ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ХЕШ-КОДОВ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

И.А. Сухинин, В.А. Липницкий

Работа рассматривает возможность использования нейронных сетей для генерации стойких хеш-кодов. Искусственные нейронные сети — реализации математических моделей, построенных по принципу организации и функционирования сетей нервных клеток живого организма. Одной из основных особенностей ИНС является возможность обучения. Эта возможность отличает ИНС от традиционных программ с заранее запрограммированными алгоритмами решения.

Хеширование — преобразование входного массива данных произвольной длины в выходную битовую строку произвольной длины — хеш-код. Такие преобразования называются хеш-фукнциями. Случаи, когда двум различным входным массивам данных соответствуют одинаковые выходные строки, называются коллизиями.

Среди множества существующих хеш-функций выделяют криптографически стойкие хеш-функции, которые могут быть использованы в криптографии. Эти фукнции должны удовлетворять трем основным требованиям: необратимостью, стойкостью к коллизиям первого рода, стойкостью к коллизиям второго рода. Одним из дополнительных требований к криптографически стойким хеш-функциям является сильное изменение значения при малейшем изменении входящего значения. С его помощью гарантируется стойкость защищенных данных даже при утечке их малейшей части.

Для использования в качестве криптографически стойкой хеш-функции можно задействовать многослойный персептрон. Для создания простой хеш-функции достаточно трех слоёв нейронов. Каждый из нейронов должен обладать нелинейной функцией активации. Количество выходов сети зависит от планируемой длины выходного блока информации. Количество входов сети необходимо подбирать экспериментально. Также необходимо настроить весовые коэффициенты сети так, чтобы разным входам соответствовали разные выходы. Преимуществом нейросетевого подхода к построению криптографически стойкой хеш-функции является то, что для получения результата не требуется многократных итераций и сложных преобразований, что, в свою очередь, позволяет получить значительный выигрыш во времени выполнения.