На правах рукописи

НИКИТИН Андрей Павлович

МНОГОУРОВНЕВАЯ МНОГОАГЕНТНАЯ СИСТЕМА ФИЛЬТРАЦИИ СПАМА В ОРГАНИЗАЦИИ

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Уфа 2009

Работа выполнена
на кафедре вычислительной техники и защиты информации
Уфимского государственного авиационного технического университета

Научный руководитель	д-р техн. наук, проф. **Валеев Сагит Сабитович**
Официальные оппоненты	д-р. техн. наук, проф. **Аралбаев Ташбулат Захарович**
	канд. техн. наук, доц. **Дуленко Вячеслав Алексеевич**
Ведущая организация	Информационный центр Министерства внутренних дел по Республике Башкортостан

Защита состоится 20 февраля 2009 г. в ___ часов
на заседании диссертационного совета Д-212.288.07
при Уфимском государственном авиационном техническом университете
по адресу: 450000, Уфа-центр, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета.
Автореферат разослан 19 января 2009 г.

Ученый секретарь
диссертационного совета
д-р техн. наук, проф. **С. С. Валеев**

Общая характеристика работы

Актуальность темы

Основной задачей исследований в области защиты информации является совершенствование известных методов и разработка новых методов, алгоритмов обеспечения безопасности информации в процессе её сбора, хранения, обработки, передачи и распространения. Одним из направлений исследований в этой области является разработка методов и алгоритмов фильтрации спама. В Правилах оказания телематических услуг связи (Постановление Правительства Российской Федерации от 10.08.2007 № 575) дается определение спама, как телематического электронного сообщения, предназначенного неопределенному кругу лиц и доставленное абоненту или пользователю без их предварительного согласия. Также отмечается, что оператор связи должен принимать меры для воспрепятствования распространению спама. Избыточные незатребованные электронные письма нарушают доступность информационных ресурсов, необходимых пользователям, поскольку потребляют значительные ресурсы канала входящей связи, а также могут стать причиной нарушения целостности информации в случае утери сообщения при фильтрации сообщений человеком, или программой фильтрации. Вместе со спамом могут рассылаться вредоносные программы, способные привести к полному или частичному уничтожению информации или её искажению. Ряд вредоносных программ может быть использован для кражи персональных данных: номеров кредитных карт частных пользователей, имён пользователей и паролей для доступа к системам удалённого управления банковскими счетами организаций. Кроме того, конфиденциальные данные могут быть случайно или преднамеренно отправлены по электронной почте. В зависимости от принятой в организации политики безопасности, необходимо контролировать не только входящий, но и исходящий трафик. Задача поиска сведений, составляющих государственную или коммерческую тайну, в исходящем потоке электронной почты аналогична задача фильтрации спама. В этом случае для обучения системы могут использоваться не только незатребованные электронные письма, а конфиденциальные документы, представленные в электронном виде. Не смотря на использование различных систем фильтрации электронных сообщений, доля спама в общем почтовом трафике все еще достаточно высока. По мнению экспертов компании Cisco, в 2009 году объём спама впервые превысит отметку 90% почтового трафика.

Вопросам противодействия спаму посвящены исследования И. С. Ашманова, А. Шварца и др. В основном, это фильтры, построенные на байесовском подходе, что, как известно, не позволяет учитывать семантику электронных сообщений. При разработке систем фильтрации входящих сообщений недостаточно полно используется системный подход и современные технологии искусственного интеллекта для решения задачи классификации. Тем самым, задача разработки эффективных методов и алгоритмов фильтрации спама в организации является актуальной.

Объект исследования – процесс обеспечения фильтрации спама в организации.

Предмет исследования – методы и алгоритмы фильтрации спама в организации на основе технологий искусственного интеллекта.

Целью работы является повышение эффективности системы фильтрации спама в организации.

Для достижения данной цели поставлены следующие **задачи**:

1. Разработка концепции построения системы фильтрации спама в организации.
2. Разработка многоагентной архитектуры иерархической системы фильтрации спама в организации.
3. Разработка эффективного метода и алгоритма классификации электронных сообщений с учётом семантики сообщения.
4. Оценка эффективности предложенных подходов к фильтрации спама в организации.

Методы исследования

При работе над диссертацией использовались: методология защиты информации, методы системного анализа, теория множеств, теория вероятности, теория моделирования дискретных систем, теория нейронных сетей, теория многоагентных систем. Для оценки эффективности предлагаемых решений использовались методы математического и имитационного моделирования.

Основные научные результаты, выносимые на защиту:

1. Концепция построения автоматизированной системы фильтрации спама в организации.
2. Архитектура многоуровневой многоагентной системы противодействия распространению спама в организации.
3. Эффективный алгоритм классификации электронных сообщений на основе нейросетевого классификатора.
4. Прототип многоагентной системы противодействия распространения спама в организации.

Научная новизна работы

1. Предложена новая концепция построения автоматизированной многоуровневой многоагентной системы противодействия вредоносному воздействию спам-рассылок на информацию, хранящуюся и обрабатываемую в системах электронной почты, основанная на многоуровневой фильтрации спама, что позволяет повысить доступность и обеспечить целостность информации, обрабатываемой в системах электронной почты на различных уровнях иерархии организации с учетом принятой политики безопасности.
2. Разработана архитектура иерархической многоагентной системы защиты информации, обрабатываемой электронными почтовыми системами, от вредоносного воздействия спама, позволяющая строить полную и достоверную базу знаний, отражающую области интересов пользователей системы в рамках иерархии организации с учетом принятой политики безопасности.
3. Предложен эффективный метод и алгоритм классификации электрон-

ных сообщений на основе когнитивного подхода и нейросетевого классификатора, позволяющий посредством использования базы знаний эффективно решать задачу классификации поступающих электронных сообщений на различных уровнях иерархии организации.

