Висновки. Глибинне навчання є складною і потужною галуззю машинного навчання, яка використовує нейронні мережі для обробки великих обсягів даних.

Для повного розуміння цієї технології необхідно мати ґрунтовні знання основ машинного навчання та деяких розділів математики, як-от лінійна алгебра, теорія ймовірностей, теорія диференціальних рівнянь та математичний аналіз.

Машинне навчання дає змогу вирішувати різноманітні задачі, які не можуть бути розв'язані традиційними програмами, а також допомагає зрозуміти принципи розумної поведінки.

Основні задачі машинного навчання включають класифікацію, транскрипцію та переклад, а методи оптимізації, як-от градієнтний спуск, відіграють ключову роль у досягненні успішних результатів.

Отже, математика відіграє вважливу роль у глибинному навчанні, а розвиток нейронних мереж сприяє прогресу в майбутньому.

Список використаних джерел

1. Neural Ordinary Differential Equations. arXiv / R. T. Q. Chen, Y. Rubanova, J. Bettencourt, D. Duvenaud. 2018. 12 p.

2. Michelucci U. Fundamental Mathematical Concepts for Machine Learning in Science. Dubendorf: Springer, 2024. 249 p.

3. Goodfellow I., Bengio Y., Courvill A. Deep Learning. Cambridge, Massachusetts: MIT Press, 2016. 800 p.

УДК 004.422.5

Слободяник Р. Р., здобувач вищої освіти,
Поремський Ю. В., канд. техн. наук,
старший викладач кафедри інформаційних технологій

ОСОБЛИВОСТІ ВИКОРИСТАННЯ АЛГОРИТМІВ У КІБЕРБЕЗПЕЦІ

Донецький національний університет імені Василя Стуса, м. Вінниця

У світі сучасних інформаційних технологій алгоритми відіграють вирішальну роль у забезпеченні кібербезпеки. Вони застосовуються для захисту систем, мереж і даних від несанкціонованого доступу, модифікації чи втрати. Одним із головних завдань кібербезпеки є забезпечення конфіденційності, цілісності та доступності інформації, що досягається через використання алгоритмів шифрування, хешування, цифрових підписів, а також методів машинного та глибинного навчання [1].

Алгоритми шифрування є основою кіберзахисту. Вони дають змогу перетворювати відкриті дані у зашифровану форму, недоступну для сторонніх. Наприклад, Advanced Encryption Standard (AES) використовується у багатьох сучасних системах для захисту конфіденційних даних. Алгоритми типу RSA

забезпечують ефективний захист завдяки використанню пар ключів – приватного та публічного [1].

Алгоритми хешування (SHA-256, MD5) забезпечують перевірку цілісності даних і безпечне зберігання паролів. Наприклад, під час введення користувачем пароля система порівнює збережений у базі хеш значення з отриманим після хешування введеного пароля. Це виключає ризик зберігання відкритих паролів [1].

Натомість цифрові підписи, реалізовані за допомогою алгоритмів, як-от ECDSA, забезпечують автентичність електронних документів та повідомлень. Вони допомагають ідентифікувати підписанта та виявляти зміни в документі, якщо вони відбулися [1].

Крім традиційних алгоритмів, активно розвиваються методи машинного навчання (ML) та глибинного навчання (DL). Ці технології дають змогу ефективно виявляти загрози шляхом аналізу великих обсягів даних. Наприклад, Convolutional Neural Networks (CNN) аналізують мережевий трафік для виявлення аномалій, а Graph Neural Networks (GNN) моделюють складні зв’язки у кібербезпекових даних [2, 3].

Моделі на основі Federated Learning (FL) дають змогу забезпечувати конфіденційність даних під час навчання моделей машинного навчання, оскільки дані залишаються на локальних пристроях. Такий підхід застосовується у фінансових системах для виявлення шахрайства [2].

Сучасні розробки також включають технологію Adversarial Learning, яка забезпечує стійкість систем до атак з використанням модифікованих даних. Ця технологія дає змогу виявляти навіть складні форми шкідливих дій [2].

Розуміння ролі алгоритмів у кібербезпеці є ключовим для створення стійких систем захисту. Вони забезпечують основу для побудови ефективних механізмів захисту від загроз та створення безпечного цифрового простору.

Список використаних джерел

1. Що таке алгоритм. Терміни та визначення кібербезпеки. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/algorithm (дата звернення 30.11.2024).

2. Machine Learning Algorithms for Detecting and Preventing Cyber Threats. URL: https://www.oxjournal.org/machine-learning-algorithms-for-detecting-and-preventing-cyber-threats/ (дата звернення 30.11.2024).

3. Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review. URL: https://www.sciencedirect.com/science/article/abs/pii/S157401372030417 (дата звернення 30.11.2024).