Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)
спеціальність *125 Кібербезпека*
(код і назва спеціальності)
освітній ступень *магістр*
освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Метод аналізу кіберзагроз з використанням штучного інтелекту»

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Владислав РЕМПІНСЬКИЙ**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Лариса МИРУТЕНКО	
Нормоконтроль	Сергій ДАКОВ	

Київ 2024

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Ремпінський Владислав Юрійович (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Метод аналізу кіберзагроз з використанням штучного інтелекту

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес виявлення кіберзагроз з використанням штучного інтелекту
Предмет досліджень	Метод аналізу кіберзагроз та технології штучного інтелекту.
Мета	Вдосконалення методу виявлення кіберзагроз використовуючи технології ШІ.
Вихідні дані для проведення роботи	Технології та алгоритми штучного інтелекту, методи аналізу кіберзагроз.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна полягає в модифікації методу оцінки кіберзагроз на базі технології штучного інтелекту

Практична цінність полягає у створені коду для аналізу трафіку, який допомагає вдосконалювати системи виявлення та реагування на інциденти, вдосконалюючи алгоритми, збільшуючи швидкість реакції та покращуючи точність виявлення загроз.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	17.11.2023 – 26.11.2023
Аналіз літературних джерел	27.11.2023 – 24.12.2023
Розробка плану для досягнення мети роботи	25.12.2023 – 14.01.2024
Аналіз аспектів ШІ	15.01.2024 – 28.01.2024
Аналіз використання ШІ у кібербезпеці	29.01.2024 – 11.02.2024
Аналіз кіберзагроз з використанням ШІ	12.02.2024 – 18.02.2024
Обгрунтування специфіки використання методу	19.02.2024 – 25.02.2024
Розробка концепції та практичне використання методу	26.02.2024 – 03.03.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	06.05.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 17.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Збільшення продуктивності виявлення потенційних загроз для трафіку.

Соціальний ефект Підвищення рівня захищеності передачі даних користувачами.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Лариса МИРУТЕНКО
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв
до виконання _____ Владислав РЕМПІНСЬКИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка містить 107 сторінок основного тексту, 13 рисунків, 1 таблицю, 1 додаток та 50 літературних джерел.

Об’єкт дослідження: процес виявлення кіберзагроз з використанням штучного інтелекту

Мета кваліфікаційної роботи: вдосконалення методу виявлення кіберзагроз використовуючи технології ШІ.

Методи дослідження: аналіз, методи порівняння, структурний.

У роботі досліджено використання алгоритмів штучного інтелекту для ідентифікації, класифікації та прогнозування кіберзагроз. Розглянуто методи машинного навчання та глибокого навчання, їх ефективність у виявленні складних зразків поведінки, які можуть вказувати на потенційні загрози, а також обговорено переваги та обмеження цих технологій у контексті кібербезпеки.

Проведено аналіз потенціалу алгоритмів машинного та глибокого навчання для виявлення та класифікації кіберзагроз. Оцінено їхню здатність розпізнавати аномалії в даних та прогнозувати майбутні атаки на основі попередніх інцидентів.

Запропоновано покращення системи Виявлення та Реагування на Інциденти

Розроблено концепцію методу аналізу кіберзагроз.

Практичне значення роботи полягає у створені коду для аналізу трафіку, який допомагає вдосконалювати системи виявлення та реагування на інциденти, вдосконалюючи алгоритми, збільшуючи швидкість реакції та покращуючи точність виявлення загроз.

Результати здійснених у дипломній роботі досліджень можуть бути використані для впровадження запропонованого методу в організації.

Наукова новизна дослідження полягає у в розробці та тестуванні нових методів оцінки інтеграції систем кібербезпеки та підвищення їх ефективності.

Напрямки подальших досліджень включають поглиблений аналіз нових методів.

Ключові слова: аналіз трафіку, штучний інтелект, кіберзагрози, інциденти, машинне навчання, глибинне навчання.

ЗМІСТ

ВСТУП

Постановка проблеми. У цей час зростання суспільного життя у світі характеризується становленням інформаційного суспільства. Україна бере участь у створенні глобального інформаційного ринку та міжнародних інформаційних процесів. Відомо, що вона відіграє важливу роль у процесі державного будівництва та захисту державних інтересів на міжнародній арені. Важливим аспектом управління процесами та бізнесом є широкий і миттєвий доступ до інформації, що підвищує його ефективність. Широке впровадження нових комп'ютерних і мобільних систем йде рука об руку з інформацією сучасного суспільства.

Одним із факторів, що сприяють інформаційній безпеці, є використання технологій штучного інтелекту. Адже штучний інтелект є одним із трендових напрямків, який охоплює всі розвинені країни світу. Світ ризикує втратити можливість для технологічного прогресу, якщо не подбати про безпеку штучного інтелекту. Глобальний ринок технологій на основі штучного інтелекту буде розділений між конкуруючими країнами, що ускладнить і сповільнить державний розвиток ключових секторів економіки.

Під штучним інтелектом розуміють набір технологічних рішень, які дозволяють імітувати когнітивні функції людини та досягати результатів, рівних результатам інтелектуальної діяльності людини при виконанні певних завдань.

Аналіз останніх досліджень і публікацій. Численні праці як вітчизняних, так і зарубіжних вчених, зокрема О. В. Адамчука, О. А. Баранової, О. В. Глазового, Т. Г. Каткової, М. В. Карчевського, К. О. Гернеса, С. Ю. Владиковича та ін. Петряєва, О. Є. Радутний, Ю. О. М. Сидорчук, В. М. Фурашева. , О. О. Ястреб, Є. О. Харитонова, О. І. Харитонов та ін.

Мета дослідження: вдосконалення методу виявлення кіберзагроз використовуючи технології ШІ.

Для реалізації мети поставлено такі завдання:

– аналіз фундаментальних аспектів штучного інтелекту;

- аналіз можливостей інтеграції з існуючими системами безпеки;
- аналіз кіберзагроз;
- оцінка ефективності розроблених алгоритмів;
- провести практичні приклади застосування штучного інтелекту в кібербезпеці.

Об’єкт дослідження: процес виявлення кіберзагроз з використанням штучного інтелекту.

Предмет дослідження: метод аналізу кіберзагроз та технології штучного інтелекту.

У цьому дослідженні присутня аналіз методів використання штучного інтелекту для ефективного виявлення, аналізу та прогнозування кіберзагроз. Це включає створення алгоритмів машинного навчання, які можуть аналізувати великі обсяги даних та ідентифікувати аномальні патерни, що вказують на потенційні атаки. Робота також орієнтована на вивчення можливостей інтеграції цих методів у сучасні системи кібербезпеки та визначення їхньої ефективності у захисті від кіберзагроз. Результати дослідження спрямовані на поліпшення здатності організацій до вчасного виявлення та запобігання кібератакам.

Науковий внесок цього дослідження полягає в модифікації методу оцінки кіберзагроз на базі технології штучного інтелекту.

Робота побудована таким чином, що в кожному розділі будуть послідовно розкриватися різні аспекти проблеми, починаючи від теоретичних основ і закінчуючи практичним застосуванням розроблених методів.

РОЗДІЛ 1
ФУНДАМЕНТАЛЬНІ АСПЕКТИ ШТУЧНОГО ІНТЕЛЕКТУ

1.1 Еволюція та історичний розвиток штучного інтелекту

У сучасному суспільстві все частіше постає проблема залежності від новітніх технологій. Тому перед вченими та філософами майже щодня постають нові питання про людину та її життя в новому сучасному технологічному світі.

Історія розвитку штучного інтелекту почалася з філософських часів. З давніх-давен люди досліджували власну природу і процес пізнання світу, а пізніше розширили ці знання нейрофізіологами і психологами у вигляді ряду теорій про функціонування людського мозку і процес мислення. Саме тоді була сформована гіпотеза про можливість створення інтелектуального біомеханічного робота з усіма властивостями людського мозку. Проблема створення та розвитку штучного інтелекту сьогодні є найбільш актуальною.

Як зазначив Погореленко: «штучний інтелект є продуктом наукових поглядів представників різних країн». Це також унікальний і неповторний продукт технічного прогресу, який дозволяє машинам навчатися, отримувати користь від людей і власного досвіду, адаптуватися до нових умов в рамках своїх застосувань, виконувати різні завдання, які виконувалися протягом тривалого часу. Прогнозувати події та оптимізувати ресурси різного характеру під силу лише людині [1].

Як вказують Галина Машлій; Ольга Мосій; Мар’яна Пельчер: «Уперше термін «штучний інтелект» ввів професор Дартмутського коледжу Джон МакКарті ще в 1956 році.»

За словами Джона Маккарті: «Штучний інтелект — це розділ комп’ютерної лінгвістики та інформатики, який формалізує завдання, схожі на людські. Іншими словами, комп’ютер робитиме те саме, що робили ми».

Вважається, що розробка сучасних систем штучного інтелекту почалася в 1950-х роках. Програма, розроблена А. Ньюеллом і призначена для доведення

математичних теорем, сприяла розвитку штучного інтелекту, вона отримала назву «Logic-Theoretical». Ця робота ознаменувала початок першого етапу досліджень у галузі штучного інтелекту, пов’язаного з розробкою програм, які вирішують задачі на основі використання різноманітних евристик. Цей етап призвів до появи та поширення терміну штучний інтелект.

У 60-х роках були зроблені спроби знайти загальні методи вирішення широкого класу задач шляхом моделювання складного процесу мислення. Однак чим ширший клас завдань, які може вирішувати програма, тим слабша її здатність розв'язувати ту чи іншу проблему. У цей період почало формуватися інтуїтивне програмування.

Евристичне програмування — це розробка стратегії дій на основі аналогії чи прецеденту.

У 1969 році у Вашингтоні відбулася перша Всесвітня конференція зі штучного інтелекту [2].

Штучний інтелект на початку свого становлення розвивався у функціональному або аналітичному напрямку, коли людина командує машиною (роботою) для виконання інтелектуальних спеціальних завдань творчого характеру (ігри, переклад з однієї мови на іншу, малювання тощо).

Слідом за аналітичним напрямом виник синтетичний, або моделюючий, напрямок, а потім були зроблені спроби змоделювати творчу діяльність мозку в цілому. Об'єкти дослідження синтетичного програмування стали мішенями мисленнєвої діяльності людини.

Метою творчої процедури є не процедури (функції) інтелектуальної діяльності, а методи створення таких процедур, методи навчання новому виду інтелектуальної діяльності.

З 1970-х років зусилля вчених були зосереджені на таких основних напрямках:

– Розвиток методів презентації, тобто методів побудови проблем у спосіб, який можна легко вирішити;

– Розробка методів пошуку, тобто відповідних способів управління ходом вирішення роботи, щоб вона вирішувалася в реальному часі за допомогою реальних засобів.

Однак у 70-х роках штучний інтелект піддався критиці, і фінансування було скорочено. Дослідники ШІ не змогли адекватно оцінити складність проблем, з якими вони стикаються. Їхній надмірний оптимізм породжував неймовірно великі надії та очікування, а коли обіцяних результатів не було, фінансування було припинено.

Друге народження науки про штучний інтелект почалося у 1980-х роках. Було реалізовано його великий потенціал як у дослідженні, так і у розвитку виробництва. У рамках нової технології з'явилися перші комерційні програмні продукти. У цей період почала розвиватися сфера машинного навчання. Досі передача знань спеціалізованого експерта в машинну програму була виснажливим і тривалим процесом. Найважливішим кроком останніх років є створення систем, які автоматично розвивають і розширюють запас евристичних правил. На початку десятиліття в різних країнах були запущені найбільші національні та міжнародні дослідницькі проекти в історії обробки даних щодо інтелектуальних комп’ютерів наступного покоління [3].

У червні 1997 року групі дослідників з IBM дістався неабиякий приз у вигляді 100 000$. Неабияким він став і тому, що припадав пилюкою понад 17 років. Його заснував професор Едвард Фредкін, залишивши нагороду тим, хто напише алгоритм, який переможе найкращого шахіста планети.

З десятків невдалих спроб айті-фахівців усього світу вирізнялася машина від хлопців з IBM. Їхній алгоритм мусив не тільки розуміти дошку і правила, але й передбачати наступні кроки. Також у травні 1997 року Deep Blue став на двобій із Гарі Каспаровим. Програвши першу і вигравши другу партії, Deep Blue зіграв наступні три внічию. Вирішальна шоста партія була за роботом. Після матчу Каспаров неодноразово говорив, що помічав «занадто розумні» кроки у грі Deep Blue, та висловлював підозри, що машині допомагали гросмейстери. Пропозицію Гарі зіграти реванш Deep Blue відхилив і залишився з «поясом» переможця.

У 2005 році відомий Державний департамент США використав бездушний штучний інтелект у своїх цілях. Дослідницький центр Міністерства оборони США зіткнувся з проблемою зв'язку з бойовими підрозділами. Потрібен був пристрій, який міг би регулярно перевозити спорядження та боєприпаси солдатам, куди не міг

проїхати звичайний транспорт. "BigDog" повинен бути рятівником. Чотириногий робот з центральною вагою і зростом близько одного метра, з купою датчиків всередині, рухався складними маршрутами зі швидкістю 6,4 км/год. Протягом багатьох років Boston Dynamics, його розробники, навчили робота ходити по крижаній і слизькій поверхні, а також відновлюватися після ударів. У 2015 році розробку та фінансування проекту припинили: Bigdog нарощував занадто багато шуму, тим самим викриваючи позицію американських солдатів [4].

У 2008 році столітня історія технології розпізнавання голосу досягла свого апогею. IBM Shoebox, яка 60 років тому розпізнала 16 різних слів у секретних методах розпізнавання голосу часів холодної війни від ФБР та Агентства національної безпеки. Ця величезна кількість даних стала в нагоді Google, і в 2008 році вони випустили програму Голосовий пошук, попередницю сучасного Google Assistant.

За словами Андрія Сабініча: «За допомогою свого алгоритму розпізнавання мовлення Google не лише перекладав голос у текст, а й враховував особисті дані та контент користувача. Простими словами, «Де найближчий банкомат?» штучний інтелект нарешті враховував геолокацію людини. Принцип роботи технології був дуже простий: голос конвертувався в файл, перелітав на сервери Google, проходив через пошукову систему і повертався людині з розгаданим файлом результатів. Сьогодні Amazon Alexa або Siri неможливо уявити без цієї технології.

У 2014 році Google почав інвестувати мільярди доларів у безпілотні автомобілі зі штучним інтелектом, а Skype успішно запустив онлайн-переклад мовлення під час розмов.

Останнім досягненням у сфері створення штучного інтелекту став людиноподібний робот на ім’я Софія, створений гонконгською компанією Hansen Robotics і набув великої популярності в ЗМІ завдяки своїй схожості з людиною (її образ був заснований на актрисі Одрі Хепберн), 60 емоцій і під час публічних дискусій Набір відповідей виразу обличчя з неоднозначними твердженнями [5].

Однак, західні дослідники заперечують, що роботів можна назвати штучним інтелектом. За словами керівника лабораторії штучного інтелекту компанії "Facebook", робот Софія - це чат-бот, який використовує технологію розпізнавання

мови Google для визначення запитань за ключовими словами та вибору найбільш підходящої відповіді із заданої бази даних.

Іншими словами, історія розвитку штучного інтелекту зайняла дуже багато часу, щоб стати самостійною сферою у світі, і зараз він продовжує розвиватися і розвиватися. Вчені всього світу досліджують все нові й нові межі та горизонти можливостей штучного інтелекту. Штучний інтелект має величезні можливості в майбутньому.

1.2 Ключові концепції

Можливість використання штучного інтелекту (ШІ) викликає інтерес не лише в експериментальних та прикладних технологічних сферах, а й у соціально-економічних сферах. Паралельно з тим, як людство намагається вдосконалити технології та вирішити філософські питання, пов’язані зі штучним інтелектом, держави та міжнародні організації також ламають голову над іншими загадками щодо визначення правової природи штучного інтелекту, результатів його роботи та можливості його впровадження. Правові та організаційні аспекти використання нематеріальних активів [6].

В даний час для штучного інтелекту використовують більш «вузьку» інтерпретацію, інтерпретуючи його як програму (або набір програм) для вирішення конкретних індивідуальних завдань, основними компонентами якої є машинне і глибоке навчання. У широкому розумінні кінцевим продуктом технології штучного інтелекту є система, яка не може імітувати, але самостійно «мислить» на основі програмування незалежних дій (це також називають «сильним штучним інтелектом»).

Звичайно, така технологія ще не впроваджена повністю і є сумніви щодо її загального впровадження. Незалежно від обраного визначення, ключовою особливістю штучного інтелекту є здатність комп’ютера імітувати людську поведінку та можливості людського мозку.

Машинне навчання (machine learning) – підмножина (підгалузь) штучного інтелекту, що складається з технік і методів, які дозволяють комп’ютеру (у широкому сенсі – програмі, системі, роботі тощо) навчатися на основі даних і підвищувати точність виконання завдань у певному кількість часу без додаткового програмування. Основою машинного навчання є створення комп’ютером незалежних алгоритмів на основі моделі, заданої особою, і даних (набору даних), завантажених і обраних нею, зарезервованих для навчання та безпосереднього використання. Під час навчання алгоритму з пробними наборами даних передбачається втручання людини [7].

Глибинне навчання (deep learning) — підмножина штучного інтелекту, частина машинного навчання, чиї алгоритми розроблені для навчання так само, як навчаються люди, БЕЗ людського втручання. Саме глибоке навчання дозволяє комп’ютеру вирішувати складніші проблеми. Моделі глибокого навчання потребують фільтрації великих обсягів даних через кілька рівнів обчислень і постійного коригування для покращення результатів навчання. Іншими словами, що відрізняється від машинного навчання з точки зору даних і методу навчання, так це використання нейронних мереж із нейронами, шарами та зв’язками. Приклад: десять років тому програми розпізнавання голосу навчалися користувачам, які промовляли десятки слів у програмі, щоб позначати власні голосові дані. Сучасні програми (Apple Siri, Amazon Alexa і Google Assistant), які розпізнають голосові команди будь-якої людини без необхідності додаткового навчання, є глибоким навчанням.

Нейронна мережа (neural networks) — аспект штучного інтелекту (зазвичай визначається як алгоритм), який має на меті імітувати роботу мозку (тобто аналітичні механізми) за допомогою штучних нейронів, створених у формі одного або кількох шарів. Це один із фундаментальних будівельних блоків технології штучного інтелекту. Саме збільшення кількості прихованих і вхідних шарів нейронних мереж часто визначає глибинне або машинне навчання [8].

Обробка природної мови (Natural Language Processing, NLP) — це сфера, яка дозволяє комп’ютерам розуміти, аналізувати та створювати людську мову. Він використовується для автоматичного перекладу, розпізнавання мови, аналізу тексту та багато іншого.

Розпізнавання образів (Computer Vision) — це дозволяє комп'ютерам аналізувати та розуміти візуальні дані, такі як зображення чи відео. Він використовується для розпізнавання об'єктів, розуміння сцени та навіть медичної діагностики на основі зображень.

Автоматизація рішень (Automated Decision Making) — штучний інтелект можна використовувати для автоматизації прийняття рішень на основі вхідних даних і встановлених правил. Це може включати автоматичні рекомендації, керування процесами та багато іншого.

Самонавчання (Self-learning). Деякі системи штучного інтелекту можуть вивчати нові дані без необхідності додаткового програмування. Вони постійно вдосконалюються, користуючись своїм досвідом.

Генетичні алгоритми (Genetic Algorithms) — це метод оптимізації, який імітує процеси природного відбору. Вони використовуються для пошуку оптимальних рішень у складних областях.

Експертні системи (Expert Systems) — системи, які використовують бази знань і правила для роботи в певних областях. Вони можуть відтворювати рішення експертів у своїй галузі [9].

Багатоагентні системи (Multi-agent Systems) — це системи, в яких кілька агентів працюють разом для досягнення спільних цілей. Вони можуть моделювати складні соціальні взаємодії та ринкові процеси.

Етика та безпека (Ethics and Safety) — ця концепція стосується етичних аспектів використання ШІ, захисту приватності даних, уникнення впереджень та забезпечення безпеки в системах ШІ.

Ці концепції лежать в основі розробки та застосування штучного інтелекту в різних сферах, від технологій до медицини та бізнесу.

1.3 Розподіл та типологія алгоритмів штучного інтелекту

Сучасні нейронні мережі складають основу таких технологій, як штучний інтелект, комп'ютерне бачення та аналіз відео. Можна сказати, що нейронна мережа

імітує нейронну діяльність і процеси мислення людини (рисунок. 1.1). Різниця в тому, що мислення замінюється розрахунком. Метою розрахунку є моделювання процесу розпізнавання людей людьми та його логічні наслідки.

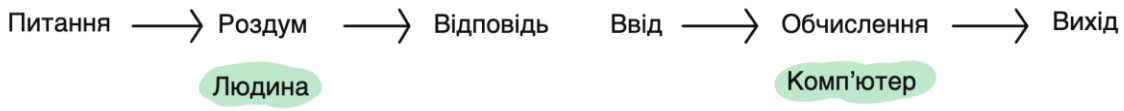

Рисунок 1.1 – Мислення та обчислення

Проте між архітектурою мозку та архітектурою комп'ютера є принципова різниця. Звичайні комп'ютери обробляють дані дуже швидко, але в основному дані обробляються послідовно на основі чітко визначених алгоритмів і конкретних вхідних даних. Приблизного місцезнаходження в їхніх підрахунках немає. Мозок тварин або людини працює набагато повільніше, ніж комп'ютер, але може паралельно обробляти велику кількість сигналів і подібний за своєю природою. Тому загального результату часто можна досягти швидше. Біологічні нейрони — це нервові клітини в організмі людини, які мають багато входів: дендрити, виходи: аксони та закінчення аксонів: термінали. Аксони також можна назвати синапсами. По нейронах передається подразнення нерва у вигляді електрохімічних імпульсів.

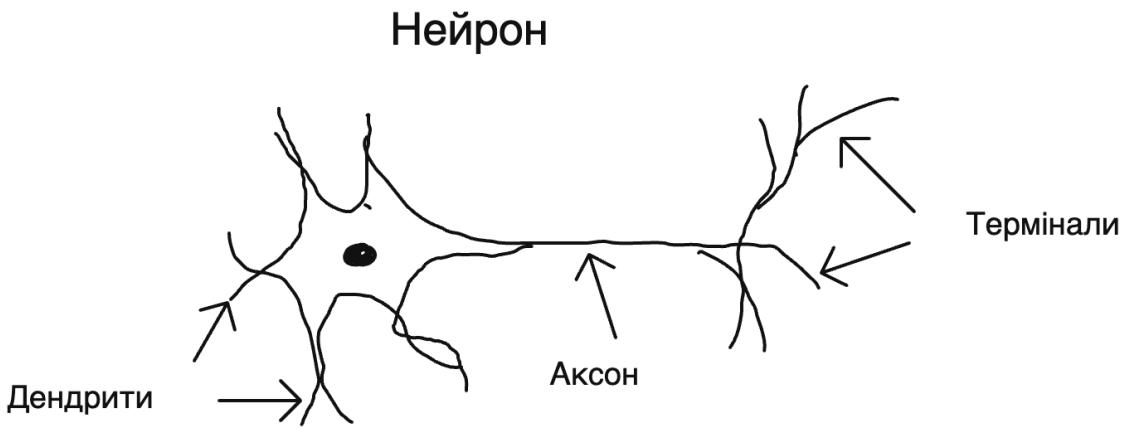

Рисунок 1.2 – Нейрони людини

Як показано на рисунку 1.2, "нейронна мережа" людей і тварин дуже спрощена. На цій схемі показані взаємопов'язані нейрони. Вихідний сигнал аксона одного нейрона використовується як вхідний сигнал для дендритів іншого нейрона (рисунок 1.3).

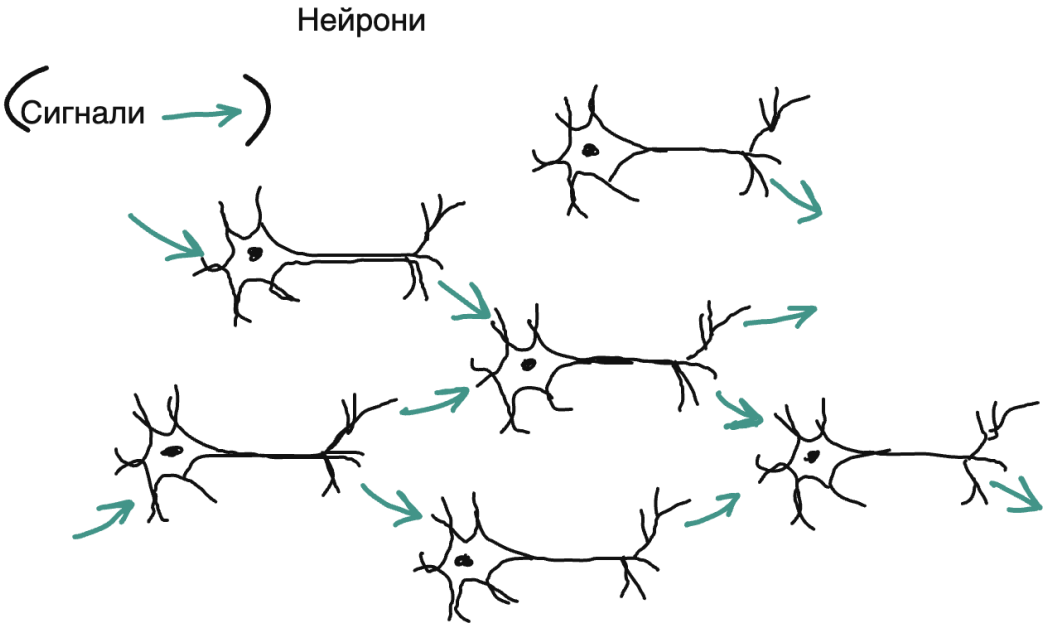

Рисунок 1.3 – Спрощена принципова схема нервової системи людини як нейронної мережі

Перед тим, як сигнал передається іншим нейронам, відбувається певна передача сигналу в ядрі нейрона. Комп'ютерна нейронна мережа імітує нейронну структуру нервової системи людини і тварин. На рисунку 1.4 нижче показано дуже спрощену нейронну мережу, що складається з трьох шарів обчислювальних вузлів "нейронів", які мають кілька входів і кілька виходів і можуть бути з'єднані один з одним [10].