4. Разработан программный прототип многоагентной системы противодействия распространению спама в организации, позволяющий оценить эффективность предложенного метода и алгоритма.

Практическая ценность полученных результатов

Практическая значимость полученных результатов заключается в повышении эффективности функционирования системы противодействия распространению спама в локальной вычислительной сети организации.

Использование предложенного метода классификации электронных сообщений позволяет учесть в процессе анализа семантическую компоненту сообщения, тем самым снизить уровень ошибочной классификации на 5-10%.

Результаты работы внедрены в филиале "Уфимская городская телефонная сеть" ОАО "БашИнформСвязь", Уфимском филиале ОАО "Вымпелком", ОАО МТУ "Кристал", г.Уфа, Уфимском филиале ОАО "Уралмонтажавтоматика".

Апробация работы

Основные научные и практические результаты диссертационной работы докладывались и обсуждались на следующих конференциях:

- 7, 9, 10 Международных научных семинарах «Компьютерные науки и информационные технологии» (CSIT), Уфа, 2005, 2007; Анталия, Турция 2008;
- XXXII Международной молодёжной научной конференции «Гагаринские чтения», Москва, 2006;
- VIII Всероссийской молодёжной научной конференции «Королёвские чтения», Самара, 2005;
- Международной молодёжной научной конференции «Туполевские чтения», Казань, 2005;
- VIII Международной научно-технической конференции «Проблемы техники и технологии телекоммуникации», Уфа, 2007;
- I Международной научно-технической конференции «Актуальные проблемы безопасности информационных технологий», Красноярск, 2007.

Публикации

Результаты диссертационной работы отражены в 16 публикациях: в 9 научных статьях, в том числе 1 статья в рецензируемом журнале из списка периодических изданий, рекомендованных ВАК, в 7 тезисах докладов в материалах международных и российских конференций.

Структура и объем работы

Диссертационная работа состоит из введения, четырех глав, заключе-

ния, приложений, библиографического списка и изложена на 135 страницах машинописного текста. Библиографический список включает 138 наименований литературы.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы исследований в области повышения защищённости информации, получаемой, хранящейся, обрабатываемой и передаваемой в системах электронной почты. Формулируется цель работы и решаемые в ней задачи, обсуждается научная новизна и практическая ценность выносимых на защиту результатов.

В первой главе выполнен анализ различных видов спама с точки зрения их угроз защищённости информации, а также рассмотрены достоинства и недостатки известных подходов к противодействию этим угрозам. Делается вывод о необходимости разработки новой архитектуры системы противодействия распространению спама, методов и алгоритмов фильтрации, позволяющих более эффективно, по сравнению с существующими системами, обеспечивать фильтрацию спама.

Во второй главе рассматривается задача разработки концепции 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 и достоверности. Выполнен анализ основных потоков информации в системе обработки сообщений (рис. 1).

Рисунок 1 – Информационные потоки в системе обработки электронных почтовых сообщений

На рис.1 использованы следующие обозначения: H_I – полезные сообщения, поступающие на вход фильтра входящих сообщений; S_I – спам, поступающий на вход фильтра входящих сообщений; H_I' – полезные электронные сообщения, поступающие с выхода фильтра входящих сообщений; S_I' – спам, поступающий с выхода фильтра входящих сообщений; H_O – полезные электронные сообщения, поступающие на вход фильтра исходящих сообщений; S_O – спам, поступающий на вход фильтра исходящих сообщений; C_O – сообщения, содержащие конфиденциальные сведения, поступающие на вход фильтра исходящих сообщений; H_O' – полезные электронные сообщение, поступающие с выхода фильтра исходящих сообщений; C_O' – сообщения, со-

держащие конфиденциальные сведения, поступающие с выхода фильтра исходящих сообщений; S_O' – спам, поступающий с выхода фильтра исходящих сообщений.

Проанализировано влияние спама S на доступность информации (рис. 2). Показано, что если в некоторый момент времени t_0 объём поступающих в электронные почтовые ящики организации полезных H и спам-сообщений S превысит пропускную способность канала связи PB, соединяющего организацию с Интернет-провайдером, то некоторая часть электронных сообщений L, в том числе и полезные, будет получено с опозданием, и пользователи не смогут своевременно получить доступ к сообщениям. Тем самым, возникает очередь из запоздавших сообщений, что приводит к еще большей временной задержке при доступе к требуемой информации. Если в момент времени t_1 суммарный объём поступающих полезных сообщений и спама станет меньше пропускной способности канала связи организации с Интернет-провайдером, то пользователи в дальнейшем смогут оперативно получать доступ к сообщениям.

