УДК 004.492.3

РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ IOT-РЕШЕНИЙ

Невесенко В.Н. (Национальный Исследовательский Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Коржук В.М.
(Национальный Исследовательский Университет ИТМО)

Цель исследования – повышение уровня конфиденциальности данных, циркулирующих в инфраструктуре IoT-системы путем разработки модели системы обнаружения вторжений для продукта в области IoT. В статье рассмотрены существующие методы обеспечения информационной безопасности в области IoT, проанализированы их достоинства и недостатки, и, на основании полученных данных, производится разработка модели.

Введение. В настоящее время непрерывно расширяется объем мирового рынка в сфере IoT, но, вместе с этим, проведение работ, направленных на обеспечение их информационной безопасности недостаточно. Так, согласно авторитетному изданию «Security Lab», за 2017 год только 22% специалистов проверяли подключенные устройства на наличие вредоносного ПО. Существующие решения в области обеспечения конфиденциальности информации в IoT-системах предполагают ресурсозатратные решения с применением различных протоколов шифрования, что снижает скорость и удобство использования IoT-решений.

Основная часть. Производится моделирование топологии сетевой инфраструктуры испытуемой IoT-системы, анализ уязвимостей, определяются предполагаемые угрозы защищенности данных с последующей оценкой показателя конфиденциальности информации с использованием необходимых метрик оценки. Далее, производится разработка модели системы обнаружения вторжения на основе Open-Source решений с последующим ее внедрением в смоделированную ранее инфраструктуру сети. Для получившейся модели проводится тестирование реакции на выявленные ранее угрозы защищенности данных. Проводится повторная оценка уровня конфиденциальности информации с последующим сравнительным анализом значений до и после внедрения системы обнаружения вторжений.

Выводы. В ходе исследования была разработана модель системы обнаружения вторжений для IoT-решений, учитывающая особенности устройств, связанные с типом соединения, скоростью обработки информации и ресурсозатратностью. Представленная модель позволяет оперативно обнаруживать аномальный трафик и своевременно предотвращать атаки на IoT-систему.

Невесенко В.Н. (автор) Подпись

Коржук В.М. (научный руководитель) Подпись