УДК 004.056.52; 004.891.3

СОЗДАНИЕ СИСТЕМ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИИ DLP С ПРИМЕНЕНИЕМ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ ВЫЧИСЛЕНИЯ

© Марченко Е.А., Жуков С.В.

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация

e-mail: KatyushenkaMarchenko@mail.ru

Data Loss Prevention (DLP), в переводе с английского «предотвращение потери данных», является комплексом стратегий, политик и технологий, направленных на предотвращение несанкционированного раскрытия и потери конфиденциальной информации в организации. Оно включает в себя меры для обнаружения, мониторинга и предотвращения утечек данных.

Целью DLP является защита конфиденциальных, чувствительных и регулируемых данных, таких как персональная информация, финансовые данные, интеллектуальная собственность и другие важные данные, которые могут быть предметом несанкционированного доступа, утечек или утраты.

DLP-системы могут использовать различные методы для обнаружения потенциальных утечек данных, включая мониторинг сетевого трафика, анализ содержимого файлов, контроль использования съемных устройств и шифрование данных. Они также могут предоставлять функциональность для блокирования или предупреждения о попытках несанкционированного доступа или передачи конфиденциальных данных. Они могут быть реализованы на уровне сети, на уровне хостовой системы или на уровне конечных устройств. Такие системы могут включать в себя сочетание аппаратных и программных компонентов, а также использование аналитики данных и машинного обучения для улучшения обнаружения и предотвращения потери данных [1].

Многослойная нейронная сеть прямого распространения является наиболее популярной формой искусственных нейронных сетей (ИНС), которые обладают способностью к обучению путем изменения весов и порогов внутри сети (см. рисунок).

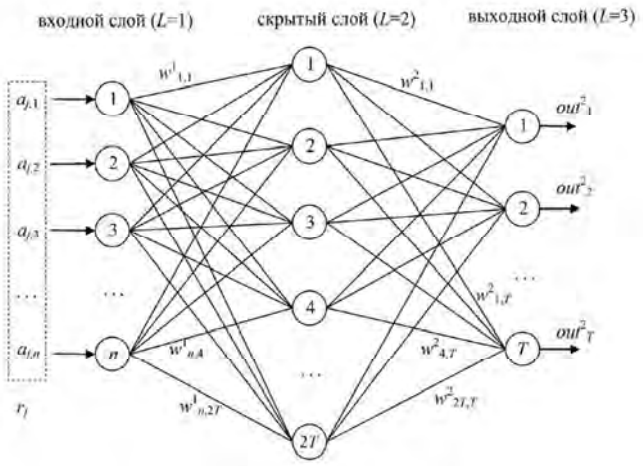

Рисунок – Многослойная нейронная сеть прямого распространения.

Обучение многослойной нейронной сети прямого распространения имеет несколько преимуществ:

1. Способность к аппроксимации сложных функций. Многослойная нейронная сеть способна аппроксимировать сложные нелинейные функции, такие как распознавание образов, классификация данных или предсказание значений.

2. Гибкость и адаптивность. Многослойная нейронная сеть может быть гибко настроена и адаптирована под различные задачи и типы данных.

3. Обработка больших объемов данных. Благодаря параллельным вычислениям и возможности использования мощных вычислительных ресурсов они могут быстро анализировать и извлекать полезную информацию из больших наборов данных.

Эти преимущества делают многослойные нейронные сети прямого распространения мощным инструментом для обработки и анализа данных в различных областях и задачах машин [2].

Использование искусственного интеллекта в DLP стремится к успешному соединению новых технологий с человеческими способностями, чтобы эффективно объединить их преимущества. Компании вовлекают экспертов по нейронным сетям и машинному обучению для выбора, создания и применения инновационных методов и решений на основе данных, совмещая их с уже существующими традиционными решениями DLP.

Нейронные сети могут внести значительный вклад в DLP-системы следующими способами:

1. Обнаружение утечек данных. Нейронные сети могут быть обучены на основе различных шаблонов и характеристик конфиденциальных данных для обнаружения потенциальных утечек.

2. Классификация данных. Они могут использоваться для классификации данных и идентификации конфиденциальной информации. Это помогает в определении, какие данные требуют особой защиты и контроля.

3. Анализ поведения пользователей. Нейронные сети могут изучать поведение пользователей и выявлять аномалии или подозрительные действия, которые могут указывать на возможные нарушения безопасности или утечки данных.

4. Проактивная защита. Они могут помочь в реализации проактивных мер безопасности, предотвращая потенциальные утечки данных до их возникновения.

Все эти возможности нейронных сетей способствуют улучшению эффективности DLP-систем и помогают предотвратить несанкционированное раскрытие и утрату конфиденциальных данных [3].

Библиографический список

1. Методики интеллектуального выбора и оценки DLP-системы для решения проблем информационной безопасности / А.Р. Айдинян, О.Л. Цветкова, П.В. Черняков, Д.С. Сокол // Молодой исследователь Дона. Донской государственный технический университет. 2018. № 1 (10). С. 1–4. URL: https://cyberleninka.ru/article/n/metodiki-intellektualnogo-vybora-i-otsenki-dlp-sistemy-dlya-resheniya-problem-informatsionnoy-bezopasnosti (дата обращения: 16.05.2023). DOI: 10.26583.

2. Дубровин В.И., Субботин С.А. Методика синтеза и обучения многослойной нейронной сети классификации образов // Радиоэлектроника, информатика, управление. 2002. № 2 (8). URL: https://cyberleninka.ru/article/n/metodika-sinteza-i-obucheniya-mnogosloynoy-neyronnoy-seti-klassifikatsii-obrazov (дата обращения: 31.05.2023).

3. Писаренко И.В. Нейросетевые технологии в безопасности // Информационная безопасность. 2009. № 4. С. 34–35. URL: https://lib.itsec.ru/articles2/Oborandteh/neyrosetevye-tehnologii-v-biznese (дата обращения: 16.05.2023).