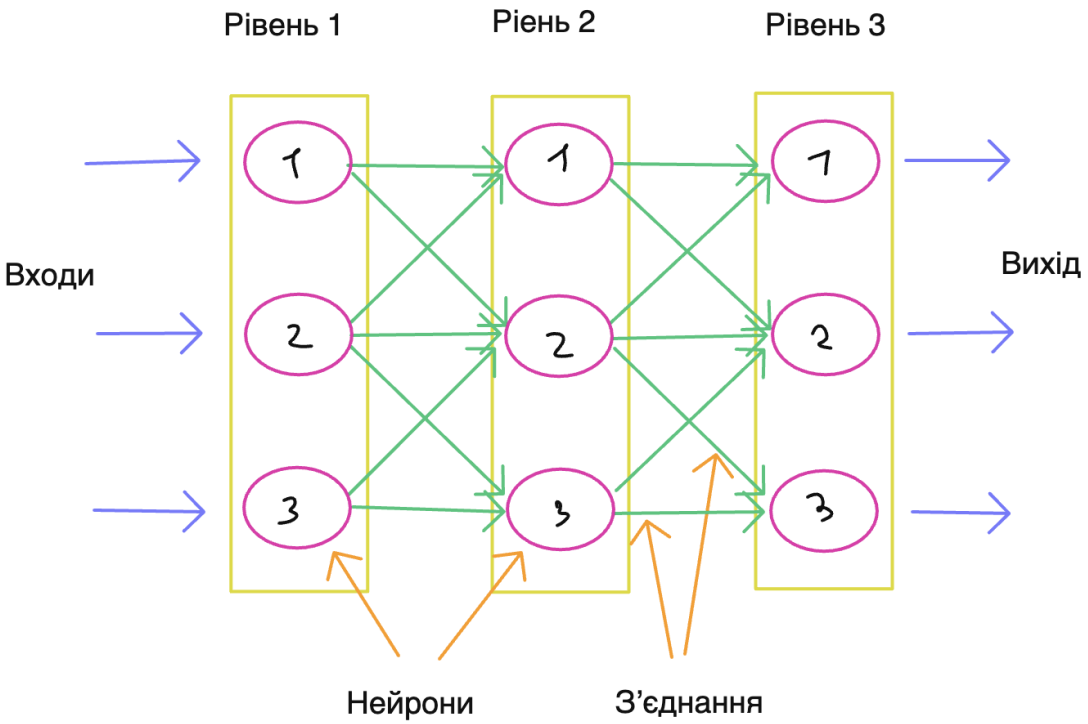

Рисунок 1.4 – Спрощене представлення нейронної мережі

Загалом, функція нейронної мережі полягає в тому, щоб пов'язати вхідний сигнал з вихідним сигналом, який відповідає заздалегідь визначеному цільовому значенню з матриці вихідних сигналів. Позначення (i, o) жирним шрифтом означає, що параметр насправді є матрицею. Взаємодія між нейронами в мережі регулюється "вагами" (w), які можуть бути змінені на основі різниці (e) або помилки між вихідним сигналом o та його цільовим значенням. Цей процес зміни вагових коефіцієнтів відомий як "навчання" нейронної мережі.

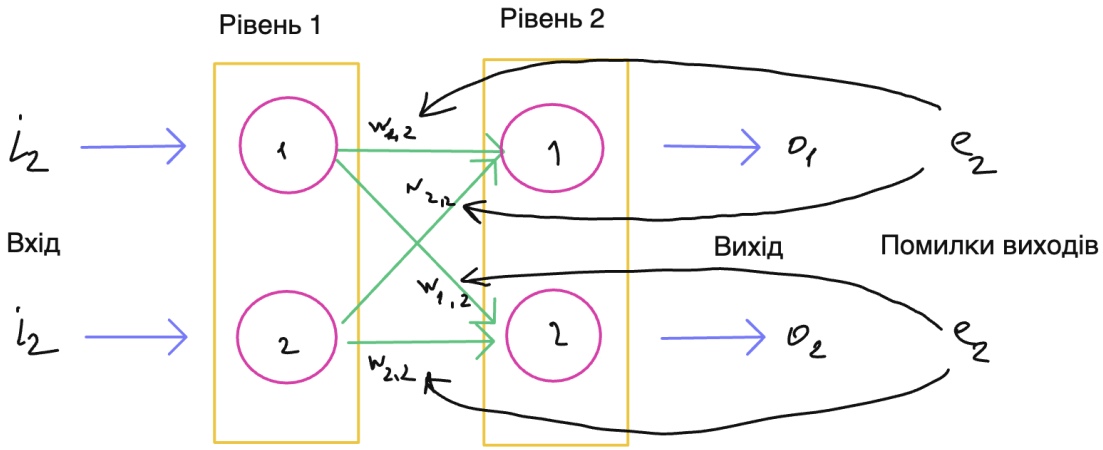

Рисунок 1.5 – «Тренуйте» нейронну мережу

Час «навчання» нейронної мережі встановлює зв'язок між вхідним сигналом і вихідним сигналом. Якщо матриця піксельних зображень представлена як вхідний сигнал, то під час перегляду зображення в «навчальній» мережі буде вихід, що показує ступінь кореляції між вхідним зображенням і форматом у файлі зображення. Навчальні дані - це різниця між вихідним сигналом і значенням помилки-e, де "вага" w вибирається для корекції сигналу [11]. Реакція сигналу корекції помилок залежить від ваги зв'язку між нейронами. Чим більша «глибина» мережі, тобто нейронних одиниць, прихованих у мережі, тим більш адаптивною є мережа і тим краще можна отримати налаштування матриці вхідного сигналу. Процес машинного навчання нейронної мережі (machine learning) можна проілюструвати, знайшовши форму найглибшої діри в горі. У машинному навчанні нейронна мережа «досліджує» глибокі зовнішні ефекти, щоб знайти багатовимірну функцію для кожного нейрона, і повторює цей процес для кожного рівня нейронів у мережі (права частина зображення). Це як людина, яка знайшла в темряві діру на горі. Ліхтарик у його руці світить лише на один крок вперед (ліворуч на рисунку 1.6). Геодезист знайшов найнижчу точку і пішов туди, потім використав ліхтарик тощо, поки не досяг дна печери він знову запалює.

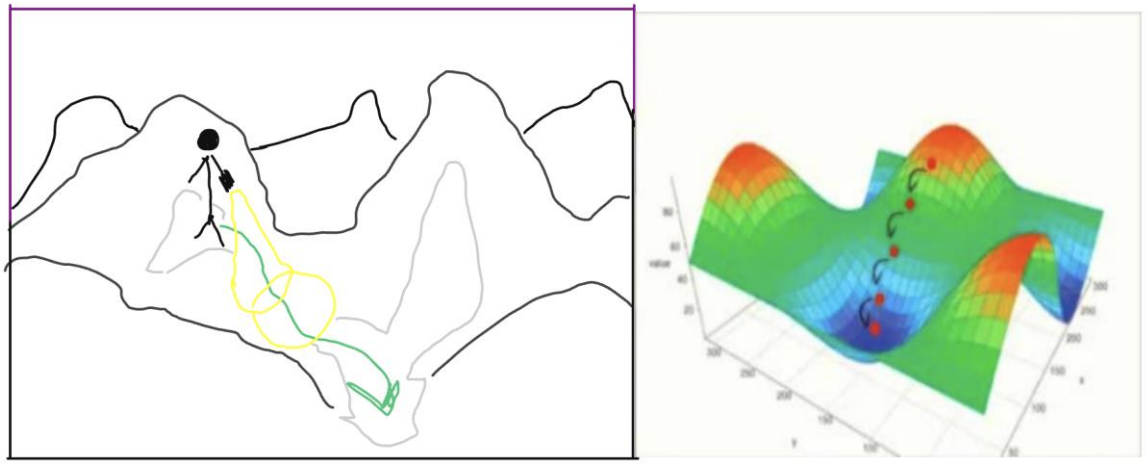

Рисунок 1.6 – Графічне зображення процесу навчання нейронної мережі

Так само нейромережа прагне мінімізувати відхилення у вихідному сигналі кожного нейрона, відповідно змінюючи його вхідний ваговий коефіцієнт w. На відміну від людини, яка обробляє дані послідовно, нейронні мережі можуть одночасно регулювати ваги всіх нейронів на всіх рівнях. Тривалість навчання нейронної мережі може варіюватися від декількох секунд до декількох днів, залежно від складності завдання, глибини нейронної мережі та швидкості обробки даних обчислювальним обладнанням [12].

Концепція розумного агента.

Термін «інтелектуальний агент» у штучному інтелекті означає суть спостереження та вивчення навколишнього середовища (наприклад, обладнання, роботів, різноманітних пристроїв тощо), а їх поведінка є розумною, тобто вони зрозумілі та завжди в русі. Прагніть до досягнення будь-якої мети. У цьому випадку інтелектуали функціонують за допомогою ембріонів, які мислять подібно людському мисленню, або інтелектуально розвинених організмів. Вони здатні: вирішувати проблеми, пов'язані з відсутністю попередніх рішень; приймати рішення на основі необхідних об'єктивних умов для дій; широко і опосередковано відображати реальність; досліджувати і розкривати нові аспекти; встановлювати і досягати проміжних цілей. Зазвичай інтелектуальні агенти використовуються в таких контекстах, як ігри або виконання спеціалізованих завдань. Ці агенти, часто роботи, імітують різноманітні форми людської поведінки. У сфері штучного інтелекту агенти

бувають різних форм, включаючи ті, що мають базову поведінку, ті, що керуються конкретними цілями, і ті, що навчаються на власному досвіді, серед інших.

Алгоритм Q-навчання для інтелектуальних агентів.

Навчання з підкріпленням — це метод посилення навчання. На цьому етапі навчання агенти, що діють у певному середовищі, отримують "винагороду" у вигляді накопичених балів за свої дії. Основна мета інтелектуального агента - розробити модель поведінки, яка дозволить йому оптимально діяти в конкретному середовищі.

В основі Q-навчання лежить так звана функція:

$$Q[s,a] = R[s,a] + Gamma \cdot Max(Q[s',a'],$$

де, s-елемент множини станів S(S1,S2…Sn), в них може перебувати агент;

a-елемент множини дії агента A(A1,A2…An);

s`-елемент попереднього стану з множини станів S(S1,S2…Sn);

a`-елемент попередньої дії агента A(A1,A2…An);

Гамма- швидкість навчання від 0 до 1 (рекомендовано 0,8).

Алгоритм навчання Q можна пояснити досить поширеним прикладом, який описаний у багатьох матеріалах.

Визначення колективного інтелекту

Колективний інтелект або груповий інтелект — нове положення в теорії інтелекту. Природний приклад колективного інтелекту базується на аналізі багатьох біологічних форм поведінки, які мають розумні рішення для вирішення конкретних проблем. До цих істот належать мурахи, бджоли, птахи, риби та інші істоти, які утворюють колонії або зграї, працюють за певним алгоритмом, використовують цифрові переваги для пошуку їжі та уникнення загрози хижаків. Головними характеристиками колективного інтелекту є: існування груп (їх багато); Вміння використовувати метод обміну інформацією в групі; наявність мішені; чітке підпорядкування людей меті; Алгоритми, розроблені в області колективного інтелекту, використовуються тільки для поєднання задач оптимізації з проблемами продавця.

Евристика — це рішення, яке включає ідеї, які не гарантовано будуть правильними або хорошими, але достатні для вирішення проблеми. Якщо остаточне рішення не знайдено, ви можете зробити рішення швидше [12].

Евристичний алгоритм — використовується для вирішення задач. Точність алгоритму не була доведена у всіх випадках, але відомо, що він може забезпечити гарне рішення в більшості випадків. Також можна знати (тобто довести), що евристичний процес недійсний. Його слід використовувати лише в дуже малих кількостях, якщо він дає неправильні результати, або якщо він дає неправильні результати, але все ще дійсний.

Евристичні алгоритми широко використовуються для вирішення задач високої обчислювальної складності; тобто потрібно багато часу, щоб змінити весь пошук варіантів, іноді технічно неможливо, але з швидким алгоритмом, але теоретично недостатньо придатним. Через відсутність стандартних рішень як базових знань у сфері штучного інтелекту на Заході широко використовуються евристичні алгоритми. Антивірусні програми, комп'ютерні ігри тощо. Використовуються різні евристики. Наприклад, шахові програми в основному реалізуються в іграх, заснованих на евристичних алгоритмах (для першої партії можуть використовуватися таблиці, а для зворотної – таблиці Налімова), але в проміжних іграх кількість ходів часто може привести до успішного результату. і немає кінцевого результату для довгострокового алгоритму прямої гри [13].

Можливість (допустимість) використання евристик для вирішення кожної конкретної задачі залежить від співвідношення вартості вирішення задачі конкретним і наближеним способами, частоти помилок і в тому числі статистичних аспектів евристики. Крім того, важливо мати «фільтр здорового глузду» або неупереджену оцінку реакції людей. Розглянемо гіпотетичний приклад. Припустимо, що існує відомий, але дуже складний і точний алгоритм, який може вирішити цю проблему, і ця евристика повинна запускатися менше ніж 1000 разів і зазвичай дає прийнятний результат (приблизно 95% часу). Для простоти припускаємо, що значення позитивного результату є постійним, як і значення похибки.

Як свідчить сучасна практика, робота найскладнішого алгоритму в більшості випадків не відбудеться випадково, але завжди можна занурити всю систему в хаос. Наприклад, несподівана «надзвичайна ситуація» в США в 2010 році майже не спустошила фондовий ринок. Причиною цього стали «конфлікти» між комп'ютерними алгоритмами, що взаємодіють з фінансовими даними, в результаті чого вони почали працювати непередбачувано. Буквально за кілька хвилин основні акції втратили понад 90% своєї вартості, а потім одразу відновили вартість, але ця подія спричинила величезні штрафи та збитки.

1.4 Майбутнє штучного інтелекту

Майбутнє штучного інтелекту (ШІ) — це динамічна галузь, яка швидко розвивається, і щодня з'являються нові досягнення та застосування. ШІ здійснив революцію в багатьох галузях, від охорони здоров'я до фінансів, і його потенціал для зростання здається безмежним. У цій статті ми заглиблюємося в майбутнє ШІ та його вплив на суспільство [14].

Ключовим моментом в еволюції штучного інтелекту є розширення можливостей машин виконувати завдання, які традиційно вважалися специфічно людськими. Наприклад, системи штучного інтелекту тепер здатні писати тексти, писати музику і навіть робити фотографії. У майбутньому штучний інтелект вирішуватиме складніші завдання, такі як навчання та набуття знань, що значно підвищить ефективність та продуктивність різних підприємств Значним каталізатором майбутнього розвитку штучного інтелекту є все більше впровадження ШІ в повсякденне життя. Інтелектуальні персональні асистенти, такі як Siri від Apple і Alexa від Amazon, все частіше з'являються в багатьох будинках. У майбутньому ці системи можуть бути вдосконалені таким чином, що дозволять контролювати безліч пристроїв і послуг за допомогою простих голосових команд [15].

Незважаючи на всі ці технологічні досягнення, широке використання інтелекту може мати багато етичних і соціальних наслідків. Наприклад, оскільки машини стають більш гнучкими та можуть виконувати людську роботу, існує ризик того, що

вони замінять працівників у багатьох галузях. Це може призвести до великої кількості роботи та відсутності доходу, і для суспільства важливо враховувати ці проблеми, оскільки ШІ продовжує розвиватися.

Незважаючи на перешкоди, перспективи штучного інтелекту дуже райдужні. В міру того, як машини стають все більш розумними, вони можуть допомогти нам у вирішенні основних глобальних проблем, таких як зміна клімату та хвороби. ШІ також відкриває нові можливості для творчості та людського розуміння, допомагаючи нам реалізувати те, що колись вважалося недосяжним.

Таким чином, майбутнє штучного інтелекту багате на захоплюючі можливості та перешкоди. У міру розвитку цієї галузі ми повинні зважувати потенційні переваги та ризики цієї технології. За умови ретельного та сумлінного розвитку, ШІ може позитивно змінити наш світ.

1.4.1 Новітні дослідження та розробки

Штучний інтелект використовує комп'ютери та машини для імітації здатності людського розуму вирішувати проблеми та приймати рішення. По суті, ШІ передбачає програмування комп'ютера, робота чи іншого пристрою так, щоб він мислив, як високоінтелектуальна людина.

За останні кілька десятиліть з'явилося багато визначень штучного інтелекту (ШІ). Цей термін часто асоціюється з проектуванням систем, які демонструють подібні до людських інтелектуальні процеси, такі як міркування, інтерпретація значення, узагальнення або навчання на основі минулого досвіду. Сьогодні ШІ може виконувати дуже складні завдання, такі як доведення математичних теорем або гра в шахи [16].

Деякі програми в таких галузях, як медицина, комп'ютерні пошукові системи, аналіз голосу і тексту, досягли рівня людських знань.

Ступінь, до якого система ШІ може імітувати людські здібності, слугує мірилом для класифікації типів ШІ. Існує чотири основні типи штучного інтелекту:

– Реакційні машини

- Обмежена пам'ять
- Теорія розуму
- Обізнаність

1. Реактивні машини. Реактивні машини були раннім підходом у розвитку штучного інтелекту, представляючи собою початкову форму ШІ з обмеженими технічними можливостями. Вони просто копіюють здатність людського мозку реагувати на певні типи стимулів.

Ці початкові програми не мають функцій пам'яті, тобто не можуть використовувати минулий досвід. По суті, така система не може "засвоювати" нову інформацію або застосовувати її в майбутніх діях.

Зазвичай такі системи ШІ розгортаються для швидкого реагування на випадковий набір вхідних даних. Однак вони не здатні "відстежувати" дані і використовувати результати для прогнозування майбутніх подій. Deep Blue від IBM, який переміг шахового гросмейстера Гаррі Каспарова в 1997 році, є прикладом реактивного комп'ютера зі штучним інтелектом.

2. Обмежена пам'ять. Фундаментальною формою ШІ, здатного "вчитися" на власному досвіді, є інформаційна система, що базується на пам'яті.

Цей метод дозволяє системам реагувати і вчитися на минулих подіях, забезпечуючи технічну майстерність і прийняття обґрунтованих рішень. Сучасні інтелектуальні системи можуть адаптуватися і навчатися, особливо ті, що використовують глибоке навчання [17].

Системи штучного інтелекту з обмеженою пам'яттю покладаються на значні навчальні дані, щоб бути в курсі подій, які відбуваються в реальному часі. Крім того, ці системи можуть "вчитися" на минулому досвіді і застосовувати ці знання для прийняття кращих рішень у майбутньому.

Більшість сучасних систем штучного інтелекту відповідають цьому опису. Наприклад, сканер відбитків пальців є прикладом системи ШІ з обмеженою пам'яттю. Комп'ютер ідентифікує шаблони відбитків пальців на основі збережених даних і швидко реагує. Коли палець торкається одного зі збережених зображень, пристрій

відчиняє двері, дозволяючи працівникові увійти. Якщо перші два типи ШІ широко відомі, то останні два є більш концептуальними або теоретичними.

3. Теорія розуму. Наступним етапом у системах штучного інтелекту, який дослідники активно вивчають, є ідея пізнання.

Теорія штучного інтелекту охоплює його здатність сприймати потреби, емоції, переконання та когнітивні процеси живих істот, з якими машина взаємодіє, принаймні на ментальному рівні. Хоча ШІ стрімко розвивається і залишається в центрі уваги провідних дослідників, досягнення в інших галузях ШІ мають важливе значення для досягнення рівня теорії розуму.

4. Самосвідомість. Самосвідомий ШІ є найменш вивченою формою штучного інтелекту, оскільки він все ще залишається суто теоретичним. Кінцевою метою є досягнення самосвідомості.

Самосвідомі системи ШІ були б набагато складнішими, ніж людський мозок. Однак неясно, скільки часу знадобиться на розробку такого штучного інтелекту. Впровадження самосвідомих систем ШІ може зайняти десятиліття або навіть століття. Приклади технологій штучного інтелекту:

- Siri, Alexa та інші розумні помічники
- Безпілотні автомобілі
- Роботи-порадники
- Чат-боти
- Фільтри електронної пошти для спаму
- Рекомендації Netflix

Принцип штучного інтелекту.

Одним з основних елементів штучного інтелекту є машинне навчання. ШІ покладається на спеціалізоване обладнання та програмне забезпечення для створення і навчання алгоритмів машинного навчання. Хоча не існує спеціальної мови програмування, призначеної для штучного інтелекту, деякі з найпоширеніших мов включають Python, R та Java [16].

Системи штучного інтелекту функціонують, накопичуючи великі масиви навчальних даних, досліджуючи їх на наявність закономірностей і кореляцій та

використовуючи ці закономірності для прогнозування майбутніх подій. Наприклад, чат-бот з функцією текстової розмови може навчитися взаємодіяти в реальних людських розмовах, або інструмент розпізнавання зображень може бути навчений розпізнавати і класифікувати об'єкти на зображеннях, аналізуючи мільйони прикладів.

В основі розробки ШІ лежать три ключові концепції: навчання, міркування та самокорекціяя

Навчання передбачає збір даних і перетворення їх на цінну інформацію. Правила, або алгоритми, надають детальні інструкції комп'ютерним програмам для виконання конкретних завдань.

Міркування фокусується на здатності ШІ вибирати найбільш підходящий алгоритм для конкретної ситуації [15].

Самокорекція підкреслює здатність ШІ постійно коригувати та вдосконалювати свою роботу, поки не буде досягнуто бажаного результату.

1.4.2 Потенційні напрями розвитку

Термін «штучний інтелект» досить складний і може мати досить різні тлумачення. Сама галузь дуже молода, термінологія та принципи були встановлені в 1956 році Джоном Маккарті на науковій конференції, що проходила в Прінстонському університеті. Штучний інтелект можна визначити двома виразами: «здатність досягати цілей шляхом застосування стратегій, заснованих на навчанні або адаптації до навколишнього середовища, що забезпечується алгоритмами оптимального або субоптимального вибору серед широкого діапазону можливостей»; «Техногенні системи та системи, що працюють у фізичному чи цифровому світі, розглядають комплексну мету та вибирають найкращі дії (відповідно до заданих параметрів), які потрібно виконати для досягнення мети на основі сприйняття середовища, інтерпретації зібраних структурованих або неструктурованих даних та інформація, отримана з цих даних [3].

Штучний інтелект зазвичай має три основні сфери дослідження [3]:

- машинне мислення, яке займається плануванням, представленням знань та оптимізацією;
- машинне навчання, яке фокусується на навчанні штучного інтелекту на основі вхідних даних;
- робототехніка, яка передбачає управління складними механізмами.

Фактичне використання ШІ дуже різниться. Банки використовують системи штучного інтелекту для розрахунку даних андеррайтингу та клірингової діяльності за допомогою актуарної математики, яка передбачає створення моделей, які можна використовувати для навчання штучного інтелекту.

Методи розпізнавання образів поділяються на 2 основних напрямки: вивчення і класифікація властивих живим організмам здібностей до розпізнавання образів і розробка теорії і методів створення алгоритмів, призначених для вирішення конкретних завдань прикладного призначення.

Розробники ігор використовують штучний інтелект у різних сферах, зокрема для динамічного дизайну рівнів, імітації поведінки живих організмів, розрахунку економічних стратегій тощо.

Одне з найважливіших застосувань ШІ — наукові дослідження. Штучний інтелект відіграв ключову роль у відкритті сотень екзопланет, просуванні біологічних досліджень і розробці ліків від хвороб, моделюванні хімічних і фізичних процесів тощо.

Отже, ШІ — це сфера зі значним потенціалом, що лежить в основі наукового прогресу. Використання цих технологій має вирішальне значення для розвитку науки.

