**Ву Вьет Тханг Исследование и разработка многоэтапной системы анализа трафика локальной беспроводной сети на основе методов машинного обучения и её применение в задаче обнаружения вторжений**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Ву Вьет Тханг

Введение

Глава 1. Анализ современных методов обнаружения вторжений в локальных беспроводных сетях

1.1. Устройство и архитектура локальных беспроводных сетей

1.2. Классификация вторжений в локальных беспроводных сетях

1.2.1. Атаки ключей

1.2.2. Атаки получения потока ключей

1.2.3. Атаки доступности

1.2.4. Атаки «человек посередине» (Man-in-the-Middle - MITM)

1.3. Анализ существующих методов и алгоритмов обнаружения сетевых

вторжений

1.4. Выводы по первой главе

Глава 2. Разработка моделей и алгоритмов обнаружения вторжений в локальных беспроводных сетях

2.1. Общий подход к анализу трафика ЛБС с целью выявления злонамеренных действий

2.2. Разработка алгоритма обнаружения аномалий FLDS

2.3. Разработка метода инкрементной кластеризации с частичным привлечением учителя на основе графов

2.4. Выводы по второй главе

Глава 3. Экспериментальная проверка разработанных алгоритмов обнаружения вторжений на основе машинного обучения

3.1. Данные для экспериментов

3.1.1. Набор данных CHAMELEON

3.1.2. Набор данных ADFA

3.1.3. Набор данных AWID

3.1.4. Набор данных UCI

3.2. Эксперименты по проверке алгоритма обнаружения аномалий FLDS

3.2.1. Эксперименты на наборе данных CHAMELEON

3.2.2. Эксперименты на наборе данных ADFA

3.2.3. Эксперименты на наборе данных AWID

3.3. Эксперименты по проверке инкрементного метода кластеризации с частичным обучением на основе графов

3.4. Выводы по третьей главе

Глава 4. Разработка многоэтапной системы обнаружения и классификации злонамеренных действий

4.1. Состав системы обнаружения и классификации злонамеренных действий

4.2. Описание работы системы обнаружения и классификации злонамеренных действий

4.2.1. Захват данных

4.2.2. Загрузка данных

4.2.3. Предварительная обработка

4.2.4. Классификатор

4.2.5. Инкрементная модель кластеризации (IncrementalSSGC, ISSGC)

4.2.6. Модель выявления аномалий (FLDS)

4.3. Интерфейс системы обнаружения и классификации злонамеренных

действий

4.4. Тестирование системы обнаружения и классификации злонамеренных действий

4.4.1. Тестирование разработанной системы на наборе данных AWID

4.4.2. Эффективность работы модуля FLDS

4.5. Выводы по четвертой главе

Заключение

Список сокращений

Список литературы

Приложение А

Приложение Б

Приложение В

Введение