

## СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

**Викладач:** кандидат технічних наук, доцент Решевська Катерина Сергіївна

**Кафедра:** комп'ютерних наук, I корпус, ауд. 39

**E-mail:** reshka82zp@gmail.com

**Телефон:** (061) 289-12-57

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

<b>Освітня програма, рівень вищої освіти:</b>		Комп'ютерні науки Бакалавр					
<b>Статус дисципліни:</b>		Вибіркова					
<b>Кредити ECTS</b>	3	<b>Навч. рік:</b>	2024-2025	<b>Рік навчання</b>	4	<b>Тижні</b>	13
<b>Кількість годин</b>	90	<b>Кількість змістових модулів<sup>1</sup></b>	4	<b>Лекційні заняття – 14</b> <b>Практичні заняття –26</b> <b>Самостійна робота – 50</b>			
<b>Вид контролю:</b>		Залік					
<b>Посилання на курс в Moodle</b>			<a href="https://moodle.znu.edu.ua/course/view.php?id=13953">https://moodle.znu.edu.ua/course/view.php?id=13953</a>				
<b>Консультації:</b> особисті – щотижнево за розкладом (1 год.), дистанційні (за попередньою домовленістю) – e-mail, Zoom							

## ОПИС КУРСУ

В межах дисципліни «Стратегії кібербезпеки» вивчаються типи шкідливого програмного забезпечення та атак, стратегії, які використовують організації для захисту від атак та технології, продукти і процедури, які використовуються для захисту інформації у мережі.

**Метою** викладання навчальної дисципліни «Стратегії кібербезпеки» є формування у студентів та слухачів знань методів та засобів захисту інформаційних ресурсів, які реалізовані у сучасних базових технологіях інформаційної безпеки.

Основним завданням вивчення дисципліни «Стратегії кібербезпеки» є: отримання навичок роботи з програмним забезпеченням для захисту інформації у мережі.

## ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У результаті вивчення дисципліни студенти повинні:

**знати:**

- сучасні загрози безпеці у інформаційних системах;
- технічні методи і засоби захисту інформації;
- криптографічні методи захисту інформації;
- програмні методи і засоби захисту;
- методи захисту інформації в розподілених інформаційних системах;
- організаційно-правове забезпечення захисту інформації.

**вміти:**

- забезпечувати безпеку операційної системи шляхом її налагодження;
- програмувати сучасні методи захисту інформації з використанням бібліотек мов програмування;

<sup>1</sup> 1 змістовий модуль = 15 годин (0,5 кредита ECTS)

- впроваджувати використання засобів захисту інформації у СКБД;
- розробляти стеганографічні підходи приховування даних у графічних зображеннях;
- розробляти програмні засоби для підписання та перевірки ЕЦП електронних документів.

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

ЗК6 Здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критичне оцінювання інформації, оперувати нею у професійній діяльності;

ЗК8 Здатність вчитися і оволодівати сучасними знаннями;

ЗК9 Здатність до адаптації та дії в новій ситуації

СК 6 Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

СК 12 Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

СК 15 Здатність забезпечувати інформаційну безпеку в інформаційних системах з використанням сучасних методів аутентифікації, формування політик прав доступу та шифрування.

**Очікувані результати навчання:**

ПР3 Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

ПР13 Використовувати методи захисту інформації в інформаційних системах.

## ОСНОВНІ НАВЧАЛЬНІ РЕСУРСИ

Презентації лекцій, методичні рекомендації до виконання лабораторних робіт та індивідуального завдання, тести у системі Moodle

## КОНТРОЛЬНІ ЗАХОДИ

### Поточні контрольні заходи

Поточний контроль передбачає такі **теоретичні** завдання:

- усне опитування з теоретичного матеріалу за темою на початку кожного лабораторного заняття. Перелік питань з кожної лабораторної роботи розміщено у файлі з завданням до лабораторної роботи у системі Moodle.
- поточний тест за пройденим матеріалом.

Поточний контроль передбачає таке **практичне** завдання:

- виконання практичних робіт.

### Підсумкові контрольні заходи:

**Індивідуальне завдання** – програмна реалізація криптографічного методу шифрування даних.

**Підсумковий тест** – підсумкове тестування з курсу за обмежений час у системі Moodle.

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**  
**МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ**  
**Силабус навчальної дисципліни**



Контрольний захід		Термін виконання	% від загальної оцінки
<b>Поточний контроль (max 60%)</b>			
Змістовий модуль 1	Опитування з теоретичного матеріалу	Тиждень 1	2
	Практична робота 1	Тиждень 1	2
	Опитування з теоретичного матеріалу	Тиждень 2	2
	Практична робота 2	Тиждень 2	2
	Опитування з теоретичного матеріалу	Тиждень 3	2
	Практична робота 3	Тиждень 3	2
Змістовий модуль 2	Опитування з теоретичного матеріалу	Тиждень 4	2
	Практична робота 4	Тиждень 4	2
	Опитування з теоретичного матеріалу	Тиждень 5,6	2
	Практична робота 5	Тиждень 5,6	2
	Поточний тест	Тиждень 7	10
Змістовий модуль 3	Опитування з теоретичного матеріалу	Тиждень 8	
	Практична робота 6	Тиждень 8	2
	Опитування з теоретичного матеріалу	Тиждень 9	2
	Практична робота 7	Тиждень 9	2
	Опитування з теоретичного матеріалу	Тиждень 10	2
	Практична робота 8	Тиждень 10	2
Змістовий модуль 4	Опитування з теоретичного матеріалу	Тиждень 11	2
	Практична робота 9	Тиждень 11	2
	Опитування з теоретичного матеріалу	Тиждень 12	2
	Практична робота 10	Тиждень 12	2
	Поточний тест	Тиждень 13	10
<b>Підсумковий контроль (max 40%)</b>			
Підсумковий тест			20
Індивідуальне завдання			20
<b>Разом</b>			<b>100%</b>

