Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

Интерпретируемый ML

Александров Валентин Валерьевич

Москва, 2021

Содержание

Аннотация

Целью данной работы является изучение средств для создания системы автоматического обнаружения инсайдерских угроз по поведенческой информации пользователей. Рассмотрен ряд различных существующих решений, которые основаны на синтетическом наборе данных инсайдерских угроз CMU CERT. На основе анализа моделей, для разработки выбрана архитектура нейросетевой модели с LSTM-кодировщиком поведения и CNN-классификатора. Результаты нейросетевых моделей сравниваются с классическими алгоритмами машинного обучения. В процессе работы были испробованы различные техники и изменения для улучшения качества предсказаний моделей такие как применение embedding-слоя в LSTM-кодировщике, взвешенная функция потерь, использование Batch Normalization, добавление дополнительных признаков, в том числе признаков о содержимом файлов.

Введение

Заключение

Текст заключения

Список использованных источников

1. *Беркутов, А.М.* Системы комплекстной электромагнитотерапии / А.М. Беркутов. — М.: Бином, 2000.

2. *И.Е. Золотухина, В.С. Улащик.* Основы импульсной магнитотерапии / В.С. Улащик И.Е. Золотухина. — Витебск: Витебская областная типография, 2008.

3. *Улащик, В.С.* Физиотерапия. Универсальная медицинская энциклопедия / В.С. Улащик. — Минск: Книжный дом, 2008.

4. *С.А. Гуляр, Ю.П. Лиманский.* Постоянные магнитные поля и их применение в медицине / Ю.П. Лиманский С.А. Гуляр. — Киев: Ин-т физиол. им. А.А. Богомольца НАН Украины, 2006.