МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Волинський національний університет імені Лесі Українки

Факультет інформаційних технологій і математики

СИЛАБУС

«Штучний інтелект в кібербезпеці»

нормативної навчальної дисципліни

підготовки бакалавра з кібербезпеки

галузь знань 12 Інформаційні технології

спеціальність 125 «Кібербезпека»

освітньо-професійна програма «Інформаційна безпека»

Луцьк – 2024

Силабус навчальної дисципліни «Штучний інтелект в кібербезпеці» підготовки бакалавра, галузі знань 12 Інформаційні технології спеціальності «Кібербезпека» за освітньо-професійною програмою «Інформаційна безпека».

Розробник: Собчук В. В., професор кафедри комп’ютерних наук та кібербезпеки, доктор технічних наук, професор.

Погоджено
Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки

протокол № 4 від 21.11.2024 р.

Завідувач кафедри:  Гришанович Т. О.

1.Опис навчальної дисципліни

Таблиця 1

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність,

освітня програма, освітній ступінь</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Денна форма навчання</td><td></td><td>Нормативна</td></tr>
<tr><td rowspan="6">Кількість годин/кредитів 120/4</td><td rowspan="6">Галузь знань
12 «Інформаційні технології»
Спеціальність
125 Кібербезпека та захист інформації
освітньо-професійна програма
Кібербезпека та захист інформації</td><td>Рік навчання 4</td></tr>
<tr><td>Семестр_7-ий</td></tr>
<tr><td>Години:120</td></tr>
<tr><td>Кредити: 4</td></tr>
<tr><td>Лекцій: 34 год.</td></tr>
<tr><td>Лабораторні роботи : 46 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td></td><td>Самостійна робота 30 год.</td></tr>
<tr><td></td><td>Консультації: 10 год.</td></tr>
<tr><td></td><td>Форма контролю: екзамен</td></tr>
<tr><td>Мова навчання</td><td></td><td>українська</td></tr>
</table>

ІІ. Інформація про викладача

ПІП: Собчук Валентин Володимирович
Науковий ступінь: доктор технічних наук
Вчене звання: професор
Посада: професор кафедри комп’ютерних наук та кібербезпеки
Контактна інформація (номер мобільного зв’язку, електронна адреса): +380503398113, vvsobchuk@ukr.net
Дні занять (посилання на електронний розклад):
https://us04web.zoom.us/j/7639442912?pwd=GQ7a6Mq99IamC2mMAMzzh8EF016gEj.1

ІІІ. Опис дисципліни

1. Анотація курсу

Навчальна дисципліна «Штучний інтелект в кібербезпеці» головним завданням має підготовку висококваліфікованих фахівців у галузі кібербезпеки. Здобувачі дізнаються про сучасні методи машинного навчання та глибокого навчання, а також про їх застосування для виявлення кіберзагроз, аналізу великих обсягів даних та захисту інформаційних систем. Практичні заняття допоможуть освоїти інструменти та бібліотеки для розробки власних моделей ШІ. Здобувачі за результатам вивчення дисципліни будуть готові до виконання проєктів, в рамках яких зможуть застосувати отримані знання для вирішення реальних задач кібербезпеки.

В сучасному світі кіберзагрози є складними та постійно розвиваються за своєю природою. Надійна кібербезпека стала як ніколи важливою в сучасну цифрову епоху, оскільки підприємства критичної інфраструктури, цивільного та промислового секторів намагаються бути на крок попереду в умовах постійних загроз несанкціонованого доступу до інформаційної інфраструктури.

Штучний інтелект (ШІ) відіграє важливу роль у кібербезпеці. На початках, ШІ використовував прості правила для відстеження мережевого трафіка та дій користувачів. Правила, створені людьми, допомагали виявляти підозрілу активність, але мали обмеження. Згодом, наприкінці минулого століття, ШІ став більш розвиненим завдяки прогресу в машинному навчанні. Нині він може самостійно встановлювати правила, зменшуючи потребу в ручному введенні даних. Використання алгоритмів глибокого навчання дозволило ШІ ефективніше виявляти потенційні загрози та сприяти тому, що кібербезпека стає більш надійною. Сучасний генеративний штучний інтелект або інтелектуальний ШІ – третя хвиля, що забезпечує безліч переваг у кібербезпеці, від автоматизації повторюваних завдань і мінімізації людських помилок до використання прогнозової аналітики для підтримки виявлення загроз. Водночас ШІ виявився безцінним в автоматизації реагування на інциденти безпеки. Технології, як-от машинне навчання та глибоке навчання, які є складовими ШІ, змінили спосіб роботи кібербезпеки. Сучасний ШІ може аналізувати великі обсяги даних, вчитися на них, виявляти закономірності та приймати рішення для виявлення та усунення потенційних загроз.

