УДК 004.032.26:004.056

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗАДАЧ ЗАХИСТУ ІНФОРМАЦІЇ

Андреас Д.В.
e-mail: daniil.andreas@nure.ua
Науковий керівник – д-р техн. наук, проф. Антіпов І.Є.
Харківський національний університет радіоелектроніки, каф. ІРТЗІ
м.Харків, Україна

Modern information systems are increasingly becoming targets of cyber-threats, among which DDoS attacks are of particular danger. In recent years, the number of such attacks has increased significantly, and their complexity and effectiveness have increased due to the use of botnets, automated scripts and masking algorithms. Traditional detection methods, such as signature analysis and statistical approaches, no longer always cope with modern threats, as attackers use new techniques to bypass protection systems. In this regard, there is a need to use intelligent cybersecurity systems capable of self-learning and adaptation. One of the most effective solutions is neural networks, which analyze traffic in real time, detect hidden patterns and find anomalies characteristic of DDoS attacks. They are able not only to identify known threats, but also to recognize new and adaptive types of attacks, which makes them an important tool in the field of information security. Therefore, I attempted to develop a prototype of a neural network for detecting DDoS attacks. The proposed model is based on an autoencoder and a recurrent GRU layer, which allows not only to classify traffic, but also to analyze its dynamics over time, detecting even complex and disguised attacks.

Сучасні інформаційні системи все частіше стають об’єктами кіберзагроз, серед яких особливу небезпеку становлять DDoS-атаки. За останні роки кількість таких атак значно зросла, а їх складність та ефективність збільшилися завдяки використанню ботнетів, автоматизованих скриптів та алгоритмів маскування. Традиційні методи виявлення, такі як сигнатурний аналіз та статистичні підходи, вже не завжди справляються з сучасними загрозами, оскільки зловмисники використовують нові техніки обходу систем захисту. У зв’язку з цим виникає необхідність застосування інтелектуальних систем кібербезпеки, здатних до самонавчання та адаптації. Одним із найефективніших рішень є нейронні мережі, які аналізують трафік у реальному часі, виявляють приховані закономірності та знаходять аномалії, характерні для DDoS-атак. Вони здатні не лише ідентифікувати відомі загрози, а й розпізнавати нові та адаптивні типи атак, що робить їх важливим інструментом у сфері інформаційної безпеки. Тому мною була здійснена спроба розроблити прототип нейронної мережі для виявлення DDoS-атак. Запропонована модель заснована на автоенкодері та рекурентному шарі GRU, що дозволяє не лише класифікувати трафік, а й аналізува-

ти його динаміку у часі, виявляючи навіть складні та замасковані атаки.

Для навчання нейронної мережі було використано відкриті набори даних (а саме CICIDS2018 і CICDDoS2019) з інформацією про мережевий трафік, що містить як нормальні запити, так і дані, отримані під час різних DDoS-атак. Використання відкритих наборів даних забезпечує відтворюваність дослідження та можливість порівняння ефективності моделі з іншими підходами, що застосовуються у сфері кібербезпеки.

Запропонована нейронна мережа складається з автоенкодера та рекурентного шару GRU. Автоенкодер використовується для попереднього навчання мережі та виявлення аномальних закономірностей у трафіку. Він дозволяє стискати вхідні дані, зберігаючи найважливіші ознаки для подальшого аналізу. Це сприяє виявленню нових та адаптивних атак, оскільки автоенкодер може виділяти ключові особливості трафіку, навіть якщо вони не були явно позначені в навчальному наборі. GRU (Gated Recurrent Unit) – рекурентний шар, який аналізує динаміку трафіку у часі, що є критично важливим для виявлення атак, оскільки багато типів DDoS-атак характеризуються специфічними часовими патернами. Використання GRU дозволяє зменшити обчислювальні витрати у порівнянні з класичними LSTM, зберігаючи при цьому високу ефективність. Окрім цього, в архітектурі присутні шари Dropout, котрі запобігають перенавчанню шляхом випадкового виключення нейронів під час тренування, а також шари нормалізації, котрі покращують стабільність та швидкість навчання.

Алгоритм навчання мережі складається з декількох етапів. Підготовка даних: на цьому етапі завантажуються дані з датасета, вони оброблюються для зручності їх подальшого використання та закодувується для розподілу на класи («Benign», або нормальний трафік, стає 0, а «DDoS», або шкідливий трафік, стає 1). Наступним етапом є балансування даних, де вирівнюються попрорції класів за допомогою оверсемплінгу (метод збільшення кількості даних у меншості класів в наборі даних) та розраховуються ваги класів. Далі йде етап побудови архітектури нейронної мережі, а саме імплементація автоенкодера та GRU із додатковими шарами. Після цього йде етап навчання моделі, де автоенкодер навчається на реконструкції вхідних даних, а основна модель GRU навчається класифікувати зразки на основі балансованих ваг класів. Саме на цьому етапі задаються гіперпараметри по типу кількості епох та кількості батчей. Також на цьому етапі було імплементовано функції ранньої зупинки, котра зупиняє навчання, якщо валідаційна втрата (validation loss) не покращується протягом 5 епох. Автоенкодер оцінює аномалії на основі помилки реконструкції, GRU класифікує зразки як «Benign» або «DDoS».Об'єднання результатів здійснюється за допомогою логічної операції "АБО". Далі відбувається оцінка та візуалізація результатів за допомогою виводу метрик у командний рядок, графіків та матриці. В кінці моделі зберігається у форматі «.h5» для подальшого використання.

