МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Кафедра _____*кібербезпеки*_____
(назва кафедри, яка забезпечує викладання дисципліни)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ДАТАМАЙНІНГ В СИСТЕМАХ БЕЗПЕКИ

(назва навчальної дисципліни)

рівень вищої освіти_____*перший (бакалаврський)*_____
перший (бакалаврський) / другий (магістерський)

галузь знань_____*12 Інформаційні технології*_____
(шифр і назва)

спеціальність _____*125 Кібербезпека*_____
(шифр і назва)

освітня програма _____*Кібербезпека*_____
(назви освітньої програми)

вид дисципліни _____*спеціальна (фахова) підготовка; обов’язкова*_____
(загальна підготовка /спеціальна (фахова) підготовка; обов’язкова/вибіркова)

форма навчання _____*денна*_____
(денна / заочна/дистанційна)

Харків – 2022 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни
_____ ДАТАМАЙНІНГ В СИСТЕМАХ БЕЗПЕКИ_____
(назва дисципліни)

Розробники:

__*проф, д.т.н., проф.*_____ _____ *Олександр МІЛОВ*
(посада, науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

__*доц, к.е.н., доц.*_____ _____ *Станіслав МІЛЕВСЬКИЙ*
(посада, науковий ступінь та вчене звання) (підпис) (ім'я та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри

_____*кібербезпеки*_____
(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від "_22_"__серпня___2022 року № 1

Завідувач кафедри _____ *Сергій ЄВСЕЄВ*
(підпис) (ім'я та прізвище)

ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми _____125 “Кібербезпека”_____

_____

Кафедра _____кібербезпеки_____
(назва кафедри на якій викладається дисципліна)

Гарант ОП _____ 22.08.2022р _____ *Сергій ЄВСЕЄВ*
(Підпис, дата) (ім’я та прізвище)

Завідувач кафедрою _____ 22.08.2022р _____ *Сергій ЄВСЕЄВ*
(Підпис, дата) (ім’я та прізвище)

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

№ зп	Дата засідання кафедри-розробника РПНД	Номер протоколу	Підпис завідувача кафедри (яка викладає)	Підпис завідувача кафедри (на якій викладається)	Підпис гаранта освітньої програми
1					
2					
3					
4					
5					

МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни "Датамайнінг в системах безпеки" – формування у студентів системи теоретичних знань і практичних навичок з основ, принципів та методів інтелектуального аналізу даних. В результаті освоєння дисципліни студенти отримають фундаментальний базис знань з основ, сучасної методології та особливостей застосування інтелектуальної обробки даних; виконають вивчення та опанування стандартів Data Mining; набудуть уміння роботи з системами Data Mining різного призначення і різної проблемної орієнтації; отримають практичні навички до інтелектуального аналізу даних на основі методів обчислювального інтелекту включно з великими та погано структурованими даними, їхньої оперативної обробки та візуалізації результатів аналізу в процесі розв'язування прикладних задач систем та процесів захисту інформації для формування контуру безпеки бізнес-процесів в комп'ютерних системах на основі технологій data-mining та запобіганню зовнішніх кібер-загроз.

Компетентності та результати навчання

Компетентності	Результати навчання
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН–17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН–19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-

Компетентності	Результати навчання
	телекомунікаційних (автоматизованих) системах; РН–25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації

Компетентності	Результати навчання
	в інформаційно-телекомунікаційних системах; РН–49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН–50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН–51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН–52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–12 розробляти моделі загроз та порушника; РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН–16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН–28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН–29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН–30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до

Компетентності	Результати навчання
	інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН–53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
Математичний аналіз	Основи криптографічного захисту
Лінійна алгебра	
Теорія ймовірностей і математична статистика	
Дискретна математика	
Інформатика	
Програмування	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Всього (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари		Контрольні роботи (кількість робіт)	Залік	Екзамен
8	**120/4**	**48**	**72**	**16**	**32**	–	–	**2**	–	+

Співвідношення кількості годин аудиторних занять до загального обсягу складає 53 (%).

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	2	3	4	5
1	Л	2	**<u>Тема 1.</u> Інтелектуальний аналіз даних – DataMining.** Докладно розглядаються поняття DataMining. Описано виникнення, перспективи, проблеми Datamining. Наведен погляд на технологію DataMining як на частину ринку інформаційних технологій. Докладно розглядається поняття даних. Пояснюється значення понять об'єкт та атрибут, вибірка, залежна й незалежна змінна. Докладно обговорюються типи шкал. Приводяться різні типи наборів даних. Коротко розглянуті поняття бази даних і СУБД. Описуються стадії DataMining та дії, які виконуються в рамках цих стадій. Розглянуто відомі класифікації методів DataMining. Наведено порівняльну характеристику деяких методів, заснована на їхніх властивостях. Характеризується основна суть завданьDataMining й їхня класифікація. Докладно розглянуті поняття "інформація", "знання",	**1**
	СР	3	а також зіставлення й порівняння цих понять.	

