ЗАТВЕРДЖЕНО

Вченою радою факультету
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ВК «ШТУЧНИЙ ІНТЕЛЕКТ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
Володимир ВОРОТНІКОВ

Розробник: кандидат технічних наук, доцент, доцент кафедри комп'ютерної інженерії та кібербезпеки Ігор ПУЛЕКО

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів _4_	Галузь знань 12 «Інформаційні технології»	___за вибором__ (нормативна, за вибором)	
Модулів – __	Спеціальність 125 – Кібербезпека та захист інформації	Рік підготовки:	
Змістових модулів – __		_3_	_3_
Загальна кількість годин - _120_		Семестр	
		_5_	_5_
Тижневих годин для денної форми навчання: аудиторних _4_ самостійної роботи – __	Освітній ступінь «магістр»	Лекції	
		32 год.	__ год.
		Практичні	
		__ год.	__ год.
		Лабораторні	
		32 год.	__ год.
		Самостійна робота	
		_72_ год.	__ год.
		Вид контролю: _залік_	

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 40 % аудиторних занять, 60 % самостійної та індивідуальної роботи;

для заочної форми навчання − __% аудиторних занять, __ % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є набуття студентами знань, умінь і здатностей (компетенцій) щодо розробки та застосування методів штучного інтелекту в задачах кібербезпеки для ефективного вирішення завдань професійної діяльності.

Завданнями вивчення навчальної дисципліни є:

– отримання студентами фундаментальних систематизованих знань про підходи, моделі і методи, розроблені в рамках наукового напрямку «штучний інтелект» за весь період його існування;

– освоєння студентами основних методів штучного інтелекту, що застосовуються в системах кібербезпеки;

– ознайомлення студентів з новими методами і підходами до вирішення традиційних завдань, що розробляються в рамках напряму "штучний інтелект" та застосовуються для рішення завдань кібербезпеки;

– формування у студентів аналітичних здібностей, які б дозволяли їм робити обґрунтований вибір вивчених моделей і методів при вирішенні завдань з проблемної області, в якій вони спеціалізуються (кібербезпека).

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності «125 – Кібербезпека та захист інформації»:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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.

Отримані знання з навчальної дисципліни стануть складовими наступних **результатів** навчання за спеціальністю «125 – Кібербезпека та захист інформації»:

РН-2 - організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН-4 - аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

РН-6 - критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

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-19 - застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

3. Програма навчальної дисципліни

Змістовний модуль 1.
Концептуальні положення систем штучного інтелекту в задачах кібербезпеки, нечіткі множини та штучні нейронні мережі

Тема 1. Напрямки застосування штучного інтелекту в кібербезпеці.

Історія розвитку штучного інтелекту. Напрямки досліджень в галузі штучного інтелекту. Напрямки застосування штучного інтелекту в кібербезпеці. Недоліки і проблеми сучасного штучного інтелекту.

Тема 2. Нечіткі множини та логіко-лінгвістичне моделювання в задачах кібербезпеки.

Теорія нечітких множин. Методи побудови функцій приналежності нечітких множин. Нечіткі оператори. Логіка роботи нечіткої системи. Практичне застосування нечіткої логіки в задачах кібербезпеки.

Тема 3. Нейронні мережі та їх застосування в задачах кібербезпеки.

Аналогія з мозком людини. Штучний нейрон. Архітектура з'єднань штучних нейронів. Навчання штучної нейронної мережі. Основні етапи розв'язання задач за допомогою нейромереж. Перцептрон Розенблата. Нейромережа зворотного поширення похибки (Back Propagation). Мережа Delta Bar Delta. Мережа Extended Delta Bar Delta. Мережа спрямованого випадкового пошуку. Нейрона мережа вищого порядку або функціонально - зв'язана нейрона мережа. Мережа Кохонена. Мережа квантування навчального вектора (Learning VectorQuantization). Мережа зустрічного поширення (CounterPropagation). Ймовірнісна нейрона мережа. Мережа Хопфілда. Мережа «Машина Больцмана». Мережа Хемінга. Мережа мережної моделі з двонаправленою асоціативною пам’яттю. Мережа адаптивної резонансної теорії (ART).

Змістовний модуль 2.
Еволюційні методи та методи засновані на знаннях в задачах кібербезпеки

Тема 4. Еволюційне моделювання та генетичні алгоритми в задачах кібербезпеки.

