**Джаммул Самих Мохаммед Идентификация трафика сетей передачи данных в реальном времени**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Джаммул Самих Мохаммед

СПИСОК СОКРАЩЕНИЙ

ВВЕДЕНИЕ

ГЛАВА 1. ПОСТАНОВКА ЗАДАЧИ ИДЕНТИФИКАЦИИ ТРАФИКА В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

1.1. Сравнительный анализ существующих моделей трафика сетей передачи данных

1.2. Анализ существующих методов классификации трафика в сетях передачи данных

1.3.Математическая постановка задачи идентификации сетевого трафика

1.4.Выводы по главе

ГЛАВА 2.РАЗРАБОТКА МОДЕЛИ ИДЕНТИФИКАЦИИ ТРАФИКА

СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

2.1 .Модель идентификации трафика сетей передачи данных на основе

скрытой марковской модели

2.2.Определение значений параметров модели идентификации

трафика

2.3.Определение наблюдаемых параметров модели идентификации

трафика

2.4.Определение начальных значений параметров модели

2.5. Определение пороговой функции идентификации приложения

2.6. Выводы по главе

ГЛАВА 3. РАЗРАБОТКА И ИССЛЕДОВАНИЕ АЛГОРИТМОВ И

ПРОГРАММНЫХ СРЕДСТВ ИДЕНТИФИКАЦИИ СЕТЕВОГО ТРАФИКА

Стр.

3. 1 .Подготовка трафика для идентификации

3.2. Алгоритмы идентификации сетевого трафика на этапе обучения и тестирования

3.3.Выбор сетевых приложений и описание набора трафика на этапах обучения и тестирования

3.4.Сравнение полученных и известных результатов идентификации сетевого трафика

3.5.Выводы по главе

ГЛАВА 4. РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ И

АЛГОРИМОВ ИДЕНТИФИКАЦИИ ТИПОВ ПРИЛОЖЕНИЙ ТУННЕЛЬНОГО ТРАФИКА

4.1.Модель идентификации типа приложений в туннеле сетевого трафика

4.2.Параметры модели идентификации типа приложения в туннеле трафика

4.3. Разработка алгоритмов и программ идентификации типов приложений в туннели трафика

4.4.Тестирование модели идентификации типов приложений в туннеле трафика

4.5.Выводы по главе

ОБЩИЕ ВЫВОДЫ И ЗАКЛЮЧЕНИЕ

СПИСОК ЛИТЕРАТУРЫ

ПРИЛОЖЕНИЕ А. Исходные коды программных модулей, примеры

файлов наблюдаемых данных и вычисленных параметров модели

ПРИЛОЖЕНИЕ Б. Акты внедрения

СПИСОК СОКРАЩЕНИЙ

ДП - длина пакета

ИВП - интервал времени между пакетами ИТ - идентификация трафика

ИТПТТ - идентификация типа приложения в туннеле трафика

МГС - модель гауссовой смеси

СММ - скрытая марковская модель

СПД - сети передачи данных

AR - autoregressive

ARIMA - autoregressive integrated moving average ARMA - autoregressive moving average

FARIMA - autoregressive fractionally integrated moving average

FBM - fractional Browning motion

FGN - fractional Gaussian noise

FTP - file transfer protocol

HTTP - hypertext transfer protocol

HTTPS - hypertext transfer protocol secure

MA - moving average

P2P - peer two peer

SSH - secure shell

TOR - the onion router