Висновки до розділу 1

Штучний інтелект — це продукт наукових досліджень та технологічного прогресу, який почав свій шлях ще з філософських часів. Історія розвитку ШІ почалася з досліджень людського мозку та процесу мислення, що відобразилося у розробці перших програм для розв'язання інтелектуальних завдань. З появою перших комерційних програм у 1980-х роках розвиток штучного інтелекту отримав друге

народження, що відкрило нові можливості у сфері машинного навчання та розпізнавання мовлення. Сьогодні штучний інтелект використовується у безлічі галузей, від автономних автомобілів до роботів-асистентів. Незважаючи на досягнення, деякі дослідники заперечують, що роботи можна назвати штучним інтелектом, проте ця технологія продовжує розвиватися та відкривати нові перспективи для майбутнього.

ШІ може бути вузькою, коли вона використовується для вирішення конкретних завдань, або широкою, коли вона може самостійно "мислити". Ключовими концепціями ШІ є машинне навчання, глибинне навчання, нейронні мережі, обробка природної мови, розпізнавання образів, автоматизація рішень, самонавчання, генетичні алгоритми, експертні системи, багатоагентні системи, етика та безпека. Ці концепції використовуються для розробки та застосування ШІ в різних сферах.

Алгоритми штучного інтелекту можна узагальнити як методи, які імітують нейронну діяльність та процеси мислення людини. Нейронні мережі, що складають основу штучного інтелекту, працюють подібно до біологічних нейронів, які обробляють електрохімічні імпульси. Взаємодія між нейронами в мережі регулюється вагами, які змінюються під час навчання. Навчання нейронної мережі полягає в знаходженні оптимального зв'язку між вхідним та вихідним сигналами. Крім того, інтелектуальні агенти використовуються для вирішення завдань у різних контекстах, таких як ігри або спеціалізовані завдання. Алгоритм Q-навчання допомагає інтелектуальним агентам розвивати модель поведінки для оптимальних дій у конкретному середовищі. Колективний інтелект базується на аналізі біологічних форм поведінки, які мають розумні рішення для вирішення проблем. Евристичні алгоритми широко використовуються для вирішення задач високої обчислювальної складності, але їх точність не завжди гарантована. Важливо мати «фільтр здорового глузду» при використанні евристик для вирішення задач.

Майбутнє штучного інтелекту є динамічним та швидко розвивається. ШІ вже здійснив революцію в багатьох галузях, від медицини до фінансів, і його потенціал для зростання здається безмежним. З розвитком технологій, машини стають все більш розумними та здатними виконувати складні завдання, що раніше вважалися

специфічно людськими. Інтелектуальні асистенти та інші системи ШІ все частіше з'являються в повсякденному житті, що вказує на все більше впровадження цієї технології.

Проте, разом з потенційними перевагами ШІ приходять і етичні та соціальні проблеми. Існує ризик заміщення людей машинами у багатьох галузях, що може призвести до безробіття та відсутності доходу. Тому важливо уважно враховувати ці проблеми та шукати способи вирішення їх.

Майбутнє штучного інтелекту є захоплюючим та повним можливостей. ШІ може допомогти у вирішенні глобальних проблем, таких як зміна клімату та хвороби, а також відкриває нові можливості для творчості та розвитку людського розуміння. З правильним розвитком та використанням, ШІ може позитивно змінити наш світ.

РОЗДІЛ 2
ШТУЧНИЙ ІНТЕКЛЕКТ У КІБЕРБЕЗПЕЦІ

2.1 Роль штучного інтелекту в кібербезпеці

Штучний інтелект у сфері кібербезпеки є досить широкою галуззю знань, яка потенційно може бути використана організаціями для зниження ризиків і збільшення доходів, виявлення кіберзагроз і шахрайства. Відстежувати нові віруси та зловмисне програмне забезпечення стає все важче; Таким чином, інструменти на основі штучного інтелекту можуть полегшити виявлення загроз і реагування на них, використовуючи статистику кібератак, щоб визначити найкращий спосіб протидії. Штучний інтелект може виявити зловмисне програмне забезпечення ефективніше, ніж людина. Штучний інтелект впроваджується в організаціях із декількома рівнями безпеки, як-от аналіз безпеки та керування інцидентами, і допомагає покращити виявлення аналітиками безпеки всіх загроз у мережі організації [18].

Сьогодні термін "штучний інтелект" (ШІ) глибоко увійшов у повсякденне життя. Хоча пристрої з функціями штучного інтелекту все ще намагаються повністю розуміти проблеми і знаходити рішення, ШІ перевершує людські можливості в мінімізації помилок в операційних завданнях і виявленні аномалій в різних процесах. ШІ відіграє ключову роль в оцінці людських помилок. У сфері кібербезпеки очікується, що системи на основі ШІ захищатимуть організації від онлайн-загроз, виявлятимуть типи шкідливого програмного забезпечення, забезпечуватимуть дотримання стандартів безпеки та допомагатимуть у розробці вдосконалених стратегій запобігання атакам і відновлення після них.

Очікується, що до 2022 року витрати на системи інформаційної безпеки та управління ризиками сягнуть 174 мільярдів доларів, з яких приблизно 50 мільярдів доларів буде спрямовано на захист клієнтських систем. Очікується, що продажі хмарних безпекових платформ і додатків зростуть до $1,63 млрд у 2023 році, а систем безпеки додатків - до $4,5 млрд. Ринок послуг з інформаційної безпеки також зростає,

збільшившись з $62 млрд до $66,9 млрд минулого року. Проте, самі по собі фінансові інвестиції не вирішують проблему. Більшість фахівців з інформаційної безпеки сьогодні зосереджені на аналізі логів, запобіганні спробам злому, розслідуванні можливих випадків шахрайства тощо. Вони стикаються з величезним робочим навантаженням. Істотна нестача кадрів змушує індустрію безпеки все більше і більше звертатися до рішень зі штучного інтелекту. MarketsandMarkets повідомляє, що ринок інструментів штучного інтелекту для кібербезпеки з 2019 по 2026 рік зростатиме в середньому на 23,3% на рік, збільшившись з $8,8 млрд до $38,2 млрд. (рис. 2.1)

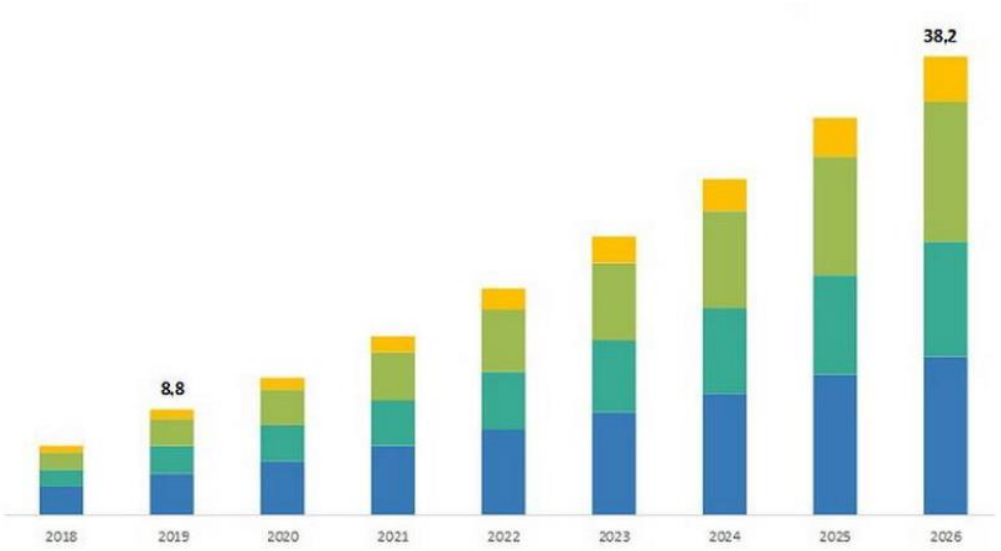

Рисунок. 2.1 – Динаміка ринку засобів ШІ для кібербезпеки, $ млрд

Широкий потенціал технологій штучного інтелекту, безумовно, може бути використаний для посилення кібербезпеки. Оскільки в сучасному світі зростає обсяг даних, інформація зберігається і передається через Інтернет різними методами. Крім того, безпечна передача даних має важливе значення в боротьбі з кіберзлочинністю і відповідає принципам кібербезпеки [19]. З розвитком інформаційних технологій кіберпростір перетворюється на поле бою для різних видів кіберзлочинності і вважається військовими експертами четвертою сферою ведення бойових дій поряд із сушею, морем і повітрям.

Чим раніше вдасться виявити порушення цілісності даних, тим меншою буде вартість їх відновлення. Постійне збільшення часу, необхідного для усунення

порушень, корелює зі збільшенням серйозності зловмисних атак, з якими стикається більшість компаній. Автоматизація безпеки та інтелектуальні інструменти, які забезпечують контроль над центром безпеки, можуть допомогти покращити здатність організації зменшувати шкоду від злому.

2.2 Методи штучного інтелекту для захисту від кіберзагроз

Методи ШІ — це методи, які дозволяють імітувати поведінку людини для виконання певних завдань і можуть поступово «навчатися», використовуючи отриману інформацію.

Наприклад, чат-боти використовують штучний інтелект для усунення зловмисників; «розумні помічники» за допомогою штучного інтелекту роблять висновок про небезпеку ситуації на основі аналізу набору показників; Механізми рекомендацій автоматично вибирають дані користувача на основі перевірених даних (на основі створення віртуального профілю користувача та профілю поведінки) [20].

Зрозуміло, що до методів штучного інтелекту відносяться методи машинного навчання для забезпечення здатності до самонавчання, також широко використовуються елементи методів математичної логіки для забезпечення певних алгоритмів дій, що працюють за певними правилами.

В даний час методи штучного інтелекту широко використовуються в кібербезпеці як частина систем SIEM, які є фреймворками безпеки, які дозволяють аналізувати ситуацію і давати рекомендації користувачеві щодо дій. Основним прикладом можуть бути онлайн-продукти, які надають посилання користувачеві незалежно від того, чи є посилання шкідливим чи небезпечним. Штучний інтелект також можна використовувати в наступальних методах безпеки, особливо для автоматизованого тестування на проникнення, щоб імітувати голос цільового користувача або писати листи на основі його стилю розмови.

Рішення з кібербезпеки використовують різні програми штучного інтелекту, такі як SIEM-системи, спам-фільтри, засоби безпечної автентифікації користувачів та інструменти прогнозування злому. Ці програми переглядають базу даних минулих

дій, щоб оцінити, чи є кожна поведінка зловмисною чи ні. IBM вважає, що глобальні втрати від витоку даних можуть бути зменшені, якщо організації впровадять автоматизовані рішення для забезпечення безпеки. Організації без автоматизації безпеки стикаються з витратами, пов'язаними з порушеннями, на 95% вищими, ніж організації з повною автоматизацією [21].

Експертні системи. Експертні системи, один із найвідоміших інструментів штучного інтелекту, являють собою пакети програмного забезпечення, які допомагають отримати відповіді на запити, надані клієнтом або надані іншим пакетом програмного забезпечення. Ці системи містять вміст знань, у якому експертні знання зберігаються в певній прикладній області. Ці системи також включають механізм міркування, який забезпечує доступ до відповідей на основі наданої інформації та іншої додаткової інформації щодо умов навколишнього середовища.

Експертна система запрограмована на пошук відповідей на питання в певній області застосування, яку переглядає користувач, або іншого продукту. У кібербезпеці вони використовуються для вибору заходів безпеки та визначення того, як будуть використовуватися обмежені активи. Експертні системи безпеки допомагають персоналу установи боротися з кібератаками. Це робиться шляхом перевірки журналів атак на базу знань, якщо це відомий процес, або ігнорування, якщо процес невідомий. Якщо така процедура відсутня в базі знань, експертна система використовує алгоритми механізму логічного висновку та знаходить наближене рішення на основі досвіду.

Машинне навчання — це сфера штучного інтелекту, яка дозволяє комп’ютеру навчатися, використовуючи дані із зразків (шаблонів), які не запрограмовані на передбачення всіх можливих ситуацій. «Два найпоширеніші типи машинного навчання — контрольоване та неконтрольоване. Контрольоване навчання використовується, коли доступний набір надійно відомих прикладів атак, особливо для вирішення проблем класифікації. Мета навчання під наглядом — навчити комп’ютер передбачати значення або правильно класифікувати шаблон вхідної атаки. Неконтрольоване навчання використовується, коли дійсний набір даних недоступний. Кластеризація — це техніка неконтрольованого навчання, яка

призводить до групування подібних прикладів у кластери. Кластеризація використовується для виявлення шаблонів у даних. У деяких випадках кластеризація виконується для класифікації немаркованого набору даних і використання отриманого класифікованого набору даних для контрольованого навчання [22].

Оскільки загрози кібербезпеці постійно змінюються та розвиваються, необхідні автоматичні та негайні реакції. Таким чином, методи машинного навчання, особливо глибокого навчання, які не вимагають попередньої підготовки або покладаються на попередні класифікації, надані експертами, можуть бути особливо важливими при застосуванні підходів штучного інтелекту до кібербезпеки.

Нейронні мережі. Глибоке навчання.

Відсутність великих наборів даних про кібератаки є поширеною проблемою в дослідженнях кібербезпеки. Така ситуація зазвичай пояснюється вимогами конфіденційності, коли компанії не хочуть ділитися своїм досвідом атак, але в той же час база даних відомих загроз поступово заповнюється, що дозволяє застосовувати методи глибокого навчання. Основою таких методів є великі і часто незбалансовані набори даних, які часто використовуються для ручної кластеризації. У сфері кібербезпеки нейронна мережа може визначити, чи є документ зловмисним чи законним, без втручання людини. Ця технологія забезпечує кращі результати, ніж інші методи, і дозволяє виявляти шкідливі програми [23].

Дата майнінг.

Інтелектуальний аналіз даних — це пошук значущих закономірностей і тенденцій у великій базі даних. Методологія аналізу даних спрямована на отримання цінної інформації з великої кількості баз даних і виявлення прихованих закономірностей, які неможливо виявити статистичними методами. Машинне навчання — це широка сфера досліджень, яка включає бази даних, статистику, експертні системи, візуалізацію, високопродуктивні обчислення, нейронні мережі та методи представлення знань. Інтелектуальний аналіз даних працює за допомогою головного комп’ютера, який збирає дані різними способами (наприклад, кластеризація, класифікація, аналіз зв’язків, узагальнення, регресійні моделі та аналіз послідовності).

Основні приклади програм для дата майнінгу для кібербезпеки:

- методи виявлення атипових видів діяльності;
- аналіз посилань для відстеження вірусів;
- класифікація та групування декількох кібератак на основі їх профілів;
- прогнозування можливих майбутніх атак на основі отриманої інформації.

Розумні агенти

Інтелектуальний агент (ІА) — це автономна сутність, яка сканує датчики, контролює домени за допомогою приводів і координує свої дії для досягнення цілей. Розумний агент також може вивчати або використовувати інформацію для досягнення своїх цілей. Агенти можуть адаптуватися до реального часу, швидко вивчати нові речі, спілкуючись із середовищем, і мати можливість зберігати та відновлювати моделі на основі пам'яті. Як правило, інтелектуальні агенти використовуються для захисту від атак типу «відмова в обслуговуванні» (DoS/DDoS). Крім того, пошук необхідної інформації в мережі, розподілена обробка даних і т.д. Вони також ефективні в питаннях [24].

Застосування штучного інтелекту в кібербезпеці. Ступінь інтересу служб інформаційної безпеки до штучного інтелекту залежить від сфери застосування. Консалтингова компанія Capgemini опублікувала результати опитування, в якому взяли участь 850 топ-менеджерів з 10 країн (Австралія, Англія, Німеччина, Індія, Італія, Іспанія, Нідерланди, США, Франція, Швеція). При цьому 20% респондентів працювали IT-директорами, а 10% – керівниками служби IT-безпеки. Компанії представляли сім сфер діяльності: виробництво споживчих товарів, роздрібна торгівля, банківський сектор, страхування, автомобілебудування, житлово-комунальне господарство, телекомунікації. За даними Capgemini, якщо до 2019 року лише кожна п'ята організація використовувала ШІ для кібербезпеки, то до 2020 року його використовуватимуть понад 60% таких організацій. Майже половина (48%) респондентів заявили, що бюджети ШІ на кібербезпеку збільшаться в середньому на 29% у 2021 фінансовому році. Основними варіантами використання ШІ для кібербезпеки є безпека мережі та захист даних. Рішення IoT все ще відстають, але з'явилися лише в останні роки (табл. 2.1).

Таблиця 2.1 – Рівень фінансування сфер застосування засобів штучного інтелекту

№	Сфера застосування засобів ШІ	Ступінь використання фінансів на захист, %
1.	Мережева безпека	75
2.	Безпека даних	71
3.	Безпека кінцевих точок	68
4.	Безпека систем ідентифікації	65
5.	Безпека додатків	64
6.	Хмарна безпека	59
7.	Безпека Інтернету речей	53

Кількість атак на інформаційні системи з кожним роком стрімко зростає. При цьому атаки стають більш складними, а збиток від них вище. Потенційні цілі тепер включають мережеву інфраструктуру, пристрої IoT і розумні домашні пристрої. «Класичні» антивірусні засоби вже не можуть впоратися з такими спалахами, і на допомогу приходять рішення на основі штучного інтелекту.

Хоча це може здатися відмінним від сучасних рішень кібербезпеки, методи штучного інтелекту є більш надійними та гнучкими та можуть покращити захист від зростаючої кількості превентивних кіберзагроз. Однак, незважаючи на інтенсивні зміни, внесені штучним інтелектом у сферу кібербезпеки, відповідні системи ще не готові повністю адаптуватися до середовища та внести зміни у свою ситуацію. На сьогоднішній день штучний інтелект ще не став основним засобом безпеки. У той момент, коли людський інтелект планує атакувати розумну систему безпеки, система дає збій. У той же час це не означає, що ми не повинні використовувати методи штучного інтелекту в цілях збереження. Навпаки, ми повинні знати його межі і правильно їх використовувати.

2.3 Переваги та недоліки використання штучного інтелекту в кібербезпеці

Одне з основних застосувань штучного інтелекту в кібербезпеці — створення складних алгоритмів, які допомагають виявляти і запобігати кібератакам. Ці

алгоритми можуть оцінювати великі масиви даних і розпізнавати закономірності, які можуть свідчити про поточну або майбутню загрозу. Обробляючи цю інформацію на швидкостях і в масштабах, що перевищують людські можливості, системи ШІ можуть швидко виявляти потенційні та існуючі кіберзагрози і діяти швидко, істотно мінімізуючи ризики і наслідки кібератак. Крім того, ШІ може впорядкувати рутинні завдання з кібербезпеки, значно полегшуючи роботу IT-фахівців. Системи на основі штучного інтелекту можуть проводити автоматизоване сканування мереж на наявність вразливостей, виявляти загрози і навіть впроваджувати заходи зі зниження ризиків, наприклад, встановлювати виправлення для програмного забезпечення або блокувати шкідливі IP-адреси. Такий рівень автоматизації не лише підвищує ефективність, але й забезпечує послідовний підхід до практик кібербезпеки [25].

Ще одним ключовим застосуванням штучного інтелекту в кібербезпеці є систематизація розвідувальної та оперативної інформації про кіберзагрози. Використовуючи методи машинного навчання, системи штучного інтелекту можуть швидко досліджувати великі масиви даних з таких джерел, як додатки для обміну повідомленнями, соціальні мережі, потоки електронної пошти, канали Telegram, форуми в темному інтернеті тощо, щоб виявити загрозливі тенденції та вразливості. Такий аналіз у режимі реального часу дозволяє вам бути на крок попереду і коригувати свої стратегії кібербезпеки, щоб передбачити ситуації та ризики. Крім того, штучний інтелект часто використовується для покращення реагування на інциденти шляхом виявлення та припинення кіберзагроз. З огляду на потенційні наслідки кібератак, моніторинг і мінімізація збитків мають вирішальне значення для підтримки належного функціонування комп'ютерного обладнання та систем. Технології штучного інтелекту дозволяють аналізувати характер і особливості кібератаки, оцінювати вразливість системи та розробляти оптимальні заходи реагування для локалізації та вирішення проблем. Це створює можливості для зменшення негативних наслідків кібератак та їх впливу на нормальне функціонування інформаційно-комунікаційних систем, а також організацій державного та приватного секторів [26].

Однією з головних переваг ШІ є його здатність швидко та ефективно аналізувати великі масиви даних. ШІ може швидко оцінювати величезні обсяги даних, які людина не може швидко обробити. Це дає змогу виявляти загрози на ранніх стадіях і швидко підтверджувати рішення щодо їхнього запобігання та блокування. Штучний інтелект також допомагає спростити процес виявлення та реагування на кібератаки. Він може безперервно моніторити мережі в режимі 24/7, щоб виявити аномальну поведінку, яка може свідчити про кібератаку. Крім того, ШІ може автоматично реагувати на загрози, запобігаючи доступу хакерів до систем і захищаючи від витоку конфіденційних даних.

Ще одним ключовим аспектом використання ШІ в кібербезпеці є його здатність застосовувати машинне навчання на основі попереднього досвіду. ШІ може використовувати дані попередніх кібератак для вдосконалення своїх алгоритмів і підвищення точності виявлення ризиків і загроз у майбутньому. ШІ сприяє ефективному захисту від автоматизованих або цілеспрямованих кібератак. Зрозуміло, що ШІ є життєво важливим і ефективним інструментом у боротьбі з кіберзагрозами, але він не може повністю замінити людський нагляд. Хоча дехто вважає, що інтелектуальні системи позбавлені людських помилок: вони працюють швидше за людей і роблять менше помилок, що дозволяє майже повністю усунути людину від процесів захисту, залишивши їй лише завдання моніторингу та корекції. Однак, хоча ШІ може допомогти автоматизувати ідентифікацію та реагування на кіберзагрози, ми вважаємо, що остаточні рішення щодо безпеки та забезпечення комплаєнсу все ще залишаються за людиною. Іншими словами, ШІ значно допомагає кібербезпеці, але не може повністю замінити людський фактор. ШІ збільшує масштаб і швидкість кібербезпеки, забезпечуючи ефективний захист від кібератак і загроз [27].

Алгоритми ШІ можуть революціонізувати виявлення нових кібератак, посилити захист систем, передбачити сценарії, пов'язані з появою нових вразливостей, створити нові та більш досконалі методи захисту від шкідливого програмного забезпечення тощо. Таким чином, ШІ спрощує управління мережевою безпекою, зводячи до мінімуму помилки та недогляди без шкоди для якості. Це робить ШІ потужним інструментом захисту від кібератак. ШІ підтримує команди

реагування на інциденти (CERT) у створенні потужних людино-машинних сервісів і спільних проектів, розширюючи знання, навички та можливості для зміцнення кібербезпеки та покращення кіберзахисту. Завдяки ШІ стає можливим прогнозування загроз і отримання розвідданих про кіберподії в режимі реального часу.

Основним пріоритетом у використанні ШІ для кібербезпеки є здатність передбачати кібератаки ще до того, як вони повністю матеріалізуються, що дозволяє вчасно посилити захист. Ще однією перевагою є мінімізація людського фактору, тобто ШІ не піддається різним психологічним впливам або втомі. Реакція автоматизованих AI-систем безпеки на кіберзагрози відбувається швидше і знижує ризик людської помилки. Таким чином, ШІ допомагає керувати небезпекою та попереджати про неї, виявляти загрози та реагувати на них у режимі реального часу, визначати пріоритетність потенційних ризиків, а також знаходити можливості та ресурси для протидії реальним і потенційним загрозам. Це підкреслює значний потенціал ШІ для посилення кібербезпеки [28].

Крім того, технології штучного інтелекту можна використовувати для виявлення вразливостей безпеки в системах і мережах, дозволяючи їх заздалегідь усунути. Загалом використання штучного інтелекту в кібербезпеці допомагає бути на крок попереду проти кіберзагроз. За цих умов штучний інтелект може революціонізувати підхід до вирішення складних проблем у сфері кібербезпеки та стати її невід’ємною частиною. Системи штучного інтелекту можна навіть навчити розпізнавати поведінкові аномалії та попереджати про небезпеку, виявляти нові штами зловмисного програмного забезпечення та захищати важливі дані.

Трансформації та динамічний розвиток передових технологій змінюють цифровий світ, включаючи інструменти та тактику кібербезпеки. Важливою сучасною подією стало відкриття нового генеративного інструменту штучного інтелекту ChatGPT (Generative Pre-trained Transformer) у листопаді 2022 року. Це чат-бот зі штучним інтелектом, розроблений OpenAI, дослідницькою установою, яка вивчає та спеціалізується на штучному інтелекті та зробила революційний крок у своєму розвитку. Може складати тексти на задані теми та відповідати на запитання зрозумілою мовою. Випуск чат-бота ChatGPT став революційним кроком у сфері

технологій і дав поштовх для активного розвитку продуктів штучного інтелекту. Водночас зростає ризик дезінформації, а персональні дані користувачів можуть опинитися під загрозою. Сучасна генеративна технологія штучного інтелекту, яка може генерувати текст із текстових підказок, захопила громадськість із моменту запуску чат-бота ChatGPT понад шість місяців потому та стала додатком, який швидко зростає у всьому світі. На цьому тлі штучний інтелект став причиною занепокоєння через його здатність створювати підроблені зображення та іншу дезінформацію. У січні 2023 року кількість активних користувачів ChatGPT досягла 100 мільйонів. Спочатку цей чат-бот був доступний безкоштовно, пізніше компанія оголосила про запуск підписки на ChatGPT за 20 доларів у США. Розробник чат-бота заборонив деяким країнам користуватися його сервісами через введені санкції, тому в РФ він поки недоступний. 18 лютого 2023 року Міністр цифрової трансформації України М.Федоров повідомив, що ChatGPT доступний в Україні, але ця програма не працюватиме на тимчасово окупованій Російською Федерацією території України, щоб не допустити її використання військовим агресором [29].

