МЕТОД ВИЯВЛЕННЯ АТАК НА BGP-МАРШРУТИЗАЦІЮ ЗІ СТОРОНИ КЛІЄНТА

Чухлєбов І.Я., Ільїна І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Атаки на протокол граничного шлюзу (BGP) є серйозною загрозою для стабільності та безпеки Інтернету. Вони дозволяють зловмисникам перехоплювати або перенаправляти інтернет-трафік, що призводить до втрати конфіденційності, зниження доступності ресурсів та підвищення ризиків кібербезпеки для клієнтських систем.

Зокрема, маршрутизаційні атаки, такі як BGP-хайджекінг та маніпуляція маршрутами, спрямовані на підрив функціонування мереж і потребують ефективних засобів виявлення.

Використання методів машинного навчання для моніторингу та аналізу аномалій у BGP-трафіку є перспективним напрямом для протидії таким атакам [1-3].

Метою дослідження є розробка методу виявлення аномалій у BGP-маршрутизації зі сторони клієнта на основі машинного навчання, який дозволить швидко ідентифікувати підозрілі зміни в маршрутах.

Результати дослідження демонструють, що методи машинного навчання здатні забезпечити високу точність виявлення аномалій у BGP-маршрутизації, зокрема в умовах нових видів атак, які не були відомі на момент навчання. Виявлено, що запропонований підхід здатний оперативно ідентифікувати підозрілі маршрути, що дозволяє знизити ризик успішної атаки на маршрутизацію.

Використання машинного навчання для виявлення атак на BGP-маршрутизацію зі сторони клієнта є ефективним засобом підвищення кібербезпеки мереж. Модель забезпечує надійний контроль і раннє виявлення аномалій, що сприяє захисту телекомунікаційних систем від загроз BGP-маніпуляцій.

Список літератури

1. Ruban, I., V. Martovytskyi, and N. Lukova-Chuiko. "Approach to classifying the state of a network based on statistical parameters for detecting anomalies in the information structure of a computing system." Cybernetics and Systems Analysis 54 (2018): 302-309.

2. Martovytskyi, Vitalii, et al. "DEVISING AN APPROACH TO THE IDENTIFICATION OF SYSTEM USERS BY THEIR BEHAVIOR USING MACHINE LEARNING METHODS." Eastern-European Journal of Enterprise Technologies 117.3 (2022). DOI: 10.15587/1729-4061.2022.259099

3. V. Martovytskyi, I. Ruban, H. Lahutin, I. Ilina, V. Rykun and V. Diachenko, "Method of Detecting FDI Attacks on Smart Grid," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2020, pp. 132-136, doi: 10.1109/PICST51311.2020.9468005.