УДК 004.8

ВНЕДРЕНИЕ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМЫ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ БОТОВ

Негров Ю.В., студент гр. ПИб-192, IV курс
Научный руководитель: Корниенко И.Л., старший преподаватель
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

Нейронные сети - мощный инструмент для обработки и анализа данных, который становится все более распространенным во многих сферах жизни, включая системы безопасности [1].

Давайте сначала разберемся, как работают нейронные сети [2]. Нейронные сети работают на основе обучения с учителем или без учителя, в зависимости от того, каким образом они обрабатывают данные. В случае обучения с учителем нейронные сети используют набор данных, который уже проаннотирован и содержит информацию о том, какой тип данных является «хорошим», а какой «плохим». Нейронные сети, обученные с помощью этого метода, могут обнаруживать угрозы в данных, используя уже известные паттерны (рис. 1). В случае обучения без учителя нейронные сети используют неаннотированные данные, чтобы самостоятельно обнаруживать паттерны и аномалии (рис. 2). Это позволяет выявлять угрозы, которые не были известны на момент обучения [3].

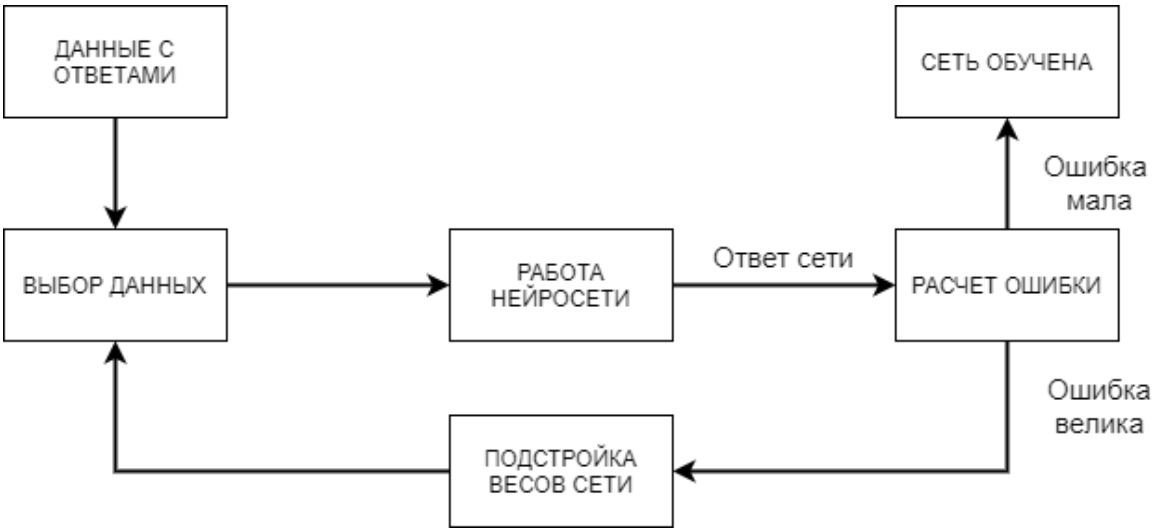

Рисунок 1 — Обучение нейронной сети с учителем

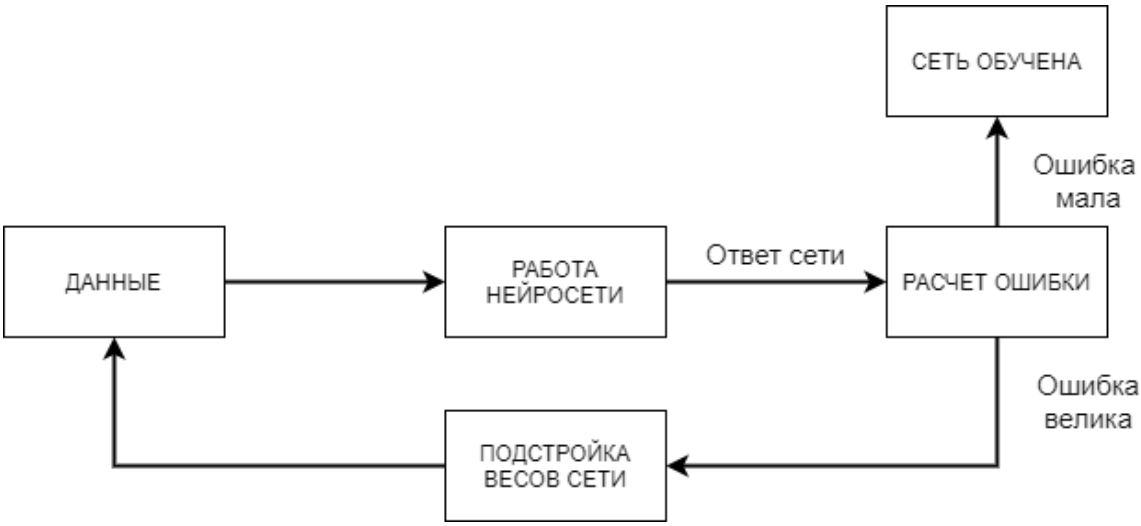

Рисунок 2 — Обучение нейронной сети без учителя

Если нейронные сети являются мощным инструментом, то появляются вопросы «где» и «как» их использовать в сфере безопасности. Одним из способов использования нейронных сетей является их интеграция с ботами [4]. В основе этого подхода лежит идея использования нейронных сетей для обучения ботов, которые могут автоматически определять и реагировать на угрозы безопасности [5]. Например, боты могут быть обучены распознавать вредоносный код, вредоносные ссылки (рис. 3), фишинговые атаки и другие виды кибератак, сканировать систему на наличие уязвимостей (рис. 4), а также анализировать данные, полученные от других ботов и систем безопасности.

