УДК 004.838.2

МОНИТОРИНГ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ АППАРАТА ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Левкович С.С. (Университет ИТМО), **Гатчин Ю.А.** (Университет ИТМО), **Глебов Р.Г.** (Университет ИТМО), **Кашицин Н.О.** (Университет ИТМО)
Научный руководитель – доктор технических наук, профессор Гатчин Ю.А. (Университет ИТМО)

Существующие системы обнаружения вторжений (СОВ), которые на сегодня используются для мониторинга и анализа безопасности информационных систем (ИС), разработаны на основе использования правил и сигнатур. Такие системы нуждаются в постоянном обновлении для эффективного обнаружения атака на ИС. Порой эти обновления выполняются вручную или автоматизированно через определенный промежуток времени. При малейшем несовпадении сигнатуры атаки с заданной сигнатурой в СОВ - такой тип атаки не буде распознан. В современном мире, каждый день, появляются все новые типы атак на ИС, поэтому обычные СОВ не всегда способны обеспечить идентификации атаки. В данной работе будет представлено решение на эту проблему - использование СОВ на основе аппарата искусственных нейронных сетей.

Системы обнаружения вторжений на информационные системы на протяжении длительного времени используются как один из основных инструментов защиты ИС. Сейчас СОВ в основном представлены в виде программного или аппаратно-программного решений. За последние годы количество и характер несанкционированных атак на ИС значительно увеличились, вследствие чего возросла и нагрузка на СОВ. Постоянное изменение характера сетевых атак на ИС требует создания технического решения с гибкой адаптивной системой защиты, которая способна анализировать большое количество сетевого трафика с постоянно меняющимися условиям сетевой активности. Таким возможным решением является разработка СОВ с использованием аппарата ИНС.

Главное применение нейронной сети в СОВ - это обнаружение атак на системном и сетевом уровне: подбор пароля; вирусы и трояны; сниффинг и спуфинг пакетов; DoS-атаки; несанкционированные вход пользователя и запуск программ. Использование нейросети в СОВ для мониторинга информационной безопасности (ИБ) определяется ее особенностями: она сначала производит обучение для обнаружения атак путем настройки архитектуры сети и весов синапсов; она обнаруживает атаки по неполным и даже частично недостоверным исходным данным; она позволяет определять новые типы атак, так как нейросеть производит новые данные на основе накопленных данных об атаках.

Нейронная сеть может достичь превосходных результатов в решении таких сложных инженерных задач как распознавание образов, классификация, мониторинг и прогнозирование. Повышение эффективности выявления инцидентов информационной безопасности с помощью ИНС является актуальной научно-технической задачей. В ходе исследования этого вопроса были проанализированы существующие российские и зарубежные разработки в области защиты ИБ, а именно, мониторинг и выявление угроз на ИС. В данной статье был сделан следующий вывод, что применение нейросетей в СОВ позволяет повысить эффективность мониторинга за счет ее возможности обнаруживать атаки, сигнатура которых частично отличается от находящейся в базе данных СОВ.

Левкович С.С. (автор) Подпись

Гатчин Ю.А. (научный руководитель) Подпись