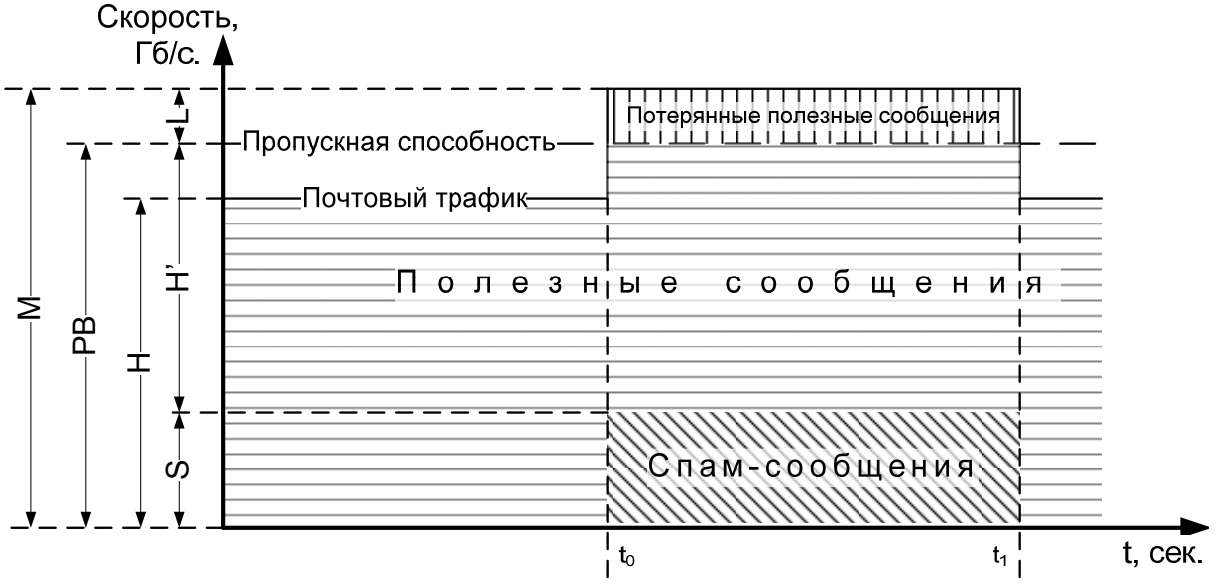

Рисунок 2 – Нарушение доступности информации

Нарушение спамом доступности информации в формализованном виде может быть представлено в виде следующих условий:

$$\text{Если } t \in [t_0; t_1], \text{ то } S > 0;$$

$$\text{Если } S > (PB - H), \text{ то } M > PB \Rightarrow L > 0, H - H' \neq \varnothing;$$

где

$$M = H + S,$$

$$H \cap S = \varnothing,$$

$$L = M - PB.$$

Спам также может быть причиной нарушения целостности информации (рис. 3).

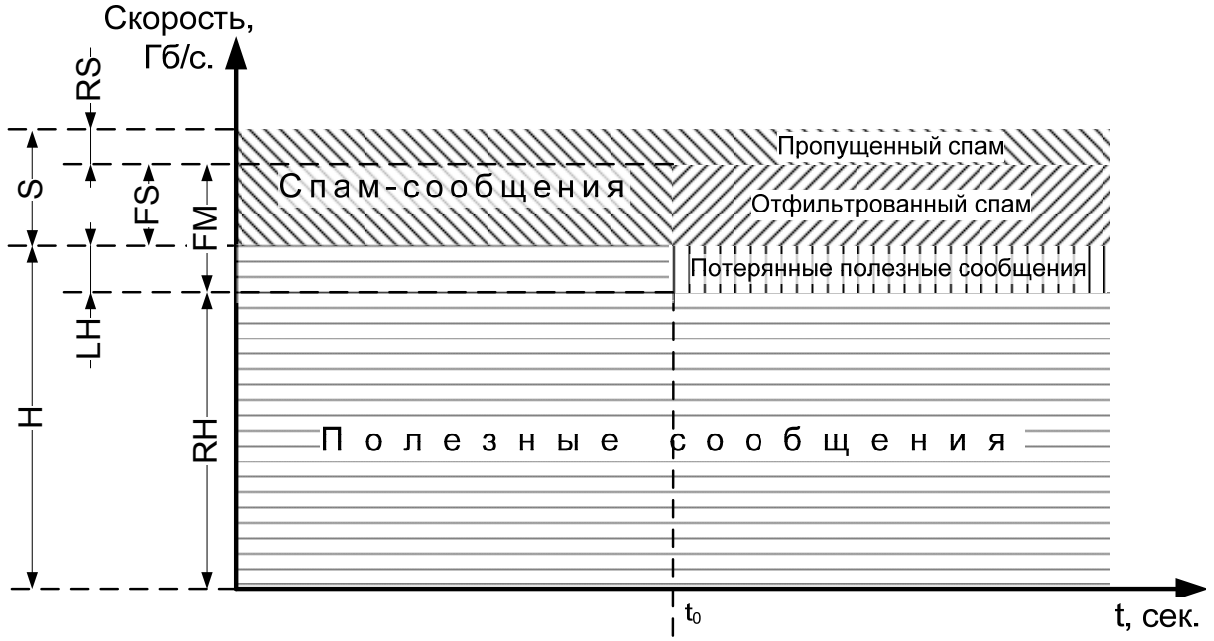

Рисунок 3 – Нарушение целостности информации

Предположим, что в некоторый момент времени t_0 пользователи, осуществляющие ручную классификацию электронных сообщений, ошибочно отфильтруют часть полезных электронных писем *LH*, а также ошибочно пропустят часть спама *RS*. К аналогичным последствиям может привести применение неэффективных средств автоматической фильтрации спама.

Нарушение спамом целостности информации в формализованном виде может быть представлено с помощью следующих соотношений:

$$H = RH + LH,$$
$$S = FS + RS,$$
$$FM = FS + LH,$$
$$M = H + S,$$
$$H \cap S = \varnothing,$$
$$M' = RH + RS,$$
$$M' = M - FM,$$

где *FM* – отфильтрованные электронные сообщения; *FS* – отфильтрованные электронные спам-сообщения; *RH* – количество полезных электронных сообщений, оставшихся после фильтрации; *M′* – количество всех входящих электронных сообщений после фильтрации.

В работе выполнен сравнительный анализ достоинств и недостатков спам-фильтров, выполняющих централизованную и распределённую фильтрацию.

Показано, что достоинствами фильтров, осуществляющих централизованную фильтрацию, являются возможность быстрого обнаружения и отсечения массовых рассылок одинаковых сообщений, а также возможность оперативной адаптации к вновь разработанным методам обхода известных способов фильтрации, используемых в спам-фильтрах. К недостаткам фильтров, осуществляющих централизованную фильтрацию, отнесена невозможность

учёта интересов конкретного пользователя, что приводит к принятию ошибочного решения о пропуске спама или блокировании полезного письма.

