

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ

Декан математичного фа-
культету

_____ Гоменюк С.І.
(підпис) (ініціали та прізвище)

«_____» _____ 202_

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Сучасні проблеми кібербезпеки

(назва навчальної дисципліни)

блоку освітніх компонентів вільного вибору студента в межах Університету

підготовки бакалаврів
(назва освітнього ступеня)

денної та заочної форм здобуття освіти

ВИКЛАДАЧ: Горбенко В.І., к.ф.-м.н., доцент
(ПІБ, науковий ступінь, вчене звання, посада)

Обговорено та ухвалено
на засіданні кафедри програмної інженерії

Протокол № _____ від “___” _____ 2025 р.
Завідувач кафедри програмної інженерії

_____ А.О.Лісняк
(підпис) (ініціали, прізвище)

2025 рік

Запорізький національний університет
Силабус навчальної дисципліни
(Сучасні проблеми кібербезпеки)



Зв'язок з викладачем:

E-mail: vgorbenko@znu.edu.ua

Сезн ЗНУ повідомлення:

Телефон: (061) 289-76-14

Інші засоби зв'язку: Telegram

Кафедра: програмної інженерії, I корпус, ауд. 19

1. Опис навчальної дисципліни

Метою вивчення навчальної дисципліни є формування базових знань і навичок із кібербезпеки, адаптованих до загальних потреб студентів усіх спеціальностей. У рамках навчання розглядаються основні визначення та поняття кібербезпеки, загрози та принципи захисту персональних даних, принципи створення надійних паролів та використання багатофакторної аутентифікації, захист у соціальних мережах. Студенти дізнаються про сучасні загрози, такі як фішинг, соціальна інженерія, шкідливе програмне забезпечення, а також про те, як їх розпізнавати та уникати. Особливу увагу приділено етичним аспектам цифрової взаємодії та відповідальності користувачів. Також у рамках курсу розглядаються питання кібербезпеки підприємств та національні стратегії і політики з цього питання.

Самостійна робота курсу передбачає розширене вивчення теоретичних питань, підготовку та виконання тестів розділів, а також виконання аналізу певного матеріалу, наданого викладачем.

Паспорт навчальної дисципліни

Нормативні показники	денна форма здобуття освіти	заочна форма здобуття освіти
1	2	3
Статус дисципліни	Вибіркова	
Семестр	5-й	5-й
Кількість кредитів ECTS	3	3
Кількість годин	90	90
Лекційні заняття	28 год.	28 год.
Самостійна робота	62 год.	62 год.
Консультації	особисті – вівторок, з 11:00 до 13:00, I корпус, ауд. 19; дистанційні – Zoom або GoogleMeet, за попередньою домовленістю	
Вид підсумкового семестрового контролю:	залік	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=17271	

Запорізький національний університет
Силабус навчальної дисципліни
(Сучасні проблеми кібербезпеки)



2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	Методи навчання	Форми і методи оцінювання
1	2	3
ЗК 02. Здатність зберігати моральні, культурні, наукові цінності та примножувати досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	Лекції, проблемно-пошукові та дослідницькі методи самостійної роботи	Тестування, виконання індивідуальних дослідницьких завдань
ЗК 03. Здатність до абстрактного мислення, аналізу та синтезу.		
ЗК 07. Навички використання інформаційних і комунікаційних технологій.		
ЗК 08. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.		

3. Зміст навчальної дисципліни

Змістовий модуль 1. Основні концепції кібербезпеки

Історичні аспекти виникнення та розвитку кібербезпеки. Основні цілі кібербезпеки. Класифікація об'єктів кібербезпеки. Основні визначення та поняття, принципи та технології, а також роль кібербезпеки на сучасному етапі цифровізації. Джерела кіберзагроз та можливі їх наслідки. Основні задачі кібербезпеки. Приклади кіберзагроз та їх реалізацій.

