УДК 004.3

А. И. Власов, канд. техн. наук, **И. Г. Цыганов**,
МГТУ им. Н. Э. Баумана

Архитектура корпоративной многоагентной автоматизированной системы фильтрации информационных потоков

Рассматривается архитектура многоагентной автоматизированной системы, позволяющей реализовать функции коллективной фильтрации информационных потоков в масштабе систем корпоративного уровня. Излагается методика построения подобных систем на основе агентов, имеющих подобный функциональный состав. Приводится специализация агентов трех типов (центральный агент фильтрации, агент пользователя и агент управления), рассматриваются особенности построения каждого из них и принципы их взаимодействия в единой системе. Приводится описание состава и методов использования ключевых информационных структур системы.

Введение

Автоматизированные системы фильтрации (АСФ) информационных потоков (ИП) представляют собой класс распределенных систем, позволяющих обнаруживать в потоке данных информацию заданного характера и осуществлять блокировку ее передачи. Еще совсем недавно интенсивность потоков информации была относительно небольшой, что позволяло настраивать применяющиеся в АСФ ИП фильтры вручную, для чего привлекались знания и навыки экспертов. В современных условиях, когда основным требованием к АСФ ИП является сокращение времени реакции системы на стремительно изменяющиеся условия внешней среды, ключевой проблемой становится разработка адаптивных средств фильтрации, способных перестраиваться в автоматическом режиме, обеспечивая минимальное участие человека.

Одной из наиболее важных и сложных проблемных областей, в которых требуется разработка адаптивных АСФ ИП, связана с построением средств защиты от незапрашиваемой рассылки сообщений электронной почты в глобальной сети Интернет. Незапрашиваемая рассылка (НР), называемая также англоязычным термином "спам", — это массовая рассылка сообщений (как правило, рекламного характера), инициируемая отправителем без учета потребностей и вопреки желанию адресатов [1, 2]. Особое внимание к адаптивным АСФ НР объясняется лавинообразным ростом числа распространителей НР, видов сообщений НР (СИР), применением методов обхода фильтров, включающих модификацию формальной (маршрутная информация) и текстовой части сообщений [3]. В данной работе мы будем в основном ссылаться на проблемы построения корпоратив-

ных АСФ НР, однако мы надеемся, что приведенные здесь решения имеют более общий характер.

В настоящее время практически все современные программные средства, имеющие отношение к передаче сообщений электронной почтой (например, клиентские системы *TheBat!*, *Microsoft Outlook*, серверные системы *Sendmail*, *Postfix* и др.), оснащаются средствами фильтрации НР и имеют интерфейс для интеграции с АСФ НР сторонних производителей. Среди специализированных АСФ НР следует выделить следующие наиболее характерные: *Bogofilter* [4], *SpamAssasin* [5], *Vipul Razor* [6], а также отечественный продукт *SpamTest/Kaspersky AntiSpam* [7].

Хотя каждая приведенная АСФ НР предоставляет достаточно богатый набор средств фильтрации, их настройка и обновление остаются сложной задачей, требующей постоянного участия администратора, обладающего специальными знаниями.

Если пользователь получает СНР, которое пропустила АСФ НР, он в лучшем случае имеет возможность отправить уведомление на имя администратора, который в свою очередь настраивает систему фильтров. Таким образом, роль пользователей оказывается пассивной, а интервал времени между первичным обнаружением ошибки фильтрации и соответствующей настройкой АСФ НР может составлять от нескольких часов до нескольких дней и даже недель, что зависит от загруженности администратора. Кроме того, во всех современных системах даже в том случае, если удалось достаточно быстро перенастроить систему фильтров, выявленные СНР, которые уже попали в пользовательские почтовые ящики, оттуда не удаляются и доставляются конечным получателям как будто это обычные сообщения. Это значительно снижает эффект от использования АСФ НР, поскольку НР распространяется пакетным способом (сотни писем за одну рассылку).