2. Пререквізити/постреквізити

Пререквізити: Базові знання інформаційних технологій та захисту інформації, знання програмування, теорії ймовірностей і математичної статистики, фізики, комп'ютерних мереж, архітектури обчислювальних систем, програмних та програмно-апаратних комплексів ЗЗІ.

Постреквізити: Знання та вміння будуть актуальними для роботи з організації сучасних захищених систем в різних сферах, де використовуються технології штучного інтелекту, включаючи підприємства критичної інфраструктури, фінанси, промислове виробництво тощо.

3. Мета дисципліни – сформувати у здобувачів комплексний набір теоретичних знань та практичних навичок професійних компетенцій з кібезбезпеки для забезпечення комплексного захисту інформації на об'єктах інформаційної діяльності де все більшу роль відіграють технології штучного інтелекту.

4. Результати навчання (компетентності).

Знання теоретичних основ та вміння свідомого поводження з інформацією в умовах використання сучасних інформаційно-комунікаційних засобів та враховування отриманих знань у практичної діяльності за обраної спеціальності.

Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

Загальні компетенції:

- Здатність застосовувати знання у практичних ситуаціях (ЗК 1).
- Знання та розуміння предметної області та розуміння професійної діяльності (ЗК 2).
- Здатність вчитися і оволодівати сучасними знаннями (ЗК 5).
- Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя (ЗК 8).

Спеціальні компетенції:

- Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації (СК 2).
- Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації (СК 3).
- Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження (СК 5).
- Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності (СК 9).

Володіти навичками програмування, навичками збору, очищення, перетворення та візуалізації даних для подальшого аналізу за допомогою алгоритмів машинного навчання, розробляти, тренувати та оцінювати моделі машинного навчання для вирішення конкретних задач кібербезпеки.

4. Завдання (навчальні цілі) навчальної дисципліни – забезпечення стабільних базових теоретичних знань, теорії і практики роботи з ШІ**;** розуміння математичних основ, що лежать в основі алгоритмів машинного навчання (лінійна алгебра, теорія ймовірностей, математична статистика). Глибоке розуміння концепцій машинного навчання, глибокого навчання, нейронних мереж та інших сучасних підходів в галузі ШІ. Знання основних алгоритмів класифікації, регресії, кластеризації та інших методів, що використовуються в задачах кібербезпеки. Навички збору, очищення, перетворення та візуалізації даних для подальшого аналізу за допомогою алгоритмів машинного навчання.

Сприяти ефективному формуванню у здобувачів наступних професійних компетентностей:

- Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків (РН 1).
- Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність (РН 4).
- Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення (РН 5).

- Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат (РН 6).
- Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності (РН 7).
- Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення (РН 8).
- Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації (РН 9).
- Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи (РН 15).
- Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів (РН 19).

5. Структура навчальної дисципліни

№ п/п	Назва теми*	Кількість годин			
		Лекції	П.р.	Л.р.	С. р.
Змістовий модуль 1 "Основи штучного інтелекту"					
1	Тема 1. Вступ до штучного інтелекту. *Визначення, історія та еволюція, галузі застосування, сильна і слабка форми.*	2		2	
2	Тема 2. Машинне навчання. *Основні поняття та типи машинного навчання; навчальні алгоритми: наївний байєсівський класифікатор, лінійна регресія, дерева рішень, оцінка моделей машинного навчання.*	4		6	4
3	Тема 3. Глибоке навчання. *Нейронні мережі: архітектура, навчання, застосування. Конволюційні нейронні мережі (CNN) та їх застосування в обробці зображень. Рекурентні нейронні мережі (RNN) та їх застосування в обробці послідовностей.*	4		6	4
	Всього за МК-1	**10**		**14**	**8**
Змістовий модуль 2 "Штучний інтелект та кібербезпека"					
8	Тема 4. Застосування ШІ в атаках. *ШІ для створення фішингових листів, генерації зловмисного коду, бходу систем виявлення вторгнень.*	2		4	2
9	Тема 5. Захист від атак, що використовують ШІ. *Виявлення аномалій в мережевому трафіку за допомогою ШІ. Класифікація шкідливого програмного забезпечення. Аналіз поведінки користувачів для виявлення внутрішніх загроз.*	3		4	2
10	Тема 6. ШІ для захисту даних. *Виявлення витоків даних. Захист конфіденційності даних. Дезінформація та фейкові новини.*	3		4	2
11	Тема 7. Етичні аспекти ШІ в кібербезпеці. *Упередженість в алгоритмах машинного навчання. Прозорість і пояснюваність моделей ШІ. Відповідальність за дії ШІ.*	2		2	2