В случае распределенной фильтрации учитывается область интересов пользователя, но не используется опыт других пользователей организации.

Рассмотрены три основных возможных способа формирования базы знаний полезных сообщений и спама для фильтров, осуществляющих централизованную фильтрацию.

В первом случае для формирования базы знаний используются сообщения, классифицированные всеми пользователями. В этом случае уровень ошибок первого рода повышается, а уровень ошибок второго рода снижается. Данный способ формирования баз знаний можно представить следующим образом:

$$B = b_1 \cap b_2 \cap \ldots \cap b_n = \bigcap_{k=1}^{n} b_k .$$

где B – база знаний организации;

b_k – база знаний k-го пользователя почтовой системы;

n – количество пользователей системы электронной почты.

Рассматриваемый способ формирования базы знаний используется достаточно широко.

Во втором случае решение включать сообщение, классифицированное пользователем, в свою базу знаний система принимает на основе рейтинга пользователя, который, в свою очередь, зависит от того, сколько, с точки зрения других пользователей, данный пользователь сообщений пометил верно, и сколько неверно. В этом случае уровень ошибок первого рода повышается, а уровень ошибок второго рода понижается. Данный способ формирования баз знаний можно представить следующим образом:

$$B = (b_1 \cap b_2) \cup (b_1 \cap b_3) \cup \ldots \cup (b_1 \cap b_n) \cup (b_2 \cap b_3) \cup \ldots \cup (b_2 \cap b_n) \cup \ldots \cup (b_{n-1} \cap b_n) = \bigcup_{k=1,\, j=1}^{k=n,\, j=n,\, k \neq j} (b_k \cap b_j).$$

В третьем случае для формирования базы знаний используются сообщения, помеченные как спам хотя бы одним пользователем. В этом случае уровень ошибок первого рода понижается, а уровень ошибок второго рода может повыситься. Данный способ формирования баз знаний можно представить следующим образом:

$$B = b_1 \cup b_2 \cup \ldots \cup b_n = \bigcup_{k=1}^{n} b_k .$$

В работе предлагается процедура формирования базы знаний интеллектуальной системы борьбы со спамом, объединяющей в себе все преимущества серверных и персональных фильтров. Для этого каждый пользователь системы вручную классифицирует все сообщения с помощью почтовых клиентов. Затем система фильтрации выделяет леммы, принадлежащие каждому

классу сообщений, и передаёт их на уровень отдела, где все списки объединяются, поскольку предполагается, что области профессиональных интересов сотрудников одного отдела совпадают. На последнем этапе процедуры формирования базы знаний системы фильтрации используют только сообщения, одинаково классифицированные всеми отделами, что связано с различием области интересов отделов в организации. При такой схеме формирования базы знаний достигается высокая эффективность функционирования предлагаемой системы фильтрации спама, потому что при создании базы знаний уровня отдела увеличивается обучающая выборка, а при создании базы знаний уровня организации сохраняется низкий уровень ошибок вследствие исключения из обучающей выборки случайных сообщений.

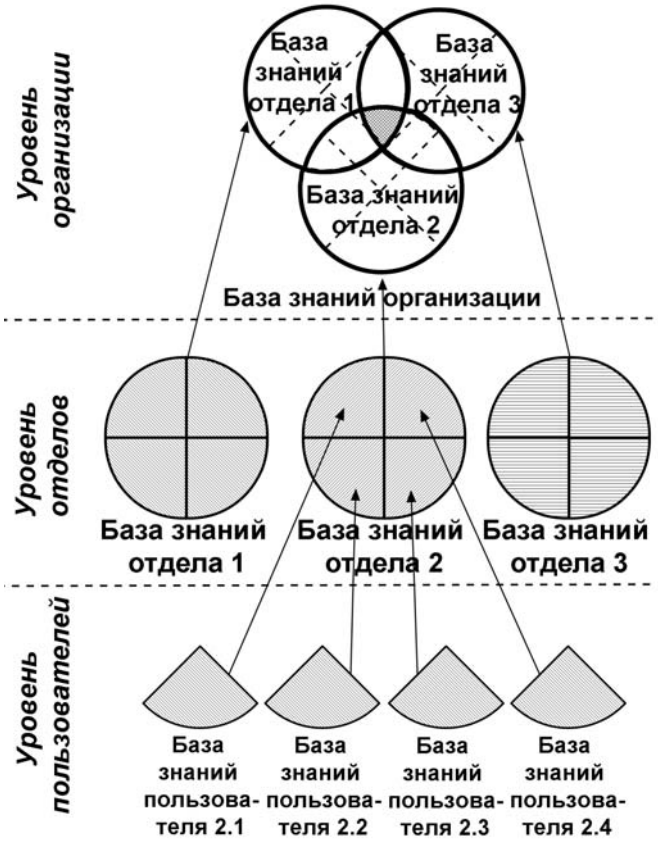

Рисунок 4 – Иерархическая процедура формирования базы знаний многоуровневой системы фильтрации спама

Данный способ формирования баз знаний можно представить следующим образом:

$$B_1 = b_{11} \cup b_{12} \cup \ldots \cup b_{1n} = \bigcup_{k=1}^{n} b_{1k} \ , \qquad (1)$$

$$Base = B_1 \cap B_2 \cap \ldots \cap B_p = \bigcap_{k=1}^{p} B_k \ . \qquad (2)$$

Учитывая (1) и (2) можем получить описание процедуры формирования базы знаний:

$$Base = \left(b_{11} \cup b_{12} \cup ... \cup b_{1n}\right) \cap \left(b_{21} \cup b_{22} \cup ... \cup b_{2m}\right) \cap ... \cap \left(b_{p1} \cup b_{p2} \cup ... \cup b_{po}\right) =$$

$$= \bigcap_{k=1}^{p} \left(\bigcup_{j=1, j \neq k}^{r} b_{k,j} \right).$$

где p – количество отделов в организации;

n – количество сотрудников в первом отделе организации;

m – количество сотрудников во втором отделе организации;

l – количество сотрудников в p-ом отделе организации;

b_{pl} – база знаний, сформированная l-ым сотрудником p-го отдела;

B_k – база знаний k-го отдела организации;

$Base$ – база знаний сообщений организации.

