Автор: Шуршев В.Ф., Тагиров Р.Р.
16.06.2025 19:06 - Обновлено 16.06.2025 19:08

НЕЙРОСЕТЕВАЯ МОДЕЛЬ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ

ШуршевФ.В., д.т.н. профессор,

ТагировР.Р., магистрант,

АГТУ, г. Астрахань, Россия

Аннотация. Рассмотрена гибридная нейросетевая архитектура, которая может бы автоматически обнаруживать отклонения в поведении сетевого трафика на основе его структуры. Предложена комбинированная оценка аномальности, учитывающая ошибку реконструкции и реакцию на изменение внутренних признаков. Для повышения точности введена комбинированная функция потерь, регулируемая параметром, позволяющим настраивать вклад каждой компоненты.

Ключевые слова: нейронные сети, обработка информации, обнаружение аномалий, информационная безопасность.

Автор: Шуршев В.Ф., Тагиров Р.Р.
16.06.2025 19:06 - Обновлено 16.06.2025 19:08

Одной из наиболее острых проблем в области информационной безопасности является выявление аномалий в сетевом трафике. Основная причина заключается в том, что классические системыIDS ориентированы на заранее известные векторы атак и не способны адекватно реагировать на ранее неизвестные виды угроз. В связи с этим актуальной становится задача разработки методов, способных обнаруживать аномалии на основе поведения сетевого трафика. Перспективным направлением в решении данной задачи является использование нейронных сетей, в частности автокодировщиков. Эти модели способны выявлять скрытые закономерности, характерные для нетипичного поведения, что позволяет повысить точность обнаружения угроз.

Модель нейронной сети

В состав предлагаемой нейронной сети входят три основные компонента: энкодер, декодер и дискриминатор. Каждый из них реализован в виде многослойного перцептрона с использованием полносвязных слоёв с функцией активации LeakyReLU с исключением равным 20%, а также – гиперболического тангенса и сигмоиды в выходных слоях. Кодировщик состоит из трёх последовательных слоёв. Первый слой содержит 64 нейрона и имеет функцию активации LeakyReLU с параметром отрицательного наклона равным 0.2. Для предотвращения переобучения применяется исключение с шансом 20%. Второй и третий слои имеют по 32 нейрона и также используют функцию активации LeakyReLU с тем же параметром отрицательного наклона и исключением 20%. Декодер симметрично повторяет структуру энкодера и имеет выходной слой, который состоит из 80 нейронов с функцией активации tanh. Это позволяет ограничить значения выходных признаков в диапазоне -1 до 1.

...

полный текст во вложении