**Демина Раиса Юрьевна Формирование обучающего множества для бинарной классификации объектов (на примере информационных технологий антивирусного анализа)**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Демина Раиса Юрьевна

ВВЕДЕНИЕ

ГЛАВА 1. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ БИНАРНОЙ КЛАССИФИКАЦИИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ АНТИВИРУСНОГО АНАЛИЗА

1.1 Роль бинарной классификации в информационных технологиях

1.2 Общая схема классификации

1.3 Факторы, влияющие на эффективность классификации

1.4 Влияние состава обучающего множества на верность распознавания

1.5 Задача увеличения верности классификации

1.6 Задача сокращения времени обучения

1.7 Взаимосвязь основных концептов предметной области

1.8 Выводы по первой главе. Постановка цели и задач исследования

ГЛАВА 2. МЕТОДИКА ФОРМИРОВАНИЯ ОБУЧАЮЩЕГО МНОЖЕСТВА

2.1 Анализ байтового состава файлов обучающего множества, обеспечивающего большую верность распознавания

2.2 Мера схожести объектов

2.3 Алгоритм отбора объектов в обучающее множество

2.4 Особенности программной реализации алгоритма расчета матрицы схожести

2.5 Экспериментальная проверка методики формирования ОМ

2.6 Выводы по второй главе

ГЛАВА 3. СОКРАЩЕНИЕ ВРЕМЕНИ ОБУЧЕНИЯ КЛАССИФИКАТОРА

3.1 Определение наиболее затратной по времени процедуры при обучении классификаторов

3.2 Сравнительный анализ возможных алгоритмических решений

3.3 Общий подход к модификации алгоритмов сортировки

3.4 Расширенный бинарный поиск

3.5 Особенности программной реализация алгоритма РБП

3.6 Экспериментальная проверка вычислительной эффективности предложенного алгоритма

3.7 Выводы по третьей главе

ГЛАВА 4. ВНЕДРЕНИЕ РЕЗУЛЬТАТОВ В ДЕЯТЕЛЬНОСТЬ АНТИВИРУСНОЙ КОМПАНИИ SECURITYSTRONGHOLD

4.1 Антивирусный пакет StrongholdAntimalware компании SecurityStronghold

4.2 Программный модуль «Формирование обучающего множества для задач статического эвристического анализа»

4.2.1 Общие сведения о работе системы

4.2.2 Функциональное назначение

4.2.3 Инсталляция и выполнение программного продукта

4.2.4 Руководство пользователя

4.3 Модуль «Расширенный бинарный поиск»

4.3.1 Общие сведения о работе системы

4.3.2 Функциональное назначение

4.3.3 Подключение библиотеки

4.4 Система сбора статистики

4.5 Анализ результатов внедрения

4.6 Выводы по четвертой главе

ЗАКЛЮЧЕНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СПИСОК ЛИТЕРАТУРЫ

Приложение А Результаты проверки различных обучающих множеств

Приложение Б Графики байтового распределения для «хорошего» ОМ

Приложение В Свидетельства о государственной регистрации программ для ЭВМ

Приложение Г Акты внедрения результатов диссертационного исследования