ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ МІСЬКОГО ГОСПОДАРСТВА
імені О. М. БЕКЕТОВА

ЗАТВЕРДЖУЮ
Перший проректор
_____ (Стадник Г.В.)
«_____» _____

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

вид дисципліни, шифр за ОП	*вибіркова*
семестр	*7-й*
кількість кредитів ЄКТС	*4*
форма підсумкового контролю	*диф. залік*
мова викладання, навчання та оцінювання	*українська*
кафедра	*Комп'ютерних наук та інформаційних технологій*
для здобувачів вищої освіти:	
рівень вищої освіти	*перший (бакалаврський)*
галузь знань	*12 Інформаційні технології*
спеціальність	*126 Інформаційні системи та технології*
освітня програми	*Інформаційні системи та технології*
форма навчання	*денна*

2020 – 2021 НАВЧАЛЬНИЙ РІК

Розробники Робочої програми з дисципліни

Прізвище та ініціали	Посада	Науковий ступінь, вчене звання	Підпис
Карпенко М. Ю.	Доцент mikola.karpenko@kname.edu.ua	к. т. н., доцент	

Робочу програму схвалено на засіданні кафедри комп'ютерних наук та інформаційних технологій

Протокол від "30" червня 2020 року № 19

Завідувач кафедри _____ (Новожилова М. В.)

Схвалено на засіданні НМР Університету

Протокол від "27" 08 2020 року № 12

Секретар НМР _____ (Лущикевич Ж.С.)

1. Мета дисципліни

Метою вивчення дисципліни є формування у студентів знань щодо: основних підходів, методів та практичних прийомів захисту комп'ютерної інформації, а також можливостей сучасного програмного забезпечення для вирішення завдань інформаційної безпеки.

2. Міждисциплінарні зв'язки

Вивчення цієї дисципліни безпосередньо спирається на дисципліни «Організація баз даних та знань», «Теорія ймовірностей, ймовірнісні процеси та математична статистика», «Прикладні задачі дискретного аналізу», «Об'єктно-орієнтоване програмування».

3. Результати навчання

Програмний результат навчання*	Методи навчання	Форми оцінювання	Результати навчання за дисципліною
ПРН 25 Застосовувати інструментальні засоби високо-продуктивних обчислень на основі хмарних сервісів і технологій, паралельних обчислень при розробці й експлуатації розподілених систем.	Словесні, наочні, практичні	Поточний контроль: усне опитування, тестування в Moodle, практична перевірка умінь, усний захист звітів з практичних робіт Підсумковий контроль: диф. залік (письмово за білетами)	Мати навички налагодження технічних засобів захисту інформаційних систем. Вміти застосовувати інструментальні засоби високопродуктивних обчислень на основі хмарних сервісів. Мати навички організації паралельних обчислень при вирішення завдань захисту інформації
ПРН 26. Вміти розробляти front-end та back-end додатки із застосуванням технологій XML, JavaScript і DOM.			Вміти розробляти front-end додатки для вирішення завдань захисту даних Вміти розробляти back-end додатки для вирішення завдань захисту даних
ПРН 27. Здійснювати ідентифікацію і класифікацію типів інформаційних загроз щодо безпеки даних, включаючи мережеву безпеку, та реалізовувати методики захисту критичних даних.			Знати методи ідентифікації і класифікації типів інформаційних загроз Вміти реалізовувати методики захисту критичних даних.

4. Програма навчальної дисципліни

Модуль 1 ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Змістовий модуль 1 Інформаційні загрози

Розглядаються основні поняття та визначення щодо захисту даних, законодавство України в галузі захисту інформації, види інформаційних загроз, види захисту від інформаційних загроз. Також розглядаються програмні системи захисту, апаратний захист даних, організаційні заходи захисту даних.

Змістовий модуль 2. Безпека і захист даних

Розглядаються питання криптографічного захисту інформації, класичні симетричні криптосистеми, сучасні симетричні криптосистеми (алгоритм DES), сучасні симетричні криптосистеми (алгоритм IDEA), стандарти шифрування ГОСТ 28147–89, сімейство алгоритмів RC, принципи асиметричних криптосистем, у т.ч. криптосистема RSA, криптосистема Ель–Гамаля, Рабіна, криптографічні протоколи.

Змістовий модуль 3. Мережева безпека

Розглядаються питання щодо ідентифікації та аутентифікації користувачів, використання електронного цифрового підпису, парольної та біометричної ідентифікації, особливості фізичного, технічного та програмного захисту інформації, противірусного захисту, безпеки сучасних мережевих технологій, методи і засоби захисту від атак через Інтернет.

