ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Стратегії кібербезпеки

підготовки бакалаврів

денної форми здобуття освіти

освітньо-професійна програма Комп'ютерні науки

спеціальності 122 Комп'ютерні науки

галузі знань 12 Інформаційні технології

ВИКЛАДАЧ: Решевська Катерина Сергіївна, к.т.н., доцент, 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
Стратегії кібербезпеки

Зв`язок з викладачем: Решевська Катерина Сергіївна
E-mail: reshka82zp@gmail.com
Сезн ЗНУ повідомлення: https://moodle.znu.edu.ua/course/view.php?id=13768
Телефон (кафедра): 289-12-57
Кафедра комп'ютерних наук, ауд. №39, 1 корпус ЗНУ

1. Опис навчальної дисципліни

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.

Дисципліна «Стратегії кібербезпеки» вивчається у 7-му семестрі. Необхідними для вивчення дисципліни «Стратегії кібербезпеки» є знання, уміння і навички, засвоєні при вивченні дисципліни «Комп'ютерні мережі» та «Технології захисту інформації». Дисципліна «Стратегії кібербезпеки» може служити підготовчою базою для кваліфікаційної роботи.

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Стратегії кібербезпеки

Паспорт навчальної дисципліни

Нормативні показники	**денна форма здобуття освіти**	**заочна форма здобуття освіти**
1	***2***	***3***
Статус дисципліни	**Обов'язкова**	
Семестр	7-й	7-й
Кількість кредитів ECTS	6	6
Кількість годин	180 год.	180 год.
Лекційні заняття	28 год.	10 год.
Лабораторні заняття	28 год.	8 год.
Самостійна робота	124 год.	162 год.
Консультації	Дистанційно: Ідентифікатор конференції Zoom: 511 572 8748; Код доступу: 1s1gNH	
Вид підсумкового семестрового контролю:	**залік**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=13768	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	**Методи навчання**	**Форми і методи оцінювання**
Компетентності		
Здатність до абстрактного мислення, аналізу та синтезу	лекція-візуалізація, пояснення, демонстрація, виконання завдань лабораторних робіт, метод-мікрофон	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Здатність застосовувати знання у практичних ситуаціях	лекція-візуалізація, кейс-метод пояснення, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Знання та розуміння предметної області та розуміння професійної діяльності	лекція-візуалізація, пояснення, демонстрування, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування
Здатність застосовувати методи та засоби забезпечення	лекція-візуалізація, пояснення,	**Поточний контроль**: захист лабораторних робіт,

інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури	демонстрування, виконання завдань лабораторних робіт, аналіз	опитування, тестування **Підсумковий контроль:** тестування
Програмні результати навчання		
Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних	лекція-візуалізація, пояснення, демонстрування, виконання завдань лабораторних робіт	**Поточний контроль**: захист лабораторних робіт, опитування, тестування **Підсумковий контроль:** тестування

3. Зміст навчальної дисципліни

Змістовий модуль 1. Основи кібербезпеки та інформаційні ресурси Поняття кібербезпеки та її роль у сучасному цифровому середовищі. Рівні кіберзахисту: особистий, корпоративний, державний. Принципи інформаційної безпеки: конфіденційність, цілісність, доступність. Стани даних: обробка, зберігання, передавання. Модель безпеки (куб МакКамбера). Типи корпоративних даних: транзакційні, фінансові, інтелектуальна власність. Загрози та вразливості користувачів. Загрози інформаційним пристроям.

Змістовий модуль 2. Соціальна інженерія та захист Сутність соціальної інженерії та експлуатація людського фактору. Різновиди соціальної інженерії. Тактики: авторитет, залякування, дефіцит, терміновість, довіра, знайомство, консенсус. Підглядання через плече, пошук у смітнику, impersonation, hoaxes, піггібекінг, тейлгеттінг, watering hole, тайпсквотинг, кампанії впливу, модифікація електронних листів, видавання себе за інших. Поштова безпека: спам, фішинг, spear phishing, вішинг, фармінг, уелінг. Базові заходи захисту від кібератак. Роль обізнаності користувачів у системі кібербезпеки.

