2022307 Программный компонент системы «Интернет вещей»

Оглавление

Введение ... 2
1 Теоретические основы защиты информации систем Интернета вещей ... 4
1.1 Терминология информационной безопасности ... 4
1.2 Угрозы информационной безопасности ... 7
2 Обеспечение безопасности информационных систем Интернета вещей 20
2.1 Характеристика технологий, применяемых для защиты информации 20
2.2 Защита от несанкционированного использования и искажения информации ... 23
3 Анализ Snort как программного компонента системы Интернета вещей 31
3.1 Понятие, становление и использование технологии «Snort» ... 31
3.2 Особенности построения Snort как сетевой системы IDS и IPS ... 36
3.2.1 Анализ систем обнаружения вторжений (IDS) ... 36
3.2.2 Анализ систем предотвращения вторжений ... 38
3.2.3 Анализ существующей классификации СОВ ... 42
3.2.4 Анализ методов обнаружения вторжений ... 45
3.2.5 Анализ системы сетевого обнаружения вторжений ... 48
3.2.6 Сравнение и выбор систем обнаружения вторжений ... 50
4 Место и роль Snort в нейросетевых технологиях для обнаружения компьютерных атак в системе Интернета вещей ... 51
4.1 Возможности анализа трафика при помощи нейросети на базе Snort 52
4.2 Методика построения нейросети с целью обнаружения сетевых компьютерных атак на основе программного комплекса «Snort» ... 54
5 Реализация программной части для Интернета вещей, с использованием анализа трафика при помощи нейросети для IDS и IPS ... 71
5.1 Краткое руководство пользователя Snort ... 71
5.2 Разработка виртуального модуля для Интернета вещей, с использованием анализа трафика при помощи нейросети, позволяющего находить вторжения и атаки ... 75
Заключение ... 83
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ ... 85
ПРИЛОЖЕНИЕ. ФРАГМЕНТ ЛИСТИНГА ПРОГРАММНОГО КОДА ... 88