В связи с этим актуальной остается задача построения АСФ НР, обеспечивающей своевременное реагирование в ответ уже на первое заявление об ошибках фильтрации. Для этого предлагается использовать многоагентную АСФ НР, имеющую следующие особенности. Во-первых, в системе реализуются фильтры на базе нейронной сети с переменной структурой [8], которая настраивается по замкнутому циклу на основе обучающей выборки, состоящей из примеров выявленных СНР и обычных пользовательских сообщений. Во-вторых, используется режим, позволяющий формировать обучающую выборку автоматически на основании голосования пользователей (допускается полное отсутствие участия администратора) [9]. В-третьих, голосование пользователей может влиять на статус сообщений даже в том случае, если они уже направлены в пользовательскую часть системы.

Общее описание архитектуры системы

Структура предлагаемой АСФ НР строится из функционально однородных агентов. Потоки данных, циркулирующие в агенте АСФ НР, представлены на рис. 1. На этом рисунке блок фильтров (БФ) осуществляет разделение однородного потока входящих сообщений на два: поток НР и поток прочих сообщений. СНР могут блокироваться или подвергаться другим видам обработки, прочие сообщения пропускаются без изменений. Блок предоставления (БП) обеспечивает различные технические функции при реализации взаимодействия с обслуживаемыми системами. К числу таких функций принадлежат функции передачи, маршрутизации, накопления, упорядочивания, отображения, предоставления сообщений по запросам и т. д. Под обслуживаемыми системами понимается либо агент более низкого уровня, либо конечный пользователь (человек). Блок управления (БУ) концентрирует на себе потоки данных из различных источников и генерирует на их основе управляющие воздействия, обеспечивая взаимосвязь элементов внешней и внутренней среды данного агента.

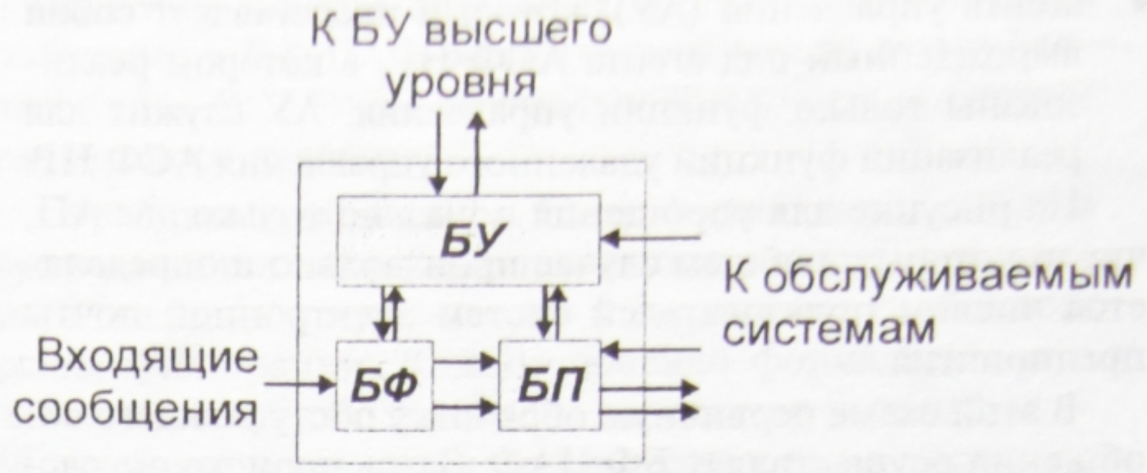

Рис. 1. Потоки данных в агенте АСФ НР

Каскадное объединение агентов в сеть или иерархию позволяет построить АСФ НР практически любой конфигурации, отвечающей требованиям оперативного реагирования на ошибки фильтрации. На рис. 2 представлена структура и потоки данных в типовой АСФ НР корпоративного уровня, которая состоит из агентов трех видов:

- единственного центрального агента фильтрации (ЦАФ), обслуживающего всех пользователей корпоративной системы;
- множества агентов пользователей (АП), ориентированных на обслуживание только одного пользователя;

