ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ

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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

підготовки _____бакалаврів_____

денної та заочної форми здобуття освіти

освітньо-професійна програма ___КІБЕРБЕЗПЕКА_____

спеціальності ____122 Кібербезпека та захист інформації_____

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__2026 р.
Завідувач кафедри комп'ютерних наук

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

Погоджено
Гарант освітньо-професійної програми

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

2026 рік

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Управління ризиками інформаційної безпеки

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=17938
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

Курс присвячений теоретичним основам і практичним методам управління ризиками інформаційної безпеки. Розглядаються поняття ризику, загроз, вразливостей і впливів; моделі та процеси оцінювання ризиків; методології та стандарти управління ризиками (ISO/IEC 27005, ISO 31000, NIST SP 800-30). Особливу увагу приділено практичним аспектам ідентифікації активів, визначенню потенційних загроз і сценаріїв атак, кількісним і якісним методам оцінки ризиків, розробці стратегій реагування, а також впровадженню заходів контролю для мінімізації ризиків. Розглядаються сучасні інструменти аналізу ризиків і підходи до моніторингу ефективності системи управління безпекою.

Компетентності, отримані під час вивчення дисципліни «Управління ризиками інформаційної безпеки», є базовими для подальшого опанування дисциплін у галузі кібербезпеки, інформаційного менеджменту, а також для виконання завдань виробничої практики та кваліфікаційної роботи.

Метою вивчення навчальної дисципліни «Управління ризиками інформаційної безпеки» є формування у студентів системного розуміння процесів управління ризиками у сфері інформаційної безпеки, набуття знань щодо методів аналізу, оцінювання та оброблення ризиків, а також розвиток практичних навичок застосування міжнародних стандартів і засобів автоматизації процесів ризик-менеджменту.

У результаті вивчення навчальної дисципліни «Управління ризиками інформаційної безпеки» студент зможе:

- ідентифікувати активи, загрози та вразливості інформаційних систем;
- застосовувати методи якісної та кількісної оцінки ризиків;
- формувати та аналізувати ризик-профіль організації;
- розробляти та обґрунтовувати стратегії управління ризиками;
- впроваджувати та оцінювати ефективність заходів контролю безпеки;
- використовувати сучасні стандарти (ISO/IEC 27005, NIST SP 800-30, ISO 31000) та програмні інструменти для управління ризиками.

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=17938	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	**Методи навчання**	**Форми і методи оцінювання**
Компетентності		
ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/ або кібербезпеки. ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. СК 1 Здатність розробляти та застосовувати математичні моделі, аналізувати статистичні дані розробляти прогностичні моделі для	лекція-візуалізація, пояснення, демонстрування, дискусія, аналіз, виконання завдань практичних робіт	**Поточний контроль:** захист лабораторних та самостійних робіт, опитування, тестування **Підсумковий контроль:** тестування

виявлення та дослідження загроз у комп'ютерних системах.		
Результати навчання		
ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень ПРН 22 – Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки. ПРН 28 – Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.	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. Вступ до управління ризиками інформаційної безпеки

Тема 1. Основні поняття управління ризиками інформаційної безпеки

Поняття ризику, загрози, вразливості та впливу. Мета та завдання управління ризиками ІБ. Місце ризик-менеджменту в системі управління інформаційною безпекою організації.

Змістовий модуль 2. Стандарти та нормативно-правова база управління ризиками

Тема 2. Стандарт ISO 31000

Принципи, структура та процес управління ризиками за стандартом ISO 31000. Загальна модель ризик-менеджменту для організацій будь-якого типу.

Тема 3. Стандарт ISO/IEC 27005

Специфіка застосування ISO/IEC 27005 для управління ризиками інформаційної безпеки. Етапи оцінювання та оброблення ризиків.

Тема 4. Стандарти та нормативно-правова база управління ризиками

Огляд міжнародних стандартів і фреймворків (NIST SP 800-30, NIST CSF, COBIT, ISO/IEC 27001). Порівняльний аналіз підходів.

Тема 5. Нормативні документи України та ЄС у сфері кібербезпеки

Законодавство України щодо захисту інформації та кібербезпеки. Регламенти ЄС (GDPR, NIS2, DORA) та їх вплив на управління ризиками.

Змістовий модуль 3. Активи, загрози та вразливості інформаційних систем

Тема 6. Активи інформаційної системи

Класифікація активів (інформаційні, технічні, людські). Методи ідентифікації та інвентаризації активів. Визначення критичності активів для організації.

Тема 7. Визначення загроз і вразливостей

Джерела та класифікація загроз. Поняття вразливості. Методи виявлення вразливостей інформаційних систем.

Тема 8. Огляд типових кіберзагроз для інформаційних систем (SOC, CERT звіти)

Аналіз актуальних кіберзагроз на основі звітів центрів моніторингу безпеки (SOC) та команд реагування на інциденти (CERT).