Таким чином, штучний інтелект може успішно допомагати захищатися від кібератак за допомогою: автоматичного виявлення загроз за допомогою алгоритмів машинного навчання та результатів виявлення проблем у функціонуванні систем, які можуть свідчити про порушення безпеки; машинне навчання використовується для аналізу великих обсягів даних і прогнозування розвитку ситуації на основі виявлених вразливостей і шаблонів, що дозволяє навчити системи штучного інтелекту розпізнавати невідомі або непередбачувані атаки; Прогностична аналітика надає можливість передбачити майбутні загрози, наприклад облікові дані працівників, які, швидше за все, будуть скомпрометовані та які типи атак можуть відбутися в певний день, допомагаючи заздалегідь визначити потенційні проблеми та визначити, де вони знаходяться в системі. блокувати заздалегідь; Виявлення аномалій у мережевому трафіку чи інших потоках даних шляхом аналізу шаблонів ідентичності або відмінностей між ними. Цей тип моніторингу допомагає виявити аномальну поведінку до того, як вона переросте в майбутню шкідливу діяльність; автоматизація безпеки та шахрайство чи фішинг тощо. Впровадження нових політик безпеки та

протоколів, які захищають від кібератак, таких як загрози. Автоматизація безпеки економить час і кошти; Значне зменшення помилок, спричинених людським фактором, і забезпечення економічно ефективних рішень зі 100% точністю [30].

Застосування технологій штучного інтелекту в кібервійні є дуже важливим. Моніторинг інтернет-ресурсів у соціальних мережах та електронних ЗМІ, особливо за допомогою штучного інтелекту, дозволяє виявляти дезінформацію, таємну російську пропаганду, системні тенденції та проблеми та завчасно вживати заходів. В умовах кібервійни Україна має активізувати зусилля для підтримки своїх національних інтересів шляхом використання сучасних інформаційних технологій та алгоритмів штучного інтелекту для забезпечення національної безпеки України. На тлі описаного позитивного досвіду використання технологій штучного інтелекту в забезпеченні кібербезпеки та наявності його незаперечних переваг ця технологія не позбавлена проблем і недоліків.

Одна з головних проблем полягає в тому, що кіберзлочинці та хакери можуть використовувати технології штучного інтелекту для створення більш складних і цілеспрямованих атак. Як наслідок, ретельно сплановані кібератаки з використанням технологій штучного інтелекту становлять сьогодні значну глобальну загрозу. Це свідчить про те, що хакери та кіберзлочинці можуть використовувати ці технології для здійснення потужних та інноваційних кібератак. Наприклад, шкідливе програмне забезпечення зі штучним інтелектом може навчатися та адаптуватися, щоб уникнути виявлення традиційними засобами мережевої безпеки. Кіберзлочинці можуть використовувати ШІ для виявлення закономірностей, що вказують на вразливість програмного забезпечення в комп'ютерних мережах, дозволяючи хакерам виявляти і використовувати ці вразливості на власний розсуд. Підписи шкідливого програмного забезпечення постійно змінюються, що дозволяє зловмисникам обходити статичні засоби захисту, такі як брандмауери та системи виявлення периметра. Так само шкідливе програмне забезпечення на основі штучного інтелекту може затримуватися в системі, збираючи дані та відстежуючи поведінку користувачів, поки не буде готове розпочати нову фазу атаки. Враховуючи економічну динаміку кібератак, зловмисники знають, що проводити атаки часто простіше і дешевше, ніж розробляти

ефективний захист. Крім того, ШІ є інноваційною технологією, яка створює нові кіберзагрози [31].

За допомогою штучного інтелекту, зокрема нейронних мереж, стало можливим створювати високоякісні зображення, відео- та аудіоконтент, призначені для введення в оману пересічних користувачів і маніпулювання системами розпізнавання облич. Ця техніка маніпуляції зображеннями за допомогою штучного інтелекту, відома як "глибокий фейк", успішно використовується для шахрайських схем та інших незаконних дій. Це шкідливе програмне забезпечення дозволяє кіберзлочинцям видавати себе за іншу людину, імітуючи її зовнішність, вираз обличчя та голос. Наприклад, в одному гучному кейсі керівник відділу компанії отримав телефонний дзвінок від сторонньої особи, яка, використовуючи голос генерального директора, попросила переказати 220 000 євро, які були відправлені шахраю. Експерти з кібербезпеки Check Point Research виявили, що хакери знайшли спосіб використовувати чат-бот ChatGPT для створення шкідливого програмного забезпечення та фішингових електронних листів. Раніше кібер-експерти Check Point Research використовували ChatGPT для пошуку скомпрометованих облікових даних, реквізитів платіжних карт, шкідливого програмного забезпечення та інших незаконних товарів. Вони також виявили, що можна створити скрипт даркнет-ринку, на якому цими товарами можна буде торгувати.

Це означає, що хакери можуть використовувати штучний інтелект для обходу систем захисту та створення складніших і досконаліших кібератак. У цьому контексті було б доречно забезпечити захист даних і алгоритмів штучного інтелекту від кібератак і злому. Хакери можуть використовувати шкідливі алгоритми для введення в систему ШІ, щоб обійти системи захисту. З цієї причини необхідно посилити заходи щодо захисту систем, що працюють на основі штучного інтелекту, і проводити регулярні перевірки на наявність вразливостей. Також необхідно навчити ШІ різним кібератакам і кіберзагрозам, використовуючи при цьому актуальні дані про нові види і види. За цих умов для індустрії кібербезпеки важливо випереджати ці події та постійно впроваджувати інновації проти нових загроз. Тобто постійно актуальним є завдання посилення кіберзахисту на основі нового формату нових сучасних

технологій, що динамічно розвиваються, що породжує нові загрози. На даний момент не існує надійного та універсального методу захисту від кібератак на системи штучного інтелекту. Тому будь-яке використання технологій штучного інтелекту може принести користь і водночас створити нові потужні загрози та виклики [32].

Тому світова спільнота активно зацікавлена у поширенні та впровадженні та регулюванні технологій штучного інтелекту у сфері кібербезпеки. Як наслідок, необхідність правового регулювання, особливо з точки зору нагляду за штучним інтелектом, стає головною темою для обговорення в усьому світі. Це питання залишається відкритим, оскільки не існує міжнародних керівних принципів або правових структур для використання ШІ. Оскільки рішення на основі штучного інтелекту можуть порушувати права людини на недоторканність приватного життя, життєво важливо звернути увагу на організаційні та правові аспекти використання ШІ в кібербезпеці. Оскільки уряди провідних країн світу розробляють свою політику щодо ШІ в різних секторах, існує нагальна потреба в етичних настановах і правових стандартах для управління використанням ШІ в кібербезпеці. Тому розробка та вдосконалення законодавства, що регулює технології штучного інтелекту, є ключовим пріоритетом для країн G7. ШІ несе в собі певні ризики для безпеки, оскільки він може продукувати неправдиві новини та спричиняти суспільні потрясіння, якщо вихідні дані є невірними. Тому регулювання галузі штучного інтелекту на законодавчому рівні та створення відкритого середовища для її розвитку на основі демократичних цінностей і принципів є вкрай важливим.

Не можна без перебільшення недооцінювати роль і значення штучного інтелекту в забезпеченні кібербезпеки. Штучний інтелект стає невід’ємною частиною сучасної архітектури кібербезпеки. У зв'язку з динамічним і перспективним розвитком передових технологій штучний інтелект широко використовується для виявлення кіберзагроз, створення ефективних механізмів захисту від кібератак і підтвердження оперативних управлінських рішень. Можливості штучного інтелекту сприяють вдосконаленню процесів моніторингу змін у середовищі загроз на кіберфронті, виявленню кібератак і покращенню стану кібербезпеки в цілому. Технології штучного інтелекту дозволяють постійно автоматизувати процеси

сканування мереж для виявлення та реагування на кібератаки. Повністю виключити людський фактор при використанні штучного інтелекту у сфері кібербезпеки абсолютно неможливо, оскільки остаточне рішення щодо результатів використання штучного інтелекту належить людині. Отже, ШІ допомагає людині, але не замінює її [33].

Висновки до розділу 2

Штучний інтелект відіграє важливу роль в кібербезпеці, допомагаючи організаціям знижувати ризики і збільшувати доходи. ШІ може виявляти кіберзагрози і шахрайство, а також допомагати у виявленні і реагуванні на нові віруси та зловмисне програмне забезпечення. Штучний інтелект може ефективніше виявляти зловмисне програмне забезпечення, ніж людина, і впроваджується в організаціях для поліпшення виявлення загроз і керування інцидентами. Очікується, що витрати на системи кібербезпеки будуть зростати, а ринок інструментів штучного інтелекту для кібербезпеки буде зростати на 23,3% на рік. Технології штучного інтелекту можуть допомогти забезпечити безпечну передачу даних і боротьбу з кіберзлочинністю. Виявлення порушень цілісності даних в ранній стадії може допомогти зменшити вартість їх відновлення, а автоматизація безпеки та інтелектуальні інструменти можуть покращити здатність організацій зменшувати шкоду від злому.

Методи штучного інтелекту в кібербезпеці включають в себе різні підходи, такі як чат-боти, експертні системи, машинне навчання, нейронні мережі, дата майнінг та розумні агенти. Ці методи дозволяють виявляти та усувати кіберзагрози, а також роблять прогнози щодо майбутніх атак. Використання штучного інтелекту в кібербезпеці дозволяє підвищити рівень захисту від кібератак та зменшити можливі втрати від них. Однак, необхідно пам'ятати про обмеження та межі використання штучного інтелекту в цілях забезпечення безпеки, а також про необхідність постійного вдосконалення та адаптації систем до змінюючихся умов.

Штучний інтелект допомагає підвищити ефективність захисту від кібератак, але водночас створює нові виклики та загрози, які потребують постійного вдосконалення

та регулювання. Тому важливо розвивати етичні та правові стандарти для використання штучного інтелекту в кібербезпеці, щоб забезпечити безпеку та прозорість в цій сфері.

РОЗДІЛ 3
КІБЕРЗАГРОЗИ ТА ЇХ АНАЛІЗ

3.1 Класифікація кіберзагроз

Враховуючи ключову роль і присутність інформаційних комунікацій та різноманітних електронних пристроїв і програмних продуктів у житті сучасних високотехнологічних суспільств у всьому світі, впровадження інформаційних технологій та інтенсифікація інформаційних процесів стали майже повсюдними. Зрозуміло, що IT-інновації проникли в усі сфери життя, а кіберзагрози та їхні прояви зберігатимуться й надалі. Таким чином, розуміння обсягу загроз, на які необхідно звернути увагу при створенні ефективної системи кібербезпеки, має вирішальне значення. Водночас процес ідентифікації кіберзагроз потребує всебічного аналізу їх характеру та подальшої категоризації зібраної інформації. З огляду на те, що кіберзагрози можуть бути найрізноманітнішими за своєю природою — від молодіжного вандалізму до складних урядових кібероперацій, існує нагальна потреба чітко класифікувати ці загрози за різними критеріями. При цьому слід акцентувати увагу на тому, що хоча спектр кіберзагроз у цифровому світі відносно обмежений, діапазон їх потенційних проявів практично необмежений. Систематизація потенційних кіберзагроз за певними класифікаційними ознаками дозволить забезпечити необхідний рівень конфіденційності при їх ідентифікації та закласти підґрунтя для ефективних заходів протидії [34].

Загальноприйняті методи класифікації кіберзагроз здебільшого передбачають їх поділ на інформаційні загрози, загрози інформаційній безпеці або загрози розподіленим системам обробки даних, серед інших типів. По суті, ці класифікації акцентують увагу на оцінці загроз на основі їх інформаційного аспекту, а не кібернетичної складової. Така ситуація виникає через відсутність чіткого розуміння визначення кіберзагроз.

Кіберзагроза — це реальна або потенційна дія чи чинник, що створює небезпеку життєво важливим національним інтересам України у кібернетичному просторі, негативно впливає на кібернетичну безпеку держави, кібернетичну захищеність та захищеність її ресурсів.

Виходячи зі встановлених критеріїв, кожна кіберзагроза повинна мати наступні характеристики:

- Об'єктом загрози є власник або представник інтересу, який потребує захисту.
- Джерелом загрози є іноземні держави, вітчизняні та іноземні організації, групи осіб, самоорганізовані технічні системи та інші, дії (функції) яких можуть негативно вплинути на інтереси об'єкта в будь-якій сфері.
- Методи та засоби реалізації загроз передбачають дію або серію скоординованих дій, які можуть завдати шкоди інтересам об'єкта захисту.
- Причини кіберзагроз охоплюють комплексну характеристику, яка поєднує наявність відповідних можливостей і намірів джерела загрози з уразливістю об'єктів, що захищаються.
- Потенційні наслідки або негативні впливи від реалізації загрози включають шкідливі зміни або відсутність позитивних змін у стані об'єкта захисту, які відповідають меті та цілям загрози.

Упорядкування цих характеристик дозволяє узагальнити їх у загальній схемі, як показано на рис. 3.1.

На основі наведеного визначення кіберзагроз та враховуючи особливості функціонування комп’ютерних (інформаційних) систем застосовано їх класифікацію за такими ознаками:

- тип кібернетичної системи (КС), на яку спрямована кіберзагроза;
- елемент КС, спрямований безпосередньо на реалізацію кіберзагроз;
- використовувані уразливості (системи та її елементів);
- місцезнаходження джерела (суб’єкта) кіберзагроз;
- спосіб реалізації кіберзагроз;
- середовище розповсюдження;

– навмисність;
– походження;
– повторення зовнішнього вигляду;
– приховування прояву;
– масштаби наслідків реалізації загрози;
– Ієрархія управління в КС;
– доцільність реалізації кіберзагроз;
– час виникнення кіберзагроз;
– умовність застосування.

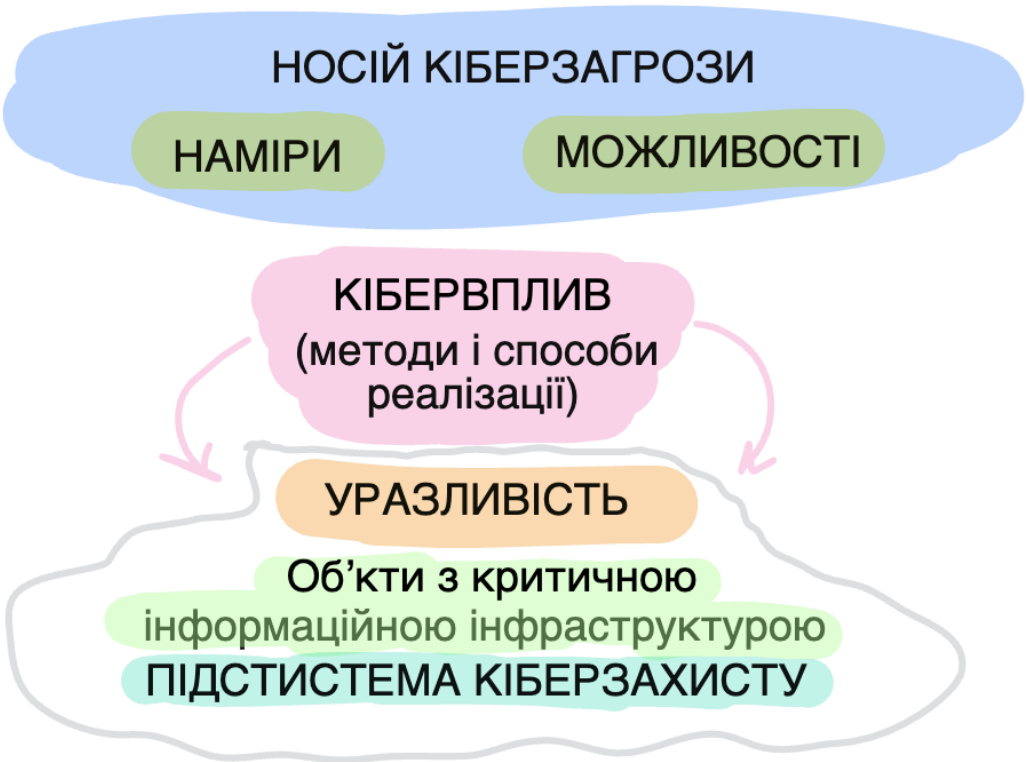

Рисунок. 3.1 – Узагальнена схема ознак кіберзагрози

Розглянемо кожен знак докладніше.

За видом КС (її фізичною природою), на яку спрямовані кіберзагрози, розрізняють:

– технічні;
– біологічні;

– соціальні;
– комбіновані.

Варто зазначити, що тип КС, що підлягає захисту, значно обмежує не лише обсяг потенційних загроз, але й можливі заходи протидії таким загрозам. Так, наприклад, розглядаючи суто технічну КС, загрози біологічного чи соціального характеру можна ігнорувати; це зменшить перелік можливих засобів захисту та протидії [35].

Відповідно до елемента КС, на який безпосередньо спрямовано (або які кіберзагрози здійснюються), можна виділити наступні класи загроз:

– загрози об’єкту управління;
– загрози управлінському питанню;
– загрози каналу передачі даних;
– комплексні загрози.

Класифікація такої ознаки, як елемент КС, на який спрямована загроза, дає змогу підвищити ефективність протидії за рахунок раціонального використання сил і засобів (ресурсів) для захисту. Завчасна концентрація ресурсів захисту на певному компоненті системи безпеки під загрозою дозволяє забезпечити необхідний рівень захисту всієї системи з найменшими витратами.

Залежно від використовуваних уразливостей (системи та її елементів) виникають такі загрози:

– загрози через уразливості компонентів КС;
– загрози, що виникли внаслідок використання вразливостей підсистеми захисту КС (якщо така підсистема існує);
– загрози, реалізовані з використанням недоліків в алгоритмах керування та обробки інформації (сигналів).

Класифікація загроз за використовуваною вразливістю дозволяє підвищити точність локалізації загроз і мінімізувати витрати на впровадження заходів захисту КС.

Загрози слід розрізняти за розташуванням джерела (суб’єкта) кіберзагроз відносно цілі:

– системи, які взаємодіють з КС, можуть слугувати джерелами зовнішніх загроз, тоді як компоненти цих систем можуть бути джерелами внутрішніх загроз.

Зовнішні кіберзагрози можна розділити на дві категорії: загрози з боку операційного середовища КС та загрози з боку конкуруючих (ворожих) систем. До першої категорії належать такі загрози, як стихійні лиха та революції. Прикладом другої категорії загроз є загрози з боку протиборчих сторін у військовому конфлікті.

Клас внутрішніх кіберзагроз поділяється на гілки залежно від конкретного складу КС. Наприклад, внутрішні кіберзагрози для сучасних систем управління інформацією можуть включати загрози з боку носіїв інформації; технічних пристроїв; програмного забезпечення; засобів захисту інформації (апаратних, алгоритмічних, програмних); оператора (обслуговуючого персоналу) та ін.

Раннє виявлення джерела загрози дозволяє вжити активних (превентивних) заходів щодо неї [36].

Спосіб реалізації кіберзагроз залежить від конкретного об'єкта та його характеристик (технічних, соціальних, біологічних, психологічних), але загалом виділяють такі типи загроз:

– загрози, пов'язані з активним втручанням у функціональність КС (активні кіберзагрози);
– загрози, що безпосередньо не впливають на діяльність КС (пасивні кіберзагрози);
– загрози з комплексним впливом.

Залежно від середовища, через яке поширюються загрози, існують класи, що відповідають існуючим небезпечним середовищам:

– інформаційні;
– комунікаційні;
– комп'ютерно-мережеві;
– соціотехнічні.

Середовище, в якому поширюються кіберзагрози, впливає і на методи протидії їм. Наприклад, фізичне знищення каналів зв'язку для захисту від атаки типу "відмова

в обслуговуванні" може бути недоцільним (хоча й можливим), але може вважатися ефективним проти превентивного удару противника, який готується до збройного нападу.

Загрози можна класифікувати за намірами:

– навмисні;
– ненавмисні.

Навмисні загрози передбачають свідомий намір завдати шкоди КС або її елементам, тоді як ненавмисні загрози виникають незалежно від волі джерела загрози.

Загрози також можна класифікувати за походженням:

– створені людиною (антропогенні, техногенні);
– природні.

Техногенні загрози виникають внаслідок людської діяльності або функціонування технічних систем, тоді як природні загрози є наслідком природних процесів, що відбуваються в живому та неживому середовищі.

Загрози можна класифікувати за частотою виникнення:

– періодичні (періодичні, аперіодичні);
– неперіодичні.

Класифікація загроз як періодичних дозволяє в майбутньому вживати більш ефективних заходів протидії шляхом створення профілю загрози та впровадження перевіреного алгоритму протидії. Неперіодичні загрози вимагають більше ресурсів для пом'якшення наслідків через необхідність додаткового вивчення та моделювання. Частота може бути визначена, наприклад, як кількість разів, коли певна кіберзагроза виникає протягом певного періоду [37].

Залежно від видимості загрози, загрози можна класифікувати на такі категорії

– приховані;
– неприховані.

Рівень прихованості загроз визначає складність алгоритмів ідентифікації, що впливає на час, необхідний для виявлення загрози, і в кінцевому підсумку визначає ймовірність її виявлення в прийнятні терміни.

Реалізація однієї або комбінації кіберзагроз з наведених вище категорій може призвести до різного масштабу наслідків для КС або її компонентів. Відповідно, кіберзагрози можна класифікувати:

– локальні;
– частково системні;
– загальносистемні.

Локальні загрози характеризуються незначними порушеннями функціонування окремого елементу КС, які не впливають на загальну роботу КС.

Загрози частково системного характеру призводять до виходу з ладу якогось елемента або частини КС; Це може негативно вплинути на виконання деяких функцій КС або її призначення в цілому, з можливістю відновлення ураженої ділянки.

Загальносистемні загрози спрямовані на пошкодження різних частин або ключових елементів системи; Це неминуче призводить до виходу з ладу КС в цілому, без можливості відновлення її роботи [38].

Відповідно до ієрархії управління в КС кіберзагрози виділяються:−на вищому (стратегічному) рівні;

– середнього (оперативного) рівня;− нижчого (тактичного) рівня.

Головним фактором, що впливає на ймовірність конкретної кіберзагрози, є її залежність від конкретних подій. Тобто реалізація одних кіберзагроз можлива лише за умови відповідної позитивної події (чи набору подій), тоді як реалізація інших не потребує виконання такої умови.

Відповідно, ми розділимо кіберзагрози відповідно до правил застосування:

– умовний;
– безумовний.

За часом виникнення кіберзагрози виділимо:

– загрози, закладені у створенні КС;
– загрози, які виникають під час функціонування КС.

Недоліки в проектуванні та плануванні CS або її власних компонентів є слабкими місцями, які можуть бути використані для порушення надійної роботи системи. Такі вразливості виникають під час роботи системи або виявляються під час

її роботи (для комп’ютерних систем це «загрози нульового дня»). Виявлення вразливостей, введених у роботу КС, дозволяє значно підвищити захист таких систем від кіберзагроз на ранніх етапах експлуатації. Уразливості, які з’являються з часом, є більш небезпечними, оскільки їх важко передбачити або передбачити, що ускладнює протидію загрозам, які використовують такі вразливості [39].

Характеристичний принцип, який використовується в класифікації кіберзагроз, дозволяє описати будь-яку загрозу набором якісних і кількісних характеристик, які можна використовувати для моделювання та подальшого опису такої загрози.

Класифікація кіберзагроз надає можливість поділу на підкласи та гілки, що дуже корисно при розробці списку загроз для кожної конкретної КС, пов’язаної з необхідним рівнем деталізації.

3.2 Стратегії ідентифікації кіберзагроз

Останнім часом суспільство все частіше стикається з різними видами кібератак: збої в наданні електронних по слуг, перешкоджання роботі державних установ, фішингові атаки через електронну пошту, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційно-психологічний тиск. про населення, кібертероризм, кібершпигунство, поширення інформації в національний інформаційний простір країни, перешкоджання діяльності або знищення підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки для економіки та безпеки країни [39].

Для зміцнення кібербезпеки та підготовки до пом'якшення соціальної агресії в кіберпросторі Україна вжила низку заходів, що стосуються стратегічних, правових, політичних, технічних та організаційних аспектів забезпечення кібербезпеки (рис. 3.2).