Схема информационных потоков в предлагаемой системе противодействия распространению спама представлена на рис. 5.

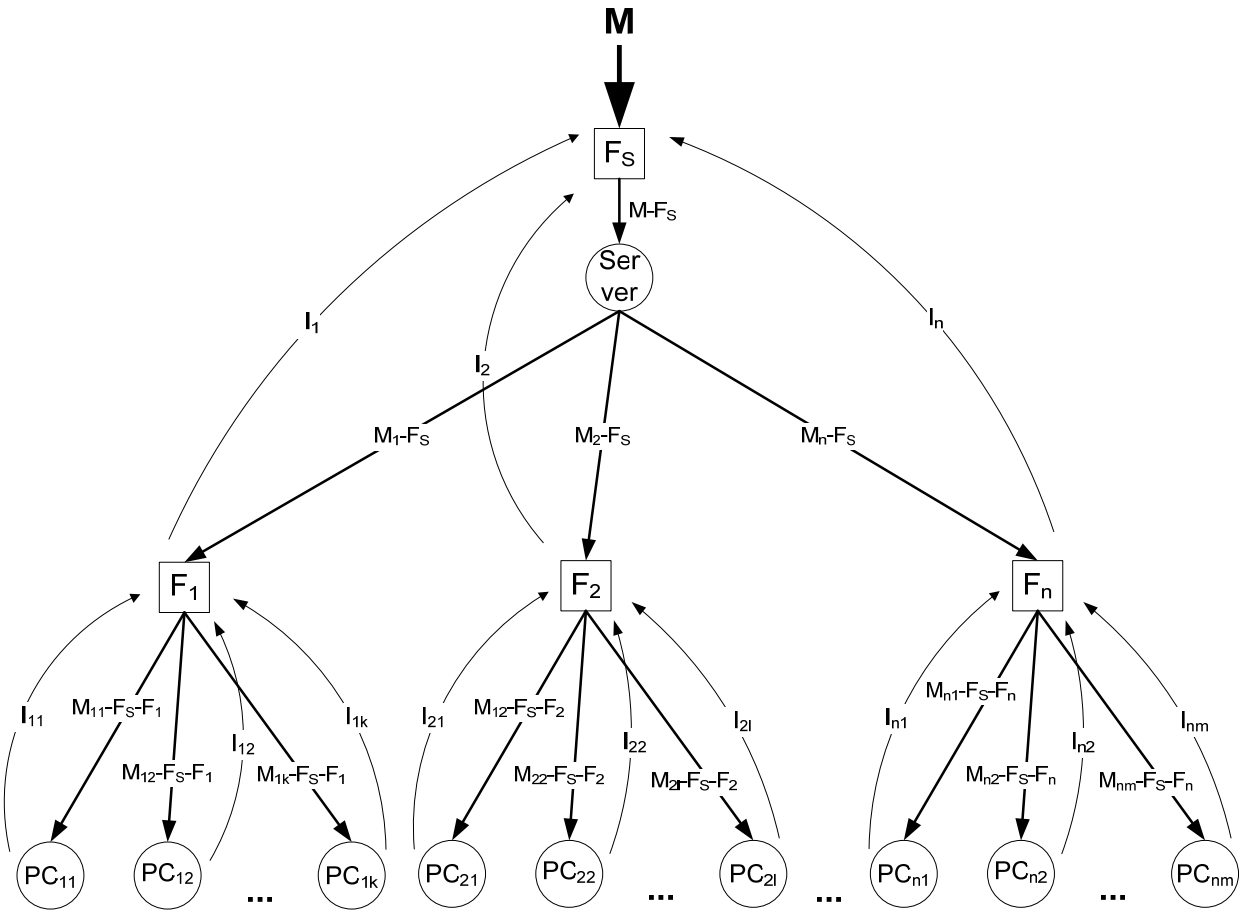

Рисунок 5 – Информационные потоки в многоуровневой системе борьбы со спамом

Информационные потоки в многоуровневой системе противодействия спаму могут быть представлены следующим образом:

$$M - F_S = \left(M_1 - F_s\right) \cup \left(M_2 - F_s\right) \cup ... \cup \left(M_n - F_s\right) = \bigcup_{k=1}^{n} \left(M_k - F_S\right), \qquad (3)$$

$$M_k - F_S = \left(M_{k,1} - F_S - F_k\right) \cup \left(M_{k,2} - F_S - F_k\right) \cup \ldots \cup \left(M_{k,m} - F_S - F_k\right) = \\ = \bigcup_{j=1}^{m} \left(M_{k,j} - F_S - F_k\right), \quad (4)$$

С учетом (3) и (4) получаем выражение для входящих потоков электронных сообщений:

$$M - F_S = \bigcup_{k=1}^{n} \left(\bigcup_{j=1}^{m} \left(M_{k,j} - F_S - F_k\right) \right).$$

Далее запишем выражение для потока информации, содержащей обучающие выборки:

$$I = I_1 \cap I_2 \cap \ldots \cap I_m = \bigcap_{k=1}^{n} I_k \ , \quad (5)$$

$$I_k = I_{k,1} \cup I_{k,2} \cup \ldots \cup I_{k,m} = \bigcup_{j=1}^{m} I_{k,j} \ . \quad (6)$$