Природний відбір у природі. Основні поняття генетичних алгоритмів. Особливості генетичних алгоритмів. Задачі оптимізації і застосування алгоритмів. Опис типового генетичного алгоритму. Класичний генетичний алгоритм. Представлення даних у генах. Приклади кодування параметрів задачі в генетичному алгоритмі. Основна теорема про генетичні алгоритми.

Будівельні блоки (Building blocks). Еволюційні алгоритми. Еволюційні алгоритми в нейронних мережах.

Тема 5. Представлення знань і вивід на знаннях в задачах кібербезпеки.

Поняття даних та знань. Класифікація знань. Моделі представлення знань. Виведення на знаннях.

Змістовний модуль 3.
Інтелетуальні агенти та машинне навчання в задачах кібербезпеки

Тема 6. Теоретичні основи інтелектуальних програмних агентів.

Основні властивості програмних агентів. Архітектури агентів. Мультиагентні системи.

Тема 7. Машинне навчання в системах кібербезпеки.

Складові машинного навчання та штучний інтелект. Класифікація методів машинного навчання. Класичне навчання. Навчання з підкріпленням. Ансамблі. Штучні нейронні мережі.

Змістовний модуль 4.
Технології комп’ютерного зору в задачах кібербезпеки

Тема 8. Комп’ютерний зір та попередня обробка зображень

Сучасний погляд на комп’ютерний зір. Типові задачі комп'ютерного зору. Системи комп'ютерного зору. Цифрове подання зображень. Характеристики якості зображення. Радіометрична корекція цифрових зображень. Цифрові фільтри.

Тема 9. Розпізнавання образів в задачах кібербезпеки

Постановка завдання. Сегментація зображень - загальний підхід. Сегментація, що заснована на методах класифікації. Контрольована класифікація. Основи загальної теорії розпізнавання образів. Підходи до розпізнавання зображень. Локалізація об'єктів на зображеннях. Ознаки об'єктів на зображенні.

4. Структура (тематичний план) навчальної дисципліни

Кредитні модулі	Змістовні модулі	Кількість годин			
		Всього	Лекції	Лабораторні заняття	Самостійна робота
1	2	3	4	5	6
№ 1	**Змістовний модуль 1. Концептуальні положення систем штучного інтелекту в задачах кібербезпеки, нечіткі множини та штучні нейронні мережі**				
	Тема 1. Напрямки застосування штучного інтелекту в кібербезпеці.	6	1	-	5
	Тема 2. Нечіткі множини та логіко-лінгвістичне моделювання в задачах кібербезпеки	10	1	4	5
	Тема 3. Нейронні мережі та їх застосування в задачах кібербезпеки.	30	4	12	14
	Разом змістовий модуль 1	***46***	***6***	***16***	***24***
№ 2	**Змістовний модуль 2. Еволюційні методи та методи засновані на знаннях в задачах кібербезпеки**				
	Тема 4. Еволюційне моделювання та генетичні алгоритми в інтелектуальних системах.	10	2	4	2
	Тема 5. Представлення знань і вивід на знаннях в задачах кібербезпеки	4	2	-	2
	Разом змістовний модуль 2	***14***	***4***	***4***	***4***
№ 3	**Змістовний модуль 3. Інтелетуальні агенти та машинне навчання в задачах кібербезпеки**				
	Тема 6. Теоретичні основи інтелектуальних програмних агентів.	8	2	-	6
	Тема 7. Машинне навчання в системах кібербезпеки	22	2	4	16
	Разом змістовний модуль 3	***30***	***4***	***4***	***22***
№ 4	**Змістовний модуль 4. Технології комп'ютерного зору в задачах кібербезпеки**				
	Тема 8. Комп'ютерний зір та попередня обробка зображень	15	1	4	10
	Тема 9. Розпізнавання образів в задачах кібербезпеки	15	1	4	10
	Разом змістовний модуль 4	***30***	***2***	***8***	***20***
	РАЗОМ	***120***	***16***	***32***	***72***