Рисунок. 3.2 – Комплекс реалізованих заходів з безпечного функціонування кіберпростору станом на 2019 рік

Стратегічна політика у сфері кібербезпеки

Життєво важливим компонентом соціально-економічної безпеки будь-якої країни є Національна стратегія кібербезпеки (НСК). Україна представила свою Стратегію кібербезпеки 27 січня 2016 року. Кібербезпека та інформаційна безпека є ключовими у запобіганні загрозам національній безпеці. Деталі реалізації Стратегії кібербезпеки викладені в щорічних планах уряду, де органи влади визначають кроки для запобігання та реагування на кіберінциденти, які можуть сприяти створенню системи національної безпеки. Для нагляду та управління роботою різних суб'єктів у сфері кібербезпеки були створені окремі державні служби з конкретними функціями для досягнення цілей кібербезпеки:

– створено спеціальну управлінську структуру для координації співпраці між державними органами. Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України здійснює безпосередній нагляд за захистом і безпекою України від кібератак. Він здійснює

моніторинг подій у критичних інформаційно-телекомунікаційних системах з метою підвищення ефективності систем державного управління у формуванні та реалізації державної політики у сфері кібербезпеки відповідно до Стратегії кібербезпеки Великої Британії [40].

– діяльність органу державної влади у сфері протидії кіберзлочинності, кіберзахисту конфіденційних даних, формування та реалізації відповідної державної політики. Заходи щодо захисту державних інформаційних ресурсів та інформації в кіберпросторі покладаються на Державну службу безпеки персонального зв'язку та Інформація України (ССЗІ) – це особа, яка координує діяльність відділу кібербезпеки з питань кібербезпеки та вживає організаційних і технічних заходів щодо запобігання, виявлення та реагування на кіберінциденти та кібератаки та ліквідації їх наслідків. ДССЖІ контролює роботу Групи реагування на комп'ютерні надзвичайні ситуації Уряду України (CERT-UA) та Державного центру кіберзахисту, які реалізують організаційно-технічний план кібербезпеки в рамках кібербезпеки система безпеки.
– враховуючи існуючу потребу в захисті персональних даних громадян в тій же мірі, що і конфіденційних даних компаній, Україна створила незалежний державний регуляторний орган відповідно до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Нагляд за дотриманням законодавства про захист персональних даних здійснює Уповноважений Верховної Ради України з прав людини.

Глобальний загальний. З метою посилення міжнародного співробітництва та інтеграції регуляторних елементів у сфері кібербезпеки відповідно до міжнародних стандартів та стандартів ЄС і НАТО Україна прийняла Конвенцію Ради Європи про кіберзлочинність та інші міжнародні угоди. За підтримки Трастового фонду НАТО в СБУ та СБУ створено ситуаційні центри [9], завданням яких є виявлення, запобігання та ліквідація кібератак на Україну. Тому в Національній поліції України працює Національний контактний пункт, який працює в режимі 24/7 з реагування на

комп'ютерні злочини та обмін інформацією. З метою посилення стабільності критично важливих систем кібербезпеки Уряд України регулярно бере участь у міжнародному співробітництві у відповідь на кіберінциденти, надаючи інформацію про хороші міжнародні знання та алгоритми реагування на нові кіберінциденти. Посилення повноважень України у цій сфері відбулося за рахунок розвитку міжнародного співробітництва у сфері кібербезпеки, участі у заходах із зміцнення довіри в кіберпросторі, що здійснюються під контролем ОБСЄ, поглиблення співпраці України з ЄС та НАТО. Забезпечення кібербезпеки та дотримання національних інтересів. У процесі співпраці з міжнародними організаціями, пов'язаними з реагуванням на кіберінциденти, було організовано надзвичайні ситуації за участю України у FIRST Incident Response and Security Teams Forum, де приєднується до команд CERT (Computer Emergency Response Team) у країнах Європи [41].

Освітні програми з кібербезпеки. Оскільки кіберзагрози не можна обмежити якоюсь однією сферою, усі зацікавлені сторони повинні знати про фактори ризику, мати навички та можливості для їх усунення та вживати відповідних заходів для їх запобігання під час завантаження. Україна активно співпрацює з провідними організаціями для підвищення обізнаності про кібербезпеку на всіх рівнях комерційних і некомерційних організацій.

Політичний рівень. Основними завданнями, які стоять перед державними органами України у сфері перевірки інформації та цифрового контролю є: моніторинг інформаційних точок; дотримання законодавства щодо права на інформацію; виконання законів, що регулюють фільтрацію вмісту в Інтернеті; недопущення використання новітніх інформаційних технологій для поширення шкідливих для суспільства ідей і звинувачень (расизм, шовінізм, радикальний націоналізм); правовий захист національної культури та мови від контролю країн знання; Знайти сприйнятий громадськістю баланс між свободою вираження поглядів і поширення інформації та необхідністю держави забезпечувати політичну свободу; запобігати культурній експансії інших онлайн-ресурсів; перетворення державних органів на використання програмно-технічного забезпечення їх розробки та виробництва.

Необхідно приділяти увагу аналізу національної стратегічної ситуації щодо кіберзагроз, дані про відповідні події необхідно збирати та поширювати регулярно, принаймні раз на рік, для більш ефективного реагування, створювати публічні звіти про кіберзагрози та публікувати їх у своєчасно. відповідний веб-сайт.

Міжнародна співпраця. Країні необхідно активізувати участь у зміцненні взаємної довіри у сфері кібербезпеки та виробленні спільних підходів проти кіберзагроз, консолідації зусиль щодо розслідування та запобігання кіберзлочинам, запобігання використанню кіберпростору в протиправних і військових цілях. В організації спільних міжнародних проектів, спрямованих на створення кіберпотенціалу [25].

Сучасний ландшафт загроз підкреслює нагальну необхідність співпраці між країнами для запобігання поточних онлайн-загроз, покращення розслідувань, вирішення проблем та переслідування правопорушників, долаючи таким чином перешкоди у сфері кібербезпеки. З огляду на глобальний взаємозв'язок сучасних суспільств і значні економічні та соціальні виклики, які створюють кібератаки, міжнародні зусилля мають бути об'єднані та адаптовані для зміцнення кібербезпеки та захисту важливих інформаційних систем у світлі переходу до цифрової економіки та інформаційного суспільства.

Навчальний захід з кібербезпеки. Важливо підвищити обізнаність щодо кібербезпеки на всіх рівнях, починаючи від роботи центрів комп’ютерної безпеки і закінчуючи впровадженням програм навчання комп’ютерній безпеці. У сфері інформування громадськості слід розробити та впровадити навчальні програми з комп’ютерної безпеки не лише у вищій, але й у початковій та середній освіті.

У сьогоднішньому небезпечному середовищі кіберпростору організаціям необхідно змінити свій підхід до кібербезпеки. Це вимагає підвищення обізнаності щодо важливості інвестування в кібербезпеку як невід’ємної частини будь-якої національної стратегії розвитку ІКТ.

Організаційний рівень. У нинішній політичній ситуації надзвичайно важливим є посилення кібербезпеки виборчих систем та критичної інфраструктури, сприяння

реалізації Стратегії кібербезпеки України та посилення реагування на кіберінциденти [43].

Рекомендується докладати більше зусиль для встановлення державно-приватного партнерства, а також для розробки та впровадження механізму обміну інформацією між державними установами, приватним сектором та громадянами щодо загроз критичній інформаційній інфраструктурі. Для своєчасного реагування на кіберінциденти та впровадження практичних заходів, які посилять оволодіння ситуацією в кіберпросторі, важливо організувати тренінги для висококваліфікованих спеціалістів у сфері кібербезпеки та цифрової криміналістики за участю міжнародних експерти.

Компанії критичної інфраструктури повинні дотримуватися принципу «безпека перш за все». Оскільки понад 90% несанкціонованого доступу, пошкоджень і атак викликані людським фактором, компаніям необхідно запровадити прості нормативні правила, щоб мінімізувати можливі джерела загроз і збитків, наскільки це можливо.

Науково-технічний рівень: Передбачає організацію та керівництво науковими дослідженнями і розробками в галузі комп'ютерної безпеки, розвиток інформаційних технологій, використання математичних методів для багатовимірних даних, розробку технологій комплексного захисту апаратного та програмного забезпечення. Вона також включає створення технологій для виявлення ознак пошкодження пасивними методами. Ця стратегія повинна здійснювати моніторинг кібератак, створювати інструменти управління системами для протидії масштабним організованим атакам, забезпечувати раннє попередження про атаки та ідентифікувати джерело атаки.

Таким чином, вирішення проблеми кібербезпеки потребує цілісного підходу та скоординованих зусиль державних органів, приватного сектору та громадянського суспільства на національному, регіональному та міжнародному рівнях для захисту, готовності, реагування та відновлення після інцидентів. Це передбачає визначення політичних, науково-технічних, організаційних та освітніх орієнтирів, вивчення соціально-політичних питань та знань, створення ефективної системи кібербезпеки, заснованої на комплексних заходах з протидії кіберзагрозам та підтримці безпечного мережевого інжинірингу. Розробка та впровадження ефективних методів і стратегій

реагування на кіберагресію, які можуть бути використані проти кіберзагроз, забезпечення швидкого реагування на динамічні зміни в кіберпросторі, запобігання збройним конфліктам і загрозам у кіберпросторі.

3.3 Аналіз випадків кіберінцидентів

Еволюція кібератак, яка спостерігається за останні кілька років, показує, що принципово змінилися не лише суб'єкти та об'єкти кібервпливу, а й їх цілі та завдання – від примітивних кібератак на компанію-конкурента до міждержавних конфліктів у кіберпросторі. Важливі зміни в кіберпросторі та навколо нього, викликані найвідомішими подіями останніх кількох років, мало впливають на військово-політичних лідерів провідних країн світу; Якість пошуку їх вирішення визначатиме найближчі ідеї розвитку кіберпростору. людське суспільство. Кіберпростір та пов'язані з ним нові виклики та загрози, які призвели до появи нового поля протидії, вимагають всебічного огляду найважливіших кіберподій, що відбулися за останні роки, з метою розробки спільного плану протидії. За словами експертів, кіберподії, які надихнули розвиток програми в усьому світі, відбулися в Естонії в травні 2007 року, в Грузії в серпні 2008 року, в Ірані в липні 2010 року і у Франції в грудні 2010 року. У М'янмі (Бірмі) в 2010 році , у Бельгії у березні 2011 року, на Близькому Сході у 2012 році, в Україні у 2014 та 2017 роках. Але перш ніж фіксувати потреби у створенні кіберінцидентів та їх наслідки, доцільно розпочати еру кібернетичних подій у комп'ютерних мережах.

Кібератаки в Естонії (2007) — перша відома широкомасштабна кібератака проти національної безпеки країни. Кібератаки були здійснені кількома хвилями на тлі російських спецслужб, які руйнували суспільно-політичну ситуацію в країні під виглядом «опору» «протистояння» руху пам'ятника «Бронзовому солдату» в Таллінні. Пік атак припав на 9 травня 2007 року. Зловмисники змогли порушити роботу кількох веб-сайтів, урядових і банківських служб, і служби були закриті через відмову в обслуговуванні.

Кібератака на комп'ютерні системи державних установ Естонії почалася 27 квітня 2007 року під час загострення російсько-естонських відносин через перенесення пам'ятника Бронзовому солдату в Таллінні. Атаки хакерів частково знищили сайти парламенту Естонії, підприємств, банківських установ і ЗМІ. На думку деяких оглядачів, кібератака в Естонії є однією з найбільш ефективних і масових атак в історії інтернету [42].

Події розвивалися трьома хвилями: перші атаки були зафіксовані 28 квітня, наступна, більш сильна хвиля була зафіксована 4 травня, найсильніша, третя хвиля була зафіксована 9 травня 2007 року. Інтернет-трафік з-за кордону зріс у чотири рази, а зламані сайти стали недоступними. Через атаки майже 90% банківських транзакцій в Естонії зазнали проблем з транзакціями або не могли бути виконані нормально. Трафік, створюваний зловмисниками, на піку досягав 100 Мбіт/с. Для здійснення атак використовувалися ресурси мережі Storm. Незабаром після цього боти BlackEnergy атакували сайт видання delfi.ee під час судів над учасниками квітневих заворушень 2007 року.

Естонська сторона від початку звинуватила РФ у здійсненні кібератаки, але пізніше міністр оборони країни відкинув ці звинувачення через відсутність доказів. Однак пізніше того ж року депутат Держдуми РФ Сергій Марков на прес-конференції визнав, що один із його помічників причетний до організації кібератак. У 2007 році лідер придністровського руху «Наші» Костянтин Голоскоков визнав, що ця організація причетна до нападів на Естонію. У відповідь Естонія оголосила "персонами нон грата" Сергія Маркова та лідера руху "Наші" Василя Якименка. Оскільки Придністров'я не визнає жодна країна світу, притягнути до відповідальності тих, хто здійснював кібератаки з цього регіону, не вдалося.

Кібератаки на Грузію, які сталися у зв'язку зі збройним нападом Російської Федерації на країну (2008). Традиційно кібератаки поділяють на дві хвилі. Перша хвиля почалася 7 серпня 2008 року, за день до початку гарячої фази збройного нападу на Грузію. DDoS-атаки (атаки на відмову в обслуговуванні) на державні веб-сайти та ЗМІ є кращими. Під час другої хвилі були підроблені різні сайти, а також DoS-атаки проти більш широкого кола сайтів (великі приватні компанії тощо).

Кібератака на Іран (2010). Особливої уваги заслуговує кіберінцидент в Ірані з мережевим хробаком Stuxnet. У різних дослідженнях висуваються різні версії мети «Stuxnet», але більшість експертів сходяться на думці про передумови виникнення кіберінциденту та наслідки його реалізації [41].

Технічна складність створення мережевого хробака «Stuxnet» вимагає значних ресурсів, які можуть бути повністю забезпечені урядами або деякими зацікавленими урядами країн, що розвиваються. Джерелом кібератаки цього шкідливого програмного забезпечення є ядерні системи (контроль і збір даних (SCADA) виробництва Siemens). Якщо послухати про посилення активності США в кіберпросторі (Кіберкомандування США було створено в 2009 році) і розглянути політичну ситуацію на Близькому Сході (Ізраїль хоче зупинити ядерну загрозу з боку Ірану), відповідь на питання про розробник і продавець цієї кіберподії знаходиться посередині. Це базується на висновках. По-перше, Америка є однією з найрозвиненіших країн світу і, отже, найбільше залежить від високої продуктивності кібернетичних систем з різних причин у всіх аспектах. По-друге, Сполучені Штати проводять внутрішню політику розбудови та зміцнення свого кіберкомандного потенціалу. Завдання, покладені на таке військове управління, неможливо виконати без розробки спеціальних методів кібернетичної влади та кіберзахисту. По-третє, програма під кодовою назвою «Олімпійські ігри», розроблена за адміністрації колишнього президента США Д. Буша та підтримана та розширена адміністрацією президента Б. Обами, для підтвердження збільшення кількості та технічної складності кібер напади на Іран [19].

У результаті наприкінці вересня 2010 року уряд Ірану визнав серйозні недоліки в програмі енергосистеми Бушерської атомної електростанції (АЕС), яка тривала два дні. За результатами розслідування експертів було встановлено, що шкідливе програмне забезпечення, крім знищення особистих даних і пошкодження програмного коду, також призвело до виходу з ладу обладнання цієї дуже важливої сфери енергетики. для економіки. Наслідки цього кіберінциденту для Ірану матимуть значний вплив на уряди інших країн, які розвивають ядерні програми. Він створив візуальне та емоційне враження. Таким чином, у випадку з Іраном вразливість

приватного сектора до таємних кіберможливостей була вперше відкрита для світу без використання військових чи інших засобів для вирішення міжнародних політичних суперечок.

Кібератаки на Україну (2013 – тепер)

Є багато кіберінцидентів, які почалися в Україні з 2013 року і заслуговують на окрему увагу. Перша атака на інформаційні системи приватних і державних підприємств України була зафіксована під час масових протестів у 2013 році. Російсько-український конфлікт став першим конфліктом у кіберпросторі, коли через успішну атаку виходить з ладу енергосистема. Під час президентських виборів інформаційна система «Вибори» зазнала атак, багато відмов у обслуговуванні, шахрайства, кібершпигунства тощо [30].

У лютому 2014 року почалася атака Росії на Україну, яка відбувалася у кіберпросторі. Директор Агентства національної безпеки США Майкл Роджерс зазначив, що Росія, крім військових дій із захоплення Криму, розв'язала проти України кібервійну.

Кіберзагрози українській державі та суспільству можна розділити на два основних рівні. Перший – «класичні» кіберзлочини – реальні та банальні, для їх реалізації потрібні лише нові інформаційні технології.

Це злочини, пов’язані з геополітичним конфліктом (або злочини, які можуть вплинути на політичну ситуацію в державі на локальному рівні): хактивізм, кібершпигунство, кіберсаботаж. У той же час прийоми навантаження в обох випадках мають багато спільних моментів. Наприклад, методи фішингу можуть використовуватися для заволодіння коштами громадян і для кібершпигунства.

Першим великим випадком хактивізму, з яким зіткнулася Україна, стали події, пов’язані із закриттям файлообмінника ex.ua. Після спроб правоохоронних органів втрутитися в роботу файлообмінного сервісу DDoS-атаки були здійснені на понад 10 сайтів державних службовців, зокрема сайт Президента України та сайт Міністерства. МВС України. Події навколо Ex.ua вперше яскраво показали, наскільки українська держава не була готова ні ідеологічно, ні технічно до таких атак. Відсутність прямих економічних втрат стала причиною неможливості зробити реальні висновки з цих

подій, а країна виявилася неготовою до ефективної протидії агресії Російської Федерації в кіберпросторі [35].

Наступний сплеск хактивізму збігся з політичними заворушеннями з жовтня 2013 року по лютий 2014 року, також відомими як події Євромайдану. Ця боротьба розгорталася в соціальних мережах, що викликало значний інтерес до теми. З початком Євромайдану невідомі суб'єкти почали активно використовувати мережевих ботів для порушення інформаційного ландшафту, обману людей і поширення чуток. Наприклад, у Твіттері, де події відстежувалися за хештегом #euromaidan, численні мережеві боти заполонили платформу різного роду деструктивною інформацією.

Традиційні канали зв'язку, зокрема мобільні, також зазнали збоїв, таких як робо-дзвінки, які заважали активістам і політикам ефективно використовувати свої мобільні телефони [36]. Після військової інтервенції Російської Федерації в Україну спеціалізовані організації почали надавати послуги з кібербезпеки, щоб протистояти зростаючій кількості атак на інформаційні системи країни. Ці кібератаки часто були спрямовані на таємне викрадення конфіденційних даних, що надавало Росії стратегічну перевагу на полі бою. Російські кібератаки були спрямовані на українські державні установи, країни ЄС, США, оборонні відомства, міжнародні та регіональні політичні організації, аналітичні центри, засоби масової інформації та опозиційні партії.

З початку російсько-українського конфлікту з'явилися антиукраїнські хактивістські групи, такі як "КіберБеркут" і проукраїнська "КіберСотня Майдану", а також російські та українські групи "Анонім". Хоча точний рівень співпраці між хакерськими групами та урядовими установами незрозумілий, є дані, що вказують на те, що проросійські хакерські групи в Росії працюють від імені російського уряду.

Дослідники кібербезпеки, ймовірно, покращили свою здатність виявляти, відстежувати та запобігати діяльності російських хакерських груп з початку конфлікту. Це покращення може бути пов'язане зі зростанням напруженості у відносинах з російськими хакерами, що залишило їм мало місця для розвитку нових навичок, прийомів і методів [4].

Дослідники з FireEye виявили дві російські хакерські групи, які беруть участь у російсько-українському кіберконфлікті: APT29 (також відоме як Cozy Bear, Cozy Duke) та APT28 (також відоме як Sofacy Group, Tsar Team, Pawn Storm, Fancy Bear). У 2013-2014 роках інформаційні системи кількох українських державних підприємств були заражені комп'ютерним вірусом Snake/Uroborus/Turla. Це шкідливе програмне забезпечення відрізняється особливою надійністю та стійкістю до контрзаходів і, ймовірно, походить з 2005 року. У 2013 році було розпочато операцію "Армагеддон" - комплексну кібершпигунську операцію, спрямовану на інформаційні системи російських державних, правоохоронних та оборонних структур. Розвідувальні дані, зібрані в ході цієї операції, можуть підтримати Росію на полі бою. Винятком з цієї тенденції є кібердиверсійна атака на "Прикарпаттяобленерго".

Операція "Змія"

У 2013-2014 роках дослідники британської компанії BAE Systems Applied Intelligence зафіксували сплеск зараження інформаційних систем українських приватних і державних підприємств комп'ютерним хробаком (у тому числі руткітами) під назвою "Snake". Дослідники з німецької компанії GData назвали цього хробака "уроборус". Обидві групи дослідників вважають, що цей хробак може бути пов'язаний з хробаком Agent.BTZ, який скомпрометував інформаційні системи Центрального командування США у 2008 році. Виявлення хробака Ouroboros збіглося в часі зі значним загостренням конфліктів. У січні 2014 року було зафіксовано 22 випадки зараження інформаційних систем, порівняно з вісьмома випадками виявлення "уробороса" у 2013 році. Розгорнувши "ураборос" в Україні, зловмисники отримали повний доступ до соціальних мереж. Британські експерти вважають, що є достатньо доказів, які дозволяють припустити, що за використанням "уроборобів" стоять російські спецслужби [15].

Атака на "вибори"

21 травня 2014 року хакерська група "КіберБеркут" здійснила успішну кібератаку на виборчу інформаційну систему Центральної виборчої комісії (ЦВК) України. Їм вдалося вивести з ладу критичні вузли мережі та інші частини інформаційної системи ЦВК. В результаті програмне забезпечення, призначене для

відображення результатів голосування, не працювало майже 20 годин. У день виборів, 25 травня, за 12 хвилин до закриття виборчих дільниць (о 19:48 за східноєвропейським часом) зловмисники розмістили на дільницях ЦВК зображення Яроша.

Увечері 25 травня експерти CERT-UA отримали повідомлення про те, що російські телеканали оголосили про перемогу Дмитра Яроша в "президентських перегонах". На підтвердження цієї інформації російське телебачення транслювало в інтернеті зображення, відоме як "фото Яроша". Перше спростування було зафіксовано 25 травня о 20:16:56. Було знайдено повний шлях до зображення "result.jpg", який випливає з IP-адреси 195.230.85.129 у GET-запиті до сайту ЦВК, де вказано лише IP-адресу внутрішнього веб-сервера. Ця адреса знаходиться в діапазоні IP-адрес телеканалу ОРТ.

В результаті атаки російський "Перший канал" повідомив своїм глядачам, що Дмитро Ярош, лідер "Правого сектору", набрав найбільшу кількість голосів у першому турі президентських виборів в Україні. Це твердження прозвучало у вечірньому випуску новин, присвяченому президентським виборам в Україні. Свідок заявив, що в той час, як Петро Порошенко був показаний як переможець першого туру, на сайті ЦВК з'явилося "дивне зображення" (так зване "фото Яроша"). Згідно з наявною інформацією, Дмитро Ярош отримав 37,13% голосів виборців, тоді як Петро Порошенко набрав лише 29,63% [12].

Рано вранці наступного дня, 26 травня, сервери системи "Вибори", які отримували та обробляли дані про голосування, зазнали розподіленої DoS-атаки і вийшли з ладу між 1:00 та 3:00 годинами ночі. Окрім інформаційної системи ЦВК, кібератак зазнали й інші організації, віддалено пов'язані з виборами, наприклад, будь-які веб-сайти, що містять термін "вибори". Однак більшість цих атак були технічно простими. На відміну від них, атака на ЦВК була дуже складною та витонченою. За словами Миколи Коваля, тодішнього президента CERT-UA, атака на інформаційну систему ЦВК була однією з найскладніших кібератак, які він коли-небудь розслідував. Хоча відповідальність за атаки взяло на себе хакерське угруповання «КіберБеркут», Микола Коваль припускає, що серйозна вишуканість атаки може

свідчити про те, що за нею стоять підрозділи іншої держави. Крім того, у мережі CEC було виявлено зловмисне програмне забезпечення, пов’язане з APT28/Sofacy Group.

Експерти з комп’ютерної безпеки, опитані американською газетою Christian Science Monitor, заявили, що атака на інформаційну систему «Вибори» була не тільки надзвичайно небезпечною, але й попередженням майбутнього про вразливість комп’ютерних систем, задіяних у виборчому процесі. Можливість зриву виборів або маніпулювання результатами виборів набула нової ваги на президентських виборах у США 2016 року після успішної кібератаки на Демократичну партію [40].

Атака на “Прикарпаттяобленерго” 23 грудня 2015 року вперше підтверджено світову атаку на знищення електромережі: російські зловмисники зруйнували комп’ютерні електромережі в диспетчерській Прикарпаттяобленерго, закривши близько 30 підстанцій і залишивши без світла близько 230 тисяч людей. від однієї до шести годин виконується троян BlackEnergy. Водночас «Чернівціобленерго» та «Київобленерго» зазнали одночасної атаки, але з меншими наслідками. За інформацією, отриманою від когось із обленерго, зловмисники підключаються до інформаційних мереж через підмережі глобальної мережі Інтернет, що належать провайдерам у Російській Федерації.

