ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ШИФРОВАНИИ

Давлатов Мирзо-Улугбек
mirzoulugbekdavlatov@gmail.com,
ТУИТ имени Мухаммада ал-Хоразмий

Аннотация. *Криптография играет ключевую роль в обеспечении аутентификации, целостности, конфиденциальности и надежного хранения персональных данных, передаваемых через открытые сети. С развитием вычислительных технологий и увеличением их скорости устаревшие шифры заменяются более современными и адаптивными решениями. В данной статье рассматривается применение новых нейросетевых методов для шифрования данных.*

Ключевые слова: *нейронные сети, шифрование, информационная безопасность; инженерно-техническая защита информации.*

С развитием методов шифрования [1] роль математики в криптографии значительно возросла. Именно математические принципы позволили криптографии достичь такого уровня, при котором количество вычислительных операций в современных шифрах стало астрономически большим. Это привело к тому, что современные криптоалгоритмы обладают высокой стойкостью к криптоанализу, в отличие от устаревших методик, которые можно было взломать с помощью ручки и бумаги. Классический криптоанализ уже не способен эффективно справляться с взломом современных шифров.

В связи с этим все большее значение приобретают методы атак, основанные на перехвате данных, использовании шпионских устройств, атаках по сторонним каналам, применении квантовых компьютеров и бандитском криптоанализе.

Атака по сторонним (или побочным) каналам (от англ. *side-channel attack*) представляет собой класс атак, нацеленных на уязвимости в практической реализации криптосистем. Они используют недостатки физической реализации алгоритмов. Поскольку даже самый сложный криптографический алгоритм в конечном итоге реализуется программным кодом и выполняется процессором с определенной архитектурой, он неизбежно обладает характерными особенностями, которые могут быть использованы злоумышленниками.

«Классический» криптоанализ рассматривает алгоритмы шифрования исключительно с математической точки зрения, основываясь на их алгебраических свойствах, которые могут зависеть от параметров ключа.

В отличие от него, криптоанализ побочных каналов учитывает такие параметры, как время выполнения операций, потребляемую мощность, электромагнитное излучение, акустические сигналы и другие факторы. Хотя такие атаки менее универсальны, поскольку зависят от конкретного аппаратного устройства, на котором выполняется шифрование, они значительно более эффективны. На

практике большинство успешных атак связаны с уязвимостями в реализации криптографических примитивов.

Известные типы атак:

1. **Атака зондированием** – простая инвазивная атака, при которой устройство вскрывается, а затем на контакты процессора устанавливаются щупы или с помощью микроскопа исследуются ячейки памяти.
2. **Атаки по ошибкам вычислений** – основаны на преднамеренном воздействии на устройство с целью вызова ошибок. Анализируя искажения на разных этапах работы системы, можно получить информацию, позволяющую определить секретный ключ.
3. **Атаки по энергопотреблению** – пассивная атака, при которой измеряется потребляемая устройством энергия. На основе изменений энергопотребления можно извлечь информацию о выполняемых операциях и их параметрах. Осуществляется путем установки резистора в цепь питания и измерения проходящего через него тока.
4. **Атаки по электромагнитному излучению** – электронные устройства во время работы испускают электромагнитные волны. Спектральный анализ излучения позволяет определить соответствие определенных сигналов конкретным операциям, что может раскрыть информацию о работе алгоритма.

Исследования показывают, что алгоритмы DES и AES особенно уязвимы перед атаками по сторонним каналам — в некоторых случаях для их успешного проведения требуется всего 1,5 секунды или 15 измерений.

Нейронные сети, как следует из их названия, представляют собой системы, состоящие из взаимосвязанных нейронов. Каждый нейрон выполняет вычисления над входными данными и передает результаты следующему уровню сети.

Одной из ключевых особенностей нейросетей является их способность аппроксимировать любую функцию, включая криптографические алгоритмы. Моделируя существующие алгоритмы, такие как DES или AES, с помощью нейросетей, можно значительно повысить их устойчивость к атакам по сторонним каналам.

Общий вид нейронной сети представлен на рис. 1.

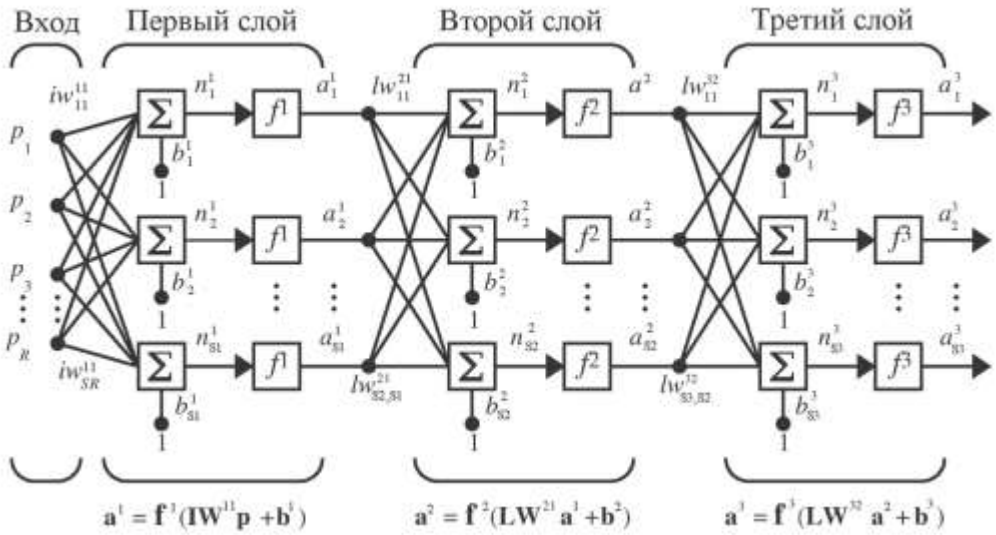

Рис. 1. Общий вид нейронной сети

Подобная структура значительно повышает защищенность от атак по сторонним каналам, поскольку:

1. **Распределение информации** – каждый нейрон содержит лишь небольшую часть данных, необходимых для корректной работы алгоритма. Это вынуждает криптоаналитика анализировать все возможные ячейки памяти, что значительно усложняет атаку.
2. **Независимость вычислений** – операции в каждом нейроне выполняются независимо от входных данных, поэтому время работы нейросети зависит только от ее архитектуры, а не от конкретного зашифрованного сообщения.
3. **Скрытие ключа и алгоритма** – веса нейронной сети не позволяют напрямую восстановить секретный ключ, а в некоторых случаях даже сам алгоритм шифрования остается недоступным для анализа.

Все эти свойства делают нейронные сети надежным инструментом для защиты от атак по побочным каналам, значительно затрудняя извлечение ключевой информации злоумышленниками.

СПИСОК ЛИТЕРАТУРЫ:

1. Элементы больших порядков в линейных группах и модификация системы эль-гамаля. URL: http://www.info-secur.ru/is_15/Zulyarkina.htm
2. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020.
3. Koblitz N. A Course in Number Theory and Cryptography. – Springer, 1994.
4. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 1996.
5. Katz J., Lindell Y. Introduction to Modern Cryptography. – CRC Press, 2020.
6. Bishop M. Computer Security: Art and Science. – Addison-Wesley, 2018.