УДК 004.056.5

А.В. Семенюк

ВДОСКОНАЛЕННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ЕФЕКТИВНОГО ВИЯВЛЕННЯ ТА БОРОТЬБИ ЗІ ШКІДЛИВИМИ ПРОГРАМАМИ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

Ця стаття присвячена вдосконаленню алгоритмів машинного навчання для виявлення та боротьби зі шкідливими програмами (вірусами, троянами, шпигунськими програмами тощо) в комп'ютерних системах. В роботі розглядаються ключові питання, пов'язані з цією тематикою, включаючи об'єкт та предмет дослідження, а також основні завдання та висновки, що виникають під час дослідження.

Ключові слова: машинне навчання, шкідливі програми, виявлення, боротьба, алгоритми, комп'ютерні системи, кібербезпека.

Abstract

This article is devoted to the most thorough machine learning algorithms for identifying and combating harmful programs (viruses, Trojans, spyware, etc.) in computer systems. The work contains key points related to this topic, including the object and subject of investigation, as well as the main tasks and principles that arise at the time of investigation.

Key words: machine learning, faulty programs, detection, combating, algorithms, computer systems, cybersecurity.

Вступ

В сучасному цифровому світі, де комп'ютери та мережі відіграють невід'ємну роль у нашому житті, кібербезпека стає дедалі важливішою. Швидке розширення мережі Інтернет та збільшення кількості цифрових пристроїв призвело до появи великої кількості загроз у формі шкідливих програм, вірусів, троянів, шпигунського ПЗ та інших видів зловмисного програмного забезпечення.

Способи атак на комп'ютерні системи стають все більш вдосконаленими, та традиційні методи виявлення та захисту нерідко виявляються неспроможними відвернути загрози. У такому контексті, машинне навчання виступає як ключовий інструмент для виявлення та боротьби зі шкідливими програмами в комп'ютерних системах.

Ця стаття присвячена дослідженню та вдосконаленню алгоритмів машинного навчання з метою підвищення ефективності виявлення шкідливих програм. Ми розглянемо основні аспекти, пов'язані з цією тематикою, включаючи різні види шкідливого програмного забезпечення, оптимізацію алгоритмів та важливість співпраці у галузі кібербезпеки. Виходячи з цих аспектів, ми розглянемо, як машинне навчання може допомогти забезпечити вищий рівень кібербезпеки в нашому цифровому світі.

Метою дослідження є покращення засобів виявлення та боротьби зі шкідливими програмами в комп'ютерних системах за допомогою методів машинного навчання.

Об’єктом дослідження є комп'ютерні системи та їхні користувачі, які стикаються з ризиком впливу шкідливих програм на їхню працездатність і конфіденційність даних.

Предметом дослідження є алгоритми машинного навчання, які використовуються для виявлення та боротьби зі шкідливими програмами в комп'ютерних системах.

Головною задачею є оптимізація алгоритмів машинного навчання, які дозволять виявляти та ефективно боротися з різноманітними шкідливими програмами. Це включає в себе завдання виявлення

нових видів шкідливого програмного забезпечення, покращення точності виявлення та зменшення кількості помилок при роботі алгоритмів.

Аналіз сучасного стану питання

Зростання кількості шкідливих програм та їхніх різновидів створює великі виклики для кібербезпеки[1]. Традиційні методи виявлення шкідливих програм недостатньо ефективні, оскільки вони не завжди можуть впоратися з новими видами загроз. Використання методів машинного навчання дозволяє покращити виявлення шкідливих програм. Алгоритми класифікації, нейронні мережі та інші методи можуть бути застосовані для аналізу поведінки програм та виявлення аномалій.

Машинне навчання стало ключовою складовою в сучасних системах кібербезпеки. Алгоритми класифікації, зокрема методи опорних векторів (SVM) та різні види нейронних мереж, використовуються для аналізу великих обсягів даних та визначення аномалій у поведінці програм.

Моделі машинного навчання навчаються на історичних даних, включаючи відомі випадки шкідливого програмного забезпечення. Це дозволяє їм розпізнавати схожість між новими програмами та відомими загрозами. Для підвищення точності та зменшення кількості помилок такі моделі можуть поєднувати різні методи аналізу, такі як аналіз вмісту файлів та аналіз поведінки програм.

Важливо розрізняти різні види шкідливого програмного забезпечення, оскільки кожен з них має свої характерні особливості та методи атаки. Наприклад, віруси проникають в файли та розповсюджуються через їхнє виконання, трояни приховуються в програмах щоденного користування, а шпигунське ПЗ слідкує за користувачем та викрадає конфіденційну інформацію.

Кожен вид шкідливого ПЗ вимагає специфічних методів виявлення. Тому вдосконалення алгоритмів машинного навчання повинно враховувати цю різноманітність та надавати засоби для розрізнення між різними видами атак.

