0.1. *Полянский А.Н., Амаров А.А., Карижов А.А.* **Система обнаружения аномальной активности в сетях пакетной передачи данных**

Повсеместное распространение глобальных и локальных телекоммуникационных сетей изменило вычислительные системы, которые стали более связанными и менее защищенными от действий злоумышленников. Складывается устойчивая тенденция к росту количества атак на вычислительные системы и сети. Технологии, средства и методы удаленных сетевых атак постоянно совершенствуются, и существующие средства защиты не позволяют полностью пресекать злонамеренный трафик. Эти обстоятельства делают разработку и внедрение методов и средств защиты информации в вычислительных сетях весьма актуальной задачей [1, 2].

Обнаружение вторжений можно определить, как интеллектуальный мониторинг событий, протекающий в сетях передачи данных, их анализ на наличие признаков нарушения политики безопасности или обхода механизмов безопасности. Достижение приемлемых уровней защиты информационных ресурсов невозможно применяя исключительно алгоритмические или программно-аппаратные решения [3]. Средства обнаружения вторжений должны включать интеллектуальные подсистемы, по крайней мере, в качестве одной из составных частей.

Целью данного исследования является разработка интеллектуальной системы обнаружения вторжений, основанной на использовании искусственных нейронных сетей. Для обучения нейронной сети использовался набор данных [4], содержащий 41 параметр, описывающий сетевое соединение, и соответствующий им тип атаки или легальной активности. Выявление существенных признаков в структуре данных показало 9 параметров, обеспечивающих наиболее полное и релевантное описание сетевого соединения. Результаты обучения и тестирования спроектированной нейронной сети показывают возможность ее применения в качестве классификатора для системы обнаружения сетевых атак.

Список литературы

[1] Мустафаев А. Г. Применение искусственных нейронных сетей в разработке системы обнаружения вторжений // Промышленные АСУ и контроллеры. 2018. № 7. С. 17–26.

[2] Mustafaev A. G. Application of artificial neural networks In the intrusion detection system // International Journal on Information Technologies and Security. 2018. Vol. 10. N. 4. P. 57–66.

[3] Mustafaev A. G., Buchaev A. Y. A Reliable Authentication Method for the Internet of Things Devices // 2020 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, 2020, P. 1–3.

[4] KDD Cup 1999 [Электронный ресурс] http://kdd.ics.uci.edu/databases/kddcup99 (дата обращения: 13.10.2020).