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	ЛЗ СР	2 3	**Лабораторне заняття №1** Навички роботи з програмою Deductor.	
2	ЛЗ СР	2 3	**Лабораторне заняття №1** Навички роботи з програмою Deductor.	**1**
3	Л СР	2 3	**<u>Тема 2.</u> Візуальний аналіз даних — VisualMining.** Розглядаються питання візуального аналізу даних. Наведені характеристики засобів візуалізації даних, методів візуалізації та методів геометричних перетворень. Порівнюються методи, орієнтовані на пікселі, а також методи аналізу ієрархічних образів та відображення іконок. Розглядаються методи й засоби візуального подання інформації, зокрема, способи подання інформації в одне-, двох-, тривимірному вимірах, а також способи відображення інформації в більш ніж трьох вимірах. Описано принципи якісної візуалізації. Викладено основні тенденції в області візуалізації.	**2–5**
	ЛЗ СР	2 3	**Лабораторне заняття №2** Візуальний аналіз даних — VisualMining	
4	ЛЗ СР	2 3	**Лабораторне заняття №2** Візуальний аналіз даних — VisualMining	**2–5**
5	Л СР	2 3	**<u>Тема 3.</u> Аналіз текстової інформації — TextMining.** Формулюються задачі аналізу текстів (етапи аналізу текстів, попередня обробка тексту, задачі TextMining). Розглядаються етапи аналізу текстів, такі як витяг ключових понять із тексту (загальний опис процесу витягу понять із тексту, стадія локального аналізу, стадія інтеграції й висновку понять), класифікація текстових документів (опис задач класифікації текстів, методи класифікації текстових документів), методи кластерізації текстових документів (наведення текстових документів, ієрархічні методи кластерізації текстів, бінарні методи кластерізації текстів), анотування текстів (виконання анотування текстів, методи витягу фрагментів для анотації). Порівнюються різноманітні засоби аналізу текстової інформації (засоби Oracle - OracleText, засоби від IBM - IntelligentMinerforText, засоби SAS Institute - TextMiner, засоби Мега-компьютерИнтеллидженс - TextAnalyst).	**1-5, 7**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	ЛЗ СР	2 3	**Лабораторне заняття № 3.** Аналіз текстової інформації — TextMining. Програми Text Analyzer, VaalMini.	
6	ЛЗ СР	2 3	**Лабораторне заняття № 3.** Аналіз текстової інформації — TextMining. Програми Text Analyzer, VaalMini.	**1-5, 7**
7	Л СР	2 3	**Тема 4. Витяг знань з Web – WebMining.** Розглянуті проблеми аналізу інформації з Web, етапи WebMining, WebMining та інші інтернет-технології, а також категорії WebMining. Описані методи витягу Web-контента (витяг Web-контента в процесі інформаційного пошуку, витяг Web-контента для формування баз даних), а також методи витягу Web-структур (представлення Web-структур, оцінка важливості Web-структур, пошук Web-документів з урахуванням гіперпосилань, кластеризация Web-структур). Наведені результати досліджень використання Web-ресурсів (дослідницька інформація, етап препроцессінгу, етап витягу шаблонів, етап аналізу шаблонів та їхнє застосування).	**1-5, 8**
	ЛЗ СР	2 3	**Лабораторне заняття № 4** Витяг знань з Web – WebMining. Програма С5.4.	**1-5, 8**
8	ЛЗ СР	2 3	**Лабораторне заняття № 4** Витяг знань з Web – WebMining. Програма С5.4.	**1-5, 8**
9	Л СР	2 3	**Тема 5. Засоби аналізу процесів – ProcessMining.** Розглянуті засоби автоматизації виконання бізнесів-процесів (бізнес-процеси, формалізація бізнес-процесів, Workflow-системи, сервісно-орієнтована архітектура, проектування бізнес-процесів). Виконан аналіз процесів (технологія ProcessMining, аналіз протоколів, стандарт запису протоколів MXML, задачі ProcessMining, проблеми аналізу протоколів). Порівнюються методи ProcessMining (перші імовірнісні методи ProcessMining, метод побудови диз'юнктивної Workflow-схеми, (α-алгоритм, методи на основі генетичних алгоритмів). Описана бібліотека алгоритмів Process Mining-Pro (архітектура Pro, ProImport Framework).	**1-3, 6**
	ЛЗ СР	2 3	**Лабораторні заняття № 5** Засоби аналізу процесів – ProcessMining. Використання ProM.	
10	ЛЗ	2	**Лабораторні заняття № 5** Засоби аналізу процесів –	**1-3, 6**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	СР	3	ProcessMining. Використання ProM.	
11	Л	2	**<u>Тема 6.</u> Пошук асоціативних правил – RulesMining.** Виконана постановка задачі. Розглянуті форми подання результатів (правила класифікації, дерева класифікації, математичні функції), методи побудови правил класифікації (алгоритм побудови 1-правил, метод NaiveBayes), а також методи побудови дерев класифікації (методика "розділяй і пануй", алгоритм покриття), методи побудови математичних функцій (загальний вид, лінійні методи, метод найменших квадратів, нелінійні методи, SupportVectorMachines (SVM), регулярізаційні мережі (RegularizationNetworks), дискретизації й рідкі сітки). Розглянута постановка задачі пошуку асоціативних правил (формальна постановка задачі, секвенціальний аналіз, різновиди задач пошуку асоціативних правил), алгоритми (алгоритм Apriori, різновид алгоритму Apriori).	**1, 6**
	СР	3		
	ЛЗ	2	**Лабораторне заняття № 6** Пошук асоціативних правил – RulesMining. Програма See 5.	
	СР	3		
12	ЛЗ	2	**Лабораторне заняття № 6** Пошук асоціативних правил – RulesMining. Програма See 5.	**1, 6**
	СР	3		
13	Л	2	**<u>Тема 7.</u> Розподілений аналіз даних.** Розглядаються системи мобільних агентів (основні поняття, стандарти багатоагентних систем, системи мобільних агентів, система мобільних агентів JADE). Продемонстровано використання мобільних агентів для аналізу даних (проблеми розподіленого аналізу даних, агенти-аналітики, варіанти аналізу розподілених даних). Побудована система аналізу розподілених даних (загальний підхід до реалізації системи, агент для збору інформації про базу даних, агент для збору статистичної інформації, агент для вирішення одного завдання інтелектуального аналізу даних, агент для вирішення інтегрованого завдання інтелектуального аналізу даних).	**1, 4**
	СР	3		
	ЛЗ	2	**Лабораторне заняття № 7** Розподілений аналіз даних. Агентне моделювання за допомогою JADE та Xelopes.	**1, 4**
	СР	3		
14	ЛЗ	2	**Лабораторне заняття № 7** Розподілений аналіз даних. Агентне моделювання за допомогою JADE та	**1, 4**