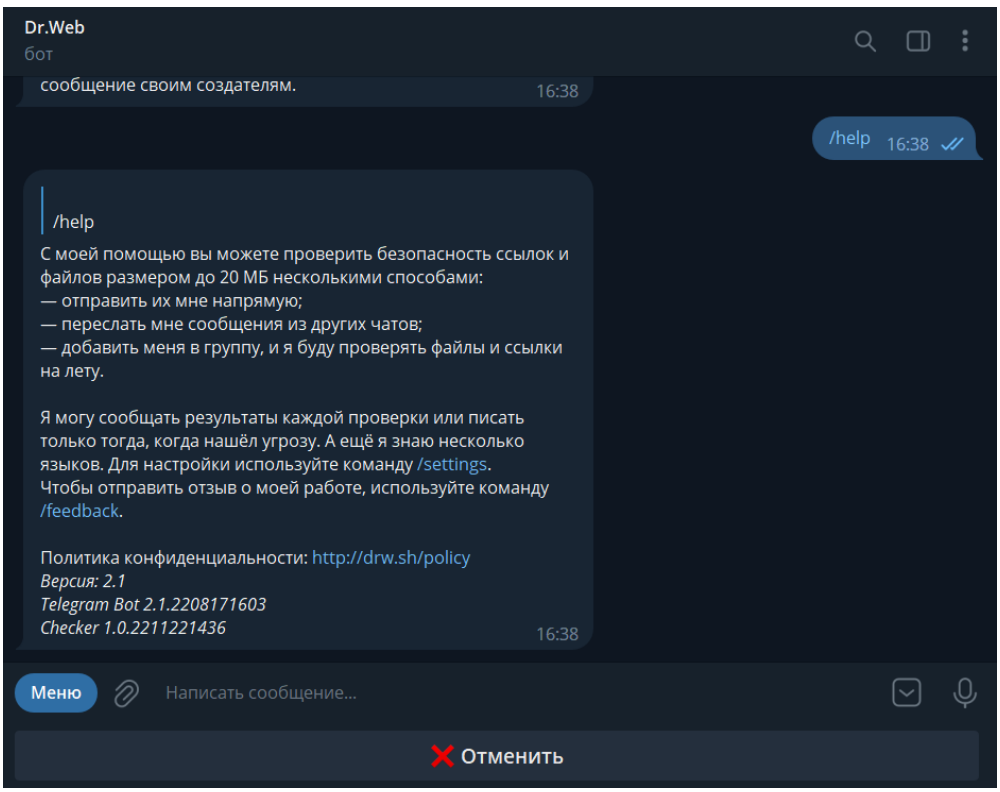

Рисунок 3 — Телеграм-бот от Dr.Web

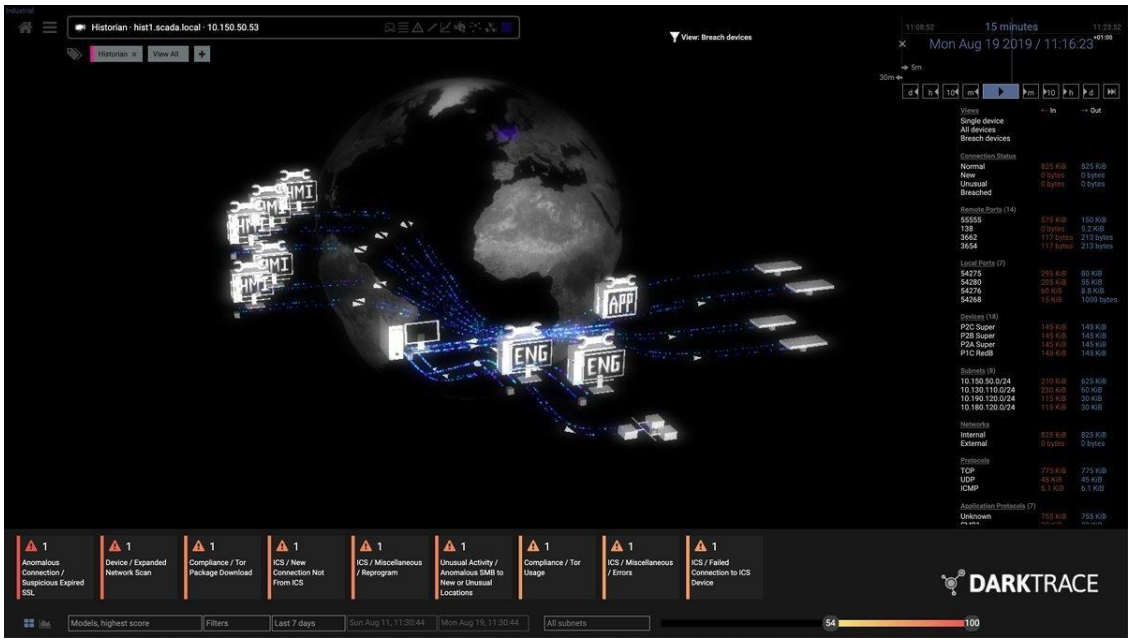

Рисунок 4 — Бот Darktrace

Кроме того, нейронные сети могут быть использованы для создания системы машинного обучения, которая будет непрерывно анализировать данные и выдавать рекомендации по улучшению системы [6].

Преимуществом использования нейронных сетей в системах безопасности является то, что они могут обрабатывать большие объемы данных в режиме реального времени. Автоматизация процесса обнаружения угроз безопасности может значительно снизить время и затраты на обработку данных, поскольку боты смогут проводить анализ данных намного быстрее, чем это делает человек. Также это может привести к сокращению рисков и минимизации потерь в случае кибератак и снижению затрат на восстановление после них, что в свою очередь способствует уменьшению потерь для бизнеса.

Но не стоит забывать о недостатках. Существует опасность, что злоумышленники могут обойти безопасность, используя слабые места в нейронных сетях или ботах. Поэтому необходимо регулярно обновлять систему и тестировать ее на уязвимости. Не стоит забывать и о ложных срабатываниях, которые могут оказаться критичными в системах безопасности. Это может стать проблемой, особенно в случае использования таких систем в крупных организациях, где блокировка доступа может привести к серьезным нарушениям