УДК 004.4

Слободян Д.А., Радюк П.М., Цивадиць П.О.

Хмельницький національний університет

МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ В ACTIVE DIRECTORY ДЛЯ ЗАХИСТУ СЕРВЕРІВ ТА БАЗ ДАНИХ ЗАСОБАМИ МАШИННОГО НАВЧАННЯ

У даній роботі запропоновано метод виявлення аномалій у середовищі Active Directory (AD) з використанням алгоритмів машинного навчання. Основна увага приділена вивченню класифікації та виявленню відхилень у поведінці користувачів, що можуть сигналізувати про загрозу безпеці. Запропоновані алгоритми, зокрема One-Class SVM та Local Outlier Factor (LOF), забезпечують виявлення аномальної поведінки в реальному часі, що дозволяє знизити кількість хибнопозитивних спрацьовувань.

This paper proposes a method of detecting anomalies in the Active Directory (AD) environment using machine learning algorithms. The main focus is on studying the classification and identifying deviations in user behavior that may signal a security threat. The proposed algorithms, in particular One-Class SVM and Local Outlier Factor (LOF), provide detection of anomalous behavior in real time, which allows to reduce the number of false positives.

Захист середовища Active Directory (AD) є ключовим аспектом сучасної корпоративної безпеки, оскільки AD керує ідентифікацією та доступом до критичних ресурсів в організації. Однією з найчастіших та найбільш небезпечних загроз є атака Kerberoasting, яка дозволяє викрадати дані без необхідності підвищених привілеїв. Статичні методи виявлення таких атак часто виявляються недостатніми, оскільки не здатні ефективно розпізнавати змінну поведінку зловмисників у реальних мережах [1]. Це створює потребу у використанні гнучких підходів на основі машинного навчання, які здатні адаптуватися до різноманітних сценаріїв аномальної активності та забезпечувати надійніший захист серверів і баз даних.

Попередні дослідження у сфері виявлення атак на середовище AD здебільшого ґрунтуються на статичних правилах або сигнатурних методах для визначення шкідливих дій [2]. Такі методи залежать від заздалегідь визначених умов та порогових значень, які можуть бути неефективними в умовах реальних мереж. Статичні правила часто спричиняють велику кількість хибнопозитивних спрацювань, оскільки вони не враховують відмінності в поведінці користувачів та систем у різних середовищах. Крім того, ці методи можуть бути вразливими до обходу, оскільки зловмисники можуть легко адаптувати свої дії, змінюючи шаблони або зменшуючи частоту запитів, щоб залишатися непоміченими.

Машинне навчання поступово інтегрується як засіб для виявлення аномалій, проте більшість попередніх досліджень обмежується базовими моделями,

які не завжди здатні ефективно розрізняти нормальні та шкідливі дії в AD, особливо під час атак на облікові дані, таких як Kerberoasting [3]. Існує необхідність у розробці методів, які не тільки підвищують точність виявлення, але й знижують кількість помилкових спрацювань, адаптуючись до специфічного середовища організації.

Мною було впроваджено підхід з використанням алгоритмів машинного навчання, зокрема One-Class SVM та LOF, для виявлення атак на облікові дані в Active Directory. Запропонована методика відходить від статичних правил і пропонує адаптивний підхід, який здатен виявляти приховані загрози на основі аналізу аномалій у поведінкових даних AD. Це дозволяє підвищити рівень захисту серверів та баз даних, одночасно зменшуючи навантаження на адміністраторів завдяки скороченню кількості хибнопозитивних сповіщень.

Основною метою дослідження є розробка методу виявлення аномалій у AD для підвищення рівня захисту серверів та баз даних, використовуючи засоби машинного навчання, зокрема алгоритми One-Class SVM та LOF. Завдання дослідження включає адаптацію обраних моделей до особливостей середовища AD, оптимізацію їх продуктивності та зменшення кількості хибнопозитивних спрацювань.

Для виявлення аномальної активності в AD алгоритм One-Class SVM виконує навчання на основі даних, які представляють нормальну поведінку, та виявляє аномалії шляхом визначення віддалених відхилень. **LOF**, навпаки, оцінює локальну щільність даних, що дозволяє виявляти точки з меншою щільністю порівняно з їхніми сусідами. Ключовими ознаками для виявлення аномалій були обрані кількість запитів на окремі послуги, тип облікового запису та IP-адреса джерела (таблиця 1).

Для тестування методів виявлення атак я створив синтетичні дані, які містять ці ознаки, що дозволило натренувати моделі та оцінити їхню ефективність на тестових даних. Це забезпечило більш контрольоване середовище для аналізу продуктивності моделей і дозволило оптимізувати налаштування гіперпараметрів під специфічні умови середовища AD.

Таблиця 1 – Характеристики використаних ознак для виявлення аномалій

Тип ознаки	**Опис**
Кількість запитів	Частота запитів на квитки від окремих користувачів або IP-адрес
Тип облікового запису	Класифікація облікових записів за типом (особистий, неособистий, системний)
IP-адреса	IP-адреса, з якої здійснено запит на квиток, з поділом на сегменти мережі
Тип запитуваної послуги	Характеризує тип доступу (додаток , база даних, тощо)

Результати тестування наведені на рис. 1, рис 2, рис 3.