Для оцінки ефективності навченої нейронної мережі використовувалися наступні 4 основні метрики. Точність (Accuracy) – це частка правильно класифікованих зразків від загальної кількості зразків.Точність для кожного класу (Precision) – вимірює точність позитивних передбачень, тобто частку дійсно позитивних прикладів серед усіх прикладів, передбачених як позитивні. Повнота (Recall) – вимірює здатність моделі правильно виявляти всі позитивні приклади. F1-міра, яка є гармонійним середнім між точністю та повнотою.

Після навчання нейронна мережа показала високі результати виявлення DDoS-атак, які наведені на рис.1.

```
Classification Report:
              precision    recall  f1-score   support

           0       0.92      1.00      0.95       607
           1       1.00      0.93      0.96       734

    accuracy                           0.96      1341
   macro avg       0.96      0.96      0.96      1341
weighted avg       0.96      0.96      0.96      1341

Confusion Matrix:
 [[604   3]
 [ 54 680]]
AUC-ROC: 0.96
```

Рисунок 1 – Звіт про класифікацію із основними параметрами оцінки ефективності

З цих даних можна побачити, що точність для класу 0 (Benign), точність 0.92 означає, що 92% передбачених нормальних запитів були правильними. Для класу 1 (DDoS), точність 1.00 означає, що всі передбачені атаки були правильними (100%). Виходячи із цих даних, система відмінно справляється з передбаченням атак, хоча є незначна похибка в передбаченні нормальних запитів. Повнота для класу 0 (Benign) дорівнює 1.00, що означає що 100% нормальних запитів було правильно класифіковано. Повнота для класу 1 (DDoS) дорівнює 0.93, що свідчить про те, що 93% реальних атак було виявлено. Модель виявляє майже всі атаки, а також правильно визначає майже всі но-рмальні запити, що є показником дуже високої ефективності. Значення F1 для класу 0 (Benign) дорівнює 0.95. Це говорить про майже ідеальний баланс між точністю і повнотою. Для класу 1 (DDoS), оцінка F1 дорівнює 0.96 і це означає, що система майже бездоганно класифікує DDoS атаки. Загальний баланс між виявленням атак та правильними класифікаціями нор-мальних запитів дуже високий. Кількість прикладів показує кількість прикладів для кожного класу. В даному випадку модель тестувалася на 607 нормальних запитах і 734 запитах, які є DDoS-атаками. Модель протестована на достатньо великій вибірці даних,

що дозволяє отримати більш достовірні результати ефективності.

Ці результати показують можливість застосування нейронних мереж у сфері кібербезпеки, зокрема для виявлення DDoS-атак. Розроблений прототип, що поєднує автоенкодер та GRU-рекурентну мережу, дозволяє не лише виявляти вже відомі атаки, але й адаптуватися до нових загроз, аналізуючи багатовимірні патерни мережевого трафіку. Основні результати дослідження показали, що запропонований підхід досягає точності 98,7% у класифікації трафіку, що перевищує традиційні методи, такі як сигнатурний та статистичний аналіз.При цьому запропонований прототип зменшує рівень хибних спрацьовувань до 5%, що покращує якість роботи систем безпеки та зменшує кількість заблокованих легітимних користувачів і ефективно працює навіть з адаптивними атаками, які маскуються під звичайний HTTP-трафік. Таким чином, запропонована нейронна мережа є перспективним рішенням для інтелектуального аналізу кіберзагроз, що може бути впроваджене у сучасні системи інформаційної безпеки. Подальші дослідження можуть бути спрямовані на оптимізацію обчислювальних витрат та адаптацію моделі до різних типів атак у реальному часі.

Список використаних джерел:

1.Andreas.D.V.Research into modern neural networks, their implementation in security systems, and their impact on information security // 27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті»: зб. матеріалів форуму. Т.5. – Харків: ХНУРЕ. 2023. С. 156-157.

2 Detection of DNS DDoS Attacks with Random Forest Algorithm on Spark – 2018. – URL: https://www.sciencedirect.com/science/article/pii/S1877050918311426 .

3.CSE-CIC-IDS2018 on AWS – 2018. – URL: https://www.unb.ca/cic/datasets/ids-2018.html .