Змістовий модуль 2. Кібербезпека програм та мереж

Роль мережевих технологій у кібербезпеці інформаційних ресурсів, її стійкості та вразливості. Засоби та технологічні рішення, що забезпечують надійність та безпечне використання мережевих систем. Визначення та класифікація мережевих кіберзагроз. Протоколи та стандарти безпеки, за допомогою яких підвищується надійність

Запорізький національний університет

Силабус навчальної дисципліни

(Сучасні проблеми кібербезпеки)



мережевої інфраструктури. Концепції та засоби захисту програмного забезпечення. Антивірусні та антималварні рішення. Файерволи та системи виявлення вторгнення. Засоби шифрування та захисту даних. Ідентифікація та аутентифікація. Безпека веб застосунків, баз даних та сховищ даних. Хмарні ресурси та застосунки і кібербезпека.

Змістовий модуль 3. Види та технології кіберзагроз

Класифікація кіберзагроз та джерела їх надходження. Комп'ютерні віруси, їх визначення, історія виникнення та класифікація. Троянські програми, їх типи та характеристики. Методи та засоби впровадження комп'ютерних вірусів та троянських програм. Шпіонаж засобами комп'ютерних програм. Кібербезпека мобільних систем та IoT. Особливості застосунків мобільних систем і їх кібербезпека. Штучний інтелект та кібербезпека.

Змістовий модуль 4. Організаційні аспекти кібербезпеки

Організаційні аспекти кібербезпеки. Засоби забезпечення безпеки інформаційних ресурсів організації/підприємства. Поняття про культуру кібербезпеки та формування її складових. Навчання та підвищення обізнаності співробітників. Управління інцидентами та розробка політик кібербезпеки. Аналіз і оцінка ризиків. Аудит та контроль ризиків кібербезпеки. Автоматизація систем підтримки кібербезпеки. Соціальна інженерія і кібербезпека.

4. Структура навчальної дисципліни

Вид заняття /роботи	Назва теми	Кількість годин		Згідно з розкладом
		о/д.ф.	з.ф.	
1	2	3	4	5
Змістовий модуль 1				
Лекція 1	Кібербезпека на сучасному етапі цифровізації	2		тиждень 1
Лекція 2	Основні задачі кібербезпеки	2		тиждень 2
Самостійна робота	Історичні аспекти виникнення та розвитку кібербезпеки			
Лекція 3	Класифікація об'єктів кібербезпеки та джерела кіберзагроз	2		тиждень 3
Лекція 4	Кібербезпека мережевих інформаційних ресурсів	2		тиждень 4
Самостійна робота	Класифікація мережевих кіберзагроз			
Лекція 5	Протоколи та стандарти кібербезпеки	2		тиждень 5
Лекція 6	Концепції та засоби захисту програмного забезпечення	2		тиждень 6
Самостійна робота	Шифрування даних			
Лекція 7	Кібербезпека веб ресурсів та веб застосунків	2		тиждень 7
Лекція 8	Кібербезпека хмарних ресурсів та застосунків	2		тиждень 8
Самостійна робота	Файервол на персональному комп'ютері			
Лекція 9	Комп'ютерні віруси та троянські програм	2		тиждень 9
Лекція 10	Шпіонаж засобами комп'ютерних програм	2		тиждень 10
Самостійна робота	Різновиди кіберзброї			
Лекція 11	Кібербезпека мобільних систем та IoT	2		тиждень 11
Лекція 12	Штучний інтелект та кібербезпека	2		тиждень 12
Самостійна робота	Приклади застосування штучного інтелекту до кібератак			
Лекція 13	Культура кібербезпеки та формування її складових	2		тиждень 13
Лекція 14	Управління інцидентами та розробка політик кібербезпеки	2		тиждень 14

Запорізький національний університет
Силабус навчальної дисципліни
(Сучасні проблеми кібербезпеки)



Самостійна робота	Приклади застосування соціальної інженерії до кібератак			
-------------------	---	--	--	--

5. Види і зміст контрольних заходів

Вид заняття/роботи	Вид контрольного заходу	Зміст контрольного заходу*	Критерії оцінювання та термін виконання*	Усього балів
1	2	3	4	5
Поточний контроль				
Змістовий модуль 1				
Самостійна робота	Тестування		тиждень 3	15
Змістовий модуль 2				
Самостійна робота	Тестування		тиждень 6	15
Змістовий модуль 3				
Самостійна робота	Тестування		тиждень 10	15
Змістовий модуль 4				
Самостійна робота	Тестування		тиждень 13	15
Усього за поточний контроль				60
Підсумковий контроль				
Форма підсумкового контролю	Вид підсумкового контрольного заходу	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
Залік	Контрольне тестування			20
	Оцінювання індивідуального завдання			20
Усього за підсумковий контроль				40