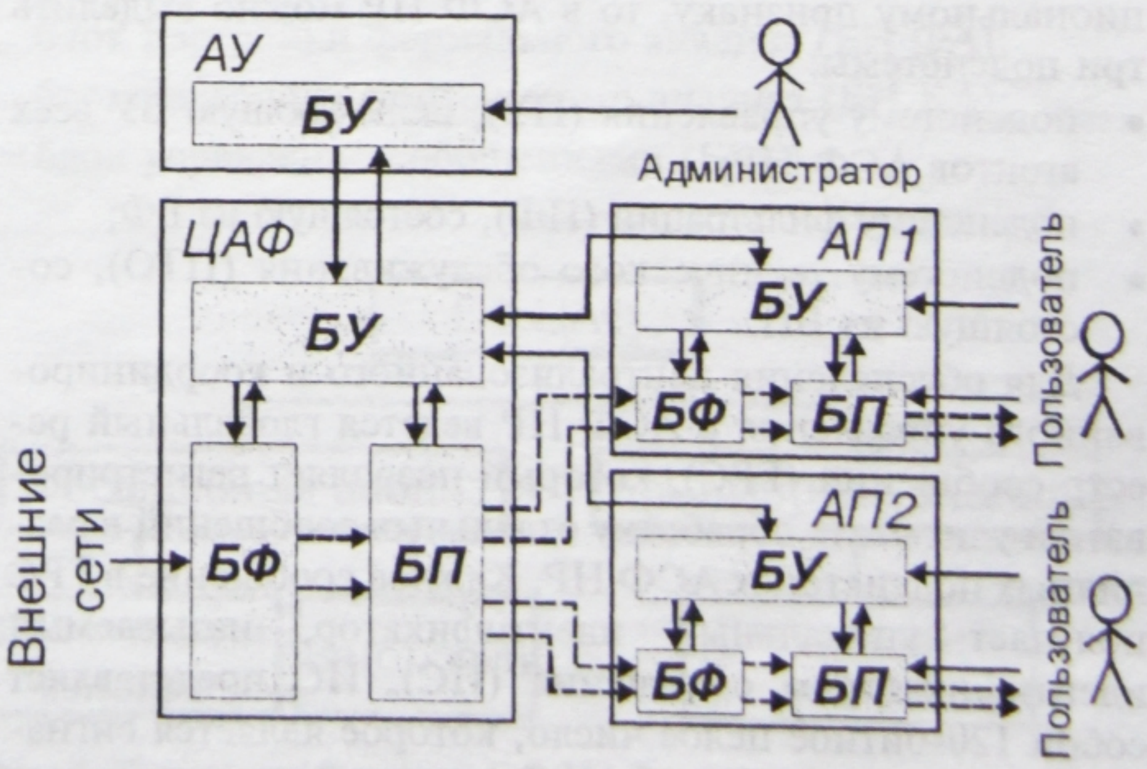

Рис. 2. Потоки данных в типовой схеме АСФ НР

- агента управления (АУ), который представляет собой вырожденный вид агента АСФ НР, в котором реализованы только функции управления. АУ служит для реализации функций удаленного управления АСФ НР.

На рисунке для упрощения показано только два АП, число которых в общем случае произвольно и определяется числом пользователей систем электронной почты предприятия.

В этой схеме первичную обработку поступающего сообщения осуществляет БФ ЦАФ. Здесь происходит распознавание общих признаков НР. Если сообщение однозначно является СНР, то оно удаляется, если нет — передается в БП ЦАФ, который выполняет функции почтового маршрутизатора, осуществляющего доставку сообщения в один или несколько АП.

В АП сообщение попадает в БФ. Здесь реализуются функции фильтрации, настраиваемые индивидуально отдельными пользователями. По результатам БФ сообщение может быть удалено или передано в БП агента пользователя, являющийся блоком, позволяющим пользователю осуществлять стандартные действия с поступившими сообщениями (прочтение, ответы и т. д.). Сообщения представляются в структурированной системе папок. БУ агента пользователя реализует функции управления в агенте пользователя и во всей АСФ НР от имени пользователя. Данный блок позволяет, в частности, участвовать пользователю в голосовании по любому доставленному сообщению. Голосование осуществляется прямым указанием о том, что данное сообщение является СНР. По мере поступления голосов по отдельным сообщениям БУ агента пользователя также может изменять статус доставленных в БП сообщений путем их автоматического перемещения в системе папок.