	Всього за МК-2	**10**		**14**	**8**
Змістовий модуль 3 "Практичні аспекти штучного інтелекту в кібербезпеці"					
8	Тема 8. Інструменти та бібліотеки для ШІ. *Python, TensorFlow, Keras, Scikit-learn, Jupyter Notebook для експериментів.*	4		4	4
	Тема 9. Розробка моделей ШІ для кібербезпеки. *Збір та підготовка даних. Вибір моделі та її навчання. Оцінка ефективності моделі.*	2		4	3
	Тема 10. Розгортання моделей ШІ в реальних системах. *Інтеграція моделей ШІ в системи кібербезпеки. Оптимізація моделей для роботи в реальному часі.*	3		4	3
	Тема 11. Тренди та перспективи розвитку ШІ в кібербезпеці. *ШІ для захисту IoT-, IIoT-пристроїв. Квантові обчислення та їх вплив на кібербезпеку. Федеративне навчання для захисту конфіденційності даних.*	3		4	2
	Тема 12. Проектування систем кібербезпеки на основі ШІ. *Життєвий цикл розробки систем кібербезпеки з використанням ШІ. Архітектура систем, що поєднують людей і ШІ.*	2		2	2
	Всього за МК-2	**14**		**18**	**14**
	Консультація		**10**		
	Всього за навчальною дисципліною	**36**	**10**	**46**	**30**

Загальний обсяг **120** *год.,* в тому числі:
Лекцій **– 36** *год.*
Лабораторні – **46** *год*
Консультації до іспиту **– '10** *год*
Самостійна робота **– 30** *год.*

6. Завдання для самостійної роботи та написання рефератів

№	Тема
1.	**Штучний інтелект у створенні та виявленні deepfakes.** Технології створення глибоких підробок, їх використання в кібератаках та методи їх виявлення.
2.	**Застосування генеративних моделей (GANs) для створення зловмисних програм.** Можливості використання GANs для генерації нових типів вірусів, троянів та іншого шкідливого програмного забезпечення.
3.	**Рівень загрози: Як ШІ змінює ландшафт кіберзагроз?** Глобальний аналіз того, як штучний інтелект змінює тактику кіберзлочинців та підвищує рівень складності кібератак.
4.	**Захист конфіденційності в системах машинного навчання.** Методи захисту даних, що використовуються в процесі навчання моделей машинного навчання, особливо з урахуванням проблем приватного машинного навчання.
5.	**Штучний інтелект та GDPR:** Вимоги GDPR щодо використання алгоритмів штучного інтелекту та виклики, з якими стикаються компанії при їх дотриманні.
6.	**Атаки на системи біометричної аутентифікації за допомогою ШІ.** Методи обману систем розпізнавання облич, відбитків пальців та інших біометричних даних за допомогою штучного інтелекту.