Загалом кібератака мала складну структуру і складалася як мінімум із таких компонентів:

- попереднє зараження мереж за допомогою фейкових листів із застосуванням методів соціальної інженерії;
- взяття під контроль АСДУ шляхом проведення відключень на підстанціях;
- несправність елементів IT-інфраструктури (джерел безперебійного живлення, модемів, RTU, комутаторів);
- знищення інформації на серверах і робочих станціях (утиліта KillDisk);
- атака на телефонні номери кол-центрів з метою відмови в обслуговуванні відключених абонентів.

Масова хакерська атака почалася щонайменше 14 квітня 2017 року, коли була зламана редакційна система MEDoc. Останній інцидент, пов'язаний з версією вірусу Petya, стався 27 червня 2017 року і був спрямований на руйнування українських

державних підприємств, бізнесу, банків, ЗМІ та інших секторів. Атака порушила роботу таких компаній, як аеропорт "Бориспіль", Чорнобильська атомна електростанція, "Укртелеком", "Укрпошта", "Ощадбанк", "Укрзалізниця" та інших великих організацій [36].

Вірус також вразив телеканал "Інтер", медіа-холдинг ТРК "Люкс" (до якого входять "24 канал", "Радіо Люкс ФМ" і "Радіо Максимум"), різні інтернет-видання та сайти телекомпаній. Крім того, Львівська міська рада та Київська міська адміністрація припинили мовлення на "Першому землекопському" та ТРК "Київ".

28 червня 2017 року Кабінет Міністрів України повідомив про завершення атаки на корпоративні та державні мережі. Масштабна деструктивна атака з використанням різновиду вірусу Petya (також відомого як NotPetya, Eternal Petya, Petna, ExPetr та ін.) була здійснена шляхом компрометації системи оновлення M.E.Doc та встановлення прихованого бекдору. Як наслідок, під час масштабної атаки зловмисники за допомогою бекдору заблокували доступ до комп'ютерів та комп'ютерних мереж близько 80% українських підприємств (у тому числі філій іноземних компаній). Вважається, що зловмисники пішли на цей крок або для забезпечення більш надійного доступу до критично важливих інформаційних систем жертв, або тому, що вважали, що зможуть легко відновити доступ. У цьому контексті важливість кібербезпеки стала значущою проблемою не лише для окремих країн, але й на міжнародному рівні. Наразі існує чимало програм міжнародного співробітництва, спрямованих на встановлення певного рівня кібербезпеки. Ці ініціативи базуються на відповідних міждержавних угодах, конвенціях та інших документах Організації Об'єднаних Націй та Європейського Союзу.

Висновки до розділу 3

Узагальнюючи вищезазначений текст, можна сказати, що класифікація кіберзагроз є важливим етапом у створенні ефективної системи кібербезпеки. З урахуванням різноманітності та складності кіберзагроз, їх класифікація за різними ознаками дозволяє краще розуміти їх природу та визначати необхідні заходи протидії.

Важливо враховувати такі критерії, як тип системи, елемент, уразливості, джерело, спосіб реалізації, середовище розповсюдження, наміри, походження, видимість та інші, щоб ефективно захищати інформаційні ресурси та системи від кіберзагроз. Класифікація допомагає узагальнити та систематизувати різноманітні загрози, що дозволяє розробляти ефективні стратегії протидії та захисту.

Україна зазнає зростаючих загроз у кіберпросторі, що вимагає вжиття стратегічних заходів для забезпечення кібербезпеки. Для цього було розроблено Національну стратегію кібербезпеки, створено спеціальні управлінські структури та вжито заходів для координації дій у сфері кібербезпеки. Крім того, Україна активно співпрацює з міжнародними партнерами для запобігання кіберзагрозам, підвищення обізнаності та реагування на кіберінциденти. Необхідно також звернути увагу на освітні програми з кібербезпеки, розвиток міжнародної співпраці та впровадження новітніх технологій для захисту важливих інформаційних систем. Важливо також забезпечити підвищення обізнаності та підготовку фахівців у сфері кібербезпеки, а також змінити підхід до кібербезпеки на організаційному рівні, забезпечивши безпеку критичної інфраструктури та встановивши державно-приватне партнерство.

За останні кілька років спостерігається еволюція кібератак, яка показує зміни в суб'єктах, об'єктах, цілях та завданнях кібервпливу. Від примітивних кібератак на компанії-конкуренти до міждержавних конфліктів у кіберпросторі. Важливі зміни в кіберпросторі та навколо нього, викликані подіями, такими як кібератаки в Естонії, Грузії, Ірані, Франції, М'янмі, Бельгії, на Близькому Сході та в Україні, вимагають всебічного огляду та розробки спільного плану протидії. Кібератаки на Україну, зокрема, показали складність та руйнівність таких атак, як атака на електромережу, атака на виборчу інформаційну систему та масштабна деструктивна атака з використанням вірусу Petya. Ці події підкреслюють важливість кібербезпеки як національної, так і міжнародної проблеми, яка потребує спільних зусиль для захисту від кіберзагроз.

РОЗДІЛ 4
АНАЛІЗ КІБЕРЗАГРОЗ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

4.1 Огляд методів аналізу кіберзагроз

Ми почнемо огляд з найпростішого і найпоширенішого методу виявлення вторгнень, заснованого на сигнатурному підході.

Методи підпису ідентифікують вторгнення за допомогою формальної моделі; це рядок символів, семантичний вираз тощо. це може бути. Першим методом виявлення вторгнення є сигнатурний аналіз. Цей метод перевіряє, чи збігаються рядки з підписом. Подпись — підпис, зразок; наприклад, програма може мати характерний рядок, який вказує на шкідливий трафік.

Підпис може містити ключове слово або команду, пов’язану з вторгненням. Якщо збіг знайдено, спрацьовує сигнал тривоги. Метод сигнатури забезпечує захист від хакерської або вірусної атаки лише в тому випадку, якщо її сигнатура (наприклад, частина тіла вірусу) відома заздалегідь і також повинна бути введена в базу даних IPS. На ефективність ІПС підписів впливають три фактори: ефективність внесення підписів до бази даних; Повнота бази даних щодо ідентифікації сигнатур вторгнень; існування інтелектуальних алгоритмів, де порівняння здійснюється з сигнатурами [10]. Перевагами методів виявлення порушень підпису є низька обчислювальна складність і низька вартість розгортання та впровадження. До недоліків сигнатурних методів можна віднести низьку ефективність виявлення невідомих атак і проблему старіння баз даних сигнатур.

Статистичні методи широко використовуються для виявлення аномалій і базуються на створенні статистичного запису поведінки системи протягом періоду дослідження. Під час навчання важлива практика. Крім того, для кожної частини роботи системи необхідно встановити діапазон значень, використовуючи відомий закон розподілу ймовірностей. Системи виявлення вторгнень використовують статистичний метод і після інсталяції «навчаються» адміністратором, який

інтерпретує політику системи виявлення відповідно до нормальної поведінки мережі (схеми трафіку, з’єднання між вузлами, протоколи та порти, що використовуються [5] IPS повідомляє адміністратор виявлення встановлення мережі або важливих відмінностей від трафіку. Метод розрахунку дуже важливий для правильності правил, тому, якщо правила правильні, система може видавати негативні результати домовленостей.

Також широко використовується статистичний метод, заснований на моделях, що створюють скінченні автомати [10]. Потужною статистичною моделлю є прихована модель Маркова (Hidden Markov Model, HMM). Приховані моделі Маркова відрізняються від ланцюгів Маркова тим, що вихідні символи автомата стохастично залежать від їх станів. Дресирувати таких моделей досить складно. Процес вибору прихованих станів займає багато часу і не відбувається автоматично. Крім того, існує необхідність періодично реконструювати HMM на оновлених даних, щоб забезпечити адаптивність цих моделей. Виявлення вторгнень базується на оцінці прихованих параметрів на основі спостережуваних параметрів. Недоліки цього математичного підходу включають складність процесу побудови моделі та обмеження у типах програм, які можна описати за допомогою статичних граматик.

Машина опорних векторів (SVM) — це набір навчених алгоритмів паралельного навчання, які використовуються для класифікації та регресійного аналізу. Метод належить до сімейства лінійних таблиць і іноді вважається прикладом регуляризації Тихонова. Цей спосіб дозволяє виконати завдання на розв’язання задачі на відповідність. Для виявлення вторгнення генерується вектор ознак, а потім виконується навчання та операція класифікатора. На основі застосування методу опорних векторів існує функція, яка може розділити вектори ознак і дізнатися стан поточної роботи програми або користувача. SVM використовується для виявлення несправностей і аномалій.

Наступним статистичним методом є використання сплайнів багатовимірної адаптивної регресії (Multivariate Adaptive Regression Splines, MARS). MARS — це метод непараметричної регресії, який можна розглядати як розширення лінійних моделей для легкого моделювання нелінійності та зв’язків між змінними. Цей метод

створює багатовимірний простір ознак, де форма елементів мережі записується в наборі векторів цього розташування. Завдання виявлення вторгнень полягає в тому, щоб провести обґрунтоване порівняння поведінки на основі заданого векторного навчального набору. Як правило, рекомендується використовувати сплайни з кількома вершинами [1].

Методи кластеризації широко використовуються при вирішенні кібернетичних задач. Виявлення раніше невідомих атак передбачає використання методів кластеризації. Багатовимірна статистична процедура, яка збирає дані, які містять інформацію про вибірку елементів, щоб упорядкувати їх у схожі групи. Для великого класу статистичних завдань він також не вивчається. Методи групування даних стосуються подібності елементів у групах. Часто групування починається з вибору центральної точки для кожної групи, а потім розподілу певних елементів між групами. На наступному кроці сервери ремонтуються, а елементи перерозподіляються. Перевага цього методу полягає в тому, що він не потребує навчального набору для виявлення аномалій. Групи різних типів створюються шляхом сортування групи елементів без міток. Використовуючи методи кластеризації, слід бути обережним, щоб визначити групи точно та подалі від викидів. Метою поєднання є визначення ступеня відділення випуску від оболонок. Викиди, що характеризуються високим ступенем відриву від кластерів, позначені як аномалії [10].

Виявлення вторгнень виконується за допомогою байєсівських мереж. Байєсова мережа — це модель, яка містить імовірнісні зв’язки між змінними. Сьогодні пропонується багато різних застосувань байєсівських мереж для виявлення мережевих аномалій. Більшість підходів спрямовані на встановлення умовних залежностей між змінними за допомогою складних байєсівських мереж [5]. Для прогнозування поведінки зловмисників або ідентифікації зловмисників байєсовські мережі можуть бути кращими, але якщо при моделюванні структури системи зроблені припущення, точність виявлення може бути значно знижена.

Однією з галузей математичного моделювання, яка сьогодні швидко розвивається, є природна кореляція. Ці методи включають штучні нейронні мережі,

штучні імунні системи та генетичні алгоритми, які активно використовуються в системах виявлення вторгнень.

Штучні нейронні мережі (ШНМ) є популярним підходом до систем виявлення вторгнень. Нейронні мережі — це набір інструментів для різних додатків: агрегації даних, вилучення ознак, зменшення розмірності тощо [11]. Для виявлення атак нейронні мережі навчаються характеристикам різних типів вторгнень і використовуються для визначення поведінки системи під час атаки. Щоб виявити аномалії, нейронна мережа визначає нормальний стан системи, а потім переходить у режим виявлення [21]. Якщо значення параметрів під час роботи відрізняються від значень у реальній системі, в системі є помилка. Для створення моделі користувача використовуються наступні параметри: години, коли він зазвичай працює, набір вузлів, з яких починається робочий сеанс, способи використання системних ресурсів [6].

Найбільш перспективними системами захисту є природні захисні мережі. Його прототипами є системи, які захищають живі істоти від зовнішніх атак і спрямовані на усунення їх наслідків, якщо вони це вже зробили. Безперечною перевагою імунних мереж є те, що вони дозволяють створити механізм захисту від невідомих вторгнень. Мережі штучного інтелекту використовуються для виявлення пошкоджень і виявлення аномалій. Використання генетичних алгоритмів у системах виявлення вторгнень може підвищити їх ефективність і гнучкість. Генетичні алгоритми засновані на принципах природного відбору та еволюції. За допомогою генетичних алгоритмів мережева технологія повинна бути зв'язана за допомогою хромосомної структури даних. При роботі з хромосомами використовуються такі операції, як відбір, кросинговер, мутація. У завданнях виявлення аномалій хромосома матиме гени, пов’язані з характеристиками: прапори, кількість клітин, служби тощо [10]. Песимістичний підхід можна пояснити гібридним процесом виявлення аномалій і несправностей за допомогою генетичного алгоритму. Продуктивність генетичного алгоритму вивчається та перевіряється за допомогою штучних даних і простого моделювання [32].

Поведінкова біометрія також використовується в системах IDPS. З його допомогою можна виявити аномалії в мережі. Спостереження за почерком клавіатури, використанням комп’ютерної миші, дослідження почерку з інтерфейсами введення-виведення для різних користувачів та іншими біометричними характеристиками дають можливість приймати рішення про наявність відхилень [1].

Виявлення атак здійснюється за правилами нечіткої логіки. Вбудовані нечіткі системи виявлення використовують набір нечітких правил для визначення ймовірності атаки на звичайні веб-сайти. Для опису трафіку в будь-якій мережі можна створити нечітку множину. Робота [14] описує, як будувати таблиці з використанням нереляційних правил, які використовуються для виявлення доступу до мережі. Нечіткі набори правил асоціації використовуються для опису регулярних і незвичайних класів. Релевантність історії визначається за допомогою метрики релевантності. Правила відносин створюються на основі звичайних прикладів навчання. Тестовий зразок класифікується як нормальний, якщо встановлений правилами сигнал перевищує порогове значення. Зразки з балами нижче порогового значення вважаються дефектними [10].

Експертні системи також використовуються в системах виявлення вторгнень. У системах MDS експертні системи дозволяють описати процес роботи системи за допомогою набору правил висновку для прийняття рішення про наявність чи відсутність вторгнення. У системах ADS експертні системи визначають нормальну поведінку системи за допомогою фактів і правил.

Графи широко використовуються в кібербезпеці. Діаграми дозволяють переводити складні види абстрактної інформації в чітку візуальну форму. Вони представляють інформацію у вигляді набору об'єктів і зв'язків між ними. Графіки атак використовуються для визначення шляхів атак у комп’ютерних мережах. Графи атак визначаються як метод, який досліджує взаємодію між вразливими місцями системи. Графіки атак показують структуру, ризики, кореляції тощо. Це дозволяє аналізувати. У дослідженні вводиться поняття «дерево атак». Це формальний метод визначення безпеки систем, який враховує можливі вторгнення. У дослідженні [19] дерева атак називаються «деревами атак». У деревах атак механізми захисту застосовуються не

тільки на рівні листового вузла, а й на будь-якому вузлі дерева. Тут було проведено якісний аналіз та ймовірнісний аналіз ризику. У [20] розглядався граф атак для візуальної ідентифікації шляхів порушника. Якщо в процесі виявлення вторгнень використовуються графіки, вони повинні відображати не тільки стани системи, але й переходи між станами та можливі недійсні шляхи.

Фрактали зарекомендували себе у вирішенні проблем кіберзахисту. Бенуа Мандельброт описав фрактали як частини, які нагадують ціле. Завдяки високому рівню алгоритмізації фрактали корисні в операціях захисту інформації в кіберпросторі. Наприклад, набір функцій безпеки веб-сайту можна представити у вигляді фракталів. Потім отримайте опис безпеки всього сайту за допомогою подібних властивостей. Цей метод використовується для симетричних систем захисту інформації, де до кожного елемента системи пред'являються однакові вимоги. У наукових дослідженнях [23] розглядається захист документів із секретами на основі фракталів. Тут показані спеціальні галереї на основі секретів, створених для підвищення ефективності та надійності екрану. Метод захисту полягає у створенні графічних елементів коробки захисту у векторному форматі, копіюванні, копіюванні та створенні захисної сітки на основі фракталів за допомогою ітераційного процесу. Фрактальні фонові мережі важко відтворити, тому що алгоритм, зразок якого відомий лише розробнику, повинен використовуватися для створення вибраного фрактального шаблону. Сьогодні існує достатня кількість алгоритмів, реалізованих з використанням теорії фракталів, але перевірка та вибір різних типів фракталів для створення IDPS потребують додаткових досліджень.

4.1.1 Традиційні методи аналізу кіберзагроз

Традиційні методи виявлення кіберзагроз покладаються на використання відомих сигнатур або відбитків пальців загроз. Ці методи працюють за принципом відповідності: якщо вхідний потік даних або поведінка системи збігається з відомою сигнатурою загрози, система виявлення втручається.

Основними характеристиками традиційних методів є:

– виявлення сигнатур: це стандартний метод, який використовується більшістю антивірусних програм. Порівняти файл або код із сигнатурами відомих вірусів або шкідливих програм;
– аналіз продуктивності: замість пошуку відомих сигнатур цей метод аналізуватиме поведінку програми, щоб визначити, чи є програма шкідливою;
– евристичний аналіз: цей метод використовує алгоритми для виявлення невідомих захворювань.

Переваги традиційних методів:

– швидкість виявлення відомих загроз;
– низький показник негативних відгуків порівняно з іншими методами.

Недоліки традиційних методів:

– нездатність виявити нові або модифіковані загрози, сигнатури яких не видно;
– необхідність регулярно змінювати файл підпису для забезпечення відповідності безпеки;
– для підтримки та оновлення доменних імен потрібно багато ресурсів.

Таким чином, хоча традиційні методи ефективні для виявлення відомих загроз, вони менш ефективні проти нових або невідомих загроз.

4.1.2 Методи аналізу кіберзагроз з використанням штучного інтелекту

Останніми роками уряди все більше уваги приділяють штучному інтелекту та його безпеці. Експерти, знайомі з проблемами кібербезпеки в країнах Співдружності Незалежних Держав (СНД), наголошують на необхідності прозорості, тестування та підзвітності в розробці алгоритмів та їхніх творців. Наприклад, Комісія з питань національної безпеки у сфері штучного інтелекту (NSCAI) у США підкреслила важливість створення верифікованих (надійних і безпечних) систем штучного інтелекту, які можна оцінити за допомогою суворого стандартизованого процесу документування. Комісія запропонувала встановити стандарти для моделей ШІ, що

охоплюють такі аспекти, як використання даних, параметри і ваги моделі, методи навчання і тестування, а також отримані результати. Ці заходи допоможуть експертам виявити слабкі місця в технологіях ШІ, ризики потенційних маніпуляцій з даними та інші непередбачувані проблеми.

У цьому контексті регуляторні органи відіграють вирішальну роль. Вони можуть створити відповідальні та підзвітні рамки для управління ШІ під час кіберінцидентів. Це життєво важливо для розробників ШІ, щоб отримувати сертифікати, проводити аудит і розуміти нюанси роботи систем ШІ. Ті, хто не дотримується цих правил під час розробки ШІ, можуть бути притягнуті до відповідальності за будь-які майбутні збитки, якщо їхні системи будуть зламані. [39].

Рекомендується сформулювати наступні основні рекомендації щодо захисту СШІ:

- перш за все, необхідно реалізувати безпечний життєвий цикл розробки SSI;
- «Традиційні» схеми завантаження програмного забезпечення можна терпіти, мінімізуючи використання коду сторонніх розробників або підтримуючи безпеку коду, який неможливо обійти в будь-якому випадку;
- атаки на платформу можна запобігти, відстежуючи спосіб обробки даних доступу, захищаючи платформу звичайними методами для боротьби з DoS-атаками, а також відстежуючи в безпеці системи витоки даних користувача [8];
- атакам на алгоритм (ворожим атакам) можна протистояти, змінивши вхідні дані та навчившись включати конкуруючі функції в набір даних. Для боротьби з цими атаками використовуються захисна дистиляція, природна екстракція, функціональне стиснення тощо. Є також спеціальні заходи, такі як;

Щоб запобігти завантаженню даних, їх потрібно використовувати, автентифікувати, фільтрувати та шифрувати під час використання. Щоб уникнути проблем із конфіденційністю, дані не слід персоналізувати. Крім того, лінійна регресія може допомогти боротися з пошкодженням даних [50]. У цих атак є конкретика.

4.2 Порівняння методів аналізу кіберзагроз

Відомо, що часові ряди — це ряди точок даних, взятих через однакові проміжки часу. Вони можуть бути корисними для виявлення аномалій або незвичних моделей поведінки в контексті кібербезпеки. Розглянемо кілька важливих застосувань.

Це важливе джерело даних у сфері мережевої безпеки. Загальні зміни симптомів, які вказують на судоми, можуть включати:

- DDoS-атака: однією з найважливіших загроз є DDoS-атака, яка намагається «захопити» сервер, надсилаючи на нього багато запитів. Часовий ряд допоможе визначити раптове збільшення трафіку;
- незвичайний вихідний трафік: несанкціонований витік даних можна виявити шляхом спостереження за неочікувано великим обсягом вихідного трафіку.

Системні журнали можуть відображати детальну інформацію про дії користувачів і процесів. Часові ряди допоможуть виявити зміни в таких моделях, як:

- часті помилки входу. Раптове збільшення кількості помилок входу може свідчити про спроби грубої атаки;
- несанкціонований доступ. Якщо користувач, який зазвичай працює вдень, раптом починає входити опівночі, це може означати, що його обліковий запис зламано.

Зловмисне програмне забезпечення може створювати характерні моделі активності, які можна виявити за допомогою часових рядів:

- витрата ресурсів. Значне збільшення використання процесора або оперативної пам’яті може свідчити про наявність шкідливого програмного забезпечення;
- моніторинг мережевої активності. Завдяки частому обміну даними з командними та контрольними серверами зловмисне програмне забезпечення може створити чіткий шаблон мережевої активності.

Моделі часових рядів можуть допомогти не тільки виявити, але й передбачити майбутні атаки:

– прогнозування пікових навантажень: за допомогою таких моделей, як ARIMA або GARCH, можна передбачити моменти пікового навантаження, які можуть вказувати на заплановані DDoS-атаки на сервери;
– сезонний аналіз: деякі атаки є сезонними, і часові ряди можна використовувати для виявлення та прогнозування цих періодів.

Час відіграє важливу роль у сучасних системах кібербезпеки. За допомогою математичних моделей часу можна аналізувати динаміку різних типів даних, виявляти аномалії та прогнозувати загрози.

Моніторинг мережі дозволяє завчасно виявляти звичайний зовнішній трафік, який вказує на несанкціонований витік даних, а також такі загрози, як DDoS-атаки. Загалом системні журнали дозволяють відстежувати активність користувачів і діяльність, виявляючи несанкціоновані спроби чи зловмисні атаки.

Важливою функцією є виявлення шкідливого програмного забезпечення, яке демонструє певні моделі поведінки, що відрізняються від звичайної поведінки системи. І, нарешті, важливу роль відіграє здатність передбачити майбутні атаки на основі історичних даних і математичних моделей.

Тому інтеграція методів реального часу в системи кібербезпеки може значно підвищити ефективність виявлення та запобігання кіберзагрозам.

Для подальшого розвитку систем кібербезпеки важливо досліджувати нові методи та алгоритми обробки в реальному часі та адаптувати їх до специфіки цієї галузі.

4.3 Практичні приклади застосування ШІ в кібербезпеці

Системи штучного інтелекту допомагають посилити кібербезпеку: розпізнають аномалії та нові типи зловмисного програмного забезпечення, повідомляють про загрози та захищають критичні дані. Поява таких технологій, як ChatGPT і Bard, ще більше розширила його можливості.

Системи штучного інтелекту, створені на основі алгоритмів машинного навчання та лінгвістичних нейронних мереж, давно стали частиною сучасних засобів захисту даних.

Сфер їх застосування багато. Перш за все, це виявлення вторгнень, коли вам потрібно знати, коли хтось увійшов у ваш простір. Система може легко розпізнати сигнатуру шкідливого коду або наявність Інтернету, щоб реагувати на звичайну поведінку користувача. Наприклад, алгоритм виявляє, що людина о 12 годині ночі звернулася до файлу з персональними даними клієнтів; Це може бути робота хакера [22].

Алгоритми машинного навчання добре фільтрують спам; Ми говоримо про фільтри електронної пошти, щоб зменшити навантаження на співробітників компанії від фішингу. Адже часто можна порадити співробітникам не відкривати підозрілі листи, але людський фактор не зрозумілий. Щоб людина не стикався з повідомленнями від шахраїв, краще встановити спам-фільтр.

Традиційні системи ШІ працюють шляхом виявлення відомих загроз. Проте щодня відкриваються нові методи злому. Тому важливо мати можливість передбачити зловмисні дії та реагувати на вразливості до їх активації. Інструменти, засновані на генеративних моделях штучного інтелекту, можуть виконувати завдання не тільки для вимірювання конкретних факторів, але й для створення контексту. Це перспективний напрям для створення антивірусних і комерційних продуктів для кібербезпеки.

Розглянемо основні переваги та можливості систем генеративного штучного інтелекту у сфері кіберзахисту:

- Виявлення атипової (аномальної) поведінки. Для класичних систем захисту ми встановлюємо певні критерії, за якими поведінка користувача буде вважатися зловмисною. Багато таких факторів збігаються; Зафіксовано інвазію. У той же час продуктивний штучний інтелект може розпізнавати критерії, яких ми ще не передбачали і ніколи раніше не стикалися. Таким чином можна зібрати кращу прогностичну модель.

