

Аппарат искусственных нейронных сетей в вопросах обеспечения информационной безопасности

Автор: Мельничук П.Ф., Левкович С.С. Нагуськин В.В., Соловьев Д.В., Исаев А.В., Гатчин Ю.А., Бондаренко И.Б.

Научный руководитель: Соловьев Денис Викторович, Университет ИТМО

Одновременно с быстрым развитием информационных технологий и появлением новых технических средств, обрабатывающих информацию, так же увеличивается количества угроз. В связи с этим, становится актуальна задача разработки новых методик защиты информации. Особое внимание в этом вопросе стоит уделить методам, где применены технологии искусственных нейронных сетей.

Искусственные нейронные сети обладают рядом особенностей и преимуществ, которые позволяют эффективно их использовать при решении задач из области информационной безопасности:

— после проведения процесса обучения, выходной сигнал искусственные нейронные сети становится в некоторой степени нечувствительным к небольшим колебаниям сигналов на входе сети, что особенно важно для решения задачи распознавания образов, например, при поиске, идентификации конкретных лиц, автомобильных номер, сравнении почерков;

— при использовании соответствующего типа сети, количества слоев, вида и количества нейронов, качества обучения, искусственная нейронная сеть способна обратить внимание на сведения, которые являются несущественными для неинтеллектуальной системы защиты;

— в процессе обучения искусственных нейронных сетей возможно выявление новых сведений, закономерностей, которые могут быть использованы для коррекции входных данных, топологии сети, с целью получения более эффективной защиты.

На данный момент можно выделить основные направления внедрения искусственных нейронных сетей в защиту информации:

— проведение испытаний подсистем и оборудования систем защиты по требованиям информационной безопасности, моделирование возникновения и вариантов разрешения внештатных ситуаций;

— обнаружение вторжений и защита от DDoS-атак с помощью самообучающихся ИНС без постоянного вмешательства человека;

— криптографические методы защиты информации, автоматизация процессов криптоанализа, снижение временных затрат на его проведение;

— построение алгоритмов прогнозирования полученных шаблонных данных с целью выявления аномалий в активности, классификации или кластеризации операций, событий;

— биометрические методы аутентификации отпечатков пальцев, сетчатки глаза, поведенческих характеристик.

Из выше изложенного можно сделать вывод, что технологии искусственных нейронных сетей активно внедряются во многие области информационной безопасности. Они представляют очень перспективную и быстро развивающую область науки, ресурсы которых эффективно используются для решения сложных задач в области защиты

информации, связанных с анализом поступающих данных, распознаванием образов, построением принятия решений.

Автор

Мельничук П.Ф.

Научный руководитель

Соловьев Д.В.

Заведующий кафедрой

Заколдаев Д.А.