7.	**Безпека моделей машинного навчання: атаки та захист.** Характеристика різних типів атак на моделі машинного навчання (наприклад, отруєння даних, обхідні атаки) та методи їх захисту.
8.	**Explainable AI (XAI).** Методи, які дозволяють зрозуміти, як приймаються рішення моделями машинного навчання, та їх важливість для забезпечення прозорості та довіри до систем ШІ.
9.	**Розробка безпечних систем ШІ:** Принципи безпечного проектування систем штучного інтелекту, включаючи захист від атак, забезпечення конфіденційності та стійкість до збоїв.
10.	**Штучний інтелект та квантові обчислення: нові виклики для кібербезпеки.** Оцінка потенційного впливу квантових комп'ютерів на системи криптографії та безпеку систем ШІ, а також можливі шляхи захисту.
11.	**Етичні дилеми у розробці автономних систем зброї.** Аналіз етичних проблем, пов'язаних із створенням та використанням автономних систем зброї, заснованих на штучному інтелекті.
12.	**Упередженість у алгоритмах машинного навчання та її вплив на кібербезпеку.** Причини виникнення упередженості у алгоритмах машинного навчання, її наслідків для систем безпеки та методів її мінімізації.
13.	**Соціальна інженерія з використанням ШІ: нові загрози та методи захисту**. Аналіз нових методів соціальної інженерії, заснованих на застосуванні штучного інтелекту, та розробка заходів протидії.
14.	**Використання ШІ для виявлення ботів та тролів у соціальних мережах.** Методи,які використовуються для ідентифікації ботів та тролів, та їх роль у дезінформаційних кампаніях.
15.	**Застосування ШІ в системах промислової автоматизації: загрози та заходи захисту.** Вразливості систем промислової автоматизації, оснащених елементами штучного інтелекту, та розробка методів забезпечення їхньої безпеки.
16.	**Використання блокчейна для безпеки систем штучного інтелекту.** Оцінка потенціалу технології блокчейн для підвищення безпеки систем штучного інтелекту, таких як децентралізоване навчання моделей та захист інтелектуальної власності.
17.	**Федеративне навчання моделей машинного навчання: переваги та виклики.** Принципи федеративного навчання та його застосування у системах кібербезпеки, а також аналіз пов'язаних з ним проблем.
18.	**Квантові обчислення та їх вплив на криптографію та системи безпеки на основі ШІ.** Загрози, пов'язані з розвитком квантових комп'ютерів, та розробка постквантових криптографічних алгоритмів.
19.	**Neuro-symbolic AI: об'єднання символічних та нейронних методів.** Підходи, які поєднують символічні та нейронні методи у штучному інтелекті, та їх потенціал для вирішення складних завдань у галузі кібербезпеки.
20.	**Регулювання штучного інтелекту: міжнародний досвід та перспективи.** Аналіз існуючих та розроблюваних нормативно-правових актів, що регулюють застосування штучного інтелекту, та їх вплив на розвиток технологій кібербезпеки.

7. Питання до екзамену

1. Визначення штучного інтелекту. Основні етапи розвитку ШІ.
2. Різниця між сильною та слабкою формою ШІ. Приклади.
3. Основні типи машинного навчання. Приклади алгоритмів для кожного типу.
4. Процес навчання моделі машинного навчання.

5. Метрики, які використовуються для оцінки якості моделі ШІ.
6. Що таке нейронна мережа? Основні типи нейронних мереж.
7. Як працюють конволюційні нейронні мережі.
8. Використання конвулюційних нейронних мереж в кібербезпеці.
9. Застосовуються рекурентних нейронних мереж. Приклади.
10. Безпека моделей машинного навчання: атаки та захист.
11. Використання ШІ для створення фішингових листів.
12. Можливості, які відкриває ШІ для генерації зловмисного коду.
13. Методи захисту від атак, що використовують ШІ.
14. Використання ШІ для виявлення аномалії в мережевому трафіку.
15. Процес класифікації шкідливого програмного забезпечення за допомогою ШІ.
16. Переваги та недоліки використання ШІ для аналізу поведінки користувачів.
17. Виявляти витоки даних за допомогою ШІ.
18. Методи захисту конфіденційності даних за допомогою ШІ.
19. Загрози пов'язані з поширенням дезінформації та фейкових новин.
20. Що таке упередженість в алгоритмах машинного навчання? Методи боротьби.
21. Важливість прозорості і пояснюваності моделей ШІ.
22. Відповідальність за дії ШІ.
23. Основні інструменти та бібліотеки використовуються для розробки моделей ШІ.
24. Опишіть процес розробки моделі машинного навчання за допомогою Jupyter Notebook.
25. Етапи процесу розробки моделі ШІ для кібербезпеки.
26. Оцінки ефективності розробленої моделі ШІ.
27. Виклики, які виникають при розгортанні моделей ШІ в реальних системах.
28. Оптимізація моделі ШІ для роботи в реальному часі.
29. Нові напрямки розвитку ШІ в кібербезпеці.
30. Квантові обчислення та їх можливий вплив на кібербезпеку.
31. Федеративне навчання і його можливе використання
32. Життєвий цикл розробки систем кібербезпеки на основі ШІ.
33. Фактори, які необхідно враховувати при проектуванні систем, що поєднують людей і ШІ.
34. Тип машинного навчання використовується для прогнозування DDoS-атак.
35. Характеристики нейронних мереж, які найбільш підходять для обробки зображень.
36. Алгоритм роботи наївного байєсівського класифікатора.
37. Переваги та недоліки використання нейронних мереж для виявлення аномалій.
38. Розрахунки точності, повноти та F1-міри для заданої матриці плутанини.