Змістовий модуль 3. Класифікація загроз і шкідливе ПЗ Класифікація кіберзагроз. Програмні атаки та програмні помилки. Саботаж і людський фактор. Фізичні загрози. Внутрішні та зовнішні загрози. Загрози локальним мережам і хмарним середовищам. Моделі хмарних сервісів (SaaS, PaaS, IaaS). Шкідливе програмне забезпечення: віруси, хробаки, трояни, логічні бомби, програми-вимагачі, бекдори, руткіти, ботнети, keylogging. Атаки нульового дня, APT-атаки, алгоритмічні атаки, атаки на ланцюг поставок, аналітика загроз та OSINT.

Змістовий модуль 4. Мережеві, прикладні та мобільні атаки DoS і DDoS-атаки. DNS-атаки (spoofing, cache poisoning, domain hijacking). URL-переспрямування. Атаки канального рівня (ARP, MAC spoofing, MAC flooding). Атаки «людина посередині» (MitM) та «людина в мобільному» (MitMo). Replay-атаки. Загрози застосункам та інформаційним системам: XSS, SQL/XML/LDAP/DLL-ін'єкції, CSRF, переповнення буфера, RCE, підвищення привілеїв, race condition, атаки на API, обхід каталогів, виснаження ресурсів. Мобільні загрози: grayware, смішинг, Bluetooth-атаки, шахрайські точки доступу Wi-Fi, «злий близнюк», вразливості WEP/WPA2/WPA3.

Змістовий модуль 5. Захист мереж

Захист бездротових мереж. Маскування SSID і фільтрація MAC-адрес. Аутентифікація та шифрування. Інфраструктура мережної безпеки. IDS і IPS. Списки контролю доступу (ACL). SNMP і NetFlow. Додатковий захист.

4. Структура навчальної дисципліни

Вид заняття /роботи	Назва теми	Кількість годин		Згідно з розкладом
		о/д. ф.	з.ф.	
1	*2*	*3*	*4*	*5*
Лекція 1	Вступ до кібербезпеки та її роль у цифровому світі	2	1	тиждень 1
Лабораторне заняття 1	Дослідження методів соціальної інженерії	2	2	тиждень 1
Лекція 2	Типові кіберзагрози та їх класифікація	2	1	тиждень 2
Лабораторне заняття 2	Аналіз загроз комп'ютерних мереж	2	2	тиждень 2
Лекція 3	Людський фактор у кібербезпеці	2	1	тиждень 3
Лабораторне заняття 3	Дослідження DNS-трафіку	2	2	тиждень 3
Лекція 4	Соціальна інженерія: сутність і принципи	2	1	тиждень 4
Лабораторне заняття 4	Аналіз загроз комп'ютерних мереж	2	2	тиждень 4
Лекція 5	Соціальна інженерія: сутність і принципи	2	1	тиждень 5
Лабораторне заняття 5	Дослідження DNS-трафіку	2		тиждень 5
Лекція 6	Зловмисне програмне забезпечення: загальні поняття	2	1	тиждень 6
Лабораторне заняття 6	Дослідження DNS-трафіку	2		тиждень 6

Лекція 7	Типи malware: віруси, хробаки, трояни, ransomware	2	1	тиждень 7
Лабораторне заняття 7	Встановлення віртуальної машини на персональному комп'ютері	2		тиждень 7
Лекція 8	Сучасні загрози: APT-атаки та zero-day	2	1	тиждень 8
Лабораторне заняття 8	Встановлення віртуальної машини на персональному комп'ютері	2		тиждень 8
Лекція 9	Атаки на бездротові мережі	2	1	тиждень 9
Лабораторне заняття 9	Читання журналів подій сервера	2		тиждень 9
Лекція 10	Захист бездротових мереж	2	1	тиждень 10
Лабораторне заняття 10	Налаштування базових функцій безпеки бездротової мережі. Пошук та усунення несправностей бездротового з'єднання	2		тиждень 10
Лекція 11	Атаки на застосунки та веб-системи	2		тиждень 11
Лабораторне заняття 11	Налаштування базових функцій безпеки бездротової мережі. Пошук та усунення несправностей бездротового з'єднання	2	1	тиждень 11
Лекція 12	Поточний стан кіберзагроз і аналітика	2		тиждень 12
Лабораторне заняття 12	Атака на базу даних SQL	2		тиждень 12
Лекція 13	Інфраструктура мережної безпеки	2		тиждень 13
Лабораторне заняття 13	Використання списку контролю доступу	2		тиждень 13
Лекція 14	Комплексна стратегія кіберзахисту та роль користувачів	2		тиждень 14
Лабораторне заняття 14	Використання списку контролю доступу	2		тиждень 14
Самостійна робота	Аналіз реальних кіберінцидентів в Україні та світі	124	162	тиждень 1-14