БУ ЦАФ является блоком, отвечающим за координацию управления в АСФ НР и выработку стратегии и тактики настройки **БФ ЦАФ**. Для этого привлекаются, во-первых, результаты голосования отдельных пользователей, во-вторых, администратор системы. Администратор участвует в управлении с помощью БУ АУ, который предоставляет удаленный интерфейс для реализации функций управления.

Если объединить отдельные блоки АСФ НР по функциональному признаку, то в АСФ НР можно выделить три подсистемы:

- подсистему управления (ПУ), включающую БУ всех агентов АСФ НР;
- подсистему фильтрации (ПФ), состоящую из БФ;
- подсистему технического обслуживания (ПТО), состоящую из БП.

Для обеспечения централизованного и координированного управления в АСФ НР ведется глобальный реестр сообщений (ГРС), который позволяет регистрировать и учитывать обработку отдельных сообщений в различных подсистемах АСФ НР. Каждое сообщение в ГРС получает уникальный идентификатор, называемый идентификатором сообщения (ИС). ИС представляет собой 120-битное целое число, которое является сигнатурой данного сообщения и рассчитывается по его содержанию с помощью применения хэш-функции (Nilsimsa). ИС является одинаковым для сообщений с одинаковым содержанием.

Основной целью ГРС является координация действий пользователей и администратора(ов) АСФ НР в целях определения статуса сообщений, связанных с данным ИС. Статус сообщения позволяет судить о том, является ли данное сообщение СНР или это обычное пользовательское сообщение. В структуре статуса сообщения (СС) выделяют две составляющие (рис. 3):

- ГСС — глобальный СС;
- множество ЛСС — локальные СС.

ГСС для данного ИС является величиной однозначно фиксирующей статус данного сообщения в АСФ НР. ГСС может принимать одно из следующих значений: *S (Spam), H (Ham), A (Auto), U (Unknown)*. Значения *S* и *H* используются в том случае, если администратор вручную указал, что *S* — данное сообщение является СНР; *H* — данное сообщение является обычным пользовательским. Значение *A* показывает, что это сообщение имеет однозначные признаки СНР, которые были выявлены автоматическими средствами АСФ НР. Значение *U* показывает, что ГСС для данного ИС однозначно не определен.

ЛСС в отличие от ГСС связан с конкретным пользователем, является однозначным для агента пользователя этого пользователя, а для прочей части АСФ НР является справочным значением. ЛСС для данного ИС определяется пользователями АСФ НР, получившими сообщение с данным ИС. ЛСС может принимать одно из шести значений:

- *"SA" (Spam Auto)* — сообщение было автоматически отнесено к НР в БФ агента пользователя;
- *"SM" (Spam Manual)* — пользователь указал вручную, что данное сообщение — НР;

