УДК 004.056

РАЗРАБОТКА АЛГОРИТМА ВЫЯВЛЕНИЯ АТАК В КОРПОРАТИВНЫХ СЕТЯХ НА ОСНОВЕ МЕТОДА «RANDOM FOREST»

Якимова С.А. (Национальный Исследовательский Университет ИТМО)

Научный руководитель – кандидат технических наук, ассистент Коржук В.М.

(**Национальный Исследовательский Университет ИТМО**)

Цель исследования – повысить показатель точности выявления атак в корпоративных сетях путем разработки алгоритма выявления атак в корпоративных сетях на основе метода машинного обучения «Random Forest». В работе рассмотрены существующие методы обеспечения информационной безопасности в корпоративных сетях, выявлены их недостатки, проанализирована роль машинного обучения в детектировании сетевых атак и, на основании полученных данных, произведена разработка алгоритма выявления атак в корпоративных сетях на основе метода «Random Forest».

Введение. Обнаружение сетевых атак в настоящее время играет важнейшую роль в вопросе безопасного применения корпоративных сетей. Сейчас практически каждая сеть обладает активными средствами предупреждения атак: например, антивирус или брандмауэр. Однако подобных методов защиты бывает недостаточно. По данным CERT, ежедневно появляется примерно 70 новых атак, что приводит к проблеме обновления базы данных сигнатур до актуальных версий. Все чаще для решения таких задач, как обеспечение информационной безопасности, прогнозирование и предупреждение сетевых атак, мониторинг трафика, используются методы машинного обучения.

Основная часть. В ходе работы производится анализ основных особенностей корпоративных сетей и их структуры. Выявляются основные уязвимости, проводится анализ существующих методов обнаружения атак в корпоративных сетях. Далее, производится сравнительный анализ существующих методов машинного обучения и выбирается наиболее подходящий из них для разработки алгоритма. На основании полученной информации разрабатывается алгоритм выявления атак в корпоративных сетях, учитывающий особенности подобных сетей. Для получившегося алгоритма производится расчёт показателей точности выявления атак с последующим сравнительным анализом между полученными и изначальными показателями.

Выводы. В ходе исследования были проанализированы корпоративные сети и существующие для них методы обеспечения информационной безопасности. По результатам исследования выявлено, что машинное обучение в настоящее время успешно справляется с определением аномалий, в частности метод «Random Forest». В результате разработан алгоритм выявления атак в корпоративных сетях на основе метода «Random Forest». Данный алгоритм учитывает особенности корпоративных сетей и способен повысить показатели точности выявления сетевых атак.

Якимова С.А. (автор) Подпись

Коржук В.М. (научный руководитель) Подпись