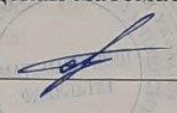


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МАТЕМАТИЧНИЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ЗАТВЕРДЖУЮ

Декан математичного факультету

 С. І. Гоменюк

« » 2021 р.

СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

підготовки бакалавра
денної (очної) та заочної (дистанційної) форм здобуття освіти
спеціальності 126 інформаційні системи та технології
освітня програма Інформаційні системи та технології

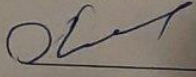
Укладач: Решевська К.С., к.т.н., доцент, доцент кафедри комп'ютерних наук

Обговорено та ухвалено
на засіданні кафедри комп'ютерних
наук

Протокол № 2 від «01» вересня 2021 р.
Завідувач кафедри

 С. В. Чопоров

Погоджено
з навчально-методичним відділом

 О. В. Лещинська

Ухвалено науково-методичною радою
математичного факультету

Протокол № 1 від «02» вересня 2021 р.
Голова науково-методичної ради
факультету

 О. С. Пшенична

2021 рік

1. Опис навчальної дисципліни

1	2	3	
Галузь знань, спеціальність, освітня програма рівень вищої освіти	Нормативні показники для планування і розподілу дисципліни на змістові модулі	Характеристика навчальної дисципліни	
		очна (денна) форма здобуття освіти	заочна (дистанційна) форма здобуття освіти
Галузь знань 12 – Інформаційні технології	Кількість кредитів – 3	Вибіркова	
		Блок дисциплін вільного вибору студента в межах спеціальності	
Спеціальність 126 – Інформаційні системи та технології	Загальна кількість годин – 90	Семестр:	
		8-й	8-й
Освітньо-професійна програма Інформаційні системи та технології	Змістових модулів – 4	Лекції	
		14 год.	4 год.
		Практичні	
		26 год.	6 год.
Рівень вищої освіти: бакалаврський	Кількість поточних контрольних заходів – 8	Самостійна робота	
		50 год.	84 год.
		Вид підсумкового семестрового контролю: залік	

2. Мета та завдання 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 вивчення навчальної дисципліни «Стратегії кібербезпеки» є засвоєння методів та засобів захисту інформаційних ресурсів, які реалізовані у сучасних базових технологіях інформаційної безпеки.

Основними завданнями вивчення дисципліни «Стратегії кібербезпеки» є:

- опанування знань з типових загроз для користувачів у мережі Інтернет;
- вироблення умінь розробляти систему заходів протидії кібер-злочинцям;
- набуття навичок з програмування симетричних та асиметричних крипто алгоритмів шифрування даних, стеганографічних методів та схеми ЕЦП.

ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

У результаті вивчення навчальної дисципліни студент повинен набути таких результатів навчання (знання, уміння тощо) та компетентностей:

Заплановані робочою програмою результати навчання та компетентності	Методи і контрольні заходи
1	2
ЗК6 Здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критичне оцінювання інформації, оперувати нею у професійній діяльності;	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.
ЗК8 Здатність вчитися і оволодівати сучасними знаннями;	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.
ЗК9 Здатність до адаптації та дії в новій ситуації	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.
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.	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.

Заплановані робочою програмою результати навчання та компетентності	Методи і контрольні заходи
СК 12 Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.
СК 15 Здатність забезпечувати інформаційну безпеку в інформаційних системах з використанням сучасних методів аутентифікації, формування політик прав доступу та шифрування.	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.
ЗК6 Здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критичне оцінювання інформації, оперувати нею у професійній діяльності;	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.
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 проєктування і використання інформаційних систем та технологій.	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.
ПР13 Використовувати методи захисту інформації в інформаційних системах.	Методи навчання: лекція-візуалізація, наочні методи, виконання завдань практичної роботи та індивідуального завдання. Контрольні заходи: захист практичної роботи, тестування.

Міждисциплінарні зв'язки.

