**Попов Илья Юрьевич Методы и алгоритмы защиты от распределенных сетевых атак типа "отказ в обслуживании"**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Попов Илья Юрьевич

СОДЕРЖАНИЕ

РЕФЕРАТ

SYNOPSIS

ВВЕДЕНИЕ

ГЛАВА 1. КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ПРИНИМАЮЩЕГО УЗЛА КОМПЬЮТЕРНОЙ СЕТИ ПОД ВОЗДЕЙСТВИЕМ СЕТЕВЫХ РАСПРЕДЕЛЕННЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

1.1 Основания для концептуального моделирования

1.2 Классификация сетевых атак типа «отказ в обслуживании»

1.2.1 Атаки типа «отказ в обслуживании» на уровнях L2-L4 модели OSI

1.2.2 Сетевые атаки типа «отказ в обслуживании» на уровнях L7 модели OSI

1.3 Анализ методов противодействия сетевым атакам типа «отказ в обслуживании»

1.3.1 Методы для противодействия сетевым атакам на уровнях L2-L4 модели OSI

1.3.2 Методы противодействия сетевым атакам типа «отказ в обслуживании» на уровне L7 приложений

1.3.3 Методы, основанные на алгоритмах машинного обучения и нейросетей

1.4 Концептуальное моделирование состояния изменения принимающего узла вследствие сетевых атак типа «отказ в обслуживании»

1.4.1 Выбор метода моделирования

1.4.2 Метод куста событий

1.4.3 Построение правил событий

1.4.4 Построение куста событий для исследования состояния принимающего узла под воздействием атак

1.4.5 Метод формализации сценариев типовых атак типа «отказ в обслуживании»

1.5 Выводы

ГЛАВА 2. МЕТОДЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК ТИПА «ОТКАЗ ОБСЛУЖИВАНИИ»

2.1 Задача детектирования сетевых атак типа «отказ в обслуживании»

2.2 Анализ сущности сетевой атаки типа «отказ в обслуживании»

2.3 Анализ атрибутов сетевого пакета

2.4 Выбор алгоритма машинного обучения с учителем для детектирования известных атак

2.4.1 Алгоритм к-ближайших соседей

2.4.2 Алгоритм регрессии

2.4.3 Алгоритм деревьев решений

2.4.4 Алгоритм случайного леса

2.4.5 Алгоритм градиентного бустинга

2.5 Метод детектирования раннее известных сетевых атак типа «отказ в обслуживании» на основе алгоритма градиентного бустинга

2.6 Алгоритм выявления сетевых распределенных атак типа «отказ в обслуживании»

2.7 Улучшение разработанного метода в целях детектирования неизвестных сетевых атак типа «отказ в обслуживании» на основе локального уровня выброса

2.7.1 Детектирование аномального сетевого трафика

2.7.2 Сбор данных для выявления неизвестных ранее сетевых атак типа «отказ в обслуживании»

2.7.3 Выбор метода для поиска аномалий в сетевого трафике на наличие сетевых атак типа «отказ о обслуживании»

2.7.4 Алгоритм локальных коэффициентов выброса

2.7.5 Метрики для оценки точности детектирования сетевых атак типа «отказ в обслуживании»

2.7.6 Алгоритм автоматизированного пополнения сценариев сетевых распределенных атак типа «отказ в обслуживании»

2.8 Выводы

ГЛАВА 3. РАЗРАБОТКА СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ РАСПРЕДЕЛЕННЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

3.1 Алгоритм обнаружения и противодействия известным сетевым атакам типа «отказ в обслуживании»

3.1.1 Этап сбора данных

3.1.2 Программные инструменты для анализа полученных данных

3.1.3 Этап обучения

3.1.4 Отбор наиболее информативных признаков

3.4.5 Исключение недообучения и переобучения

3.4.6 Результаты классификации

3.2. Алгоритм обнаружения и противодействия ранее неизвестным сетевым атакам типа «отказ в обслуживании»

3.2.1 Наблюдение за активностью пользователя

3.2.2 Анализ наблюдаемых данных

3.2.3 Детектирование потенциальных сетевых атак

3.2.4 Результат кластеризации

3.3 Блокировка сетевых распределенных атак типа «отказ в обслуживании»

3.3.1 Списки контроля доступа

3.3.2 Алгоритм работы списков контроля доступа для блокировки вредоносного трафика

3.4 Выводы

ГЛАВА 4. ОЦЕНКА РЕЗУЛЬТАТОВ РАБОТЫ МЕТОДОВ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

4.1 Выбор компонентов для разрабатываемого средства

4.2 Описание и обоснование выбранной архитектуры

4.2.1 Описание архитектуры

4.2.2 Обоснование принимаемых принципиальных конструкционных решений

4.3 Функциональная схема программно-аппаратной платформы

4.3.1 Обобщенный алгоритм противодействия сетевым атакам типа «отказ в обслуживании» на основе программируемой логической интегральной схемы

4.3.2 Алгоритм детектирования сетевых атак типа «отказ в обслуживании» на основе машинного обучения

4.4 Тестирование разработанных методов и алгоритмов для противодействия сетевым распределенным атакам типа «отказ в обслуживании»

4.4.1 Архитектура тестового стенда

4.4.2 Описание принципов тестирования предлагаемых в работе методов и алгоритмов

4.4.3 Тестирование принимающего узла с применением разработанных методов, алгоритмов для противодействия сетевым атакам типа «отказ в обслуживании»

4.4.4 Оценка результатов предлагаемых методов при детектировании комбинированных сетевых распределенных атак типа «отказ в обслуживании» и сравнение с аналогами

4.5 Выводы

ЗАКЛЮЧЕНИЕ

СПИСОК РИСУНКОВ

СПИСОК ТАБЛИЦ

СПИСОК ЛИТЕРАТУРЫ

ПРИЛОЖЕНИЯ

Приложение А. Акты о применении и внедрении

Приложение В. Результаты интеллектуальной деятельности

Приложение С. Основные публикации по теме диссертации

РЕФЕРАТ