УДК 004.056.53 + 004.89

Д. П. Урлапова
Є. О. Звуздецький
Ю. Ю. Іванов

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ПОВЕДІНКИ КОРИСТУВАЧІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВЕБСЕРЕДОВИЩ

Вінницький національний технічний університет

Анотація
У даній роботі проаналізовано принципи роботи поведінкових моделей, що дозволяють відстежувати відхилення від типових дій користувачів, які можуть свідчити про кібератаки або несанкціоновані зміни контенту.
Ключові слова: *штучний інтелект, кібербезпека, дані, виявлення аномалій, аналіз поведінки користувачів.*

Abstract
This paper analyzes the principles of behavioral models, that allow tracking deviations from typical user actions, that may indicate cyberattacks or unauthorized changes to content.
Keywords *artificial intelligence, cybersecurity, data, anomaly detection, user behavior analysis.*

Вступ

У сучасному цифровому середовищі проблема інформаційної безпеки залишається надзвичайно актуальною. Зловмисники дедалі частіше отримують доступ до легальних облікових записів адміністраторів або користувачів. Отже, вони можуть змінювати контент, додавати шкідливий код або впроваджувати власні шкідливі PHP-скрипти. Традиційні системи безпеки, які ґрунтуються лише на перевірці прав доступу або логах входів, не завжди здатні своєчасно реагувати на подібні загрози [1, 2]. Водночас, для захисту вебресурсів від атак необхідно впроваджувати додаткові методи, такі як контроль цілісності файлів та інтеграція систем виявлення аномалій. Для таких задач все більшої актуальності набуває використання методів штучного інтелекту [3, 4]. *Метою роботи* є аналіз досліджень поведінкових моделей, що дозволяють відстежувати аномальні дії користувачів, які можуть свідчити про кібератаки або несанкціоновані зміни контенту.

Результати дослідження

Методи штучного інтелекту відкривають нові можливості для створення адаптивних систем, які здатні виявляти нетипові зміни у поведінці користувачів. Системи поведінкового аналізу (*UEBA – User and Entity Behavior Analytics*) формують профіль звичної активності користувача і фіксують будь-які відхилення — наприклад, редагування старих записів, створення нетипових об’єктів або додавання фрагментів коду [1, 5].

Методи виявлення аномалій можна класифікувати на статистичні, кластеризаційні та засновані на використанні нейронних мереж. Для аналізу поведінкових даних найчастіше застосовують алгоритми без учителя: ізоляція аномалій на основі методу випадкових лісів, однокласова класифікація на основі методу опорних векторів та нейромережі автокодувальники [2, 3]. Вони дозволяють системі навчатися на основі звичайних дій користувачів і фіксувати будь-які відхилення від норми. У комерційних рішеннях *UEBA* такі технології вже використовуються для виявлення підозрілих дій у великих організаціях. Проте для освітніх або локальних вебплатформ подібні підходи майже не реалізуються, що створює можливість для досліджень у цьому напрямі.

Поєднання поведінкового аналізу з семантичним аналізом контенту дозволяє оцінювати не лише послідовність дій користувача, а й зміст зміненого матеріалу. Якщо алгоритм виявляє підозрілі конструкції або несумісність контексту змін (наприклад, редагування давніх дописів із додаванням коду), він може автоматично повідомити адміністратора, обмежити доступ або відмінити зміни [2]. У перспективі такі системи можуть функціонувати на рівні низки сайтів

одночасно через централізовану платформу аналізу подій, що забезпечить раннє виявлення схожих типів атак.

Висновки

Використання штучного інтелекту для аналізу поведінки користувачів у вебсередовищах є одним із найефективніших напрямів розвитку сучасної кібербезпеки. Поведінкові моделі дають змогу виявляти підозрілі дії, навіть коли обліковий запис не був формально зламаний. Поєднання алгоритмів машинного навчання з контент-аналізом відкриває можливості розробки систем захисту, здатних оцінювати контекст змін і мінімізовувати ризики компрометації вебресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Gheyas I.A., Abdallah A.E. Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis. *Big Data Analytics*. 2016. Vol. 1. pp. 1–30.
2. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*. 2010. pp. 305–316.
3. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. *ACM Computing Surveys*. 2009. Vol. 41. pp. 1–58.
4. Аналіз та експериментальне дослідження методу безмодельного навчання з підкріпленням / В.В. Півошенко, М.С. Кулик, Ю.Ю. Іванов, А.С. Васюра. *Вісник Вінницького політехнічного інституту*. №3. 2019. С. 40–49.
5. Berman D.S., Buczak A.L., Chavis J.S., Corbett C.L. A Survey of Deep Learning Methods for Cyber Security. *Information*. 2019. Vol. 10. pp. 1–35.

Урлапова Дар'я Павлівна — студентка бакалаврату кафедри Автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця.

Звуздецький Єгор Олегович — аспірант кафедри Автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця.

Іванов Юрій Юрійович — канд. техн. наук, доцент кафедри Автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: Yura881990@i.ua.

Urlapova Daria P. — undergraduate student, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia.

Zvuzdetskyi Yehor O. — postgraduate student, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia.

Ivanov Yurii Yu. — Cand. Sc. (Eng), Senior Lecturer, Faculty of intelligent information technologies and automation, Vinnytsia National Technical University, Vinnytsia, e-mail: Yura881990@i.ua.