Шкала оцінювання ЗНУ: 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)		

Запорізький національний університет
Силабус навчальної дисципліни
(Сучасні проблеми кібербезпеки)
6. Основні навчальні ресурси



Рекомендована література

1. Стратегія кібербезпеки України (2021 – 2025 роки). Режим доступу: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf
2. Концепція інформаційної безпеки України: Режим доступу: <https://www.osce.org/files/f/documents/0/2/175056.pdf>
3. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. - Київ : ДУТ, 2015. 288 с.
4. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. – Київ: ВІКНУ, 2016. 286 с.
5. Jajodia S., Shakarian P., Subrahmanian V.S., Swarup V. Cyber Warfare: Building the Scientific Foundation. London: Springer, 2015. 321 p.
6. Binary bullets: the ethics of cyberwarfare / edited by F.Allhoff, A.Henschke, B.J.Strawser. - New York: Oxford University Press, 2016. 296 p.
7. Greenberg A. Sandworm : a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. - New York : Doubleday, 2019. 370 p.
8. Бараненко Р.В. Кібератаки як одна із форм кібертероризму // Вчені записки Таврійського національного університету ім. В.І. Вернадського, Серія: Технічні науки, Т.32(71), №1, Ч.1, 2021, С.45-50. DOI <https://doi.org/10.32838/2663-5941/2021.1-1/07>

Запорізький національний університет
Силабус навчальної дисципліни
(Сучасні проблеми кібербезпеки)
7. Регуляції і політики курсу



Відвідування занять. Регуляція пропусків.

Курс не передбачає практичних або лабораторних занять. Студенти мають відвідувати лекційні заняття, які проводяться в режимі онлайн. Самостійна робота студентів складається із індивідуального вивчення певних тем, які надаються у кожному змістовому модулі, підготовки та проходженні тестування, а також підготовки звіту з індивідуального дослідницького завдання, що особисто перевіряється викладачем. Темі та матеріал пропущених лекцій відпрацьовуються самостійно за наданими матеріалами, за наявності посилань на відеозапис лекцій, а якість опрацювання визначається тестуванням у змістовому модулі.

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 запозичується, має супроводжуватися посиланням на першоджерело.

Роботи, у яких виявлено ознаки плагіату, до розгляду не приймаються і відхиляються без права перескладання. Якщо є невпевненість, чи підпадають зроблені 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.org та подібні) є неприпустимим. Рекомендовані бази даних для пошуку джерел:

Електронні ресурси Національної бібліотеки ім. Вернадського: <http://www.nbuv.gov.ua>

Відкритий архів публікацій Cornell University: <https://arxiv.org>

Цифрова повнотекстова база даних англomовної наукової періодики JSTOR: <https://www.jstor.org/>

Комунікація

Базовою платформою для комунікації викладача зі студентами є Moodle.

Важливі повідомлення загального характеру розміщуються викладачем на форумі курсу. Для персональних запитів використовується сервіс приватних повідомлень. Відповіді на запити студентів подаються викладачем впродовж одного тижня. 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 «Спам».

Якщо за технічних причин доступ до Moodle є неможливим, або Ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу vgorbenko@znu.edu.ua. У листі обов'язково вкажіть Ваше прізвище та ім'я, курс та шифр академічної групи.

Запорізький національний університет
Силабус навчальної дисципліни
(Сучасні проблеми кібербезпеки)
ДОДАТКОВА ІНФОРМАЦІЯ



ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ НА 2025-2026 н.р. доступний за адресою: <http://surl.li/afeagu>.

НАВЧАННЯ ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь 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. Наявність академічної заборгованості до 6 навчальних дисциплін (у 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. Процедура повторного вивчення визначається Положенням про порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: <https://tinyurl.com/y9pkmmp5>.

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. Спеціалізована допомога: (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 ЗАПОРІЗЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ (СЕЗН ЗНУ): <https://moodle.znu.edu.ua>.

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/>