Змістовий модуль 4. Методи оцінки та аналізу ризиків

Тема 9. Методи оцінки ризиків

Якісні, кількісні та змішані методи оцінки ризиків. Шкали ймовірності та впливу. Розрахунок рівня ризику.

Тема 10. Методи аналізу ризиків інформаційної безпеки

Методології аналізу ризиків: OCTAVE, FAIR, CRAMM. Порівняння підходів та вибір методології відповідно до потреб організації.

Тема 11. Карта ризиків для обраного об'єкта

Побудова карти (матриці) ризиків. Пріоритизація ризиків за рівнем впливу та ймовірності виникнення.

Змістовий модуль 5. Стратегії управління ризиками

Тема 12. Розробка стратегій управління ризиками

Стратегії реагування на ризики: уникнення, зниження, передавання, прийняття. Критерії вибору стратегії.

Тема 13. Аналіз прикладів політик безпеки з міжнародних практик (ISO, NIST)

Розгляд практичних прикладів політик інформаційної безпеки, побудованих на основі результатів оцінки ризиків.

Змістовий модуль 6. Заходи контролю інформаційної безпеки

Тема 14. Реалізація заходів контролю безпеки

Технічні, організаційні та фізичні заходи контролю. Впровадження засобів зниження ризиків.

Тема 15. Огляд заходів контролю безпеки за ISO/IEC 27001

Перелік і структура заходів контролю (Annex A) стандарту ISO/IEC 27001. Відповідність контролів визначеним ризикам.

Тема 16. Огляд заходів контролю безпеки за ISO 31000

Принципи інтеграції заходів контролю в загальну систему управління ризиками організації за ISO 31000.

Змістовий модуль 7. Моніторинг та безперервне вдосконалення управління ризиками

Тема 17. Моніторинг ризиків та ефективності контролів

Методи та інструменти моніторингу ризиків. Оцінювання ефективності впроваджених заходів контролю.

Тема 18. Приклад схеми моніторингу ризиків

Практичний приклад побудови системи моніторингу ризиків для організації, ключові індикатори ризику (KRI).

Тема 19. Безперервне вдосконалення процесів ризик-менеджменту

Цикл безперервного вдосконалення (PDCA) в управлінні ризиками. Перегляд та актуалізація ризик-профілю організації.

Змістовий модуль 8. Оцінювання зрілості процесів та практичне застосування управління ризиками

Тема 20. Аналіз зрілості процесів управління ризиками

Моделі оцінювання зрілості процесів ризик-менеджменту. Визначення рівня зрілості організації та шляхів його підвищення.

Тема 21. Приклад аналізу ризиків для організації

Комплексний практичний приклад проведення повного циклу управління ризиками інформаційної безпеки для обраної організації.

4. Структура навчальної дисципліни

Вид заняття /роботи	**Назва теми**	**Кількість годин о/д. ф.**	**Згідно з розкладом**
1	***2***	***3***	***4***
Лекція	Основні поняття управління ризиками інформаційної безпеки	2	тиждень 1
Лабораторна робота	ЛР1. Ознайомлення зі стандартами та регламентами управління ризиками ІБ	2	тиждень 1
Самостійна робота	Опрацювання основних понять управління ризиками ІБ (ризик, загроза, вразливість, вплив). Огляд ключових стандартів і регламентів (ISO 31000, ISO/IEC 27005, NIST SP 800-30)	8	тиждень 1
Лекція	Стандарт ISO 31000. Стандарт ISO/IEC 27005	2	тиждень 2
Лабораторна робота	ЛР2. Ідентифікація активів та загроз організації	2	тиждень 2
Самостійна робота	Порівняльний аналіз підходів ISO 31000 та ISO/IEC 27005 до управління ризиками. Ідентифікація активів та загроз для обраної організації	8	тиждень 2
Лекція	Стандарти та нормативно-правова база управління ризиками. Нормативні документи України та ЄС у сфері кібербезпеки	2	тиждень 3
Лабораторна робота	ЛР3. Аналіз вразливостей за відкритими базами даних (CVE, NVD, OWASP)	2	тиждень 3
Самостійна робота	Аналіз нормативно-правової бази України та ЄС у сфері кібербезпеки. Огляд баз даних вразливостей CVE, NVD, OWASP	9	тиждень 3
Лекція	Активи інформаційної системи	2	тиждень 4
Лабораторна робота	ЛР4. Побудова матриці ризиків	2	тиждень 4
Самостійна робота	Класифікація активів інформаційної системи за критичністю. Опрацювання методики побудови матриці ризиків	9	тиждень 4
Лекція	Визначення загроз і вразливостей. Огляд	2	тиждень 5