**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)	

**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**  
**МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ**  
**Силабус навчальної дисципліни**



C	75 – 84 (добре)	3 (задовільно)	Не зараховано
D	70 – 74 (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 заняття	Контрольне завдання	Кількість балів
Змістовий модуль 1.			
Тиждень 1 Лекція 1	Вступ до кібербезпеки. Атаки, поняття та методи. Зловмисники та експерти з кібербезпеки		
Тиждень 1 Практична робота 1	Захист від кібератак	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 2 Практична робота 2	Безпечне збереження паролів	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 3 Лекція 2	Захист інформації у кіберпросторі. Криптографія		
Тиждень 3 Практична робота 3	Класичні криптоалгоритми	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Змістовий модуль 2.			
Тиждень 5 Лекція 3	Контроль доступу. Приховування даних		
Тиждень 4,5 Практична робота 5	Стеганографічні методи захисту інформації	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 7 Лекція 4	Забезпечення цілісності даних. ЕЦП. Електронний сертифікат		
Тиждень 7 Практична робота 4	Програмна розробка схеми підписання та перевірки ЕЦП	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 7 Поточний тест 1		Тестові завдання в системі Moodle	10
Змістовий модуль 4.			
Тиждень 8	Програмна реалізація	Усне опитування з теми.	4



Практична робота 6	алгоритму хешування даних MD5	Виконання завдань лабораторної роботи	
Тиждень 9 Лекція 5	Концепція п'яти дев'яток		
Тиждень 8 Практична робота 7	Використання хешу для безпечного збереження паролів у БД	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 9 Практична робота 8	Робота центру сертифікації	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 10 Практична робота 9	Ідентифікація загроз	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 11,12 Практична робота 10	Аналіз протоколів забезпечення захисту інформації у мережі	Усне опитування з теми. Виконання завдань лабораторної роботи	4
Тиждень 11 Лекція 6	Захист домену кібербезпеки		
Тиждень 13 Лекція 7	Домени кібербезпеки.		
Тиждень 13 Поточний тест 2		Тестові завдання в системі Moodle	10

## ОСНОВНІ ДЖЕРЕЛА

1. Когут Ю. Кібербезпека та ризики цифрової трансформації компанії. К:Консалтингова компанія Сідкон, 2021. 372 с.
2. Когут Ю. Кібервійна та безпека об'єктів критичної інфраструктури К:Консалтингова компанія Сідкон, 2021. 332 с.
3. Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Інформаційна безпека Л:Львівська політехніка. 2019.580 с.
4. Фармагей О., Мельник Д., Петрик В., Карпович О., Остроухов В., Присяжнюк М., Чеховська М. Інформаційна безпека. К: Ліра-К. 2021. 412 с.
5. Codings Z. Computer Programming And Cyber Security for Beginners. Michigan :Independently published. 2019. 330p.
6. Остапов С. Е., Євсєєв С. П., Король О. Г.. Технології захисту інформації : навчальний посібник. Х. : Вид. ХНЕУ, 2015. 476 с.
7. Закони України: «Про інформацію», «Про доступ до публічної інформації»: чинне законодавство зі змінами та допов. Станом на 1 липн.2011р.: (офіц.. текст). – К.: ПАЛИВОДА А. В., 2011. 32 с.
8. Закон України «Про інформацію». Вводиться в дію Постановою ВР N 2658- XII ( 2658-12 ) від 02.10.92, ВВР, 1992, N 48, ст.651.
9. Закон України «Про захист персональних даних». (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)
10. Закон України «Про доступ до публічної інформації. (Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314)



11. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. ( Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286 )

12. Постанова Кабінету Міністрів України від 25.05.2011 № 616 "Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення". від 25 травня 2011 р. N 616 Київ.

[http://ito.vspu.net/Prakt\\_IT/PIDSUMOK/2014-2015/rob/Klochenok/tzi.html](http://ito.vspu.net/Prakt_IT/PIDSUMOK/2014-2015/rob/Klochenok/tzi.html)

## **РЕГУЛЯЦІЇ І ПОЛІТИКИ КУРСУ<sup>2</sup>**

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

*Відвідування лекційних і лабораторних занять є обов’язковим. Студенти, які за певних обставин не можуть відвідувати лабораторні заняття регулярно, мусять впродовж тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять.*

### **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 ви запозичуєте, має супроводжуватися посиланням на першоджерело.*

*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.*

*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>*

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

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

*Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та лабораторних занять дозволяється виключно у навчальних цілях. Будь ласка, не забувайте активувати режим «без звуку» до початку заняття.*

*Під час виконання заходів контролю (поточних та підсумкового тестів) 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 здачі індивідуального завдання, коди доступу до сесій у Cisco Webex та Zoom. – 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,*

---

<sup>2</sup> 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!





---

*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 [reshka82zp@gmail.com](mailto:reshka82zp@gmail.com). У листі обов'язково вкажіть ваше прізвище та ім'я, курс та шифр академічної групи.*

## ДОДАТОК ДО СИЛАБУСУ ЗНУ – 2020-2021

### ГРАФІК НАВЧАЛЬНОГО ПРОЦЕСУ 2020-2021 н. р. (зіпнєрпосилання на сторінку сайту)

**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>.

**ОСВІТНІЙ 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 методик 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/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](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
- для студентів Інженерного інституту ЗНУ - [alexvasik54@gmail.com](mailto:alexvasik54@gmail.com), Василенко Олексій Володимирович

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>.