8. Політика оцінювання

Здобувач має виконати у повному обсязі усі види діяльності із навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки», бути присутніми на аудиторних заняттях. Якщо здобувач відсутній на занятті, він може надіслати виконане семінарське заняття у письмовому вигляді. Претендувати на максимальну кількість балів можна, якщо семінарське виконане у вигляді презентацій, використані нові актуальні наукові джерела, робота є авторською, без порушень авторських прав.

Освітній процес відповідає «Положенню про поточне та підсумкове оцінювання знань студентів Волинського національного університету імені Лесі Українки» від 11 вересня 2020 р. (https://bit.ly/39In2ac). Іспит виставляється автоматично за умови, якщо студент виконав усі види навчальної роботи та отримав не менше ніж 75 балів зі 100 можливих.

Вирішення спірних питань у галузі академічної доброчесності здійснюється на підставі Положення про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників Східноєвропейського національного університету імені Лесі Українки (від 10 лютого 2017 р.) (https://bit.ly/3lNJD7N).

Конфліктні ситуації вирішуються згідно Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки (https://bit.ly/33MTIM).

Згідно Положення про академічну мобільність студентів (https://bit.ly/3oMzMkk), власне право неформальну освіту, здобувач може отримати найвищу кількість балів за виконання ІНДЗ, якщо взяв участь у тренінгу, конференції, науковому семінарі, проблемній групі та ін.

Здобувач вчасно здає усі види робіт. Викладач інформує про терміни здачі контрольних робіт та виконання ІНДЗ.

Здобувач має можливість скласти іспит згідно розкладу заліково-екзаменаційної сесії, має право скласти іспит повторно, а також скласти іспит комісії, у яку входять представники кафедри та деканату. Якщо за ці три можливості іспит не складено, здобувач виключається зі складу студентів ВНУ імені Лесі Українки. В університетських положеннях є право на поновлення і проходження повторного проходження навчальної дисципліни.

8.1. Розподіл балів, які отримують студенти

Методи навчання: усне опитування, інтерактивні методи навчання, лабораторні заняття, самостійна робота і екзамен.

Засоби діагностики успішності: лабораторні заняття (30 балів), бонусні бали за активність (10), самостійна робота (30 балів), екзамен (40 балів).

Поточний контроль (мах – 30 балів) Лабораторні заняття	Самостійна робота (мах – 30 балів)	Екзамен (мах – 40 балів)	Загальна кількість балів
30 годин лабораторних занять (мах 30 балів) + 10 балів за активність	67 годин (мах 30 балів)	(мах 40 балів)	100

9. Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	**Оцінка ECTS**	**Оцінка за національною шкалою**	
		для екзамену, курсової роботи (проекту), практики	**для заліку**
90-100	**A**	**Відмінно**	**Зараховано**
82-89	**B**	**Добре**	
75-81	**C**		
67-74	**D**	**Задовільно**	
60-66	**E**		
1-59	**Fx**	**Незадовільно**	**Незараховано**

РЕКОМЕНДОВАНІ ДЖЕРЕЛА

Основна література:

1. Закон України. Про основні засади забезпечення кібербезпеки України. Введено в дію постановою Верховної Ради України від 05.10. 2017 р. № 45, ст.403.
2. Закон України «Про захист інформації в інформаційнотелекомунікаційних системах», від 05.07.1994 № 80/94-ВР (Зі змінами, внесеними згідно із Законом № 1703-IV від 11.05.2004, в редакції Закону № 2594-IV від 31.05.2005, ВВР, 2005, № 26, ст. 347).
3. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
4. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
5. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок