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	СР	3	Xelopes.	
15	Л	2	**<u>Тема 7.</u> Розподілений аналіз даних.** Розглядаються системи мобільних агентів (основні поняття, стандарти багатоагентних систем, системи мобільних агентів, система мобільних агентів JADE). Продемонстровано використання мобільних агентів для аналізу даних (проблеми розподіленого аналізу даних, агенти-аналітики, варіанти аналізу розподілених даних). Побудована система аналізу розподілених даних (загальний підхід до реалізації системи, агент для збору інформації про базу даних, агент для збору статистичної інформації, агент для вирішення одного завдання інтелектуального аналізу даних, агент для вирішення інтегрованого завдання інтелектуального аналізу даних).	**1, 4**
	СР	3		
	ЛЗ	2	**Лабораторне заняття № 7** Розподілений аналіз даних. Агентне моделювання за допомогою JADE та Xelopes.	**1, 4**
	СР	3		
16	ЛЗ	2	**Лабораторне заняття № 7** Розподілений аналіз даних. Агентне моделювання за допомогою JADE та Xelopes.	**1, 4**
	СР	3		
Разом (годин)		**120**		

САМОСТІЙНА РОБОТА

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час.

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	24
2	Підготовка до лабораторних занять	48
	Разом	**72**

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Не передбачено навчальним планом

МЕТОДИ НАВЧАННЯ

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

МЕТОДИ КОНТРОЛЮ

Поточний контроль при вивченні дисципліни реалізується у формі опитувань на лекційних заняттях, захисту лабораторних робіт, тестів та проведення контрольних робіт.

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом проведення тестування, презентацій докладів за темами лекційних занять;
- з лабораторних завдань – за допомогою перевірки виконаних завдань.

Семестровий контроль проводиться у формі екзамену відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

Результати поточного контролю враховуються як допоміжна інформація для виставлення оцінки з даної дисципліни.