Вивчення дисципліни «Стратегії кібербезпеки» ґрунтується на знаннях, отриманих під час вивчення курсу «Захист інформації» з циклу професійної підготовки освітньої програми. Знання та вміння набуті при вивченні дисципліни «Стратегії кібербезпеки» необхідні для виконання курсових робіт і кваліфікаційної роботи бакалавра та подальшої професійної діяльності.

3. Програма навчальної дисципліни

Змістовий модуль 1. Вступ до кібербезпеки

Атаки, поняття та методи. Зловмисники та експерти з кібербезпеки. Захист інформації у кіберпросторі. Криптографія.

Змістовий модуль 2. Мистецтво забезпечення цілісності даних

Контроль доступу. Приховування даних. Забезпечення цілісності даних. ЕЦП. Електронний сертифікат.

Змістовий модуль 3. Концепція п'яти дев'яток.

Значення концепції п'яти дев'яток. Середовища, які вимагають п'яти дев'яток. Проєктування системи високої доступності. Ідентифікація активів.

Змістовий модуль 4 . Захист домену кібербезпеки.

Безпека операційної системи. Захист від шкідливих програм. Керування виправленнями. Брандмауери на основі хоста і системи виявлення вторгнень. Безпечний зв'язок.

а

4. Структура навчальної дисципліни

Змістовий модуль	Усьо го годин	Аудиторні (контактні) години						Самостійна робота, год		Система накопичення балів		
		Усього годин		Лекційні заняття, год		Практичні заняття, год				Теор. зав-ня, к-ть балів	Практ. зав-ня, к-ть балів	Усього балів
		о/дф.	з/дис т ф.	о/д ф.	з/дист ф.	о/д ф.	з/дист ф.	о/д ф.	з/ди ст ф.			
1	2	3	4	5	6	7	8	9	10	11	12	13
1	15	12	3	4	1	8	2	3	12	6	6	12
2	15	8	3	4	1	4	2	7	12	9	9	18
3	15	10	2	2	1	8	1	5	13	6	6	12
4	15	10	2	4	1	6	1	5	13	9	9	18
Усього за змістові модулі	60	40	10	14	4	26	6	20	50	30	30	60
Підсумковий семестровий контроль залік	30							30	30	10	30	40
Загалом	90									40	60	100

5. Теми лекційних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/д ф.
1	Вступ до кібербезпеки. Атаки, поняття та методи. Зловмисники та експерти з кібербезпеки	2	1
2	Захист інформації у кіберпросторі. Криптографія	2	1
3	Контроль доступу. Приховування даних	2	1
4	Забезпечення цілісності даних. ЕЦП. Електронний сертифікат	2	1
5	Концепція п'яти дев'яток	2	
6	Захист домену кібербезпеки	2	
7	Домени кібербезпеки	2	
Разом		14	4

6. Теми практичних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/д ф.
1	Практична робота №1 Захист від кібератак	4	1
2	Практична робота №2. Безпечне збереження паролів	2	
3	Практична робота №3. Класичні криптоалгоритми	2	
4	Практична робота №4. Стеганографічні методи захисту інформації	2	1
5	Практична робота №5. Програмна розробка схеми підписання та перевірки ЕЦП	2	1
6	Практична робота №6. Програмна реалізація алгоритму хешування даних MD5	4	1
7	Практична робота №7. Використання хешу для безпечного збереження паролів у БД	2	
8	Практична робота №8. Робота центру сертифікації	2	
9	Практична робота №9. Ідентифікація загроз	4	
10	Практична робота №10. Аналіз протоколів забезпечення захисту інформації у мережі	2	
	Разом	28	6

