

## ВСТУП ДО СПЕЦІАЛЬНОСТІ КІБЕРБЕЗПЕКА

**Викладач:** д.т.н., професор Гоменюк Сергій Іванович

**Кафедра:** програмної інженерії, I корпус, ауд 19

**E-mail:** gserega71@gmail.com

**Телефон:** -

**Інші засоби зв'язку:** Moodle (форум курсу, приватні повідомлення) викладача

<b>Освітня програма, рівень вищої освіти</b>		Кібербезпека бакалавр					
<b>Статус дисципліни</b>		Нормативна					
<b>Кредити ECTS</b>	5	<b>Навч. рік</b>	2023-24	<b>Рік навчання</b>	1	<b>Тижні</b>	14
<b>Кількість годин</b>	150	<b>Кількість змістових модулів</b>	7	<b>Лекційні заняття – 14 Лабораторні роботи – 28 Самостійна робота – 106</b>			
<b>Вид контролю</b>	Залік						
<b>Посилання на курс в Moodle</b>			<a href="https://moodle.znu.edu.ua/course/view.php?id=15936">https://moodle.znu.edu.ua/course/view.php?id=15936</a>				
<b>Консультації:</b>			понеділок з 13:00 до 14:00, I корпус, ауд. 19				

### ОПИС КУРСУ

Розвиток сучасних інформаційних технологій та їх активне застосування у всіх сферах людської діяльності призвели не тільки до покращення якості життя, а й до появи нових високотехнологічних видів злочинів, що базуються на останніх досягненнях інформатики.

Слід зазначити, що кіберзлочинність може не тільки привести до втрати інформації (і втраті реалізації фінансових збитків), а й може нести пряму загрозу здоров'ю та життю людей, оскільки багато видів критичної інфраструктури на сьогодні мають дистанційне мікропроцесорне керування та підключені до глобальної мережі Інтернет. Саме тому для запобігання виникненню проблем, які можуть завдати зловмисники при несанкціонованому доступі до комп'ютерних систем, на перший план на сьогодні виходить відносно нова наука кібербезпеки, яка є "сукупністю методів захисту у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і їх впровадження із точки зору конфіденційності, цілісності і доступності".

**Метою** вивчення дисципліни "Вступ до спеціальності кібербезпека" є ознайомлення майбутніх фахівців в галузі кібербезпеки та захисту інформації з основами їх майбутньої спеціальності. В процесі вивчення дисципліни студенти ознайомляться з історією розвитку кібербезпеки, технічним забезпеченням комп'ютерних систем, основними методами криптографії тощо.

### ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У результаті вивчення дисципліни студент повинен **знати:**

- 1) історію розвитку криптології;
- 2) основні типи кіберзлочинів;

- 3) архітектуру комп'ютера та основи організації комп'ютерних мереж;
- 4) основні поняття симетричних та асиметричних криптосистем;
- 5) цифровий підпис;
- 6) стандартні методи протидії основним кіберзагрозам.

**вміти:**

- 1) використовувати на практиці симетричні та асиметричні криптосистеми;
- 2) використовувати цифровий підпис;
- 3) користуватися стандартними програмами захисту інформації.

**Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких компетентностей:**

- КЗ 1 Здатність застосовувати знання у практичних ситуаціях.
- КЗ 2 Знання та розуміння предметної області та розуміння професії.
- КС 5 Здатність до пошуку, оброблення та аналізу інформації.

## ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, методичні вказівки до виконання лабораторних робіт, індивідуальних дослідницьких завдань розміщені на платформі Moodle:

<https://moodle.znu.edu.ua/course/view.php?id=15936>

## КОНТРОЛЬНІ ЗАХОДИ

### Методи контролю

Кожна лабораторна робота складається з теоретичної і практичної частини. Теоретична частина захищається студентом шляхом бесіди з викладачем. Практична частина перевіряється викладачем на предмет якості виконання та відповідності отриманих результатів заявленим задачам.

### Розподіл балів, які отримують студенти

Розділ	Вид контролю	Кількість балів
Розділ 1	Лабораторна робота № 1	10
	Лабораторна робота № 2	10
	Лабораторна робота № 3	10
Розділ 1	Лабораторна робота № 4	10
	Лабораторна робота № 5	10
	Лабораторна робота № 6	10
Разом		60
Залік		40
Всього за семестр		100

### Критерії оцінювання кожного з проведених видів контролю:

1. Захист лабораторної роботи відбувається після виконання завдання та завантаження відповідного звіту до системи Moodle. Один завантажений звіт без захисту лабораторної роботи може бути оцінений не вище, ніж 50% від максимального можливого значення балів. Під час захисту студент має відповісти на питання викладача та пояснити деякі етапи виконання завдання.

