АТАКИ НА НЕЙРОННЫЕ СЕТИ

Есаулов В. Н.

Аннотация: Одной из основных тенденций совершенствования современных систем обнаружения атак является применение различных методов искусственного интеллекта, среди которых особую популярность получили методы теории искусственных нейронных сетей.

Хотя эффективность нейросетевых средств обнаружения и считается доказанной, однако сфера их применения определена недостаточно четко. Особенно актуальным является вопрос определения множества Интернет-ориентированных кибератак, для выявления которых целесообразно применять нейросетевые средства.

Вступление: Одним из основных признаков развития современного общества является дальнейший рост зависимости от качества и надежности компьютеризированных информационных систем (ИС), применяемых в различных областях человеческой деятельности.

Соответствующее усиление стратегической напрямленности информационных ресурсов обусловливает необходимость повышения требований к уровню их информационной безопасности.

Основная часть: Проблема обостряется тем, что особенности глобальной сетей и Интернет, с которой интегрировано большинство отечественных ИС, позволяющих злоумышленникам, оставаясь вне пределов российской юрисдикции, реализовывать долговременные, массовые и разно вариантные кибератаки на информационные ресурсы, а своевременному применению адекватных защитных мер во многом мешает несовершенство систем обнаружения атак (СОА).

При этом, под термином кибератаки (кибернетической атаки) будем понимать реализацию в кибернетическом пространстве угроз безопасности его компонентов (а именно конфиденциальности, целостности и доступности) с учетом их уязвимостей.

Отметим, что кибернетическое пространство – это виртуальное пространство, полученное в результате взаимодействия пользователей, программного и аппаратного обеспечения, сетевых технологий для поддержания и управления процессами преобразования информации с целью обеспечения информационных потребностей общества.

Самой многочисленной и опасной для отечественных ИС является группа активного воздействия (кибероружие). Соответственно типу кибероружия, атаки разделяются на компьютерные вирусы, программные закладки и логические бомбы, электромагнитные пушки (портативные генераторы электромагнитного рода излучения большой мощности), разнообразные устройства постановки

активных коммуникационных помех, средства уничтожения, искажения и хищения информационных массивов, специальные аппаратные закладные устройства способные разрушать изоляционный материал и радиоэлектронные элементы.

Основываясь на результатах анализа научных работ, посвященных нейросетевым средствам обнаружения атак на ИС, определено, что основные направления их совершенствования заключаются в разработках:

- общетеоретических подходов к их использованию;
- методов подготовки исходных данных для нейросетевой модели;
- методов адаптации архитектуры НС к условиям поставленной задачи;
- моделей атак, адаптированных к применению нейросетевых средств обнаружения;
- нейросетевых моделей, предназначенных для обнаружения атак определенного типа;
- новых нейросетевых моделей, предназначенных для использования в СОА.

Много исследовательских работ посвящены разработке нейросетевых технологий обнаружения сетевых атак на информационные ресурсы. Предложены методы сжатия пространства признаков, что используется в НС для обнаружения сетевых атак. Ожидаемый положительный результат заключается в уменьшении срока процесса обучения НС. Разработанные методы определения типа нейросетевой архитектуры, оптимальной с точки зрения условий поставленной задачи распознавания.

Следует отметить, что, несмотря на достаточно весомые научно-практические результаты, в данной тематике далекой от решения является задача определения принципиальной пригодности применения нейросетевых средств для распознавания кибератак конкретного типа.

То есть недостаточно исследованными являются вопросы определения множества кибератак, для выявления которых целесообразно следует применять НС, что с одной стороны сужает сферу их применения и усложняет процесс их созидания, а с другой – может привести к увеличению ложных срабатываний СОА.

Выводы: указывают на то, что наиболее опасные кибератаки реализуются за счет средств активного компьютерного воздействия, которые способны нарушить функционирование ИС органов управления государственных и военных объектов, промышленности, транспорта, связи, энергетики, банков и других учреждений путем непосредственного информационного вмешательство в работу КС.

Литература:

1. Абрамов Е. С. Разработка и исследование методов построения систем обнаружения атак: дис. канд. техн. наук: 05.13.19 / Абрамов Е. С. - Таганрог, 2015. - 199 с.

2. Артеменко А.В., Головко В. А. Анализ нейросетевых методов распознавания компьютерных вирусов /Материалы секционных заседаний. Молодежный инновационный форум «ИНТРИ» – 2010. — Минск: ГУ «БелИСА», 2017. – 239 с.

3. Большев А. К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. дисс. на соискание научн. степени канд. техн. наук: спец . 05.13.19 – Методы и системы защиты информации, информационная безопасность / А. К. Большев - Санкт-Петербург, 2016. - 36 с.