	типових кіберзагроз для інформаційних систем (SOC, CERT звіти)		
Лабораторна робота	ЛР5. Оцінка ризиків за методологією OCTAVE Allegro	2	тиждень 5
Самостійна робота	Опрацювання типології загроз і вразливостей. Аналіз звітів SOC та CERT щодо актуальних кіберзагроз	8	тиждень 5
Лекція	Методи оцінки ризиків. Методи аналізу ризиків інформаційної безпеки	2	тиждень 6
Лабораторна робота	ЛР6. Формування плану оброблення ризиків	2	тиждень 6
Самостійна робота	Порівняння якісних і кількісних методів оцінки ризиків. Підготовка до оцінювання ризиків за методологією OCTAVE Allegro	8	тиждень 6
Лекція	Карта ризиків для обраного об'єкта	2	тиждень 7
Лабораторна робота	ЛР7. Розробка політики безпеки для зниження ризиків	2	тиждень 7
Самостійна робота	Побудова карти ризиків для обраного об'єкта. Аналіз пріоритизації ризиків за рівнем впливу та ймовірності	9	тиждень 7
Лекція	Розробка стратегій управління ризиками. Аналіз прикладів політик безпеки з міжнародних практик (ISO, NIST)	2	тиждень 8
Лабораторна робота	ЛР8. Моніторинг та аудит ризиків	2	тиждень 8
Самостійна робота	Опрацювання стратегій управління ризиками (уникнення, зниження, передавання, прийняття). Аналіз прикладів політик безпеки ISO та NIST	9	тиждень 8
Лекція	Реалізація заходів контролю безпеки. Огляд заходів контролю безпеки за ISO/IEC 27001	2	тиждень 9
Лабораторна робота	ЛР9. Кількісна оцінка ризиків (розрахунок SLE, ALE, ARO; підхід FAIR)	2	тиждень 9
Самостійна робота	Вивчення заходів контролю безпеки за ISO/IEC 27001 (Annex A). Розробка політики безпеки для зниження ризиків	8	тиждень 9
Лекція	Огляд заходів контролю безпеки за ISO 31000. Моніторинг ризиків та ефективності контролів	2	тиждень 10
Лабораторна робота	ЛР10. Оцінка ризиків, пов'язаних із третіми сторонами та ланцюгом постачання	2	тиждень 10
Самостійна робота	Огляд заходів контролю за ISO 31000. Опрацювання методів моніторингу та аудиту ризиків	8	тиждень 10
Лекція	Приклад схеми моніторингу ризиків. Безперервне вдосконалення процесів ризик-менеджменту	2	тиждень 11
Лабораторна робота	ЛР11. Формування реєстру ризиків (Risk Register) та плану реагування на інциденти	2	тиждень 11
Самостійна	Аналіз прикладів схем моніторингу ризиків.	9	тиждень 11

робота	Опрацювання принципів безперервного вдосконалення (PDCA) у ризик-менеджменті		
Лекція	Аналіз зрілості процесів управління ризиками. Приклад аналізу ризиків для організації	2	тиждень 12
Лабораторна робота	ЛР12. Комплексний аналіз ризиків для обраного підприємства	2	тиждень 12
Самостійна робота	Аналіз моделей зрілості процесів управління ризиками (CMMI, ISO/IEC 27005). Підготовка комплексного аналізу ризиків для обраної організації. Підготовка до підсумкового контролю	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. ISO 31000:2018. Risk management — Guidelines. 2nd ed. Geneva : ISO, 2018.
2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. 4th ed. Geneva : ISO/IEC, 2022. − 62 p.
3. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. Gaithersburg : National Institute of Standards and Technology, 2012.
4. Peltier T.R. Information Security Risk Analysis. 3rd ed. Boca Raton : Auerbach Publications, 2010. − 456 p. ISBN 978-1-4398-3956-0.
5. Landoll D.J. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. 3rd ed. Boca Raton : CRC Press, 2021. − 514 p. ISBN 978-0-367-54747-9.
6. Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Прикладні системи оцінювання ризиків інформаційної безпеки : монографія. Київ : ЦП «Компринт», 2017. − 435 с.

Додаткова

1. Freund J., Jones J. Measuring and Managing Information Risk: A FAIR Approach. Oxford : Butterworth-Heinemann, 2014. − 408 p. ISBN 978-0-12-420231-3.
2. Talabis M., Martin J. Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Waltham : Syngress, 2012. − 278 p. ISBN 978-1-59749-735-0.
3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. − URL: https://zakon.rada.gov.ua/laws/show/2163-19 .

Електронні ресурси

4. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024. − URL: https://www.nist.gov/cyberframework .
5. ISO/IEC 27001:2022. Information security management systems — Requirements. − URL: https://www.iso.org/standard/27001 .
6. ENISA Threat Landscape. European Union Agency for Cybersecurity. − URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends .
7. Regulation (EU) 2016/679 (General Data Protection Regulation). − URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj .
8. Directive (EU) 2022/2555 (NIS 2 Directive). − URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj .

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 2024-2025 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