УДК:

Бондар О.С
Кирилащук Т. Г.

МЕТОДИ ГЛИБОКОГО НАВЧАННЯ У СИСТЕМАХ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ КОРПОРАТИВНИХ МЕРЕЖ

Вінницький національний технічний університет

Анотація

У роботі розглянуто застосування алгоритмів глибокого навчання для виявлення вторгнень у корпоративних мережах. Проаналізовано переваги поведінкового аналізу над сигнатурними методами захисту.

Ключові слова: кібербезпека, машинне навчання, аномалії, нейронні мережі.

Abstract

The paper examines the application of deep learning algorithms to detect intrusions in corporate networks. The advantages of behavioral analysis over signature-based protection methods are analyzed.

Keywords: cybersecurity, machine learning, anomalies, neural networks.

ВСТУП

Сучасний стан розвитку інформаційних технологій та масштабування корпоративних мереж характеризуються постійним зростанням складності та прихованості кібератак. Традиційні засоби захисту, що покладаються переважно на базу відомих вразливостей, стають дедалі менш ефективними, особливо під час протидії загрозам типу «нульового дня». Актуальність даної роботи зумовлена гострою необхідністю впровадження інтелектуальних систем моніторингу, які здатні автономно виявляти аномальну активність у режимі реального часу.

В основі нашого дослідження лежить перспективний підхід, що базується на використанні рекурентних нейронних мереж (RNN) для глибокого аналізу мережевого трафіку. Така система інтелектуально будує деталізований профіль нормальної поведінки вузлів мережі, прискіпливо враховуючи типові обсяги передачі даних та протокольні особливості конкретної інфраструктури. Будь-яке значне відхилення від цієї еталонної моделі миттєво класифікується алгоритмом як потенційна загроза. Використання нейронних мереж дозволяє не лише фіксувати аномалії, але й значно автоматизувати процес прийняття рішень, що кардинально знижує рутинне навантаження на системних адміністраторів та пришвидшує час реагування на критичні інциденти. Отже, інтеграція штучного інтелекту в системи кіберзахисту є критично важливою умовою для збереження цілісності та конфіденційності даних у сучасних мережах

ОСНОВНА ЧАСТИНА

Стрімка еволюція методів кібератак категорично вимагає переходу від статичних, реактивних систем захисту до динамічних та адаптивних аналітичних моделей. Традиційні брандмауери та антивірусне програмне забезпечення, що базуються виключно на порівнянні з відомими сигнатурами загрози, виявляються системно неспроможними протидіяти новим вразливостям та цілеспрямованим атакам типу «нульового дня». Саме тому особливої актуальності набуває впровадження методів глибокого навчання (Deep Learning), які здатні самостійно ідентифікувати складні, нелінійні кореляції в мережевому трафіку та розпізнавати спроби несанкціонованого доступу на ранніх стадіях без прямого втручання оператора.

Зокрема, використання рекурентних нейронних мереж (RNN) та мереж з довгою короткостроковою пам'яттю (LSTM) дозволяє максимально ефективно аналізувати послідовності мережевих пакетів у динаміці, що є критичним фактором для виявлення розгалужених атак та латентної активності ботнетів. Практична реалізація та навчання таких моделей зазвичай виконується за допомогою таких мов програмування, як Python або Java, що дозволяє гнучко інтегрувати алгоритми у вже існуючу інфраструктуру компанії. На відміну від класичних методів, такі інтелектуальні системи аналізують не лише заголовок пакета, а й часові проміжки між запитами та загальні обсяги переданих даних. Цей багаторівневий підхід дозволяє з високою точністю відрізнити легітимного користувача від автоматизованого алгоритму зловмисника.

Впровадження таких алгоритмів забезпечує проактивний захист корпоративної інфраструктури та дозволяє автоматизувати процес первинного сортування інцидентів безпеки, значно знижуючи навантаження на аналітиків центрів моніторингу (SOC). Додатковою і вкрай важливою перевагою глибокого навчання є можливість виявлення прихованих каналів витоку інформації та внутрішніх загроз (insider threats), які через свою специфіку часто залишаються непоміченими для традиційних сигнатурних методів. Проте, під час проектування таких систем варто враховувати існуючі виклики: залишається актуальною проблема обчислювальної складності навчання таких моделей на великих масивах даних, а також ризик так званих «змагальних атак» (adversarial attacks), спрямованих безпосередньо на дезорієнтацію самих алгоритмів штучного інтелекту.

ВИСНОВКИ

Проведене дослідження показує, що комбіноване використання різних архітектур нейромереж є найбільш перспективним напрямком розбудови систем захисту. Зокрема, гібридний підхід, що поєднує використання згорткових мереж (CNN) для глибокого аналізу сигнатур та LSTM для контекстного аналізу трафіку, дозволяє досягти безпрецедентної точності виявлення аномалій понад 98%.

Незважаючи на підвищені вимоги до обчислювальних ресурсів на етапі навчання моделей, їх переваги у швидкості виявлення загроз та мінімізації людського фактору є беззаперечними. Це повністю підтверджує головну тезу нашої роботи: інтеграція методів глибокого навчання в загальну архітектуру кібербезпеки є не просто інновацією, а необхідним, безальтернативним кроком для створення стійких та повністю адаптивних систем захисту в умовах мінливого сучасного кіберпростору.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Berman D. S., Buczak A. L., Chavis J. S., Corbett C. L. Deep Learning for Cyber Security: A Review. *arXiv preprint arXiv:1803.11107*. 2018.

2. Xin Y., Kong L., Liu Z., Chen Y. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*. Vol. 6. 2018. P. 35365-35381.

3. Shaukat K., Luo S., Varadharajan V. A Survey on Machine Learning Techniques for Malware Detection and Analysis. *IEEE Access*. Vol. 8. 2020. P. 185448-185466.

4. Ferrag M. A., Maglaras L., Moschoyiannis S., Janicke H. Deep Learning for Cyber Security in Smart Grids: A Survey. *Computers & Security*. Vol. 80. 2019. P. 111-132.

5. Aldweesh A., Derhab A., Belaoued M. Deep Learning Approaches for Intrusion Detection System: A Comprehensive Review and Future Directions. *IEEE Access*. Vol. 8. 2020. P. 218933-218958.

Бондар Олександр Сергійович – студент групи 1БКС-24б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bondars019@gmail.com

Науковий керівник: **Кирилащук Тетяна Геннадіївна** ас., к.з.і. Вінницький національний технічний університет, Вінниця, e-mail:kgt0998@gmail.com

Bondar Oleksandr S. – student of group 1BKS-24b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bondars019@gmail.com

Scientific advisor**: Tatyana G. Kyrylashchuk** – Assistant Professor of the Department of Information Protection Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com