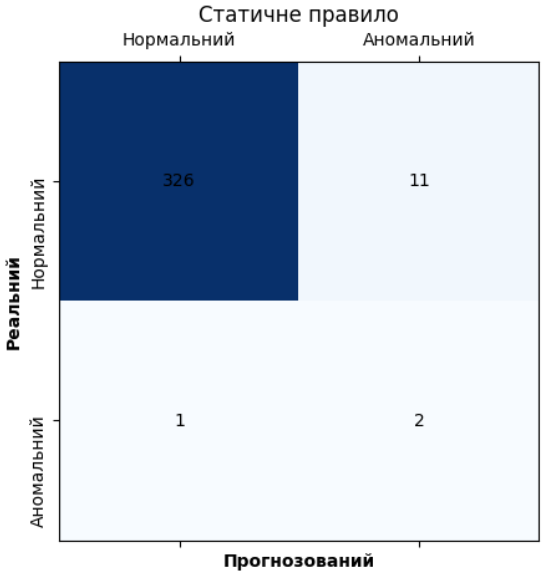

Рисунок 1 – Результати тестування моделі статичним правилом

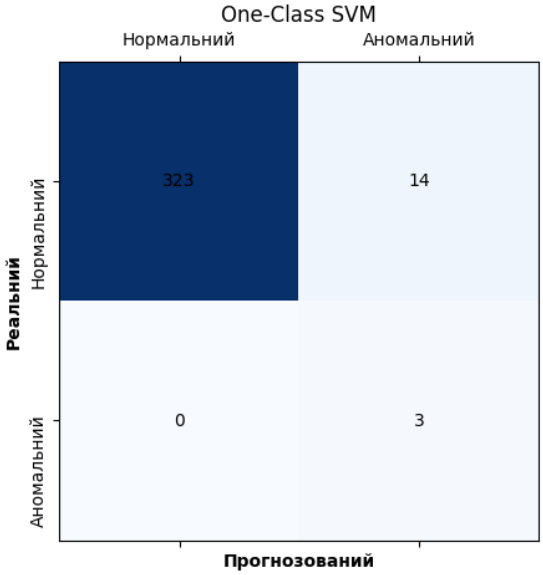

Рисунок 2 – Результати тестування моделі One-Class SVM

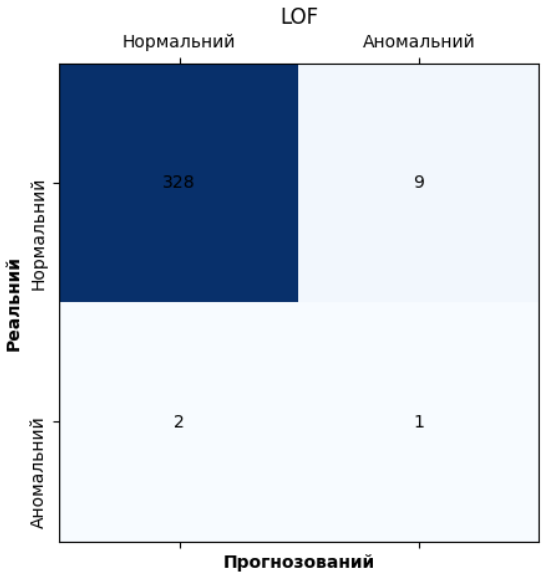

Рисунок 3 – Результати тестування моделі LOF

Результати експериментів показують, що методи машинного навчання зменшують кількість хибнопозитивних спрацювань порівняно зі статичним правилом (рис. 1), яке є менш гнучким у динамічних середовищах. **One-Class SVM** (рис. 2) виявився найбільш ефективним серед розглянутих алгоритмів, оскільки забезпечив вищу точність при мінімальній кількості хибнонегативних спрацювань, дозволяючи точніше ідентифікувати спроби атаки типу Kerberoasting.

Отже, запропонований метод виявлення аномалій у AD забезпечує вищий рівень безпеки завдяки зниженню хибних сповіщень та підвищенню точності виявлення Kerberoasting-атак. Подальші дослідження можуть бути спрямовані на розширення моделей ML, щоб охопити нові типи атак у середовищі AD та оптимізувати алгоритми для роботи в реальному часі.

Перелік посилань

1. Kotlaba, L., Buchovecká, S., & Lórencz, R., Active Directory Kerberoasting Attack: Detection using Machine Learning Techniques, 2021, pp. 376–383.
2. Chandola, V., Banerjee, A., Kumar, V., Anomaly Detection: A Survey, ACM Computing Surveys, Vol. 41, No. 3, 2009.
3. Bulatov, A., Machine Learning for Anomaly Detection in Active Directory, International Journal of Cybersecurity, Vol. 8, No. 2, 2021.