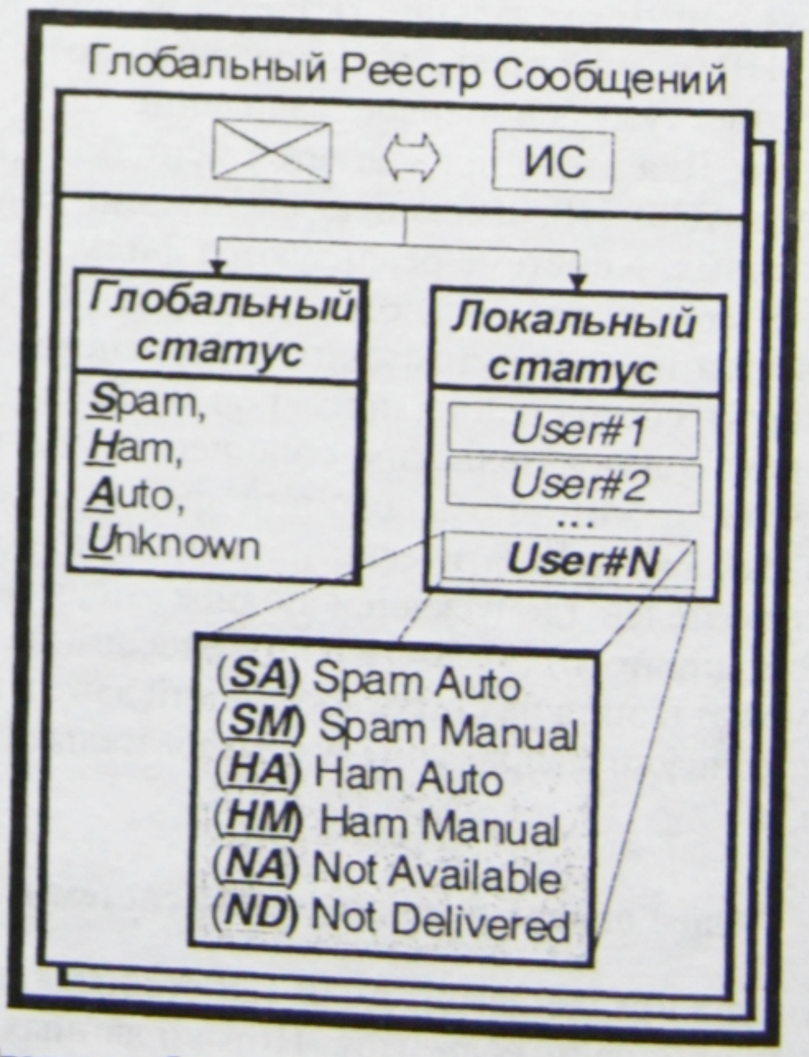

Рис. 3. Статус сообщений в АСФ НР

- *"HA" (Ham Auto)* — сообщение в БФ АП автоматически отнесено к обычным сообщениям;
- *"HM" (Ham Manual)* — пользователь вручную указал, что данное сообщение обычное;
- *"ND" (Not Delivered)* — сообщение никогда не было доставлено данному пользователю;
- *"NA" (Not Available)* — состояние на момент получения первой копии сообщения в АСФ НР, означающее, что оно еще не поступало в БФ агента пользователя.

Помимо информации о СС ГРС также хранит дополнительную информацию о состоянии сообщения, которая формализуется в виде атрибутов сообщения. Атрибуты, как и СС, могут быть глобальными или локальными. К глобальным атрибутам, например, относится дата получения сообщения, IP-адрес SMTP-системы, с которой получено сообщение и т. д. Локальные атрибуты связаны с определенным агентом пользователя и отражают, например, факт удаления, прочтения, генерации пользователем ответа на сообщение и т. д.

Функции обеспечения доступа к ГРС и его ведения обслуживаются в БУ ЦАФ. Для изменения локальных характеристик сообщения в ГРС агент пользователя обращается с уведомлениями к ЦАФ, который координирует действия различных агентов пользователя генерации ответных уведомлений.

Центральный агент фильтрации

Блок фильтрации ЦАФ используется для выявления общих признаков НР с помощью анализа различных элементов поступающего на вход сообщения. Сообщение рассматривается как сложный информационный объект, состоящий из следующих элементов: технического конверта и тела сообщения. Тело сообщения, в свою очередь, делится на заголовки и содержание. Технический конверт содержит информацию, передающуюся при установлении SMTP-соединения (IP-адрес удаленной системы, email-адрес отправителя и получателя). Заголовки сообщения содержат стандартные форматированные поля (например, From:, To: и т. д.). Содержимое определяется текстовой частью сообщения.

Особенностью рассматриваемой АСФ НР является то, что сообщение, поступающее на вход, всегда принимается целиком, и только после этого выполняется его анализ. Независимо от результатов анализа текст полученного сообщения передается в БУ ЦАФ с тем, чтобы использовать его при формировании обучающей выборки.

Перед началом анализа осуществляются расчет ИС и проверка, зарегистрирован ли данный ИС в ГРС. Если зарегистрирован и ГСС равен *S* либо *A*, то сообщение уничтожается. Если ИС не зарегистрирован в ГРС, то происходит его регистрация.

Если сообщение не уничтожено, то оно передается в последующие контуры БФ ЦАФ. Качество распознавания в них определяется величиной *G*, показывающей уровень уверенности в том, что сообщение является СНР.

Функции анализа отдельных составляющих объекта сообщения в БФ ЦАФ распределены между двумя блоками (рис. 4): блоком формального анализа и блоком контекстного анализа.