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				
Лабораторна робота №1	Захист лабораторної роботи №1	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –2	5
Лабораторна робота №2	Захист лабораторної роботи №2	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768),	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1;	5

		захист лабораторної роботи	Захист лабораторної роботи –2	
Поточний контроль	Тест 1	Відповіді на 10 тестових питань (https://moodle.znu.edu.ua/course/view.php?id=13768)	10 питань по 0,5 бала	5
Лабораторна робота №3	Захист лабораторної роботи №3	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –2	5
Тестування		Тестові завдання в Тесті 1		
Поточний контроль	Тест 2	Відповіді на 10 тестових питань (https://moodle.znu.edu.ua/course/view.php?id=13768)	10 питань по 0,5 бала	5
Лабораторна робота №4	Захист лабораторної роботи №4	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –2	5
Лабораторна робота №5	Захист лабораторної роботи №5	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –2	5
Поточний контроль	Тест 3	Відповіді на 10 тестових питань (https://moodle.znu.edu.ua/course/view.php?id=13768)	10 питань по 0,5 бала	5
Лабораторна робота №6	Захист лабораторної роботи №6	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –2	5
Лабораторна робота №7	Захист лабораторної роботи №7	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –2	5
Лабораторна робота №8	Захист лабораторної роботи №8	Виконання завдання лабораторної роботи (https://moodle.znu.edu.ua/course/view.php?id=13768), захист лабораторної роботи	Виконання лабораторної роботи: Правильне виконання –3; наявність незначних помилок –2; при наявності грубих помилок –1; Захист лабораторної роботи –2	5
Поточний контроль	Тест 4	Відповіді на 10 тестових питань (https://moodle.znu.edu.ua/course/view.php?id=13768)	10 питань по 0,5 бала	5
Усього за поточний контроль				**60**

Підсумковий контроль				
Форма підсумкового контролю	**Вид підсумкового контрольного заходу**	**Зміст підсумкового контрольного заходу**	**Критерії оцінювання**	**Усього балів**
Екзамен	Теоретичні питання тесту	20 питань (https://moodle.znu.edu.ua/course/view.php?id=13768)	Одне теоретичне питання -1 бал	**20**
	Практичне завдання	Представдлення доповіді з реальних кіберінцидентів (https://moodle.znu.edu.ua/course/view.php?id=13768)	Доповідь – 10 балів Презентація – 5 балів Відповідь на питання – 5 балів	**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)		

6. Основні навчальні ресурси

Рекомендована література

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., Євсеєв 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)

Інформаційні ресурси

1. CERT-UA. URL: https://cert.gov.ua/ (дата звернення: 25.08.25)
2. REAL-TIME CYBERSECURITY INTELLIGENCE. URL: https://www.cyberreport.news/ (дата звернення: 25.08.25)
3. CodePen.io. URL: https://feedly.com/ (дата звернення: 25.08.25)
4. The World’s First Truly Open Threat Intelligence Community.URL: https://otx.alienvault.com/ (дата звернення: 25.12.25)

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 НА 2025-2026 н.р. доступний за адресою: https://surl.li/vlweoj

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 Запорізького національного університету: https://surl.li/wdzjrl

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://surl.lu/hfjbya

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://surl.li/qgacqa
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://surl.li/unwzzm
Положення про призначення та виплату соціальних стипендій у ЗНУ: https://surl.lu/xkxmuz

ПСИХОЛОГІЧНА ДОПОМОГА. Кабінет практичного психолога **Марті Ірини Вадимівни –** навч. корп. №4, каб. №235 (понеділок, середа, четвер 9.00-11.00, 13.00-15.00), навч. корп. №9 (ІННІ) каб.57 (п'ятниця 9.00-11.00, 13.00-15.00), гуртожиток №6 (вул. Добролюбова, 19, середа 9.00-11.00, 13.00-15.00). Попередній запис за тел.: 228-76-48, (099) 253-78-73 щоденно з 9 до 15.

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://surl.li/ivcwih

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/