проведення робіт.
6. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
7. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
8. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
9. 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.
10. 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.
11. НД ТЗІ 2.5-004-99: Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
12. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
13. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.
14. ISO/IEC 11770-3 Information Technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.
15. Гупта Б., Сінг Б., Джейн В. Виявлення вторгнення за допомогою штучного інтелекту. URL: https://arxiv.org/ftp/arxiv/papers/1701/1701.02145.pdf. Нью Делі, 2014. 43 с.
16. Стьопочкіна І.В., Новіков О.М.. Методи штучного інтелекту в кібербезпеці [Електронний ресурс]: навч. посіб. для здобувачів спец. 125 «Кібербезпека» – Електронні текстові дані– Київ : КПІ ім. Ігоря Сікорського, 2022 – 82 с.
17. Харченко В. О. Основи машинного навчання: навч. посіб.– Суми : Сумський державний університет, 2023. – 264 с. https://files.znu.edu.ua/files/Bibliobooks/Inshi79/0059501.pdf
18. Liam Harrison Artificial Intelligence 2023: Learn Everything About the Revolution of Artificial Intelligence. Kindle Edition, 2023. – 105 p.
19. Khaikin S. (2019) Neural Networks: Complete Course. Dialectics, 1104 p.
20. Kumar G., Kumar K., Sachdeva M. The use of artificial intelligence-based techniques for intrusion detection. Punjab: Springer Science + Business, 2010. 387 p.
21. Rothman D. Artificial Intelligence By Example: Acquire advanced AI, machine learning, and deep learning design skills, 2nd Edition, Packt Publishing, 2020, 578 p.
22. Sikos L. F. AI in Cybersecurity. New York: Springer, 2018. 205 p.
23. Shahriar Usman Khan, Fariha Eusufzai, Md. Azharuddin Redwan, Mohiuddin Ahmed, Saifur Rahman Sabuj. Artificial Intelligence for Cyber Security: Performance Analysis of Network Intrusion Detection. Cham: Springer, 2022. 140 p.
24. Taulli T. Artificial Intelligence Basics: A Non-Technical Introduction. Publisher : Apress; 1st ed. 2019, 268 p.

Додаткова література:

1. Зайченко Ю.П. Основи проектування інтелектуальних систем. Навч. посібник. - К. : Видавничий дім «Слово». – 2004. - 352с.
2. Кононова К. Ю. Машинне навчання: методи та моделі: підручник для бакалаврів, магістрів та докторів філософії спеціальності 051 «Економіка». Харків: ХНУ імені В. Н. Каразіна, 2020. 301 с.
3. Методи штучного інтелекту в кібербезпеці: Практикум [Електронний ресурс] : навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна – Електронні текстові дані (1 файл: 388,3 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022.

4. Лунгол, О. (2024). ОГЛЯД МЕТОДІВ ТА СТРАТЕГІЙ КІБЕРБЕЗПЕКИ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ . Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 379–389. https://doi.org/10.28925/2663-4023.2024.25.379389
5. Савченко А.С., Синельніков О. О. Методи та системи штучного інтелекту: Навчальний посібник для студентів напряму підготовки 6.050101 «Комп'ютерні науки» К. : НАУ, 2017. 190 с.
6. Big data, artificial intelligence, machine learning and data protection. 2nd ed. [ebook] Information Commissioner's Office. (2017). https://ico.org.uk/media/fororganisations/documents/20
7. Machine Learning in MATLAB // https://www.mathworks.com/help/stats/machine-learning-inmatlab.html.
8. Hartmann K., Steup C. (2020). Hacking the AI – the Next Generation of Hijacked Systems. In 12 International Conference on Cyber Conflict (CyCon). https://doi.org/10.23919/CyCon49761.2020.9131724
9. Fredrikson M., Jha S., Ristenpart T. (2015). Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. In CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1322–1333. https://doi.org/10.1145/2810103.2813677
10. Kumar S. H. and Tiwary R. K. Analysis of rankbrain algorithm using machine learning. (2017).
11. Lohn A. (2020). Hacking AI. Center for Security and Emerging Technology. https://doi.org/10.51593/2020CA006
12. Rao C., Govindaraju V. Handbook of Statistics: Machine Learning: Theory and Applications, 2013. 552 с.
13. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с.
14. Valentyn Sobchuk, Roman Pykhnivskyi, Oleg Barabash (2024) Sequential IDS for Zero-Trust Cyber Defence of IoT/IIoT Networks. // Advanced InformationSystems. 2024. Vol.8, No.3. p. 92-99. https://doi.org/10.20998/2522-9052.2024.3.11