бизнес-процессов и потере доходов. Однако, при правильной настройке и использовании, риски могут быть сведены к минимуму. Например, можно использовать дополнительные слои проверки и балансировки, чтобы убедиться в правильности решений, принимаемых системой безопасности.

В целом, внедрение нейронных сетей в системы безопасности с использованием ботов - инновационный и многообещающий подход, который может помочь улучшить уровень безопасности во многих сферах жизни, от банковского сектора до государственных учреждений и крупных корпораций.

Список литературы

1. Начало работы с нейронными сетями [Электронный ресурс]. - URL: https://habr.com/ru/post/542386/, (дата обращения: 08.03.2023).
2. What Does A Face Detection Neural Network Look Like? [Электронный ресурс]. - URL: https://towardsdatascience.com/face-detection-neural-network-structure-257b8f6f85d1, (дата обращения: 08.03.2023).
3. Анализ существующих подходов к распознаванию лиц [Электронный ресурс]. - URL: https://habr.com/ru/company/synesis/blog/238129/, (дата обращения: 08.03.23).
4. Bots: An introduction for developers [Электронный ресурс]. - URL: https://core.telegram.org/bots, (дата обращения: 08.03.2023).
5. Telegram Bot API [Электронный ресурс]. - URL: https://core.telegram.org/bots/api#user, (дата обращения: 08.03.2023).
6. OpenCV [Электронный ресурс]. - URL: https://docs.opencv.org/4.x/, (дата обращения: 08.03.2023).