- Автоматичні дії. Виявлення загрози недостатньо; Вкрай важливо вчасно на це відреагувати та запровадити систему захисту. Моделі, створені алгоритмами генеративного штучного інтелекту, можуть зробити це максимально швидко.
- Робота з автоматичними атаками. Великі компанії часто атакують алгоритми, а не люди. Часто неможливо адекватно відповісти на цей виклик, оскільки шкідливі програми постійно змінюються. Але бот може і повинен протистояти іншому боту.
- Боротьба з хибнонегативними та хибнопозитивними сигналами. У сфері кібербезпеки підприємства системі необхідно відстежувати багато подій одночасно: Інтернет-трафік, доступ до веб-сайту тощо. Серед цього «шуму» легко перебільшити нормальну поведінку та витлумачити її як зловмисну (або навпаки). Зараз це серйозна проблема кібербезпеки, і генеративний штучний інтелект має хороші шанси зменшити кількість неправильно інтерпретованих сигналів [39].

Оскільки генеративні системи ШІ є новими, вони мали помітний вплив на галузь кібербезпеки. Наприклад, біометрична автентифікація, яка реалізована майже в кожному смартфоні, вважається хорошим захистом для кінцевих користувачів, але вона менш надійна в діловому світі.

Наші пальці або очі просто відрізняються від моделі людини. Але для машини це комбінація чисел. Наприклад, якщо хакер має доступ до вашої камери, він може зробити достатньо знімків, щоб створити цифровий відбиток вашого обличчя.

Тому компанії відмовляються від біометричної автентифікації на користь токенів FIDO — спеціальних пристроїв, які допоможуть під час перевірки особистості. Біометрія корисна у великих компаніях, наприклад, для ідентифікації співробітників, які входять до будівлі.

Основна загроза поширення відкритих генеративних інструментів штучного інтелекту полягає в тому, що ці технології можна використовувати не тільки для кіберзахисту, але й для кібератак. Хоча існуюча інфраструктура на рівні ChatGPT не дозволяє хакерам створювати нові віруси або змінювати існуючі віруси, вони можуть

використовувати її в режимі другого пілота. Це означає витрачати набагато менше часу на підготовку атак [43].

Наприклад, недавно з'явився автоматичний алгоритм WormGPT. Це допомагає шахраям створювати переконливі спам-повідомлення, які обходять спам-фільтри. Для цього система використовує набір даних ділових листів із зламаних корпоративних поштових скриньок.

Як наслідок, фішинг, програми-вимагачі тощо. Минулого року зросла кількість інцидентів за участю людей. При цьому кількість кіберзлочинців не зросла; Тільки тепер одна людина може розширити сферу своєї діяльності. Наприклад, щомісяця ми надсилаємо не 100 000, а 3 мільярди спам-повідомлень.

Ви можете імітувати чийсь голос. Нещодавно були зафіксовані випадки, коли шахрай підробляв голос одного з керівників компанії і по телефону наказував перевести на його рахунок кілька мільйонів доларів. Поширені схеми: шахрай дзвонить родині жертви і розповідає історію на кшталт «ваш онук в міліції, платіть, щоб його звільнили». У США від таких травм щорічно гине 20-27 мільйонів.

Наразі отримані голоси не ідеальні. Вони роботизовані та позбавлені нюансів. Ці типи атак більше використовують людську вразливість і необережність. Так само хакерам ще належить навчитися створювати надійні відеовідбитки обличчя.

Ще одним ризиком, який виник із появою таких інструментів, як ChatGPT, є погіршення якості коду. Уявімо, що розробник створює код для свого завдання, і цей код містить певні вразливості безпеки. Якщо програміст недостатньо кваліфікований, щоб зрозуміти це, проблем не уникнути.

Таким чином можуть бути порушені комерційні таємниці, а також фактичні вразливості системи безпеки. Зрештою, коли розробник надає ChatGPT частину свого коду та просить його змінити, система оновлює набір даних. Так цей код потрапляє у відкритий доступ. Потім, коли інша особа намагається створити код, який вирішує подібну проблему, ChatGPT може надати їй частину того самого коду. Фактично інтелектуальна власність буде передана іншій особі чи компанії.

Тому багато IT-компаній вже заборонили своїм розробникам використовувати генеративний ШІ під час програмування.

Компанії, яким важливі безперебійне обслуговування та робота з конфіденційними даними, все більше цікавляться інструментами кібербезпеки, які використовують штучний інтелект. Ця тенденція також помітна в Україні; особливо серед інноваційних банків і підприємств, які працюють з технологічною інфраструктурою та великими наборами даних [5].

Основним питанням, що визначає темпи розвитку інноваційних засобів захисту даних, є вартість цих технологій. Зазвичай це 6-значні чи навіть 7-значні числа. Навіть такі великі технологічні компанії, як Meta, зараз не впевнені, чи варто платити такі суми за сервери та створення наборів даних, щоб використовувати всі можливості генеративних моделей.

Але кіберзахист як послуга набирає обертів, охоплюючи традиційний захист і впроваджуючи генеративні алгоритми навчання. В Україні Київстар вважається одним із лідерів у цій ніші.

Найбільшою перешкодою для використання штучного інтелекту в кібербезпеці є RoSI (Return on Security Investment), якщо компаніям потрібно виправдати придбання нових інструментів за рахунок вартості. Загалом, обґрунтування створення корпоративного кіберзахисту таке: його вартість не повинна перевищувати збитків, які можуть виникнути від кібератаки.

Наприклад, компанія впровадила захист на основі унікальних сигнатур поширених захворювань. Захищає компанію від 30-60% атак. Якщо ця проблема знаходиться на прийнятному рівні, то не можна витрачати гроші на продукти штучного інтелекту, які відбиватимуть 80-92% атак [9].

Водночас висока вартість ресурсів для розробки продуктивного штучного інтелекту є гарантією того, що хакери не зможуть використовувати його для підготовки більш серйозних атак, ніж фішинг. Насправді зараз група хакерів може отримати доступ до необхідних систем лише за підтримки держави (наприклад, для розробки кіберзброї в інтересах цієї держави).

4.4 Концепція методу аналізу кіберзагроз

Для створення методу штучного інтелекту для аналізу кіберзагроз необхідно використовувати рекурентні нейронні мережі (RNN) разом з передовими методами машинного навчання.

Для цього необхідні такі дії:

1. Використання різноманітних джерел даних

На додаток до історичних даних про атаки, мережевих журналів, зразків шкідливого програмного забезпечення та сповіщень системи безпеки, слід збирати дані з різних джерел, таких як:

- Форуми та ринки Даркнету, відомі торгівлею інформацією про кіберзагрози.
- Загальнодоступні канали розвідки загроз, що надаються організаціями з кібербезпеки.
- Платформи соціальних мереж, де суб'єкти загроз можуть обговорювати або ділитися інформацією про свою діяльність.
- Звіти про інциденти та тематичні дослідження, що документують минулі порушення безпеки та вразливості.
- Урядові бази даних, що містять інформацію про кіберзагрози та атаки на об'єкти критичної інфраструктури або державні установи.

2. Розширення даних

Використання методів доповнення даних для збільшення різноманітності та розміру наборів даних.

Це може включати:

- Генерування синтетичних даних для імітації різних типів кібератак і змін у мережевому трафіку.
- Додавання шуму або збурень до існуючих зразків даних, щоб зробити модель більш стійкою до реальних сценаріїв.
- Включення прикладів, що демонструють несприятливі умови, щоб навчити модель розпізнавати зловмисні маніпуляції з даними та захищатися від них.

3. Використання часового і просторового контекст

Фіксування часового і просторового контексту, включивши додаткову інформацію, таку як:

- Мітки часу для відстеження часу кібератак і виявлення закономірностей або тенденцій у часі.
- Географічні метадані для визначення географічного походження або цілі кіберзагроз та атак.
- Інформація про топологію мережі для розуміння структури і зв'язку базової інфраструктури.

4. Забезпечення якості даних

Впровадження заходів забезпечення якості для надійності та цілісності зібраних даних.

Це може включати:

- Перевірку достовірності даних для виявлення та усунення винятків, помилок або невідповідностей.
- Дедуплікацію даних для усунення дублікатів або надлишкових записів у наборах даних.
- Перехресні посилання та перевірку інформації з різних джерел для підтвердження її точності та достовірності.

5. Дотримання конфіденційності та безпеки

Дотримання правил конфіденційності та безпеки при зборі та обробці конфіденційних даних.

Це включає в себе:

- Анонімізація або псевдонімізація інформації, що ідентифікує особу, для захисту приватного життя людей.
- Шифрування даних як під час передачі, так і в стані спокою, щоб запобігти несанкціонованому доступу або розголошенню.
- Впровадження контролю доступу та аудиторських слідів для моніторингу та відстеження використання даних уповноваженим персоналом.

6. Використання гібридних архітектур

Інтегрування декількох архітектур нейронних мереж, а не лише RNN та CNN, щоб використовувати їхні сильні сторони.

Наприклад:

- Графові нейронні мережі (GNN) можуть моделювати взаємозв'язки і залежності між об'єктами в складних мережах, таких як комунікаційні мережі або соціальні мережі.
- Архітектури на основі трансформаторів, такі як Transformer-XL або BERT, можуть фіксувати довгострокові залежності та контекстну інформацію в текстових даних.
- Архітектури автокодерів можна використовувати для неконтрольованого вивчення особливостей і виявлення аномалій в наборах даних з кібербезпеки.

7. Використання ансамблевих методів

Впровадження методів ансамблевого навчання, щоб об'єднати прогнози з декількох моделей для підвищення продуктивності та надійності.

Це може включати:

- Навчання декількох мереж з різною ініціалізацією або архітектурою та об'єднання їхніх прогнозів за допомогою таких методів, як усереднення або голосування.
- Створення ансамблю моделей з різними архітектурами, таких як комбінація RNN, CNN і GNN, щоб охопити взаємодоповнюючі аспекти даних.

8. Використання ієрархічні структур

Розроблення ієрархічних архітектур нейронних мереж, щоб охопити багаторівневі представлення даних.

Наприклад:

- Рекурентні або згорткові шари на нижчих рівнях для вилучення локальних шаблонів і особливостей з окремих зразків даних.
- Рекурентні або засновані на увазі механізми вищого рівня для агрегування інформації з декількох зразків даних або часових кроків і виявлення глобальних закономірностей або тенденцій.

9. Використання механізмів адаптивного навчання

Включення механізмів адаптивного навчання для динамічного налаштування архітектури та параметрів моделі на основі характеристик вхідних даних.

Сюди входять:

- Механізми уваги, які динамічно фокусуються на відповідних частинах вхідних даних, з вагами уваги, що визначаються під час навчання.
- Адаптивні шари об'єднання, які динамічно налаштовують операцію об'єднання на основі розподілу вхідних даних, наприклад, адаптивне середнє об'єднання або просторове об'єднання уваги.

10. Використання мережі з розширенням пам'яті

Дослідження архітектури нейронних мереж з розширеною пам'яттю, щоб включити в модель явні механізми пам'яті. Це дозволяє моделі зберігати і витягувати відповідну інформацію протягом більш тривалих періодів часу, полегшуючи міркування і прийняття рішень.

Приклади включають:

- Нейронні машини Тюрінга (НМТ) або диференційовані нейронні комп'ютери (ДНК), які використовують зовнішні модулі пам'яті для зберігання та доступу до інформації.
- Механізми уваги з розширенням пам'яті, де модель навчається звертати увагу на певні слоти або елементи пам'яті на основі вхідних даних і вимог завдання.

11.Використання напівконтрольованого навчання

Застосування методів напівкерованого навчання, щоб отримати максимальну віддачу від обмежених маркованих даних, використовуючи велику кількість немаркованих даних.

Це може включати:

- Навчання моделі на комбінації маркованих і немаркованих даних, використовуючи такі методи, як самонавчання або псевдомаркування для генерації міток для немаркованих зразків.

– Використання регуляризації узгодженості, коли модель заохочується до створення узгоджених прогнозів для доповнених версій тих самих вхідних даних.

12. Застосування активного навчання

Впровадження стратегії активного навчання для інтелектуального вибору найбільш інформативних зразків для анотації, зменшуючи навантаження на анотацію, одночасно максимізуючи продуктивність моделі.

Це включає в себе

– Використання оцінок невизначеності з моделі для виявлення зразків, де модель є невизначеною або може робити помилки.
– Звернення до людей-анотаторів з проханням позначити ці інформативні зразки, ітеративно покращуючи модель за допомогою нових анотованих даних.

13. Використання багатозадачного навчання

Аналіз підходів багатозадачного навчання для спільного навчання моделі ШІ на декількох пов'язаних завданнях, використовуючи спільні уявлення і покращуючи узагальнення.

Це передбачає:

– Визначення допоміжних завдань, пов'язаних з аналізом кіберзагроз, таких як класифікація шкідливого програмного забезпечення або атрибуція атак.
– Навчання моделі для одночасної оптимізації виконання основного завдання (наприклад, виявлення загроз) і допоміжних завдань, що сприяє передачі і систематизації знань.

14.Обробка потокових даних:

Посилення здатності моделі ШІ обробляти потокові дані в режимі реального часу, що дозволить негайно виявляти і класифікувати загрози в міру їх виникнення.

Це передбачає:

– Впровадження конвеєрів прийому потокових даних для безперервної подачі даних до моделі ШІ без затримок.

– Використання фреймворків потокової обробки, таких як Apache Kafka або Apache Flink, для обробки високопродуктивних потоків даних і забезпечення низької затримки обробки.

15. Застосування онлайн-навчання

Інтегрування методів онлайн-навчання, щоб дозволити моделі ШІ адаптуватися і навчатися на нових даних в режимі реального часу, забезпечуючи її актуальність і ефективність в умовах динамічного ландшафту загроз.

Це включає в себе:

– Впровадження алгоритмів інкрементного навчання, які оновлюють параметри моделі "на льоту", коли стають доступними нові марковані дані.
– Використання таких методів, як стохастичний градієнтний спуск з міні-пакетними оновленнями для ефективного навчання моделі на потокових даних.

16. Впровадження динамічного оновлення моделі

Впровадження механізмів динамічного оновлення моделі для включення нових знань та ідей в модель ШІ без переривання процесу виявлення загроз.

Це передбачає:

– Моніторинг продуктивності моделі і запуск оновлень на основі заздалегідь визначених критеріїв, таких як погіршення точності або зміни в розподілі даних.
– Використання таких методів, як версійність моделі та A/B-тестування, для плавного переходу між різними версіями моделі, мінімізуючи час простою.

17. Використання ситуаційної обізнаності

Розширити можливості ШІ-моделі щодо ситуаційної обізнаності, щоб контекстуалізувати виявлення загроз в рамках ширшого ландшафту кібербезпеки та організаційного контексту.

Це передбачає

– Інтеграцію зовнішніх каналів розвідки загроз і контекстної інформації про інфраструктуру, політики та бізнес-цілі організації.

– Використання таких методів, як графів знань або онтологічних представлень для фіксації зв'язків і залежностей між різними об'єктами і подіями в сфері кібербезпеки.

18. Внесок з відкритим кодом

Слід зробити внесок у проекти та ініціативи з кібербезпеки з відкритим вихідним кодом для обміну знаннями, інструментами та передовим досвідом з ширшою спільнотою кібербезпеки.

Це включає в себе:

– Обмін кодом, бібліотеками та інструментами, розробленими всередині організації, зі спільнотою через репозиторії з відкритим кодом, такі як GitHub.
– Співпраця з іншими організаціями та розробниками, щоб зробити свій внесок у проекти з відкритим кодом та покращити їх функціональність і безпеку.

Розглянуто приклад аналізу трафіку даних з використанням методу штучного інтелекту.

Аналіз трафіку даних з використанням штучного інтелекту (ШІ) використовується для різних цілей в області кібербезпеки та мережевої безпеки. Цей підхід дозволяє виявляти, аналізувати та відстежувати різноманітні кіберзагрози. Основні аспекти використання ШІ включають в себе:

– Виявлення Кіберзагроз (ШІ може аналізувати мережевий трафік, щоб виявляти потенційні загрози, такі як зловмисні атаки, вразливості в системах, витоки даних тощо. Алгоритми машинного навчання можуть виявляти відхилення від норми в мережевому трафіку, які можуть свідчити про атаки).
– Виявлення Аномального Поведінки (ШІ може використовувати аналіз трафіку для виявлення аномальної поведінки користувачів або пристроїв у мережі. Наприклад, алгоритми можуть виявляти незвичайний обсяг або тип даних, які передаються, або підозрілу активність від певних IP-адрес або портів).

– Ідентифікація вразливостей (Аналіз трафіку дозволяє виявити потенційні уразливості у мережевих системах шляхом аналізу трафіку, який може вказувати на некоректну конфігурацію, неправильну обробку даних або інші проблеми безпеки).
– Прогнозування Атак (ШІ може використовувати історичні дані трафіку для прогнозування майбутніх атак і ризиків, що дозволяє приймати запобіжні заходи та підготовленість до можливих загроз).
– Реагування на Загрози в Реальному Часі (ШІ може автоматично реагувати на виявлені загрози в реальному часі, наприклад, шляхом блокування підозрілого трафіку або відключення вразливих систем).
– Покращення Системи Виявлення та Реагування на Інциденти (Аналіз трафіку допомагає вдосконалювати системи виявлення та реагування на інциденти, вдосконалюючи алгоритми, збільшуючи швидкість реакції та покращуючи точність виявлення загроз).

Вдосконалено код, що створює набір даних із 3 послідовними входами та 3 вихідними значеннями в послідовності. Потім він ініціалізує ШІ з вхідним розміром 3, закритим розміром 5 і вихідним розміром 3, а також встановлює швидкість навчання. Врешті решт, він запускає цикл навчання, який навчає ШІ набору даних з використанням вдосконаленого методу.

На рисунку 4.1 здійснюється навчання нейронної мережі з використанням власного алгоритму оновлення ваг.

```
2 references
private double SigmoidDeriv(double arg)
{
    return 1.0 / (1.0 + Math.Exp(arg));
}

1 reference
public void CustomLearning(Vector<double>[] inputs, Vector<double>[] targets, int epoch, double learningRate)
{
    for (var i = 0; i < inputs.Length; i++)
    {
        var x = inputs[i];
        var y = Forward(x);
        var target = targets[i];

        var loss = -target.DotProduct(Vector<double>.Build.DenseOfEnumerable(y.Map(Math.Log)));
        var dy = y - target;
        var dh = (Why.Transpose() * dy + Vector<double>.Build.Dense(hiddenSize)).PointwiseMultiply(hprev.Map(SigmoidDeriv));
        var dbh = dh;
        var dby = dy;

        UpdateWeightsCustom(x, dy, dh, learningRate);
    }

    if (epoch % 100 == 0)
    {
        decimal totalLoss = 0.0M;
        for (var i = 0; i < inputs.Length; i++)
        {
            var x = inputs[i];
            var y = Forward(x);
            var target = targets[i];

            var minLogInput = 1e-15;

            decimal loss = -(decimal)target.DotProduct(Vector<double>.Build.DenseOfEnumerable(y.Map(v => Math.Log(Math.Max(v, minLogInput)))));
            totalLoss += loss;
        }
        Console.WriteLine($"Epoch {epoch}, loss: {totalLoss / inputs.Length}");
    }
}
```

Рисунок 4.1 – Метод навчання штучного інтелекту

На рисунку 4.2 здійснюється оновлення ваг нейронної мережі.

```
1 reference
private void UpdateWeightsCustom(Vector<double> x, Vector<double> dy, Vector<double> dh, double learningRate)
{
    Wxh -= learningRate * (dh.ToColumnMatrix() * x.ToRowMatrix());
    Whh -= learningRate * (dh.ToColumnMatrix() * hprev.ToRowMatrix());
    Why -= learningRate * (dy.ToColumnMatrix() * hprev.ToRowMatrix());
    bh -= learningRate * dh;
    by -= learningRate * dy;
}
```

Рисунок 4.2 – Оновлення для кожного шару

На рисунку 4.3 створюється і тренується рекурентна нейронна мережа (RNN) з використанням власного алгоритму навчання.

```
0 references
public static class Program
{
    static Vector<double>[] inputs = new[]
    {
        Vector<double>.Build.Dense(new[] { 0.1, 0.2, 0.3 }),
        Vector<double>.Build.Dense(new[] { 0.2, 0.3, 0.4 }),
        Vector<double>.Build.Dense(new[] { 0.3, 0.4, 0.5 }),
        Vector<double>.Build.Dense(new[] { 0.4, 0.5, 0.6 }),
    };

    static Vector<double>[] targets = new[]
    {
        Vector<double>.Build.Dense(new[] { 0.2, 0.3, 0.4 }),
        Vector<double>.Build.Dense(new[] { 0.3, 0.4, 0.5 }),
        Vector<double>.Build.Dense(new[] { 0.4, 0.5, 0.6 }),
        Vector<double>.Build.Dense(new[] { 0.5, 0.6, 0.7 }),
    };
    0 references
    public static void Main()
    {
        var rnn = new RNN(inputSize: 3, hiddenSize: 5, outputSize: 3);
        var learningRate = 0.1;
        var numEpochs = 200;

        for (var epoch = 0; epoch < numEpochs; epoch++)
        {
            rnn.CustomLearning(inputs, targets, epoch, learningRate);
        }

        var input = Vector<double>.Build.DenseOfArray(new[] { 0.2, 0.3, 0.4 });
        var output = rnn.Forward(input);
        Console.WriteLine($"Input: {input}");
        Console.WriteLine($"Output: {output}");
    }
}
```

Рисунок 4.3 – Вхідні дані для навчання та запуск

Запустивши код, ми отримаємо треновану рекурентну нейронну мережу (RNN), яка навчалася на заданих вхідних даних та цільових значеннях протягом 200 епох з використанням швидкості навчання 0.1 (Рисунок 4.4).

```
Microsoft Visual Studio Debug Console
Epoch 100, loss: 1,46366247456236775
Input: DenseVector 3-Double
0,2
0,3
0,4

Output: DenseVector 3-Double
0,233333
0,333333
0,433333
```

Рисунок 4.4 – Результат аналізу закодованого трафіку

У цьому прикладі метод CustomLearning замінює попередній метод Learning і має свою власну логіку оновлення ваг та зсувів. Метод UpdateWeightsCustom представляє власний алгоритм оновлення ваг, який можна налаштувати або змінити за власним розсудом.

Розглянемо переваги вдосконаленого методу та методу RNN.

Переваги методу RNN:

Ефективність у часових послідовностях: RNN добре працює з послідовнісними даними, оскільки зберігає попередні стани та використовує їх для роботи з поточним входом.

Простота реалізації: Реалізація RNN досить проста, особливо в порівнянні з більш складними архітектурами, такими як LSTM або Transformer.

Інтерпретація результатів: Ваги та зсуви RNN можуть бути інтерпретовані для аналізу, що допомагає зрозуміти, як мережа приймає рішення.

Недоліки:

Проблема зниклих та вибуваючих градієнтів: У довгих послідовностях RNN можуть стикатися з проблемою зниклих або вибуваючих градієнтів, що призводить до проблем з навчанням та погіршенням результатів.

Обмежена пам'ять: RNN має обмежену пам'ять, оскільки вона може запам'ятовувати лише обмежену кількість попередніх станів.

Новий метод навчання:

Переваги:

Гнучкість: Новий метод навчання може бути спеціалізованим для конкретного завдання, що дозволяє оптимізувати навчання для цілей, які не враховуються стандартними алгоритмами навчання.

Потенційна ефективність: Шляхом розробки спеціалізованого алгоритму навчання можна досягти кращих результатів у порівнянні з загальними методами.

Недоліки:

Складність реалізації: Реалізація та оптимізація власного алгоритму навчання може бути складною та часоємкою.

Потреба в експертизі: Розробка ефективного алгоритму навчання вимагає глибоких знань у галузі машинного навчання та оптимізації.

Вибір між методом RNN та новим методом навчання залежить від конкретного завдання, ваших ресурсів та експертизи в галузі машинного навчання.

Висновки до розділу 4

Методи аналізу кіберзагроз можуть бути поділені на традиційні та з використанням штучного інтелекту. Традиційні методи виявлення кіберзагроз базуються на відомих сигнатурах або відбитках пальців загроз, що дозволяє ефективно виявляти відомі загрози, але не завжди ефективні проти нових або невідомих загроз. З іншого боку, методи з використанням штучного інтелекту, такі як нейронні мережі, байєсівські мережі, генетичні алгоритми та фрактали, надають можливість виявляти аномалії та нові загрози шляхом аналізу поведінки системи та використання складних алгоритмів. Регуляторні органи відіграють важливу роль у створенні стандартів та рамок для управління штучним інтелектом у кібербезпеці, що допомагає забезпечити безпеку та відповідальність в розробці та використанні систем штучного інтелекту.

