. І. Когут (ред.) Штучний інтелект і безпека: практичний посібник / Ю. І. Когут. − Київ: Консалтингова компанія «СІДКОН»; ВД Дакор, 2024. − 294 с. − ISBN 978-617-95333-3-4.
2. Kolosnjaji B., Xiao H., Xu P., Zarras A. Artificial Intelligence for Cybersecurity: Develop AI approaches to solve cybersecurity problems in your organization / Bojan Kolosnjaji, Huang Xiao, Peng Xu, Apostolis Zarras. − Birmingham: Packt Publishing, 2024. − 358 p. − ISBN 978-1805124962.
3. Narayanan A., Kapoor S. AI Snake Oil: What Artificial Intelligence Can Do, What It Can't, and How to Tell the Difference / Arvind Narayanan, Sayash Kapoor. − Princeton: Princeton University Press, 2024. − 360 p. − ISBN 978-0691249131.
4. Czaja P., Gdowski B., et al. Cybersecurity Challenges and Opportunities of Machine Learning-Based Artificial Intelligence / Pawel Czaja, Bartlomiej Gdowski та ін. − 2025. − PDF.
5. James Arthur, Williams John. Adversarial AI: The Emerging Cybersecurity Threat of Machine Learning Manipulation − 2025.
6. Mohamed N., et al. Artificial intelligence and machine learning in cybersecurity / N. Mohamed та ін. − Neural Computing and Applications, 2025.
7. Bender E. M., Hanna A. The AI Con: How to Fight Big Tech's Hype and Create the Future We Want / Emily M. Bender, Alex Hanna. − Harper: 2025.

Електронні ресурси

1. ISO/IEC 27001:2022 (Information security management systems), https://uk.wikipedia.org/wiki/ISO/IEC_27001
2. NIST AI Risk Management Framework (AI RMF) https://www.nist.gov/itl/ai-risk-management-framework
3. AI for Cybersecurity Specialization. URL: https://www.coursera.org/specializations/ai-for-cybersecurity
4. AI in Cybersecurity Toolkit: URL: https://virtual-routes.org/ai-in-cybersecurity-toolkit/
5. AI в інструментарії з кібербезпеки. URL: https://virtual-routes.org/uk/ai-в-інструментарії-кібербезпеки/
6. Adversarial Machine Learning Courses and Certifications. URL: https://www.classcentral.com/subject/adversarial-machine-learning
7. Stellar Cyber. URL: https://stellarcyber.ai/uk/learn/ai-driven-security/
8. Garak (software). URL: https://github.com/NVIDIA/garak
9. ISACA − «IT Risk Resources» https://www.isaca.org/resources/it-risk
10. National Institute of Standards and Technology (NIST) − RMF Online Introductory Courses https://csrc.nist.gov/projects/risk-management/rmf-courses
11. National Cyber Security Centre (NCSC) − Cyber Security Toolkit for Boards https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit-V3.pdf
12. Actuarial Institute (USA) − Cyber Risk Toolkit https://actuary.org/wp-content/uploads/2022/06/CyberRiskToolkit.June22.pdf
13. Rapid7 − Info Sec Risk Management (ISRM) fundamentals https://www.rapid7.com/fundamentals/information-security-risk-management/
14. ORX Association − Cyber & information security risk management event data https://orx.org/cyber
15. Cybrary − On-line курси з кібербезпеки / управління ризиками https://www.cybrary.it/

7. Регуляції і політики курсу

Відвідування занять. Регуляція пропусків.
Відвідування усіх занять є обов'язковим. Студенти зобов'язані дотримуватися усіх строків, визначених для виконання усіх видів робіт, передбачених даною дисципліною. Пропуски та запізнення на заняття є недопустимими.

