**Уфимский государственный авиационный технический университет**

**На правах рукописи**

104.2 0 0.9 04448 -

**НИКИТИН Андрей Павлович**

**МНОГОУРОВНЕВАЯ МНОГОАГЕНТНАЯ СИСТЕМА
ФИЛЬТРАЦИИ СПАМА В ОРГАНИЗАЦИИ**

Специальность: 05.13.19 - Методы и системы защиты информации, информаци-
онная безопасность

Диссертация

на соискание ученой степени кандидата технических наук

Научный руководитель:

доктор технических наук, профессор

Валеев С. С.

Уфа 2009

V

ОГЛАВЛЕНИЕ

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ 3

ВВЕДЕНИЕ 4

ГЛАВА 1. АНАЛИЗ ЗАДАЧИ АВТОМАТИЧЕСКОЙ ФИЛЬТРАЦИИ СООБЩЕНИЙ, КАК ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 11

1. Анализ понятия спама 11
2. Анализ признаков, классифицирующих спам-сообщения 12
3. Анализ основных угроз информационной безопасности, несущих

различными видами спам-сообщений 14

1. Анализ спам-сообщений коммерческого характера 14
2. Анализ спам-сообщений некоммерческого характера 15
3. Анализ мошеннические и фишинговые спам-сообщений 15
4. Анализ ложных спам-сообщений и цепных писем 16
5. Анализ спам-сообщений "работа Джо" 16
6. Анализ спам-сообщений, содержащих вредоносные программы 16
7. Анализ отрицательная квитанция 17
8. Анализ экономического ущерба спам-сообщений 17
9. Анализ основных методов борьбы со спамом 19
10. Анализ законодательных методов борьбы со спамом 19
11. анализ организационных методов борьбы со спамом 26
12. Анализ практических действий борьбы со спамом 28
13. Анализ технических методов защиты от спама 31
14. Концепция построения системы фильтрации спама 49

Выводы по первой главе 50

ГЛАВА 2. РАЗРАБОТКА АРХИТЕКТУРЫ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ФИЛЬТРАЦИИ СПАМ-СООБЩЕНИЙ 51

1. Рассмотрение задачи классификации электронной информации,

передаваемой по каналам связи, на примере фильтрации спама 51

1. Анализ нарушения спамом безопасности информации 52
2. Разработка архитектуры системы фильтрации спам-сообщений 55
3. Разработка алгоритма заполнения БЗ системы фильтрации 67
4. Разработка алгоритма фильтрации документа 69

Выводы по второй главе 76

ГЛАВА 3. РАЗРАБОТКА АЛГОРИТМЫ КЛАССИФИКАЦИИ СООБЩЕНИЙ НА ОСНОВЕ АГЕНТА-КЛАССИФИКАТОРА 77

1. Постановка задача представления исходного сообщения в виде

семантического графа 77

1. Разработка модели сообщения на основе упрощенного семантического графа

 80

1. Разработка статистической семантической модели сообщений 80
2. Решение задачи обоснования применения линейной ассоциативной сети 81
3. Разработка нейросетевого классификатора 86

Выводы по третьей главе 90

ГЛАВА 4. РЕАЛИЗАЦИИ СИСТЕМЫ БОРЬБЫ СО СПАМОМ С ПОМОЩЬЮ МНОГОАГЕНТНОЙ ТЕХНОЛОГИИ 91

1. Этапы проектирования многоагентной системы борьбы со спамом 92
2. Архитектура многоагентной системы борьбы со спамом 94
3. Сценарии работы, функции и роли агентов системы 96
4. Обеспечение общения агентов 97
5. Архитектура отдельного агента 98
6. Программная реализация прототипа системы 100

Выводы по четвертой главе 104

ЗАКЛЮЧЕНИЕ 105

ЛИТЕРАТУРА 106

Приложение А 117

Приложение Б 121

Приложение В 130

Приложение Г 133

ЗАКЛЮЧЕНИЕ

В работе поставлена и решена задача разработки системы фильтрации спама в организации. При решении данной задачи получены следующие результа­ты и выводы:

1. Разработана концепция построения автоматизированной иерархической сис­темы противодействия вредоносному воздействию спам-рассылок на информа­цию, обрабатываемую в системах электронной почты, заключающаяся в много­уровневой фильтрации спама с использование баз знаний, различных по полноте. Реализация разработанной концепции в организации позволяет повысить точность классификации электронных сообщений на различных уровнях иерархии системы фильтрации и обеспечить целостность и доступность информации в рамках при­нятой в организации политики безопасности.
2. Разработана иерархическая архитектура системы защиты электронной почтовой информации в классе распределенных систем обработки информации на основе многоагентного подхода, которая позволяет обеспечить масштабируемость и свойство самоорганизации для гибкой реализации политики безопасности, при­нятой в организации.
3. Разработан эффективный алгоритм классификации электронных сооб­щений на основе когнитивного подхода и нейросетевого классификатора, что по­зволяет решать задачу классификации поступающих электронных сообщений на различных уровнях иерархии организации с частичным учетом семантики сооб­щения.
4. Разработана методика проектирования многоагентной системы проти­водействия распространению спама в организации с применением однотипного нейросетевого классификатора на всех иерархических уровнях обработки инфор­мации, использование которой позволяет реализовать элементы предложенной автоматизированной системы фильтрации спама в организации в виде программ­ных модулей. Как показали результаты моделирования функционирования разра­ботанной системы, уровень ошибок первого и второго рода снизилось на 5-10%.