У тексті розглянуто важливість використання часових рядів для аналізу кіберзагроз. Наводяться приклади застосування часових рядів для виявлення аномалій і незвичайних моделей поведінки в контексті кібербезпеки, таких як DDoS-атаки, несанкціонований доступ, зловмисне програмне забезпечення та прогнозування майбутніх атак. Також зазначається, що інтеграція методів реального часу в системи кібербезпеки може підвищити ефективність виявлення та запобігання кіберзагрозам, і закликає до подальшого дослідження нових методів та алгоритмів для розвитку систем кібербезпеки.

Штучний інтелект відіграє важливу роль у забезпеченні кібербезпеки, допомагаючи виявляти аномалії та нові загрози, фільтрувати спам, реагувати на вразливості та захищати критичні дані. Системи штучного інтелекту можуть виявляти атипову поведінку, автоматично реагувати на загрози, боротися з автоматичними

атаками та відстежувати багато подій одночасно. Однак, разом з перевагами, існують і ризики використання генеративних інструментів штучного інтелекту, такі як погіршення якості коду та можливість використання їх для кібератак. Незважаючи на це, компанії все більше цікавляться інструментами кібербезпеки на основі штучного інтелекту, зокрема в Україні, де ця тенденція стає все більш популярною серед інноваційних банків та підприємств. Однак важливо враховувати вартість таких технологій та їх віддачу на інвестиції в кібербезпеку.

Використовуються рекурентні нейронні мережі (RNN) та передові методи машинного навчання. Основні кроки включають збір різноманітних даних з різних джерел, розширення даних, використання часового і просторового контексту, забезпечення якості даних, дотримання конфіденційності та безпеки, використання гібридних архітектур, ансамблевих методів, ієрархічних структур, механізмів адаптивного навчання, мереж з розширеною пам'яттю, напівконтрольового навчання, активного навчання, багатозадачного навчання, обробки потокових даних, онлайн-навчання, динамічного оновлення моделі, ситуаційної обізнаності та внеску з відкритим кодом. Такий підхід дозволяє ефективно виявляти, аналізувати та реагувати на кіберзагрози в реальному часі.

ВИСНОВКИ

Штучний інтелект у кібербезпеці - це тема, яка викликає значний інтерес у сучасному світі, оскільки кіберзлочинність стає все більшою загрозою для компаній, урядів та приватних осіб. Використання штучного інтелекту у кібербезпеці може мати величезний потенціал у боротьбі з цими загрозами, але також породжує важливі питання та виклики.

По-перше, використання штучного інтелекту у кібербезпеці дозволяє виявляти загрози та атаки швидше та ефективніше. Системи ШІ можуть аналізувати величезні обсяги даних, виявляти незвичайні патерни та вчасно реагувати на потенційні загрози, забезпечуючи більшу безпеку для користувачів.

Пр-друге, застосування штучного інтелекту сприяє автоматизації процесів виявлення та відповіді на кіберзагрози. ШІ може автоматично реагувати на інциденти, виконувати аналіз подій та приймати швидкі рішення без необхідності постійного контролю людського персоналу.

По-третє, існують серйозні виклики та обмеження у використанні штучного інтелекту в кібербезпеці. Наприклад, можливість зламу або обхід захисту системи ШІ, помилки в алгоритмах, а також етичні та приватність питання пов'язані зі збором та обробкою особистих даних.

Отже, штучний інтелект має величезний потенціал у кібербезпеці, проте для досягнення максимальних результатів потрібно ретельно враховувати технічні, етичні та правові аспекти його застосування. Вирішення цих проблем може допомогти розкрити повний потенціал ШІ у забезпеченні кібербезпеки.

Завдання до кваліфікаційної роботи виконано в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Малиновський Б. М. Відоме і невідоме в історії інформаційних технологій в Україні / Б. М. Малиновський – К.: Академперіодика, 2001.– 214 с.

2. Anderson M. Robot be good / M. Anderson, S. L. Anderson // Scientific American. – 2010. – October. – pp. 53–59.

3. Все, що потрібно знати про штучний інтелект сьогодні. – [Електронний ресурс]: https://tokar.ua/read/34132

4. Галина Машлій; Ольга Мосій; Мар'яна Пельчер. «ДОСЛІДЖЕННЯ УПРАВЛІНСЬКИХ АСПЕКТІВ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ»

5. Історія розвитку галузі штучного інтелекту. – [Електронний ресурс]: http://opticstoday.com/katalog-statej/stati-na-ukrainskom/shtuchnij-intelekt/istoriya-rozvitku-galuzi-shtuchnogo-intelektu.html

6. Історія розвитку ідей та реалізації штучного інтелекту – [Електронний ресурс]: https://wiki.cuspu.edu.ua/index.php/Історія_розвитку_ідей_штучного_інтелекту_і_їх_реалізації)

7. Погороленко К.А. «ШТУЧНИЙ ІНТЕЛЕКТ: СУТНІСТЬ, АНАЛІЗ ЗАСТОСУВАННЯ, ПЕРСПЕКТИВИ РОЗВИТКУ»(3)

8. Штучний інтелект: історія та перспективи. – [Електронний ресурс]: https://naub.oa.edu.ua/2013/shtuchnyj-intelekt-istoriya-ta-perspektyvy/(6)

9. Штучний інтелект – потенційний ворог чи перший помічник в майбутньому – [Електронний ресурс]: https://blog.comfy.ua/shtuchnijj-intelekt-potencijjnijj-vorog-chi-pershijj-pomichnik-v-majjbutnomu/amp/#aoh=15709662371965&referrer=https%3A%2F%2Fwww.google.com&amp_tf=Джерело%3A%20%251%24s(2)

10. Штучний інтелект (ШІ): Що це таке і чому це важливо? – [Електронний ресурс]: https://www.everest.ua/ai-platform/analytics/shtuchnij-intelekt-ai-shho-ce-take-i-chomu-ce-v/(4)

11. Штучний інтелект: що це і яку несе небезпеку – [Електронний ресурс]: https://24tv.ua/lifestyle/shtuchniy_intelekt_shho_tse_i_yaku_nese_nebezpeku_n914662

12. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. Information Systems And Networks. 2022. № 12. С. 7-20.

13. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. № 4 (44). С. 6-11.

14. Стьопочкіна І.В., Новіков О.М. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 “Кібербезпека”. Київ: КПІ ім. Ігоря Сікорського, 2022. 82 с.

15. Шаров С.В. Сучасний стан розвитку штучного інтелекту та напрямки його використання: зб. наук. пр. Інноваційні обрії України. 2023. № 6. С.136-144. – (Громадська організація Українські студії в європейському контексті).

16. Цяпа С.М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах. Інформація і право. № 2(37)/2021. С. 51-59.

17. Tuomo Sipola, Tero Kokknen, Mika Karjalainen Artificial Intelligence and Cybersecurity: Theory and Applications. JAMK University of Applied Sciences. Publisher: Springer; 1st ed. 2023 edition 311 p. DOI 10.1007/978-3-031-15030-2

18. Narcisa Roxana Mosteanu. Artifical Inelligence and cyber security – face to face with cyber attack – a maltese case of risk management approach. Ecoforum journal. 2020. Vol 9. № 2. – [Електронний ресурс]: http://www.ecoforumjournal.ro/index.php/eco/article/view/1059

19. Rammanohar Das, Raghav Sandhane. Artificial Intelligence in Cyber Security. ICACSE 2020. IOP Publishing. Journal of Physics: Conference Series 1964 (2021). P.1-10 doi:10.1088/1742-6596/1964/4/042072. – [Електронний ресурс]: https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf

20. Гладка Ю.А., Назаренко Є.О. Аналіз застосування технологій штучного інтелекту в кібербезпеці: наукові праці третьої Міжнар. наук.-практ. конф. Сучасні

тенденції розвитку інформаційних систем і телекомунікаційних технологій, м. Київ, 25 – 26 січня 2021 р. Київ: НУХТ, 2021. С. 64-66.

21. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження

22. Кабінету Міністрів України від 02.12.20 р. № 1556 – [Електронний ресурс]: https://zakon.rada.gov.ua/laws/show/ 1556-2020-р#Text

23. Про затвердження Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021 – 2024 роки: Розпорядження Кабінету Міністрів України від 12.05.21 р. № 438 – [Електронний ресурс]: https://zakon.rada.gov.ua/laws/show/438-2021-р#Text т

24. Федоров: в Україні став доступний чат-бот зі штучним інтелектом ChatGPT. – (Українські національні новини від 18.02.23 р.). – [Електронний ресурс]: https://www.unn.com.ua/uk/news/2016033-fedorov-v-ukrayini-stav-dostupniy-chat-bot-zi-shtuchnim-intelektom-chatgpt

25. ChatGPT. The impact of Large Language Models on Law Enforcement. Europol Public Information. – [Електронний ресурс]: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20Enforcement.pdf

26. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. – [Електронний ресурс]: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

27. Веселова, Л. Ю. (2021). Адміністративно-правові основи кібербезпеки в умовах гібридної війни [Дис. д-ра]. – [Електронний ресурс]: http://oduvs.edu.ua/wp-content/uploads/2016/06/Disertatsiya_Veselovoi_L.YU..pd

28. Що таке фішинг і як від нього захиститися? – [Електронний ресурс]: https://www.tecnoseguro.com/media/k2/items/cache/a7ac92c0202d08b485ecb09c07ac6372_XL.jpg

29. Безпека у кіберпросторі. Головна. – [Електронний ресурс]: https://defpol.org.ua/index.php/produkty-tsentru/49-shliakhukrainy-do-nato/1126-bezpeka-u-kiberprostori.

30. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX|ЮРЛІГА.ЮРЛІГА. – [Електронний ресурс]: https://jurliga.ligazakon.net/analitycs/210562_borotba-zkberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix

31. Війна росії проти україни почалася з кібернападу на супутники. за годину до вторгнення були знищені «десятки тисяч» терміналів Viasat - itc.ua. ITC.ua. – [Електронний ресурс]: https://itc.ua/ua/novini/vijna-rosiyi-protiukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-znishheni-desyatkitisyach-terminaliv-viasat\

32. Канада надає україні розвіддані про кіберзагрози – tokar.ua. – [Електронний ресурс]: https://tokar.ua/read/48906

33. Як малому бізнесу захистити себе від кіберзагроз. – [Електронний ресурс]: https://businessviews.com.ua/files/news_tape/images/20/40/picture_jak-malomu-biznesuz_2040_s1.png.pagespeed.ce.A4LXWNL4hg.png.

34. Комітет з питань цифрової трансформації інформує як посилити кіберзахист підприємствам та установам. Офіційний портал Верховної Ради України. – [Електронний ресурс]: https://www.rada.gov.ua/news/razom/221800.html.

35. Стогній Д.Є. (2023). Дослідження чатів із нейронними мережами великих мовних моделей у протиправній діяльності в сфері кіберпростору.

36. Властивості інтелектуальних агентів //Студопедія. – [Електронний ресурс]: https://studopedia.com.ua/1_7219_vlastivosti-intelektualnih-agentiv.html

37. Малиновський Б. М. Відоме і невідоме в історії інформаційних технологій в Україні / Б. М. Малиновський – К.: Академперіодика, 2001.– 214 с.

38. Подгаєцький О. О. Проблема штучного інтелекту / О. О. Подгаєцький // Україна і світ: гуманітарно- технічна еліта та соціальний прогрес [зб. тез Міжнар. наук.–теор. конференції студ. та аспір.

39. Глинський Я.М. Штучний інтелект. Інтелектуальні роботи /Я.М.Глинський, В.А. Ряжська В.А. – Львів: Деол, 2002. - 168 с.

40. Комп'ютерні системи штучного інтелекту. Методичні вказівки до виконання лабораторних робіт студентами денної та заочної форми навчання

спеціальностей 123 «Комп'ютерна інженерія», 122 «Комп'ютерні науки та інформаційні технології» / Укл.: Є.В. Мелешко – Кіровоград: КНТУ, 2016. – С.8-13.І.В. Калініна, О.І. Лісовиченко Використання генетичних алгоритмів в задачах оптимізації / Міжвідомчий науково-технічний збірник. 2015. – № 1(26).

41. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Handwritten character recognition models based on convolutional neural networks, International Journal of Academic Engineering Research, 7(9), pp. 64-72.

42. Gorokhovatskyi V., Tvoroshenko I. (2023) Identification of visual objects by the search request. International scientific symposium «INTELLIGENT SOLUTIONS-S». Computational intelligence (results, problems and perspectives). Decision making theory: proceedings of the international symposium, September 28, 2023, Kyiv-Uzhorod, Ukraine, pp. 25-27.

43. Yakovleva O., Kovač M., Ardasov V. & Yeremenko I. (2023). Study on adding functionality to the Zoom online conference system for monitoring the participant activities, Public Administration and Regional Development, 19(1), pp. 158-184.

44. Liguo Zhao, Derong Zhu, Wasswa Shafik, S Mojtaba Matinkhah, Zubair Ahmad, Lule Sharif, and Alisa Craig. Artificial intelligence analysis in cyber domain: A review(2022) – [Електронний ресурс]: https://journals.sagepub.com/doi/epub/10.1177/15501329221084882

45. Bilal Alhayani, Husam Jasim Mohammed, Ibrahim Zeghaiton Chaloob, Jehan Saleh Ahmed. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry(2021) – [Електронний ресурс]: https://d1wqtxts1xzle7.cloudfront.net/66000244/1_s2.0_S2214785321016722_main-libre.pdf?1615679123=&response-content-disposition=inline%3B+filename%3DEffectiveness_of_artificial_intelligence.pdf&Expires=1715546788&Signature=PGZygrKWHtJqrrRtBNC8DPlxJMN2Nsjc10UpCFB8wRQIKDGHfmQE-75lqz8ryYVCPJjALnL3J4kT9P~I5FZvgCt2xmGm04gKP8OzAwAjXJKmuNCKvocK0j~PHbmKT0Oa3pMwrEru5QrN8IU~vNSMQhBmftj2qCBZM-j0Ru~0IHl4i7UwwQt3UyxdiFYOcVtZ-hJ5fQVq-

TI0xQEYGsuUzI1~LKRwXMXfVYPuqbEKYrvTbGtFST8MOGS4nFbV53fvrdZwYNK
ODgI1MinE9QHwYxNiT6OoHH6bnjZHY4HJX-pIYrQ-xpC--
T67AMwCZblDqN8ImBndA3XzejQcK7Mxvw__&Key-Pair-
Id=APKAJLOHF5GGSLRBV4ZA

46. Arab Mohammed Shamiulla. Role of Artificial Intelligence in Cyber Security (2019) – [Електронний ресурс]: https://d1wqtxts1xzle7.cloudfront.net/85177722/A6115119119-libre.pdf?1651244167=&response-content-disposition=inline%3B+filename%3DRole_of_Artificial_Intelligence_in_Cyber.pdf&Expires=1715546837&Signature=W9~p6E57XMdJDABZMqB2diSwwhC2jwLuy8xmzhQrOKgc0OYdhU7C1-Xep7xKJEfRJCD5pfBpe6hcuIXrVZbCmCTVl8qQ1uvLJU~pnzT59KuaVlgc6h-1GP1Sx~vHiRUTNyLyux6qawe6AsUMt1PptK6f2gO3Q33-az~H3D69NR3VLFfo5VizgdOCjSNS2RgTS6b66fkU1d~QzVvgXfQkL48sAN7daMfRZeKE3U9noWgAHlwZFt2JwgMNgWb0EtvCR6pm3jox3F3mH8JI20~UiRltIprHtBd2I8y4no0VLuVCSZVQUCJ4NbFldD56ps~eTNoSU0YAIX-rBp5eJXPDSA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

47. Ashok Manoharan, Mithun Sarker. REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXTGENERATION THREAT DETECTION (2022) – [Електронний ресурс]: https://www.researchgate.net/profile/Mithun-Sarker-4/publication/379044498_Revolutionizing_Cybersecurity_Unleashing_the_Power_of_Artificial_Intelligence_and_Machine_Learning_for_Next-Generation_Threat_Detection/links/65f8525e1f0aec67e2a65bb9/Revolutionizing-Cybersecurity-Unleashing-the-Power-of-Artificial-Intelligence-and-Machine-Learning-for-Next-Generation-Threat-Detection.pdf

48. Mohan Raparthi, Sarath Babu Dodda, SriHari Maruthi. Examining the use of Artificial Intelligence to Enhance Security Measures in Computer Hardware, including the Detection of Hardware-based Vulnerabilities and Attacks (2020) – [Електронний ресурс]: https://eelet.org.uk/index.php/journal/article/view/991/863

49. Rammanohar Das and Raghav Sandhane. Artificial Intelligence in Cyber Security (2021) – [Електронний ресурс]: https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/meta

50. Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar. Artificial intelligence for cybersecurity: Literature review and future research directions (2023) – [Електронний ресурс]: https://www.sciencedirect.com/science/article/pii/S1566253523001136

ДОДАТКИ

ДОДАТОК А. Лістинг програмного коду

```
using MathNet.Numerics.LinearAlgebra;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace AICS
{
   public class RNN
   {
      /*
      ці змінні визначають розмірності вхідного шару,
      прихованого шару та вихідного шару мережі.
      */
      private int inputSize;
      private int hiddenSize;
      private int outputSize;

      /*
       ці змінні представляють матриці ваг між різними шарами мережі
       */
      private Matrix<double> Wxh;
      private Matrix<double> Whh;
      private Matrix<double> Why;
      /*
       * ці змінні представляють вектори зсуву (bias) для
       * прихованого та вихідного шарів мережі.
       */
      private Vector<double> bh;
      private Vector<double> by;
      //ця змінна зберігає попередній стан прихованого шару мережі.
      private Vector<double> hprev;
      private Vector<double> hnext;

      //конструктор класу RNN, який ініціалізує всі
      //ваги та зсуви мережі випадковими значеннями.
      public RNN(int inputSize, int hiddenSize, int outputSize)
      {
         this.inputSize = inputSize;
         this.hiddenSize = hiddenSize;
         this.outputSize = outputSize;

         // Initialize weight matrices and bias vectors
         Wxh = Matrix<double>.Build.Random(hiddenSize, inputSize);
         Whh = Matrix<double>.Build.Random(hiddenSize, hiddenSize);
         Why = Matrix<double>.Build.Random(outputSize, hiddenSize);
         bh = Vector<double>.Build.Random(hiddenSize);
         by = Vector<double>.Build.Random(outputSize);
         hprev = Vector<double>.Build.Dense(hiddenSize);
         hnext = Vector<double>.Build.Dense(hiddenSize);
```

```
}
//метод, який реалізує передовий прохід мережі.
//Він обчислює вихідний вектор мережі для вхідного вектора x
public Vector<double> Forward(Vector<double> x)
{
    // Update hidden state
    var h = Sigmoid(Wxh * x + Whh * hprev + bh);

    // Compute output
    var y = Softmax(Why * h + by);

    // Store hidden state for next time step
    hprev = h;

    return y;
}
public Vector<double> Forward2(Vector<double> x)
{
    // Update hidden state
    var h = Sigmoid(Wxh * x + Whh * hprev + bh);

    // Compute output
    var y = Softmax(Why * h + by);

    // Store hidden state for next time step
    hprev = h;

    return y;
}
public Vector<double> Forward3(Vector<double> x)
{
    // Update hidden state
    var h = Sigmoid(Wxh * x + Whh * hprev + bh);

    // Compute output
    var y = Softmax(Why * h + by);

    // Store hidden state for next time step
    hprev = h;

    return y;
}
public Vector<double> Forward4(Vector<double> x)
{
    // Update hidden state
    var h = Sigmoid(Wxh * x + Whh * hprev + bh);

    // Compute output
    var y = Softmax(Why * h + by);

    // Store hidden state for next time step
    hprev = h;

    return y;
}
//внутрішній метод, який обчислює сигмоїдальну функцію активації для вектора x
private Vector<double> Sigmoid(Vector<double> x)
{
    return x.Map(v => 1 / (1 + Math.Exp(-v)));
}
// це внутрішній метод, який обчислює функцію активації softmax для вектора x
private Vector<double> Softmax(Vector<double> x)
{
```

```
        var expX = x.Map(v => Math.Exp(v));
        var sumExpX = expX.Sum();
        return expX / sumExpX;
    }
    // Метод стохастичний градієнтний спад, щоб оновити ваги та зміщення на основі різниці між прогнозованим і фактичним виходом
    public void Learning(Vector<double>[] inputs, Vector<double>[] targets, int epoch, double learningRate)
    {
        // Loop over input sequences
        for (var i = 0; i < inputs.Length; i++)
        {
            // Forward pass
            var x = inputs[i];
            var y = Forward(x);
            var target = targets[i];

            // Compute loss and gradients
            var loss = -target.DotProduct(Vector<double>.Build.DenseOfEnumerable(y.Map(Math.Log)));
            var dy = y - target;
            var dh = (Why.Transpose() * dy + Vector<double>.Build.Dense(hiddenSize)).PointwiseMultiply(hprev.Map(SigmoidDeriv));
            var dbh = dh;
            var dby = dy;

            // Update weights and biases
            Why -= learningRate * (dy.ToColumnMatrix() * hprev.ToRowMatrix());
            by -= learningRate * dby;
            Whh -= learningRate * (dh.ToColumnMatrix() * hprev.ToRowMatrix());
            bh -= learningRate * dbh;
            Wxh -= learningRate * (dh.ToColumnMatrix() * x.ToRowMatrix());
        }

        // Print loss for this epoch
        if (epoch % 100 == 0)
        {
            decimal totalLoss = 0.0M;
            for (var i = 0; i < inputs.Length; i++)



            {
                var x = inputs[i];
                var y = Forward(x);
                var target = targets[i];

                var minLogInput = 1e-15;

                decimal loss = -(decimal)target.DotProduct(Vector<double>.Build.DenseOfEnumerable(y.Map(v => Math.Log(Math.Max(v, minLogInput)))));
                totalLoss += loss;
            }
            Console.WriteLine($"Epoch {epoch}, loss: {totalLoss / inputs.Length}");
        }
    }

    private double SigmoidDeriv(double arg)
    {
        return 1.0 / (1.0 + Math.Exp(arg));
    }

    public void CustomLearning(Vector<double>[] inputs, Vector<double>[] targets, int epoch, double learningRate)
    {
```

```
            for (var i = 0; i < inputs.Length; i++)
            {
                var x = inputs[i];
                var y = Forward(x);
                var target = targets[i];

                var loss = -target.DotProduct(Vector<double>.Build.DenseOfEnumerable(y.Map(Math.Log)));
                var dy = y - target;
                var dh = (Why.Transpose() * dy +
Vector<double>.Build.Dense(hiddenSize)).PointwiseMultiply(hprev.Map(SigmoidDeriv));
                var dbh = dh;
                var dby = dy;

                UpdateWeightsCustom(x, dy, dh, learningRate);
            }

            if (epoch % 100 == 0)
            {
                decimal totalLoss = 0.0M;
                for (var i = 0; i < inputs.Length; i++)
                {
                    var x = inputs[i];
                    var y = Forward(x);
                    var target = targets[i];

                    var minLogInput = 1e-15;

                    decimal loss = -(decimal)target.DotProduct(Vector<double>.Build.DenseOfEnumerable(y.Map(v =>
Math.Log(Math.Max(v, minLogInput)))));
                    totalLoss += loss;
                }
                Console.WriteLine($"Epoch {epoch}, loss: {totalLoss / inputs.Length}");
            }
        }

        private void UpdateWeightsCustom(Vector<double> x, Vector<double> dy, Vector<double> dh, double learningRate)
        {
            Wxh -= learningRate * (dh.ToColumnMatrix() * x.ToRowMatrix());
            Whh -= learningRate * (dh.ToColumnMatrix() * hprev.ToRowMatrix());
            Why -= learningRate * (dy.ToColumnMatrix() * hprev.ToRowMatrix());
            bh -= learningRate * dh;
            by -= learningRate * dy;
        }
    }
    public static class Program
    {
        static Vector<double>[] inputs = new[]
        {
            Vector<double>.Build.Dense(new[] { 0.1, 0.2, 0.3 }),
            Vector<double>.Build.Dense(new[] { 0.2, 0.3, 0.4 }),
            Vector<double>.Build.Dense(new[] { 0.3, 0.4, 0.5 }),
            Vector<double>.Build.Dense(new[] { 0.4, 0.5, 0.6 }),
        };

        static Vector<double>[] targets = new[]
        {
            Vector<double>.Build.Dense(new[] { 0.2, 0.3, 0.4 }),
            Vector<double>.Build.Dense(new[] { 0.3, 0.4, 0.5 }),
            Vector<double>.Build.Dense(new[] { 0.4, 0.5, 0.6 }),
            Vector<double>.Build.Dense(new[] { 0.5, 0.6, 0.7 }),
        };
        public static void Main()
        {
```

```
        var rnn = new RNN(inputSize: 3, hiddenSize: 5, outputSize: 3);
        var learningRate = 0.1;
        var numEpochs = 200;

        for (var epoch = 0; epoch < numEpochs; epoch++)
        {
            rnn.CustomLearning(inputs, targets, epoch, learningRate);
        }

        var input = Vector<double>.Build.DenseOfArray(new[] { 0.2, 0.3, 0.4 });
        var output = rnn.Forward(input);
        Console.WriteLine($"Input: {input}");
        Console.WriteLine($"Output: {output}");
    }
  }
}
```