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Моделювання елементів теорії нечітких множин та формування нечітких правил в задачах кібербезпеки	4	
2	Моделювання простих нейронних мереж	4	
3	Дослідження складних нейронних мереж	4	
4	Дослідження радіальних та рекурентних нейронних мереж	4	
5	Дослідження методів оптимізації за допомогою генетичних алгоритмів в задачах кібербезпеки	4	
6	Дослідження методів машинного навчання в задачах кібербезпеки	4	
7	Попередня обробка зображень та простий аналіз	4	
8	Дослідження методів виявлення та кластеризації зображень в задачах кібербезпеки	4	
РАЗОМ		32	

6. Завдання для самостійної роботи

Самостійна робота студентів виконується за завданням і при методичному керівництві викладача але без його безпосередньої участі. Самостійна робота підрозділяється на самостійну роботу на аудиторних заняттях і на поза аудиторну самостійну роботу. Самостійна робота студентів включає як повністю самостійне освоєння окремих тем (розділів) дисципліни, так і опрацювання (розділів), освоюваних під час аудиторної роботи. Під час самостійної роботи навчаються читаючи та конспектуючи навчальну, наукову та довідкову літературу, виконують завдання, спрямовані на закріплення знань і відпрацювання умінь і навичок, готуються до поточного і проміжного контролю з дисципліни.

Організація самостійної роботи студентів регламентується нормативними документами, навчально-методичною літературою та електронними освітніми ресурсами

Змістовний модуль 1.
Концептуальні положення систем штучного інтелекту в задачах кібербезпеки, нечіткі множини та штучні нейронні мережі

Самостійна робота за темою 1. Напрямки застосування штучного інтелекту в кібербезпеці.

Історія розвитку штучного інтелекту.

Напрямки застосування штучного інтелекту в кібербезпеці.
Недоліки і проблеми сучасного штучного інтелекту.
Рекомендована література: 2–3, 9
Література: Основна: 1-5. Допоміжна: 3-9

Самостійна робота за темою 2. Нечіткі множини та логіко-лінгвістичне моделювання в задачах кібербезпеки.
Практичне застосування нечіткої логіки в задачах кібербезпеки.
Література: Основна: 1-15. Допоміжна: 1-17

Самостійна робота за темою 3. Нейронні мережі та їх застосування в задачах кібербезпеки.
Основні етапи розв'язання задач за допомогою нейромереж.
Мережа квантування навчального вектора (Learning VectorQuantization).
Мережа «Машина Больцмана».
Мережа Хемінга.
Мережа мережної моделі з двонаправленою асоціативною пам’яттю.
Мережа адаптивної резонансної теорії (ART).
Література: Основна: 1-8 Допоміжна: 3-5

Змістовний модуль 2.
Еволюційні методи та методи засновані на знаннях в задачах кібербезпеки

Самостійна робота за темою 4. Еволюційне моделювання та генетичні алгоритми в задачах кібербезпеки.
Еволюційні алгоритми.
Еволюційні алгоритми в нейронних мережах.
Література: Основна: 1-15 Допоміжна: 1-17

Самостійна робота за темою 5. Представлення знань і вивід на знаннях в задачах кібербезпеки.
Моделі представлення знань.
Виведення на знаннях.

Змістовний модуль 3.
Інтелетуальні агенти та машинне навчання в задачах кібербезпеки

Самостійна робота за темою 6. Теоретичні основи інтелектуальних програмних агентів.
Архітектури агентів.
Мультиагентні системи.

Самостійна робота за темою 7. Машинне навчання в системах кібербезпеки.

Класичне навчання.

Навчання з підкріпленням. Ансамблі.

Штучні нейронні мережі.

Література: Основна: 1-15. Допоміжна: 1-17

Змістовний модуль 4.
Технології комп'ютерного зору в задачах кібербезпеки

Самостійна робота за темою 8. Комп'ютерний зір та попередня обробка зображень

Варіанти радіометричної корекції цифрових зображень.

Цифрові фільтри.

Література: Основна: 1-15. Допоміжна: 1-17

Самостійна робота за темою 9. Розпізнавання образів в задачах кібербезпеки

Сегментація, що заснована на методах класифікації.

Контрольована класифікація.

Підходи до розпізнавання зображень.

Локалізація об'єктів на зображеннях.

Література: Основна: 1-15. Допоміжна: 1-17

7. Індивідуальні завдання

Індивідуальні завдання не передбачено навчальним планом

8. Методи навчання

Застосовуються словесні наочні і практичні методи навчання.