5. Структура навчальної дисципліни і розподіл часу

Змістові модулі та теми *(номери)*	Кількість годин				
	усього	у тому числі			
		лек.	практ.	лаб.	сам. роб.
МОДУЛЬ (1 семестр)	**120**	**15**	**30**	–	**75**
Змістовий модуль 1	**30**	**4**	**10**	–	**16**
Змістовий модуль 2	**30**	**6**	**10**	–	**14**
Змістовий модуль 3	**45**	**5**	**10**	–	**30**
Підсумковий контроль	**15**	–	–	–	**15**

6. Теми лекцій

Тема	Зміст (план)	Кількість ауд. годин
1	2	3
Змістовий модуль 1		
Інформаційні загрози	Основні поняття та визначення. Законодавство України в галузі захисту інформації Види	**2**

1	2	3
	інформаційних загроз.	
Різновиди захисту від інформаційних загроз	Види захисту від інформаційних загроз. Програмні системи захисту. Апаратний захист даних. Організаційні заходи захисту даних.	**2**
Змістовий модуль 2		
Принципи криптографічного захисту даних	Основні поняття криптографії. Принципи криптографічного захисту інформації. Класичні та сучасні симетричні криптосистеми.	**2**
Криптографічні алгоритми та їх особливості	Алгоритм DES. Сучасні симетричні криптосистеми. Алгоритм IDEA, стандарт шифрування ГОСТ 28147–89. Сімейство алгоритмів RC. Принципи асиметричних криптосистем. Криптосистема RSA. Криптосистема Ель–Гамаля. Криптосистема Рабіна. Криптографічні протоколи. Обмін ключем.	**4**
Змістовий модуль 3		
Основи мережевої безпеки	Проблема ідентифікації та аутентифікації користувача. Електронний цифровий підпис. Парольна та біометрична ідентифікація. Особливості фізичного, технічного та програмного захисту інформації.	**3**
Безпека інтернет та сучасних комунікації	Віруси. Захист інформації від вірусів. Антивірусні програми. Безпека сучасних мережевих технологій, методи і засоби захисту від віддалених атак через Інтернет. Захист інформації в електронних платіжних системах	**2**

7. Теми практичних занять

№	Тема	Зміст (план)	Кількість ауд. годин
1	2	3	4
Змістовий модуль 1			
1	Методи оцінки інформаційних загроз	Теоретична частина Законодавство України в галузі захисту інформації. Види інформаційних загроз. Оцінка загроз. Засоби нейтралізації загроз, їх виявлення та попередження Завдання на практичне заняття	4

		Контрольні запитання	
2	Різновиди захисту від інформаційних загроз	Теоретична частина Програмні системи захисту. Апаратний захист даних. Завдання на практичне заняття Контрольні запитання	6
Змістовий модуль 2			
3	Криптографічний захист даних	Теоретична частина Класичні симетричні криптосистеми. Сучасні симетричні криптосистеми Завдання на практичне заняття Контрольні запитання	4
4	Криптографічні алгоритми та їх особливості	Теоретична частина Сучасні симетричні криптосистеми. Сімейство алгоритмів RC. Криптосистема RSA. Криптосистема Ель–Гамаля. Обмін ключем. Завдання на практичне заняття Контрольні запитання	6
Змістовий модуль 3			
7	Мережева безпека	Теоретична частина Методи ідентифікації та аутентифікації Електронний цифровий підпис Парольна та біометрична ідентифікація Завдання на практичне заняття Контрольні запитання	4
8	Безпека сучасних комунікації	Теоретична частина Захист інформації від вірусів. Антивірусні програми. Методи захисту від атак через Інтернет. Завдання на практичне заняття Контрольні запитання	6

8. Індивідуальне завдання (ІЗ)

Навчальним планом не передбачено

9. Методи контролю та порядок оцінювання результатів навчання

Система поточного контролю базується на застосуванні таких форм контролю:

- усне опитування за матеріалами лекцій;
- усне опитування за результатами виконаного практичного заняття;
- тестування та перевірка завдань у віртуальному освітньому середовищі;
- захист звітів з лабораторних робіт.

Підсумковий контроль у вигляді диф. заліку проводиться письмово.