Політика академічної доброчесності
Кожний студент зобов'язаний дотримуватися принципів академічної доброчесності. Письмові завдання з використанням часткових або повнотекстових запозичень з інших робіт без зазначення авторства – це *плагіат*. Використання будь-якої інформації (текст, фото, ілюстрації тощо) мають бути правильно процитовані з посиланням на автора! Якщо ви не впевнені, що таке плагіат, фабрикація, фальсифікація, порадьтеся з викладачем. До студентів, у роботах яких буде виявлено списування, плагіат чи інші прояви недоброчесної поведінки можуть бути застосовані різні дисциплінарні заходи (див. посилання на Кодекс академічної доброчесності ЗНУ в додатку до силабусу). Неприпустиме складання роботи, виконаної іншою особою.

Використання комп'ютерів/телефонів на занятті
Використання мобільних телефонів, ноутбуків та інших гаджетів під час лекційних та лабораторних занять дозволяється виключно у навчальних цілях (з активованим режимом «без звуку»).

Комунікація
Комунікація викладача зі студентами здійснюється безпосередньо на заняттях та додатково за допомогою месенджерів (наприклад, Telegram), електронної пошти і в СЕЗН Moodle (форум курсу, приватні повідомлення)

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ 2025-2026 н. р. доступний за адресою: https://tinyurl.com/yckze4jd.

НАВЧАЛЬНИЙ ПРОЦЕС ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь (атестації, заліки, іспити та інші форми контролю) є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ: https://tinyurl.com/y9tve4lk.

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН, ВІДРАХУВАННЯ. Наявність академічної заборгованості до 6 навчальних дисциплін (в тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Порядок повторного вивчення визначається Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: https://tinyurl.com/y9pkmmp5. Підстави та процедури відрахування студентів, у тому числі за невиконання навчального плану, регламентуються Положенням про порядок переведення, відрахування та поновлення студентів у ЗНУ: https://tinyurl.com/ycds57la.

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ: https://tinyurl.com/57wha734. Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: Положення про порядок призначення і виплати академічних стипендій у ЗНУ: https://tinyurl.com/yd6bq6p9; Положення про призначення та виплату соціальних стипендій у ЗНУ: https://tinyurl.com/y9r5dpwh.

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога **Марті Ірини Вадимівни** (061) 228-15-84, (099) 253-78-73 (щоденно з 9 до 21).

УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КОРУПЦІЇ Запорізького національного університету: **Банах Віктор Аркадійович**
Електронна адреса: v_banakh@znu.edu.ua
Гаряча лінія: тел. (061) 227-12-76, факс 227-12-88

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Якщо вам потрібна спеціалізована допомога, будь ласка, зателефонуйте (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://tinyurl.com/ydhcsagx.

РЕСУРСИ ДЛЯ НАВЧАННЯ

НАУКОВА БІБЛІОТЕКА: http://library.znu.edu.ua. Графік роботи абонементів: понеділок-п`ятниця з 08.00 до 16.00; вихідні дні: субота і неділя.
СИСТЕМА ЕЛЕКТРОННОГО ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ (MOODLE): https://moodle.znu.edu.ua
Якщо забули пароль/логін, направте листа з темою «Забув пароль/логін» за адресою: moodle.znu@znu.edu.ua.
У листі вкажіть: прізвище, ім'я, по-батькові українською мовою; шифр групи; електронну адресу.
Якщо ви вказували електронну адресу в профілі системи Moodle ЗНУ, то використовуйте посилання для відновлення паролю https://moodle.znu.edu.ua/mod/page/view.php?id=133015.
ЦЕНТР ІНТЕНСИВНОГО ВИВЧЕННЯ ІНОЗЕМНИХ МОВ: http://sites.znu.edu.ua/child-advance/
ЦЕНТР НІМЕЦЬКОЇ МОВИ, ПАРТНЕР ГЕТЕ-ІНСТИТУТУ: https://www.znu.edu.ua/ukr/edu/ocznu/nim
ШКОЛА КОНФУЦІЯ (ВИВЧЕННЯ КИТАЙСЬКОЇ МОВИ): http://sites.znu.edu.ua/confucius