ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В СФЕРЕ КРИПТОГРАФИИ

Я.Д. Кваченюк, А.С. Николайчик, М.Г. Рогов

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Нейросети, как следует из названия, являются сетями нейронов, где каждый нейрон – это вычислительная единица, которая получает информацию, производит над ней простые вычисления и передает ее дальше.

1. Шифрование и дешифрование с использованием нейронных сетей.

Существует три основных способа шифрования данных, использующихся в большинстве случаев: хеширование, симметричное и асимметричное шифрование.

В симметричных криптосистемах в парах взаимосвязанных криптографических преобразований применяется один и тот же ключ. Для ассиметричного шифрования используются два различных криптографических ключа, образующих так называемую ключевую пару. Алгоритмы хеширования преобразуют данные произвольного размера в массив фиксированного размера – хеш-сумму [1].

Одним из примеров алгоритмов шифрования на основе нейронных сетей является нейронная сеть Хопфилда [2].

Преимуществом алгоритмов шифрования на основе нейронных сетей является их способность создавать сложные и надежные шифры.

2. Анализ криптографических алгоритмов.

Нейронные сети могут применяться для анализа криптографических алгоритмов с целью выявления уязвимостей и разработки новых методов атаки или защиты. Это включает обучение сетей на больших объемах криптографических данных для выявления слабых мест в существующих алгоритмах.

Существует три способа взлома нейросетевого протокола обмена ключом: с помощью генетической атаки, геометрической атаки и мажоритарной атаки.

Поскольку для шифровальных систем на основе нейросетевых технологий параметром, обеспечивающим безопасность передачи информации, является синаптическая глубина L нейронных сетей, то увеличение ее значения является необходимым условием для снижения вероятности успешной атаки. Так для геометрической и мажоритарной атак увеличение значения синаптической глубины является достаточным для предотвращения атаки [3].

Использование нейросетей в криптографии представляет собой мощный инструмент для защиты данных и борьбы с киберугрозами. Комбинация нейросетей с традиционными методами криптографии может повысить эффективность защиты данных и обеспечить безопасность в цифровом мире.

Список литературы

1. Угроза появления квантового компьютера для современной криптографии и шифрования [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/788590/ – Дата доступа: 18.04.2024.

2. Нейронные сети в криптографии: новые возможности и безопасность [Электронный ресурс]. – Режим доступа: https://nauchniestati.ru/spravka/primenenie-nejronnyh-setej-v-kriptografii/?ysclid=lv3q20m7c4684799624 – Дата доступа: 18.04.2024.

3. Студенческая наука - будущее государства : материалы II международной студенческой научно-практической конференции, УО «Полесский государственный университет», г. Пинск, 25 марта 2008 г. : в 2-х ч. Ч. 2 / Национальный банк Республики Беларусь [и др.]; редкол.: К.К. Шебеко [и др.]. – Пинск: ПолесГУ, 2008. – С. 91.