Словесні методи: пояснення, лекція, навчальна дискусія.

Наочні методи: демонстрація та ілюстрація.

Практичні методи навчання: лабораторні заняття.

Лекції з використанням електронних дидактичних демонстраційних матеріалів (презентації), що призначені для супроводу навчального процесу.

Самостійна робота з використанням можливості локальної мережі та Інтернет з наданням відповідних посилань на джерело інформації.

Самостійна підготовка з використанням друкованих та електронних підручників, навчальних посібників (з вільним доступом усім учасникам навчального процесу), а також інших локальних і мережевих інформаційних ресурсів.

9. Методи контролю

Кожна з форм контролю має особливості й залежить від мети, змісту та характеру навчання. У процесі навчання дисципліни використовуються наступні форми контролю:

- Поточний контроль: усне опитування (індивідуальне, фронтальне, групове), комп'ютерне тестування, виконання практичних завдань на комп'ютері згідно програми;
- Підсумковий контроль: екзамен.

10. Розподіл балів

Заняття	Л-1	Л-2	ЛР-1	Л-3	Л-4	ЛР-2	Л-5	Л-6	ЛР-3
Бали	1	1	10	1,5	1	10	1	1,5	10
Заняття	Л-7	Л-8	ЛР-4	Л-9	Л-10	ЛР-5	Л-11	Л-12	ЛР-6
Бали	1	1,5	10	1	1,5	10	1	1,5	10
Заняття	Л-13	Л-14	ЛР-7	Л-15	Л-16	ЛР-8			
Бали	1	1,5	10	1,5	1,5	10		Сума	100

Бали за лекцію нараховуються після відповіді на тести по лекції.

Додаткові бали можна отримати за:

Тези доповідей (опубліковані) – 5 б.

Наукова стаття по дисципліні – 10 б.

Участь в олімпіаді чи конкурсі студентських робіт – 10 б. (призове місце - 20 б.)

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Melanie Mitchell. Artificial Intelligence. A Guide for Thinking Humans, London. Penguin 2020. — 448 p. — ISBN 978-0-241-40483-6 . (укр.)
2. Deisenroth, M. P., Faisal, A. A., & Ong, C. S. (2020). Mathematics for machine learning. Cambridge University Press. Available: https://mml-book.github.io/book/mml-book.pdf
3. Булгакова О. С., Зосімов В. В., Поздєєв В. О. Методи та системи штучного інтелекту. Теорія та практика. Навчальний посібник. – Олді плюс, 2020, - 356 с.
4. Методи та системи штучного інтелекту: навч. посіб. / укл. Д.В. Лубко, С.В. Шаров. – Мелітополь: ФОП Однорог Т.В., 2019. – 264 с.
5. Alberto Artasanchez, Prateek Joshi. Artifcial Intelligence with Python. Second Edition. BIRMINGHAM – MUMBAI:Packt Publishing 2020. – 592 p. ISBN 978-1-83921-953-5.
6. Системи штучного інтелекту. Лабораторний практикум. Навч. посібник для здобувачів ступеня магістр за спеціальністю 123 «Комп'ютерні системи та мережі» / Стіренко С., Кочура Ю . К.: КПІ ім. Ігоря Сікорського, 2022. – 24 с. [Електронний ресурс], http:// comsys.kpi.ua
7. Russell, S., & Norvig, P. (3d or 4th Edition). Artificial intelligence: a modern approach. 5 Goodfellow I, Bengio Y, Courville A., Deep Learning // MIT, 2017 – 800 с.
8. Dumoulin, V., & Visin, F. (2016). A guide to convolution arithmetic for deep learning. arXiv preprint arXiv:1603.07285. 7 Zeiler, M. D., & Fergus, R. (2014, September). Visualizing and understanding convolutional networks. In European conference on computer vision (pp. 818-833). Springer, Cham.
9. Christopher M. Bishop. Pattern Recognition and Machine Learning. 2006 Springer Science+Business Media, 2006 – 756 p.
10. Richard S. Sutton and Andrew G. Barto. Reinforcement Learning: An Introduction Second edition, in progress. The MIT Press Cambridge, Massachusetts London, England. 2015. – 338 p.
11. Шолле Франсуа. Глибоке навчання на Python. — К. Наукова думка, 2018. — 400 с.: іл. —. ISBN 978-5-4461-0770-4
12. Мюллер, Джон Пол, Массарон, Лука. Штучний інтелект для чайників.: Пер. с англ. — К. Наукова думка, 2019. — 384 с.:ISBN 978-5-907114-57-9
13. Гифт Ной. Прагматичний ШІ. Машинне навчання і хмарні технології. – К. 2019. - 304 с.: ISBN 978-5-4461-1061-2
14. Засоби штучного інтелекту: навч. посіб. / Р. О. Ткаченко, Н. О. Кустра, О. М. Павлюк, У. В. Поліщук ; М-во освіти і науки України, Нац. ун-т