Студент вважається допущеним до семестрового екзамену з навчальної дисципліни за умови повного відпрацювання усіх практичних робіт, виконання контрольних робіт та тестових опитувань, що передбачено навчальною програмою з дисципліни.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1. – Розподіл балів для оцінювання успішності студента для іспиту

Контрольні роботи	Лабораторні роботи	КП	РГЗ	Індивідуальні завдання	Тощо	Іспит	Сума
20	40	–	–	–	–	40	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під **системою оцінювання** розуміють сукупність методів (письмові, усні і практичні тести, екзамени, проєкти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними **критеріями оцінювання** для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв'язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об'єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100 бальної шкали (табл. 2). Оцінки обов'язково переводять у національну шкалу (з виставленням державної семестрової оцінки "відмінно", "добре", "задовільно" чи "незадовільно") та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЄКТС

Рейтингова Оцінка, бали	**Оцінка ECTS та її визначення**	**Національна оцінка**	**Критерії оцінювання**	
			позитивні	**негативні**
90-100	A	Відмінно	**- Глибоке знання** навчального матеріалу, що містяться в **основних і додаткових літературних джерелах;** **- вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку; **- вміння** проводити **теоретичні розрахунки**; **- відповіді** на запитання **чіткі**, **лаконічні, логічно послідовні;** **- вміння вирішувати**	Відповіді на запитання можуть містити **незначні неточності**

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	**негативні**
			складні практичні задачі.	
82-89	В	Добре	- **Глибокий рівень знань** в обсязі **обов'язкового матеріалу**, - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **складні практичні задачі.**	Відповіді на запитання містять **певні неточності;**
75-81	С	Добре	- **Міцні знання** матеріалу, що вивчається, та його **практичного застосування;** - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **практичні задачі.**	- невміння використовувати теоретичні знання для вирішення **складних практичних задач.**
64-74	Д	Задовільно	- Знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**; - вміння вирішувати прості **практичні задачі**.	Невміння давати **аргументовані відповіді** на запитання; - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;** - невміння вирішувати **складні практичні задачі.**
60-63	Е	Задовільно	- Знання **основних фундаментальних положень** - вміння вирішувати найпростіші **практичні задачі**.	Незнання **окремих (непринципових) питань** з матеріалу модуля; - невміння **послідовно і аргументовано** висловлювати думку; - невміння застосовувати теоретичні

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	**негативні**
				положення при розвязанні **практичних задач**
35-59	FX (потрібне додаткове вивчення)	Незадовільно	**Додаткове вивчення** матеріалу може бути виконане **в терміни, що передбачені навчальним планом**.	Незнання **основних фундаментальних положень** навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; - невміння розв’язувати **прості практичні задачі.**
1-34	F (потрібне повторне вивчення)	Незадовільно	-	- Повна **відсутність знань** значної частини навчального матеріалу модуля; - **істотні помилки** у відповідях на запитання; -незнання основних фундаментальних положень; - невміння орієнтуватися під час розв’язання **простих практичних задач**

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Стандарт вищої освіти галузі знань 12 “Інформаційні технології” для першого (бакалаврського) рівня вищої освіти, який затверджено наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074 та введено в дію з 2018/2019 навчального року.

2. Робоча програма навчальної дисципліни.

3. Силабус навчальної дисципліни

4. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1	Черняк О. І. Інтелектуальний аналіз даних : підручник / О. І. Черняк, П. В. Захарченко. – К. : Знання, 2014. – 599 с.
2	Data Mining : пошук знань в даних / Гладун А. Я., Рогушина Ю. В. – К. : ТОВ «ВД «АДЕФ-Україна», 2016. – 452 с.
3	Аналіз даних та знань : навчальний посібник / Литвин В. В., Пасічник В. В., Нікольський Ю. В. – Львів : Магнолія-2006 , 2021. – 276 с.
4	Інтелектуальний аналіз даних : навчальний посібник / А. О. Олійник, С. О. Субботін, О. О. Олійник. – Запоріжжя : ЗНТУ, 2012. – 278 с.
5	Бахрушин В. Є. Методи аналізу даних : навчальний посібник для студентів / В. Є. Бахрушин. – Запоріжжя : КПУ, 2011. – 268 с.

Допоміжна література

6	Любунь З. М. Основи теорії нейромереж / З. М. Любунь /: Текст лекцій. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2007. –142 с.
7	Liubun Z. Hover Signal-Profile Detection / Liubun, V. Mandziy, H. Klein, O. Karpin, V. Rabyk // Proceedings of the XV International Scientific and Technical Conference “Computer Science and Information Technologies” – 2020. P. 7 – 10. (Scopus)
8	Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. Data Mining and Image Processing Toolkits. – [Електронний ресурс]. – Режим доступу http://datamining.itsc.uah.edu/adam/.
2. www.cyberpol.ru - Комп'ютерна злочинність і способи боротьби.
3. www.iso27000.ru - Інформаційний портал, присвячений питанням управління інформаційною безпекою.
4. www.itsec.ru - Інтернет-журнал «Інформаційна безпека».
5. www.inside-zi.ru - Інформаційно-методичний журнал «Захист інформації. Інсайд».
6. www.drweb.com – Лабораторія DrWeb.
7. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ”: https://iiiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8