УДК 004.4

Студ. М.С. Клочко
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ПРОТОКОЛ ОБМЕНА КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ НА ОСНОВЕ ДЕЦЕНТРАЛИЗАЦИИ КАК СРЕДСТВО ЗАЩИТЫ ОТ АТАК "ЧЕЛОВЕК ПО СЕРЕДИНЕ"

Актуальность протоколов обмена криптографическими ключами на основе децентрализации как средства защиты от атак «человек по середине» (Man-in-the-Middle, MITM) подчеркивается необходимостью обеспечения безопасности в современных цифровых системах, включая криптовалюты и блокчейн.

Протоколы обмена ключами могут быть уязвимы для активных MITM атак, где злоумышленник может взаимодействовать с обеими сторонами, создавая отдельные каналы для каждой из них и перехватывая сообщения 2. Это подчеркивает необходимость разработки и использования более надежных методов обмена ключами.

Атака «человек по середине» (Man-in-the-middle attack) происходит в процессе обмена данными, даже если данные зашифрованы, существует возможность, что эти данные могут быть известны другим лицам. Одна из возможностей заключается в том, что злоумышленник перехватывает средство коммуникации, используемое двумя общающимися людьми. Этот метод называется атакой «человек по середине». Эта проблема атаки «человек посередине» может быть преодолена с помощью протокола блокировки. Основной алгоритм этого протокола заключается в том, что этот протокол отправляет две части зашифрованного сообщения. Первая часть может быть результатом односторонней хеш-функции сообщения, а вторая часть - само сообщение. Это приводит к тому, что перехваченный человек не может расшифровать первое сообщение с помощью своего приватного ключа. Он может только создать новое сообщение и отправить его тому, кто получит сообщение. Вкратце, работа протокола блокировки, следующая:

1. Алиса отправляет свой публичный ключ Бобу.
2. Боб отправляет свой публичный ключ Алисе.
3. Алиса шифрует сообщение с использованием публичного ключа Боба, затем отправляет часть зашифрованного сообщения Бобу.
4. Боб шифрует свое сообщение с использованием публичного ключа Алисы, затем отправляет частично зашифрованное сообщение Алисе.
5. Алиса отправляет другую часть Бобу.
6. Боб объединяет оба сообщения Алисы и расшифровывает их

с помощью своего приватного ключа.

7. Боб отправляет другую часть Алисе.

8. Алиса объединяет оба сообщения Боба и расшифровывает их с помощью своего приватного ключа.

УДК 004.89

Студ. И.А. Старовойтов
Науч. рук. доц., канд. техн. наук Г.Л. Тимонович
(Кафедра информационных систем и технологий, БГТУ)

ОБНАРУЖЕНИЕ И ИЗБЕЖАНИЕ ПЕРЕОБУЧЕНИЯ В НЕЙРОННЫХ СЕТЯХ

Переобучение представляет собой распространенную проблему при обучении нейронных сетей. Когда модель слишком хорошо запоминает обучающие данные, она может плохо обобщать на новые, ранее не виданные примеры. Это может проявляться в форме высокой точности на обучающем наборе, но низкой точности на тестовых данных. Для примера создадим модель, не содержащую инструментов, способных предотвратить переобучение. Ее код представлен на рисунке 1.

```
model_overfit = tf.keras.Sequential([
    layers.Flatten(input_shape=(28, 28)),
    layers.Dense(512, activation='relu'),
    layers.Dense(512, activation='relu'),
    layers.Dense(10, activation='softmax')
])
 model_overfit.compile(optimizer='adam', loss='sparse_categorical_crossentropy',
                       metrics=['accuracy'])
```

Рисунок 1 – Модель с переобучением

После обучения модели создадим график, демонстрирующий потери на тестовом и тренировочном наборах данных, представленный на рисунке 2.

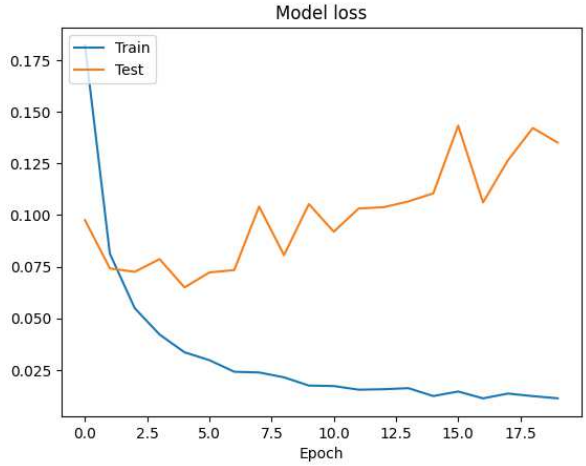

Рисунок 2 – График потерь модели