Структура навчальної дисципліни і розподіл балів

Змістові модулі	Максимальна кількість балів		
	усього	практ.	сам. роб.
МОДУЛЬ (семестр)	**100**		
Змістовий модуль 1	**25**	**15**	**10**
Змістовий модуль 2	**25**	**15**	**10**
Змістовий модуль 3	**20**	**10**	**10**
Підсумковий контроль	**30**	–	–

Види завдань, засоби контролю і максимальна кількість балів

Види завдань та засоби контролю (*тестування, контрольні роботи, індивідуальні завдання, звіти з лабораторних занять тощо)*	Розподіл балів
1	**2**
Змістовий модуль 1	**25**
Практичне завдання «Методи оцінки інформаційних загроз» (звіт з роботи, захист)	15
Практичне завдання Різновиди захисту від інформаційних загроз»	5
Завдання до самостійної роботи «Методи оцінки інформаційних загроз» (звіт з роботи, захист)	5
Змістовий модуль 2	**25**
Практичне завдання «Криптографічний захист даних» (звіт з роботи, захист)	10
Завдання до самостійної роботи «Криптографічний захист даних» (звіт з роботи, захист)	5
Практичне завдання «Криптографічні алгоритми та їх особливості» (звіт з роботи, захист)	5
Завдання до самостійної роботи «Криптографічні алгоритми та їх особливості» (звіт з роботи, захист)	5
Змістовий модуль 3	**20**
Практичне завдання «Мережева безпека» (звіт з роботи, захист)	5
Завдання до самостійної роботи «Мережева безпека» (звіт з роботи, захист)	5
Практичне завдання «Безпека сучасних комунікації» (звіт з роботи, захист)	5
Завдання до самостійної «Безпека сучасних комунікації» (звіт з роботи, захист)	5
Підсумковий контроль – екзамен	**30**
Теоретичне питання 1	10
Теоретичне питання 2	10
Задача	10

Шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, диф. заліку	для заліку
90-100	відмінно	зараховано
82-89	добре	
74-81		
64-73	задовільно	
60-63		
35-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

10. Матеріально-технічне та інформаційне забезпечення

Методичне забезпечення

1. Карпенко М. Ю. Технології захисту інформації : конспект лекцій (модуль 1) для студентів усіх форм навчання освітнього рівня «бакалавр» / М. Ю. Карпенко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2020. – 55 с., доступ https://eprints.kname.edu.ua/54822/

2. Карпенко М. Ю. Конспект лекцій з курсу «Технології захисту інформації» / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ, 2015. – 111 с., доступ https://eprints.kname.edu.ua/44130/

3. Карпенко М. Ю., Методичні вказівки до практичних занять з навчальної дисципліни «Технології захисту інформації» / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова; уклад. : М. Ю. Карпенко, Н. В. Макогон. – Харків : ХНУМГ ім. О. М. Бекетова, 2017. – 21 с., доступ https://eprints.kname.edu.ua/44131/

4. Карпенко М. Ю., Методичні вказівки до самостійної роботи з навчальної дисципліни «Технології захисту інформації» / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова; уклад. : М. Ю. Карпенко, Н. В. Макогон. – Харків : ХНУМГ ім. О. М. Бекетова, 2017. – 21 с., доступ https://eprints.kname.edu.ua/44132/

5. М. Ю. Карпенко, Методичні рекомендації до проведення практичних занять з дисципліни «Технології захисту інформації». – Х.: ХНУМГ, 2015, 33 с., доступ http://eprints.kname.edu.ua/54825/

Рекомендована література та інформаційні ресурси

6. Тарнавський, Ю. А. Технології захисту інформації [Електронний ресурс] : / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. – Назва з екрана.

7. Остапов С. Е. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

8. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. К.: НБУ, 2010.

9. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою. К.: НБУ, 2010.

10. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки. К.: Держспоживстандарт України, 2005.

11. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки ІТ. К.: Держспоживстандарт України, 2005.

12. ДСТУ ISO/IEC TR 13335-3:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом ІТ. К.: Держспоживстандарт України, 2005.

13. ДСТУ ISO/IEC TR 13335-4:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Настанови з керування безпекою інформаційних технологій. К.: Держспоживстандарт України, 2005.

14. ДСТУ ISO/IEC TR 13335-5:2005. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанови з керування мережною безпекою. К.: Держспоживстандарт України, 2005.

Обладнання, устаткування, програмні продукти

Найменування комп'ютерної лабораторії	Модель і марка персональних комп'ютерів, їх кількість	Найменування пакетів прикладних програм (у тому числі ліцензованих)	Доступ до Інтернету, наявність каналів доступу (так/ні)
Лабораторія інформатики та комп'ютерної техніки	Комп'ютер Impression P+ – 18 од. мультиме-дійний проектор	- Антивірусне ПО - Office 365 - система Maple (онлайн-версія) - програми захисту даних (Secret Disk, Prevent Restore, KeePass, SecretFolder, BL тощо) [1]	так

[1] Перелік може змінюватись з метою підтримання актуальності пакету програмних продуктів.