«Львів. політехніка». — Львів: Вид-во Львів. політехніки, 2014. — 204 с. : іл. — Бібліогр.: с. 200 (11 назв). — ISBN 978-617-607-692-6

15. Системи штучного інтелекту: навч. посіб. / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина ; за наук. ред. В. В. Пасічника ; М-во освіти і науки, молоді та спорту України. — 2-ге вид., виправл. та доповн. — Львів: Магнолія-2006, 2013. — 279 с. : іл. — (Серія «Ком'пютинг»). — Бібліогр.: с. 275—278 (58 назв). — ISBN 978-617-57-40-11-4
16. Кононюк А. Е. Основи фундаментальної теорії штучного інтелекту. — В 20-и кн. Кн.1. — К.:Освіта України. 2017.—730 с.
17. Лорьер Ж.-Л. Системи штучного інтелекту. — М.: Мир, 1991. — 568 с. ISBN 5-03-001408-X.
18. Stuart J. Russell, Peter Norvig. Artificial Intelligence: A Modern Approach. — 3. — Pearson, 2015. — ISBN 978-9332543515. (англ.)
19. Nils J. Nilsson. The Quest for Artificial Intelligence. — 1. — Cambridge University Press, 2009. — 578 с. — ISBN 978-0521116398. (англ.)

Допоміжна література

1. Корченко А.Г. Несанкционированный доступ к компьютерным системам и методы защиты. Учебное пособие. К.: КМУГА.- 1998.-116 с.

2. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2019. – №6 (червень) . – 71с.

3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.

4. Шевченко А.С. Самойлов І.В. Пономарьов О.А. Науменко О.Г. Аналіз застосування штучних нейронних мереж у задачах виявлення кіберзагроз. Збірник наукових праць ВІТІ 1/07 № 3. С. 30-035. www-xktk-efw-wc.hkneu.zbk.1/07.06_3_1/07-rfh.

5. Bhutada S., Bhutada P. Applications of Artificial Intelligence in Cyber Security. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE).2018. Vol 5. Issue 4. P. 214 – 219.

6. Roman V. Yampolskiy, M. S. Spellchecker. Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures, NY, Cornell University, 2017.– 123-128 p.

7. Leslie F. Sikos. AI in Cybersecurity. New York : Springer, 2018. 205 p.

8. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

9. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

10. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

11. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.

12. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.

13. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

14. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

15. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

16. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

17. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

12. Інформаційні ресурси в Інтернеті

1.Курс Р.В. Шамина «Машинне навчання та штучний інтелект в математиці і додатках» http://www.mathnet.ru/conf1243

2. Штучний інтелект. https://uk.wikipedia.org/wiki/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82

3. Розпорядження Кабінету міністрів України від 2 грудня 2020 р. № 1556-р. Київ «Про схвалення Концепції розвитку штучного інтелекту в Україні» https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

4. Портал штучного інтелекту - http://www.aiportal.ru

5. Системи штучного інтелекту - http://www.itfru.ru/

6. Асоціація штучного інтелекту - http://www.raai.org

7. Н.С. Константинова, О.А. Митрофанова. Онтології як системи зберігання знань. [Електронний ресурс] – Режим доступу: http://window.edu.ru/resource/795/58795/files/68352e2-st08.pdf

8. Dobrynin, V., Patterson, D. W., and Rooney, N. Contextual Document Clustering. [Електронний ресурс] – Режим доступу: http://www.sophiasearch.com/uploads/documents/contextual_document_clustering.pdf

9. Syafrullah, M., and Salim, N. Improving Term Extraction Using Particle Swarm Optimization Techniques. // Journal of Computer Science. 2010. Vol. 6. № 3. Pp. 323–329.