Загалом, розробка та вдосконалення алгоритмів машинного навчання для виявлення та боротьби зі шкідливими програмами є складним завданням, але важливим для забезпечення кібербезпеки комп'ютерних систем. Тільки поєднання новітніх технологій, співпраця та постійна оптимізація може забезпечити ефективний захист від сучасних кіберзагроз.

Співпраця між різними організаціями у сфері кібербезпеки та обмін інформацією про нові загрози є важливим елементом боротьби зі шкідливими програмами. Встановлення стандартів для обміну даними та методами виявлення може допомогти ефективніше реагувати на нові атаки та поширювати засоби для боротьби з ними.

Результати дослідження

Оптимізація алгоритмів для виявлення та боротьби зі шкідливими програмами включає в себе низку ключових аспектів:

- параметри моделей машинного навчання, такі як глибина дерева рішень у деревах рішень[2], кількість шарів у нейронних мережах та інші, мають значення для ефективності та точності виявлення. Оптимізація цих параметрів використовується для забезпечення оптимальної роботи моделей;

- використання великих наборів даних. Якість та кількість навчальних даних важлива для ефективного машинного навчання. Великі набори даних дозволяють моделям навчатися на більш репрезентативних вибірках і покращити їхню здатність виявляти шкідливе ПЗ;

- оновлення моделей. Шкідливе програмне забезпечення постійно еволюціонує, тому важливо підтримувати актуальність моделей машинного навчання. Постійне оновлення моделей та їхніх навчальних даних допомагає враховувати нові види загроз та методи атаки;

- розподілене обчислення та апаратне прискорення. Зростаюча потреба у високій швидкості виявлення та боротьби зі шкідливим ПЗ призводить до використання розподіленого обчислення на графічних прискорювачах (GPU) та спеціалізованих апаратних засобах. Це дозволяє прискорити обчислення та обробку великих обсягів даних;

- валідація та тестування. Важливо враховувати процес валідації та тестування алгоритмів для переконання в їхній ефективності та надійності. Це включає в себе перевірку алгоритмів на тестових наборах даних, проведення тестів на реальних системах та аналіз результатів;

- збереження конфіденційності даних. Під час оптимізації алгоритмів важливо забезпечити конфіденційність даних, особливо у випадках, коли моделі машинного навчання навчаються на великих обсягах секретної інформації. Заходи безпеки, такі як шифрування даних та обмеження доступу до них, грають ключову роль в цьому контексті.

Оптимізація алгоритмів є важливим етапом в розробці систем виявлення та боротьби зі шкідливим ПЗ[3]. Інновації в цій області сприяють покращенню кібербезпеки та забезпеченню захисту від зростаючої кількості кіберзагроз.

Висновки

Вдосконалення алгоритмів машинного навчання для виявлення та боротьби зі шкідливими програмами в комп'ютерних системах є критично важливим завданням у сфері кібербезпеки. Однак цей процес вимагає постійного дослідження та розвитку, оскільки хакери постійно вдосконалюють свої атаки та створюють нові види шкідливого програмного забезпечення.

З основної частини статті можна зробити наступні висновки:

- машинне навчання являється потужним інструментом для виявлення шкідливих програм завдяки своїм можливостям аналізу великих обсягів даних та виявленню навіть незначних аномалій в системі;

- завдяки машинному навчанню, можливо виявити не лише відомі види шкідливого ПЗ, але й нові загрози, які раніше не були відомі. Моделі можуть навчатися на нових даних та адаптуватися до обставин, що змінюються;

- важливо пам'ятати про різноманітність шкідливого ПЗ та розробляти специфічні методи для різних видів атак. Однак стандартизація та обмін інформацією між організаціями у сфері кібербезпеки може полегшити боротьбу з загрозами;

- оптимізація алгоритмів машинного навчання та використання потужних обчислювальних ресурсів є ключовими для досягнення високої ефективності виявлення та боротьби зі шкідливим програмним забезпеченням.

Загалом, вдосконалення алгоритмів машинного навчання для боротьби зі шкідливими програмами в комп'ютерних системах є постійним процесом і його успішність визначатиметься здатністю вчасно реагувати на нові загрози та швидко впроваджувати вдосконалені методи в практику кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Росс Андерсон. Security Engineering: A Guide to Building Dependable Distributed Systems, 2020. – 1232 с.
2. Машинне навчання. Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/ Машинне_навчання
3. Пам'ятка з кібербезпеки. Електронний ресурс. Режим доступу: https://www.it.ua/news/pamjatka-po-kiberbezopasnosti

Семенюк Андрій Васильович - Інститут докторантури та аспірантури, Вінницький національний технічний університет, м. Вінниця, e-mail: andrew.semeniuk.university@gmail.com

Semeniuk Andrew V. - Institute of doctoral and postgraduate studies, Vinnytsia National Technical University, Vinnytsia, e-mail: andrew.semeniuk.university@gmail.com