7. Види і зміст поточних контрольних заходів *

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	**Критерії оцінювання	Усього балів
1	2	3	4	5
1	Опитування з практичної роботи №1	Контрольні питання до практичної роботи, викладені у методичних рекомендаціях до практичних робіт у нульовій секції курсу у системі MoodleZNU	1 бал за кожен правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №1	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
	Опитування з практичної роботи №2	Контрольні питання до практичної роботи, викладені у методичних рекомендаціях до практичних робіт у нульовій секції курсу у системі MoodleZNU	1 бал за кожен правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №2	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
	Опитування з практичної роботи №3	Контрольні питання до практичної роботи, викладені у методичних рекомендаціях до практичних робіт у нульовій секції курсу у системі MoodleZNU	1 бал за кожен правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №3	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
Усього за ЗМ 1 контр. заходів	6			12
2	Опитування з практичної роботи №4	Контрольні питання до практичної роботи, викладені у методичних рекомендаціях до практичних робіт у нульовій секції курсу у системі MoodleZNU	1 бал за кожен правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	**Критерії оцінювання	Усього балів
	Звіт про виконання практичної роботи №4	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
	Опитування з практичної роботи №5	Контрольні питання до практичної роботи, викладені у методичних рекомендаціях до практичних робіт у нульовій секції курсу у системі MoodleZNU	1 бал за кожну правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №5	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	1 бал за кожну правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Поточне тестування №1		2 бали при виконанні завдання з лабораторної роботи	10
Усього за ЗМ 2 контр. заходів	5			18
3	Тестування з практичної роботи №6	Тестові питання до практичної роботи, викладені у базі питань системи MoodleZNU	1 бал за кожну правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №6	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
	Тестування з практичної роботи №7	Тестові питання до практичної роботи, викладені у базі питань системи MoodleZNU	1 бал за кожну правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №7	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
	Тестування з практичної роботи №8	Тестові питання до практичної роботи, викладені у базі питань системи MoodleZNU	1 бал за кожну правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	**Критерії оцінювання	Усього балів
	Звіт про виконання практичної роботи №8	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
Усього за ЗМ 3 контр. заходів	2			12
4	Тестування з практичної роботи №9	Тестові питання до практичної роботи, викладені у базі питань системи MoodleZNU	1 бал за кожну правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №9	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
	Тестування з практичної роботи №10	Тестові питання до практичної роботи, викладені у базі питань системи MoodleZNU	1 бал за кожну правильну відповідь на тестове питання з лабораторної роботи (передбачено 2 питання)	2
	Звіт про виконання практичної роботи №10	Завдання з практичної роботи викладено у методичних рекомендаціях до практичних робіт нульовій секції курсу у системі MoodleZNU	2 бали при виконанні завдання з лабораторної роботи	2
	Поточне тестування №2		1 бал за кожну правильну відповідь на одне теоретичне питання тесту	10
Усього за ЗМ 4 контр. заходів	5			18
Усього за змістові модулі контр. заходів	22			60

8. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
1	2	3	4	5
Залік	Тест в MoodleZNU	Тестові завдання з тем курсу	1 бал за вірну відповідь підсумкового тесту, всього 20 питань	20
	Практичне завдання в MoodleZNU	1) створення програмного коду криптографічного методу шифрування даних; 2) розробка звіту.	5 балів – звіт, 15 балів – виконане практичне завдання	20
Усього за підсумковий семестровий контроль				40

9. Рекомендована література

Основна:

1. Когут Ю. Кібербезпека та ризики цифрової трансформації компанії. Київ : Консалтингова компанія Сідкон, 2021. 372 с.
2. Когут Ю. Кібервійна та безпека об'єктів критичної інфраструктури Київ : Консалтингова компанія Сідкон, 2021. 332 с.
3. Яковенко Є., Журавель І., Горбатий І., Бондарев А. Інформаційна безпека. Львів : Львівська політехніка. 2019. 580 с.

Додаткова:

4. Інформаційна безпека / О. Фармагей та ін. Київ : Ліра-К. 2021. 412 с.
5. Остапов С. Е., Євсєєв С. П., Король О. Г. Технології захисту інформації : навч. посібник. Харків : Вид. ХНЕУ, 2015. 476 с.
6. Codings Z. Computer Programming And Cyber Security for Beginners. Michigan :Independently published. 2019. 330p.

Інформаційні джерела:

1. Стратегії кібербезпеки. Moodle сторінка дисципліни. URL: <https://moodle.znu.edu.ua/course/view.php?id=13768>
2. Указ президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Сайт президента України. URL: <https://cutt.ly/UOo59St>