

УДК 004.8

Воскобойник В.О.¹, Савченко Ю. В.², Семеренко П.О.³

¹ канд., техн., наук, доц. НУ «Запорізька політехніка»

² канд., техн., наук, доц. Університету митної справи та фінансів

³ студ. гр. БК-813м НУ «Запорізька політехніка»

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У БАГАТОФАКТОРНІЙ АВТЕНТИФІКАЦІЇ

Актуальність застосування штучного інтелекту (ШІ) у багатофакторній автентифікації (БФА) значно зростає в умовах зростання кіберзагроз і дедалі більшої складності атак [1-3].

Кібербезпека залишається головною проблемою в сучасному ІТ-світі оскільки кількість хакерських інцидентів зростає. Багато аспектів нашого життя перемістилися в Інтернет, що комерційний і приватний світи можуть багато втратити через порушення безпеки.

У відповідь спеціалісти з кібербезпеки розгортають арсенал засобів захисту та протидії, щоб забезпечити безпеку даних і конфіденційної інформації. Враховуючи величезну кількість і різноманітність доступних сьогодні атак, це величезне завдання.

Ціллю даної роботи є аналіз методів моделювання штучного інтелекту у багатофакторній автентифікації, а також питання щодо захисту нейронних мереж від кібератак.

У багатофакторній автентифікації застосовуються наступні методи і фактори.

Біометричні методи:

- статичні біометричні фактори: включають розпізнавання обличчя, відбитків пальців, сканування райдужної оболонки та інші фізичні характеристики користувачів;

- динамічні біометричні фактори: сюди входять такі аспекти, як аналіз голосу, манера ходьби та інші характеристики, що змінюються в реальному часі.

Поведінкові фактори:

- поведінкова біометрія: включає аналіз поведінкових шаблонів, наприклад, ритму натискання клавіш, стилю введення тексту, шаблонів використання пристрою тощо;

- аналіз контексту та дій користувача: враховує інформацію про пристрої, місцезнаходження користувача, його дії в системі та інші показники, що допомагають ідентифікувати особу на основі звичних дій.

Контекстуальні фактори: використання додаткових даних про середовище або поведінку, наприклад, місцезнаходження, часу доби, типу пристрою або мережі для оцінки ризику при спробі входу.

Гібридні методи та багатофакторна автентифікація - це комбіновані методи, які поєднують кілька різних факторів (наприклад, біометрію та поведінкові шаблони), що дозволяє забезпечити більш надійний захист.

Ця структура допомагає визначити типи ШІ-технологій, що можуть використовуватися для побудови більш гнучких та адаптивних систем автентифікації.

Глибоке навчання і комп'ютерний зір використовуються для обробки та розпізнавання складних біометричних даних, таких як обличчя, відбитки пальців та райдужка ока або іншим візуальним біометричним параметрам. Розпізнаються з візуальних даних унікальні риси користувача з високою точністю завдяки аналізу великої кількості відео- або фотозображення і аудіофайлів.

Обробка природної мови (NLP) використовується для розпізнавання голосу або обробки текстових команд як частини автентифікаційного процесу. NLP дозволяє автентифікувати користувачів на основі мовних моделей, що враховують індивідуальні особливості голосу чи манери спілкування користувача.

Аналіз поведінкових патернів включає аналіз шаблонів користувача, наприклад, швидкість введення тексту або ритм натискання клавіш. Цей підхід дозволяє ідентифікувати відхилення від звичайної поведінки користувача та виявляти можливі спроби несанкціонованого доступу.

Технології машинного навчання (ML) використовуються для аналізу поведінкових шаблонів та контексту. Вони допомагають створювати моделі на основі минулих даних користувача, що дозволяє виявляти аномалії та потенційні загрози. Наприклад, ML може відстежувати поведінкові патерни під час введення тексту або використання пристроїв.

Генеративні моделі та мережі (наприклад, GANs) застосовуються для навчання на синтетичних даних і здатні імітувати реальні поведінкові та біометричні патерни. Генеративні моделі можуть створювати додаткові дані для тренування систем безпеки, що особливо корисно для розвитку та тестування нових підходів у БФА.

Адаптивні системи, де поєднуються кілька технологій ШІ для динамічної обробки контексту та даних користувачів.

Основні виклики для ШІ у багатофакторній автентифікації:

- *конфіденційність*. Використання поведінкових та біометричних даних може призводити до проблем з конфіденційністю, оскільки необхідно зберігати та обробляти велику кількість чутливих даних;

- *підробка біометрії*. Незважаючи на точність ШІ, існують ризики підробки біометричних параметрів. Це може призвести до того, що злоумисники обійдуть систему, використовуючи, наприклад, штучно створені обличчя;

- *ефективність у реальному часі*. Реалізація в реальному часі для безперервного моніторингу вимагає великих обчислювальних ресурсів, що може впливати на продуктивність систем.

Використання штучного інтелекту для обходу багатофакторної автентифікації набуває широкого поширення в кіберзагрозах.

Також залишається актуальним питання щодо захисту нейронних мереж від кібератак.

На першому, найбільш складному етапі завдання протидії кібератакам зводиться до ідентифікації подій, пов'язаних з реалізацією в кібернетичному просторі загроз безпеці ресурсів інформаційних систем з урахуванням їх уразливостей. Іншими словами, дана ідентифікація це виявлення та класифікація будь-яких видів несанкціонованих дій по відношенню до цих ресурсів.

Також недоліками відомих коштів протидії кібератакам на мережеві ресурси інформаційних систем є висока вартість та відсутність докладної науково-технічної документації. Дослідження вчених вказують на те, що розпізнавання мережевих кібератак є використання в них апарату штучних нейронних мереж.

Розпізнавання мережевих кібератак можна визначити як процес моніторингу (реєстрації та аналізу) параметрів мережевого трафіку на наявність ознак порушення політики безпеки та спроби поставити під загрозу конфіденційність, цілісність, доступність, або обійти механізми безпеки хоста чи мережі.

В даний час процес протидії мережевим кібератакам реалізується з використанням двох основних методів: визначення аномалій та визначення зловживань. Одним з основних шляхів захисту є впровадження методів аналізу мережевого трафіку, що базуються на сучасних рішеннях теорії штучних нейронних мереж.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Guangyi Zhu, Yasir Al-Qaraghuli "AI-Assisted Authentication: State of the Art, Taxonomy and Future Roadmap" [Електронний ресурс]. – Режим доступу: <https://arxiv.org/abs/2204.12492>

2. Kutub Thakur, Md Liakat Ali, Muath A. Obaidat, Abu Kamruzzaman "A Systematic Review on Deep-Learning-Based Phishing Email Detection"[Электронный ресурс]. – Режим доступа:<https://www.mdpi.com/2079-9292/12/21/4545>

3. Ayodeji Oseni, Nour Moustafa, Helge Janicke, Peng Liu, Zahir Tari, Athanasios Vasilakos "A Survey of Artificial Intelligence in Cybersecurity"[Электронный ресурс]. – Режим доступа: <https://arxiv.labs.arxiv.org/html/2102.04661>