2. Залік проводиться у формі тестування рівня теоретичної підготовки з усіх розділів курсу та має 20 питань, які оцінюються по 2 бали кожне.

3. Підсумкова оцінка складається з суми балів, отриманих студентом за виконання лабораторних робіт, та оцінки, отриманої за залік.



**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)		

**РОЗКЛАД КУРСУ ЗА ТЕМАМИ І КОНТРОЛЬНІ ЗАВДАННЯ**

Тиждень і вид заняття	Тема змістового модулю	Контрольний захід	Кількість балів
Змістовий модуль 1			
Тиждень 1 Лекція 1	Основні поняття кібербезпеки		
Тиждень 1-2 Лабораторна робота 1	Шифр Цезаря	Захист звіту з результатами лабораторної роботи	10
Змістовий модуль 2			
Тиждень 3 Лекція 2	Архітектура комп'ютера		
Тиждень 3-4 Лабораторна робота 2	Книжний шифр	Захист звіту з результатами лабораторної роботи	10
Змістовий модуль 3			
Тиждень 5 Лекція 3	Комп'ютерні мережі та Інтернет		
Тиждень 5-6 Лабораторна робота 3	Шифр Віженера	Захист звіту з результатами лабораторної роботи	10
Змістовий модуль 4			
Тиждень 7 Лекція 4	Основи криптографії. Симетричні криптосистеми		



Тиждень 7-8 Лабораторна робота 4	Шифр XOR	Захист звіту з результатами лабораторної роботи	10
Змістовий модуль 5			
Тиждень 9 Лекція 5	Асиметричні криптосистеми		
Тиждень 9-10 Лабораторна робота 5	Метод RSA	Захист звіту з результатами лабораторної роботи	10
Змістовий модуль 6			
Тиждень 11 Лекція 6	Цифровий підпис		
Тиждень 11-12 Лабораторна робота 6	Цифровий підпис	Захист звіту з результатами лабораторної роботи	10
Змістовий модуль 7			
Тиждень 13 Лекція 7	Кіберзагрози		
Тиждень 13-14 Консультації			

## ЛІТЕРАТУРА

### Основна

1. Про основні засади забезпечення кібербезпеки України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 05.09.2023).
2. Кібербезпека : сучасні технології захисту: навч. посіб. / С. Е. Остапов, С. П. Євсєєв, О. Г. Король; М-во освіти і науки України, Харків. нац. економ. ун-т ім. С. Кузнеця. – Львів: Новий Світ – 2000, 2019. - 680 с.
3. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. – 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. Історія криптографії. URL: [https://en.wikipedia.org/wiki/History\\_of\\_cryptography](https://en.wikipedia.org/wiki/History_of_cryptography) (дата звернення: 05.09.2023).

### Додаткова

1. Комп'ютерна безпека. URL: [https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0\\_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0) (дата звернення: 05.09.2023).
2. Tanenbaum A., Wetherall D. Computer Networks, 6<sup>th</sup> edition. New Jersey: Pearson, 2021. 803 p.
3. Tanenbaum A., Todd A. Structured Computer Organization, 6<sup>th</sup> edition. New Jersey: Pearson, 2012. 800 p.
4. Welcome to Python.org. URL: <https://www.python.org/> (дата звернення: 05.09.2023).



## **РЕГУЛЯЦІЯ І ПОЛІТИКИ КУРСУ**

### **Відвідування занять. Регуляція пропусків.**

Інтерактивний характер курсу передбачає обов'язкове відвідування лекційних та лабораторних занять. Студенти, які за певних обставин не можуть відвідувати лабораторних або лекційних занять 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. Студенти, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

### **Політика академічної доброчесності**

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.

### **Використання комп'ютерів/телефонів на занятті**

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та лабораторних 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 Cisco Webex 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 технічних причин доступ до Moodle є неможливим, або ваше питання потребує термінового розгляду, направте електронного листа з позначкою «Важливо» на адресу [tupakhina@znu.edu.ua](mailto:tupakhina@znu.edu.ua). У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.



## **ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2023-2024 рр.**

*ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ 2020-2021 н. р. (посилання на сторінку сайту ЗНУ)*

**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>.

**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>.

**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/y9yfw9y>. 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 (061)228-15-84 (щоденно з 9 до 21).

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

**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](mailto: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>