ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У СИСТЕМАХ КІБЕРБЕЗПЕКИ

Якимчук М.Д., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі зростанням кількості кіберзагроз актуальним завданням є вдосконалення методів виявлення підозрілої активності в інформаційних системах. Традиційні засоби захисту, що ґрунтуються на сигнатурах відомих атак і попередньо визначених правилах, не завжди здатні своєчасно виявляти нові загрози. Багатообіцяючим напрямом розв'язання цієї проблеми є використання машинного навчання для аналізу поведінкових даних і визначення відхилень від типових сценаріїв роботи системи.

Метою дослідження є аналіз можливостей застосування методів машинного навчання для виявлення аномалій та визначення особливостей їх використання для підвищення рівня кібербезпеки інформаційних систем.

Одним із перспективних алгоритмів у цій сфері є Isolation Forest, який дає змогу визначати аномальні об'єкти на основі особливостей їх ізоляції в наборі даних [1]. На відміну від підходів, що потребують попереднього маркування всіх можливих типів атак, цей алгоритм може застосовуватися для пошуку відхилень у даних без наявності повного набору прикладів загроз. Це робить його перспективним для аналізу журналів подій, активності користувачів і поведінки програмних компонентів.

Важливим етапом застосування машинного навчання є формування набору ознак, які відображають особливості досліджуваних подій. До таких характеристик можуть належати час виконання операцій, типи запитів, частота звернень до ресурсів, результати автентифікації та обсяги переданих даних. Вибір ознак повинен відповідати специфіці системи й характерним сценаріям потенційних атак [2].

Недостатня кількість інформативних характеристик може обмежувати можливості алгоритму та призводити до пропуску окремих загроз. Водночас виявлення аномалії не завжди свідчить про кібератаку, оскільки незвична активність може бути пов'язана зі звичайними змінами в роботі системи. Тому важливо оцінювати точність моделей, зменшувати кількість хибних спрацювань і регулярно оновлювати дані для навчання.

Отже, застосування машинного навчання створює можливості для автоматизованого виявлення потенційних кіберзагроз. Подальші дослідження доцільно спрямувати на вдосконалення наборів ознак і порівняння ефективності різних алгоритмів у реальних умовах.

Список літератури

1. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. Boca Raton : CRC Press, 2020.

2. Gartner. User and Entity Behavior Analytics (UEBA) Market Guide. Gartner Research, 2023.