С учетом (5) и (6) получаем выражение для информационных потоков, используемых при формировании баз знаний системы противодействия распространению спама:

$$I = \bigcap_{k=1}^{n} \left(\bigcup_{j=1, j \neq k}^{m} I_{k,j} \right),$$

где M – поток всех входящих электронных писем; *Server* – почтовый сервер; F_S –классификатор, функционирующий на сервере организации; PC_k – персональный компьютер k-го пользователя; F_n – классификатор для n-го отдела; M_n–F_S – поток входящих электронных писем, предназначенных пользователям n-го отдела и отфильтрованных классификатором F_S; M_{nm}–F_S–F_n – поток входящих электронных писем, предназначенных m-му пользователям из n-го отдела и отфильтрованных предварительно классификатором F_S, а потом фильтром n-го подразделения F_n; I_{nm} – сообщения, вручную классифицированные m-м пользователем n-го отдела и предназначенные для обучения классификатора n-го отдела F_n; I_n – сообщения, вручную классифицированные всеми пользователем n-го отдела и предназначенные для обучения классификатора F_s.

Обучение системы состоит из трёх основных этапов: автоматической классификации поступившего сообщения, ручной классификации сообщения и обучения системы. Если после автоматической классификации уровень уверенности системы о классе сообщения превышает некоторый порог, то сообщение используется для обучения системы фильтрации спама. Если же система не уверенна в правильности оценки, то она перед обучением на данном сообщении, ожидает, пока пользователь вручную не укажет класс сообщения.

Показано, что для повышения эффективности решения задачи классификации сообщений необходимо разработать новый алгоритм классификации электронных сообщений, учитывающий не только частоту встречаемо-

сти слов, как в байесовском фильтрации, но и семантику сообщений.

В третьей главе рассматривается решение задачи разработки алгоритма классификации входного и выходного потока электронной корреспонденции на основе применения парадигмы обучаемых нейронных сетей.

На основе анализа характеристик классических систем автоматического понимания текста, делается вывод о том, что их применение в системах фильтрации нецелесообразно из-за высокой вычислительной нагрузки на компьютер пользователя, большого объема предварительной обработки электронных сообщений, большого объема служебных данных, сложности реализации.

С учетом специфики задачи фильтрации электронных сообщений, предлагается в качестве упрощенной модели текстового фрагмента использовать представление минимальной семантической единицы – предложения, в виде семантического графа. Данная модель позволяет быстро построить простую структуру, частично отражающую семантику текстового сообщения.

На первом этапе анализа входящего сообщения из него формируется множество $F = \{f_k\}$, где f_k – заданная для системы фильтрации минимальная семантическая структура, i=1…m, при этом из структуры удаляются избыточные элементы. В результате структура f_k может быть представлена в виде семантического графа S_k, определяющего связь L лексем V в f_k.

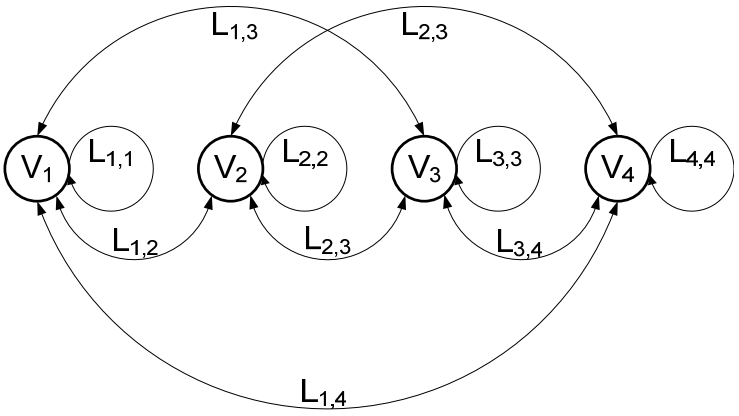

Рисунок 6 – Упрощённый семантический граф сообщения

При оценке силы связи между лексемами учитывается лексикографический порядок в f_k. После обработки всего сообщения получаем семантический граф сообщения $G =< S,V >= \bigcup_1^n s_k$, представляющий собой упрощенную семантическую модель сообщения, где S – множество вершин, содержащее лексемы сообщения, прошедшие предварительную фильтрацию на основе заданного словаря; V – множество ребер, весовые значения которых определяют силу связи лексем в f_k. Далее граф G представляется матрицей смежности Z, представляющая собой семантическую матрицу. Матрица Z имеет четко выраженную структуру, что позволяет использовать ее для повышения эффективности процедуры классификации сообщения при решении задачи

фильтрации. На следующем этапе фильтрации выполняется понижение размерности матрицы Z – сжатие образа, из нее удаляются столбцы и строки, содержащие значения элементов ниже заданного порога λ.

Далее, с учетом векторов атрибутов сообщений на базе графа G строятся две обобщенные семантические матрицы для спама Z_s и для полезных сообщений Z_e. В результате задача классификации новых сообщений сводится к построению бинарного классификатора N, определяющего принадлежность сообщения к одной из представленных семантическими матрицами категорий.

В качестве классификатора предлагается использовать линейный нейросетевой ассоциатор вида $y = w^T x$, где x – входной вектор (элементы вектора составлены из элементов семантической матрицы фильтруемого сообщения), w – вектор весов классификатора. Обучение ассоциатора выполняется на основе правила обучения Хебба. Архитектура разработанной системы многоуровневой фильтрации спама позволяет реализовать способность системы к самообучению. На рис. 7 представлено изменение доли спама и легитимных сообщений в процессе обучения системы фильтрации.

