УДК 004.85:004.056

ДОСЛІДЖЕННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ В ІНФОРМАЦІЙНО-ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ ДЛЯ ПРОГНОЗУВАННЯ РИЗИКІВ КІБЕРАТАК НА ПІДПРИЄМСТВАХ

Клименко О.Р.
Науковий керівник – асист. Пономарьова С.В.
Харківський національний університет радіоелектроніки, каф. СТ
м. Харків, Україна
тел.: +38 (067) 211-87-08, e-mail: oleksandr.klymenko1@nure.ua

Various machine learning techniques have been presented that can be used to detect and predict cyber risks, including transfer, ensemble, deep learning, and reinforcement learning. In addition, the importance of combining multiple methods for better accuracy and reliability of cyber risk prediction was found.

Інформаційно-інтелектуальні системи (ІІС) – це комп’ютерні системи, які використовуються для збору, обробки та аналізу даних для вирішення проблем. ІІС складається з різних компонентів, включаючи апаратне забезпечення, програмне забезпечення та людський фактор. ІІС можуть бути розроблені для виконання різноманітних завдань, включаючи виявлення та прогнозування ризику кібератак на підприємство.

Для найбільшої ефективності ІСС для виявлення та прогнозування ризику кібератаки на підприємство необхідно комбінувати різні методи машинного навчання. Поєднання різних методів машинного навчання може підвищити ефективність системи у виявленні та прогнозуванні ризику кібератак. Розглянемо кілька найпопулярніших способів комбінування моделей машинного навчання.

Ансамблеве навчання. Комплексні моделі навчання для виявлення та прогнозування ризиків кібератак можна об’єднати в ансамбль для підвищення ефективності системи. Ансамбль складається з великої кількості моделей, навчених на одному наборі даних, але з різними параметрами та/або алгоритмами навчання. Це дозволяє використовувати сильні сторони кожної моделі та зменшує ризик перетренованості.

Трансферне навчання – це метод використання знань, отриманих із попередньо навченої моделі, для покращення продуктивності нової моделі. У контексті виявлення та прогнозування ризику кібератак це може передбачати використання попередньо підготовлених моделей для виявлення певних моделей у поведінці користувачів, які можуть вказувати на можливу кібератаку.

Глибоке навчання – це метод вивчення нейронних мереж з великою кількістю шарів і параметрів. У контексті виявлення та прогнозування ризику кібератак глибоке навчання може допомогти визначити складні залежності та шаблони в поведінці користувача та системи, які вказують на можливість кібератак.

Навчання з підкріпленням – це метод навчання, за якого модель вчиться приймати рішення, постійно взаємодіючи з динамічним середовищем. У цьому підході модель знаходить найкращий вибір дій на основі поточного стану середовища та отримує позитивні чи негативні сигнали на основі результатів своїх дій. Цей підхід можна застосувати у сфері кібербезпеки, де модель може навчитися реагувати на кібератаки та забезпечувати захист. Наприклад, модель може навчитися розпізнавати типи кібератак і реагувати на них, запобігаючи атакам або забезпечуючи резервне копіювання важливої інформації.

Навчання з вчителем – використовується для навчання моделей на основі розмічених даних. Такі моделі можуть бути досить точними, але вони можуть бути неефективними в розпізнаванні нових шаблонів зловмисної активності. Тому можна доповнити цей метод іншими методами машинного навчання, такими як навчання без вчителя, яке дозволяє моделям розпізнавати нові шаблони зловмисної активності, навіть якщо вони не були розмічені.

Застосування моделей машинного навчання в інформаційно-інтелектуальних системах може гарантувати, що підприємства зможуть ефективно та точно ідентифікувати та прогнозувати ризики кібератак. Поєднання різних методів машинного навчання може покращити якість результатів і надати точнішу інформацію для прийняття рішень щодо кібербезпеки. Це пов'язано з тим, що окремі методи машинного навчання можуть мати свої обмеження, а поєднання різних методів дозволяє зменшити ці обмеження і покращити точність прогнозів.

Дослідження моделей машинного навчання в інформаційно-інтелектуальних системах є важливим напрямком для розробки стратегій захисту від мережевих атак. Доведено, що впровадження цих моделей забезпечує високий рівень кібербезпеки та захисту конфіденційної інформації для підприємств та інших організацій.

Список використаних джерел:

1. Гайтота, Є. В. Про перспективи Стратегії кібербезпеки України / Є. В. Гайтота, В. В. Чуницька, Г. І. Нікуліщев // Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукр. наук.-практ. конф. – Кропивницький: КНТУ, 2016. – С. 7–8. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/4948 (дата звернення: 23.03.2023).

2. Imamverdiyev Y. N., Abdullayeva F. J. Deep learning in cybersecurity. International journal of cyber warfare and terrorism. 2020, – P. 82–105. URL: https://doi.org/10.4018/ijcwt.2020040105 (date of access: 23.03.2023).

3. Lakshmanan V., Görner M., Gillard R. Practical machine learning for computer vision. O'Reilly Media, Incorporated, 2021, – 482 p.