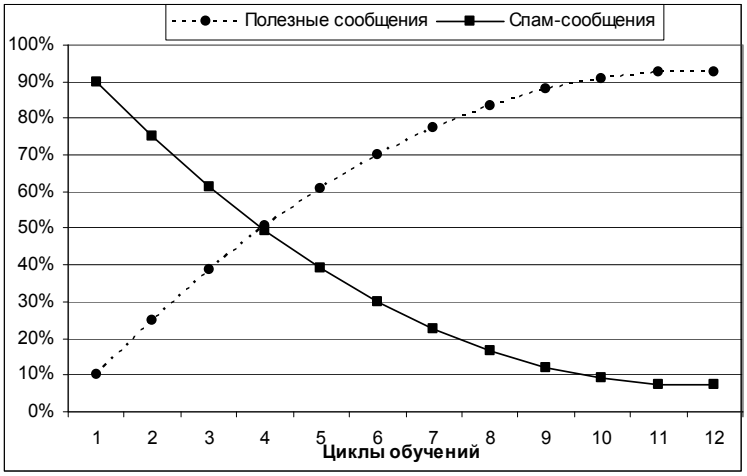

Рисунок 7 – Изменение доли спама и полезных сообщений

В четвёртой главе описывается реализация многоуровневой системы борьбы со спамом на основе многоагентного подхода.

Предлагаемая система борьбы со спамом является распределенной, каждый системный компонент, управляющий почтовыми фильтрами, имеет лишь информацию, необходимую для решения задачи, и может влиять на решение задачи только на своем участке. Это обусловлено спецификой сложной, гетерогенной, распределенной в пространстве и непостоянной по структуре системы, которой является информационная система современного предприятия. Ключевым моментом, определяющим выбор многоагентной технологии, является необходимость обеспечения автономности системы фильтрации спама. Более того, изменение структуры информационной системы предприятия, добавление или удаление какого-либо пользовательской

рабочей станции или даже сервера отдельного отдела, при использовании многоагентной технологии позволяет учитывать эти изменения. Также это позволяет повысить эффективность работы администратора сети.

Агенты могут работать в рамках следующие основные сценарии:

– работа с электронными сообщениями, включающая в себя управление почтовыми фильтрами и самообучение;

– обмен сообщениями в случае необходимости изменения параметров настроек системы фильтрации, при этом изменения могут выполнятся администратором безопасности сети или системным администратором в зависимости от принятой в организации политики безопасности;

– наблюдение за изменениями в структуре потоков электронной почты и реагирование на них, в том числе адаптация структуры многоагентной системы фильтрации спама.

Разработанная многоагентная система фильтрации спама состоит из трех уровней: верхнего, промежуточного и нижнеого. На верхнем уровне располагается основной в организации почтовый сервер, на промежуточном уровне находятся почтовые сервера отделов, нижний уровень занимают почтовые клиенты, установленные на рабочих станциях пользователей.

Роли агентов зависят от места, занимаемого ими в этой иерархии. В разные моменты времени один и тот же агент может исполнять различные роли, в зависимости от сложившийся ситуации и архитектуры локальной вычислительной сети. Функции каждого агента определяются его ролью в данный момент времени:

– для агентов всех уровней это управление почтовыми фильтрами на своем уровне;

– для агентов нижнего и промежуточного уровней это отправка обучающих выборок агенту более высокого уровня;

– для агентов верхнего и промежуточного уровней это прием обучающих выборок от агентов предыдущего уровня, формирование базы знаний, а также самообучение;

– для агентов верхнего и промежуточного уровней это мониторинг структуры информационной системы предприятия на своем уровне, реагирование на изменения в этой структуре в случае появления или удаления рабочих станций и серверов электронной почты;

– распространение служебных сообщений с верхнего уровня на нижние уровни, например, изменений параметров настроек.

Взаимодействие между агентами может выполняться в двух направлениях:

- "снизу вверх" – от агентов нижнего уровня к агентам верхнего уровня. В этом случае выполняется обучение системы борьбы со спамом;

- "сверху вниз" – от агентов на верхнем уровне к агентам на нижнем уровне. Это используется для обеспечения централизованного управления параметрами настроек системы фильтрации спам-сообщений.

Система служебных сообщений в многоагентной системе борьбы со

спамом имеет следующую структуру:

– сообщения с обучающими выборками для базы знаний;

– сообщения, регулирующие параметры настройки в многоагентной системе;

– запросы об изменениях информационной структуры предприятия, связанные с добавлением или удалением серверов или рабочих станций, на которых выполняется обработка электронной корреспонденции.

Прототип предлагаемой системы реализован на платформе JADE (Java Agent DEvelopment Framework). Особенностью данной платформы является возможность реализации поддержка распределенной обработки информации на базе многоагентной технологии, поддержка архитектуры P2P, использование языка ACL (Agent Communication Language), удовлетворяющий требованиям FIPA (Foundation for Intelligent Physical Agents)

На рисунке 8 приведены результаты сравнения эффективности разработанной системы с байсовским фильтром.

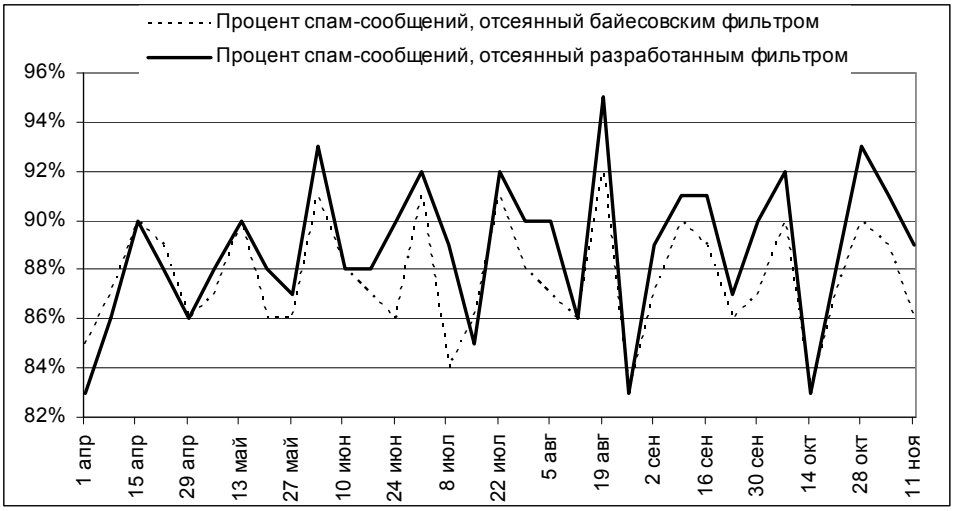

Рисунок 8 – Сравнение эффективности работы фильтров

В заключении приводятся основные научные результаты, полученные в ходе выполненных исследований, а также представлены выводы по работе.

ОСНОВНЫЕ 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%.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемом журнале из списка ВАК:

1. Многоуровневая система фильтрации спама на основе технологий искусственного интеллекта / Валеев С.С., Никитин А.П. // Вестник УГАТУ, Т. 11 № 1 (28), 2008. – С. 215-219.

Другие публикации:

2. Многоагентная антиспам система / Никитин А.П. // Компьютерные науки и информационные технологии: Труды 7-го Международного семинара (CSIT’2005), Т. 2, Уфа: Изд-во Уфимс. гос. авиац. техн. ун-та, 2005. – С. 227-229 (на англ. языке).

3. Система классификации электронных сообщений / Никитин А.П. // VIII Королёвские чтения: материалы всероссийской молодёжной научной конференции, Самара, 4-6 октября 2005 г.:– Самара: Издательство Самарского государственного аэрокосмического университета имени академика С.П. Королёва, 2005, – С. 90.

4. Модульная система классификации электронных сообщений / Никитин А.П. // Туполевские чтения: международная молодёжная научная конференция, посвящённая 1000-летию города Казани, 10-11 ноября 2005 г.: Материалы конференции. Том III. –Казань: Изд-во Казан. гос. техн. ун-та, 2005. – С. 95-96.

5. Система классификации электронных сообщений. / Никитин А.П. // XXXII Гагаринские чтения. Научные труды Международной молодёжной научной конференции в 8 томах. М.: МАТИ, 2006. Т. 4 – Стр. 26-27.

6. Система классификации электронных сообщений / Никитин А.П. // // Интеллектуальные системы обработки информации и управления: Материалы 2-й региональной зимней школы-семинара аспирантов и молодых ученых. - Т.1. - Уфа: УГАТУ, 2007. - С. 55-56.

7. Интеллектуальная система фильтрации сообщений / Никитин А.П., Валеев С.С. // Проблемы техники и технологии телекоммуникации. Материалы Восьмой международной научно-технической конференции, 26-28 ноября 2007 г. Уфимск. гос. авиац. техн. ун-т. –Уфа, 2007. –С. 246-247.

8. Интеллектуальная система автоматической классификации информации / Никитин А.П. // Мавлютовские чтения: Материалы Всероссийской молодежной научной конференции, посвященной 75-летию УГАТУ. Т. 3. Уфимск. гос. авиац. техн. ун-т, –Уфа, 2007. –С. 18-19.

9. Система интеллектуальной фильтрации спама / Никитин А.П. // Актуальные проблемы безопасности информационных технологий. Материалы I международной заочной научно-технической конференции (АПроБИТ-2007), –Красноярск, 2007. –С. 40-44.

10.Интеллектуальная антиспам система / Никитин А.П., Валеев С.С. // Компьютерные науки и информационные технологии: Труды 9-го Международного семинара (CSIT'2007), Т. 4, – Уфа-Красноусольск, 2007. –С. 57-59 (на англ. языке).

11.Интеллектуальная система фильтрации спама / Никитин А.П. // Актуальные проблемы в науке и технике: Материалы 3-й региональной зимней школы-семинара аспирантов и молодых ученых. - Т.1. - Уфа: УГАТУ, 2008. - С. 351-356.

12.Многоагентная система фильтрации спама / Валеев С.С., Никитин А.П. // Компьютерные науки и информационные технологии: Труды 10-го Международного семинара (CSIT-2008), Т. 2. –Анталия – Турция, 2008. – С. 224-227 (на англ. языке).

13.Формирование базы знаний для интеллектуальной системы борьбы со спамом / Никитин А.П. // IX Королёвские чтения: Материалы всероссийской молодёжной научной конференции. – Самара, 2008. – С. 41-43.

14.Система автоматической интеллектуальной классификации текстов / Валеев С.С., Никитин А.П. // IX Королёвские чтения: Материалы всероссийской молодёжной научной конференции. – Самара, 2008. – С. 44-46.

15.Анализ проблемы борьбы со спамом Интернет-провайдера / Никитин А.П. // Мавлютовские чтения: Материалы всероссийской молодежной научной конференции. Т. 1.. – Уфа, 2008. –С. 11.

16.Многоагентная система борьбы со спамом / Никитин А.П. // Мавлютовские чтения: Материалы всероссийской молодежной научной конференции. Т. 1. – Уфа, 2008. – С. 12.

Диссертант А. П. Никитин

НИКИТИН Андрей Павлович

МНОГОУРОВНЕВАЯ МНОГОАГЕНТНАЯ СИСТЕМА ФИЛЬТРАЦИИ СПАМА В ОРГАНИЗАЦИИ

Специальность: 05.13.19 — Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано к печати ___.01.2009 Формат 60x84 1/16.
Бумага офсетная. Печать плоская. Гарнитура Times New Roman Cyr.
Усл. печ. л. 1,0. Усл. кр. отт. 1,0. Уч. -изд. л. 0,9.
Тираж 100 экз. Заказ № ____

ГОУ ВПО Уфимский государственный авиационный технический университет
Центр оперативной полиграфии
450000, Уфа-центр, ул. К.Маркса, 12.