Обработка сообщений в блоке формального анализа осуществляется с помощью последовательного применения к техническому конверту и заголовкам сообщения правил фильтрации. Каждое правило формализуется в виде кортежа $\langle C, A \rangle$. Здесь C — множество условий, A — действия, выполняемые в случае, если и только если все перечисленные в C условия выполнены. Блок контекстного анализа реализован на базе нейросетевого классификатора, осуществляющего оценку уровня уверенности на основании анализа вхождения в текст сообщения характерных слов и словосочетаний. В структуре блока контекстного анализа выделяют две основные составляющие: блок кодирования и блок классификации. Блок кодирования преобразует содержательную часть сообщения в векторную форму. Блок классификации дает оценку уровня уверенности на основании принадлежности вектора сообщения к той или иной области векторного пространства.

В результате обработки сообщение в БФ ЦАФ может быть уничтожено (если существует уверенность в том, что оно является СНР), либо доставлено в БП ЦАФ. В последнем случае результаты анализа сообщения в БФ ЦАФ сохраняются в ГРС.

Блок предоставления ЦАФ осуществляет сервисные функции, в числе которых идентификация конкретных адресатов сообщения, создание копий сообщения для каждого из них и реализация окончательной доставки этих копий в соответствующие агенты пользователя. Таким образом, основная функция БП ЦАФ — обеспечение надежной доставки сообщений в агенты пользователя. БП ЦАФ реализован на базе стандартной серверной почтовой системы *Sendmail* (возможно также применение *Postfix*).

Блок управления ЦАФ является самым сложным блоком в АСФ НР рассматриваемой конфигурации. Этот блок координирует работу прочих элементов системы. В его составе выделяют три функционально различных блока (рис. 5):

- блок настройки формального анализа (БН ФА);
- блок настройки контекстного анализа (БН КА);
- блок управления сообщениями (БУС).

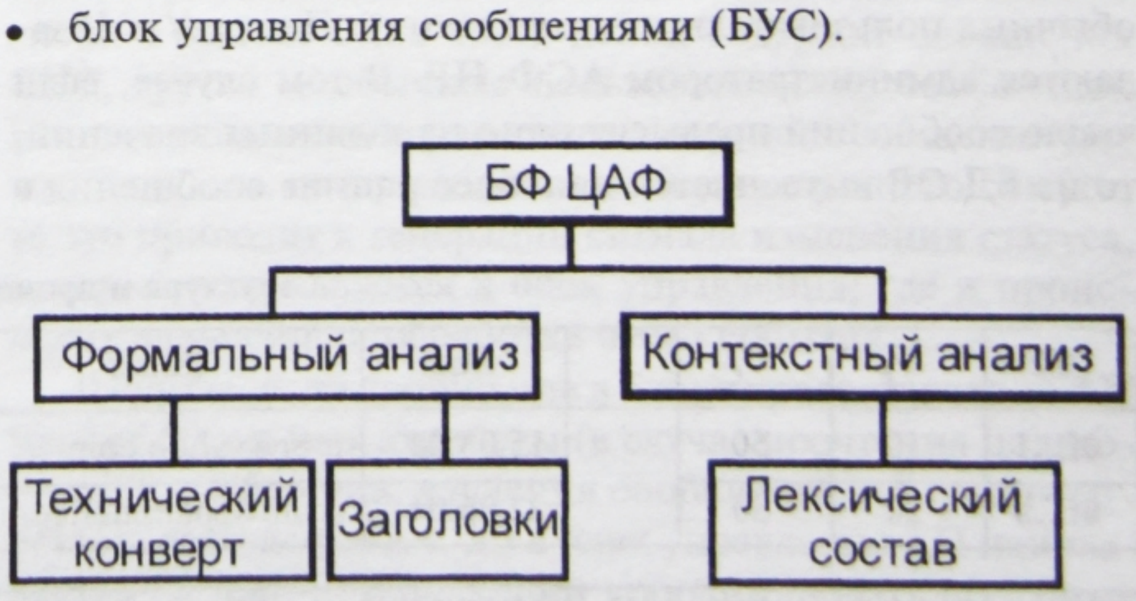

Рис. 4. Структурный состав БФ ЦАФ

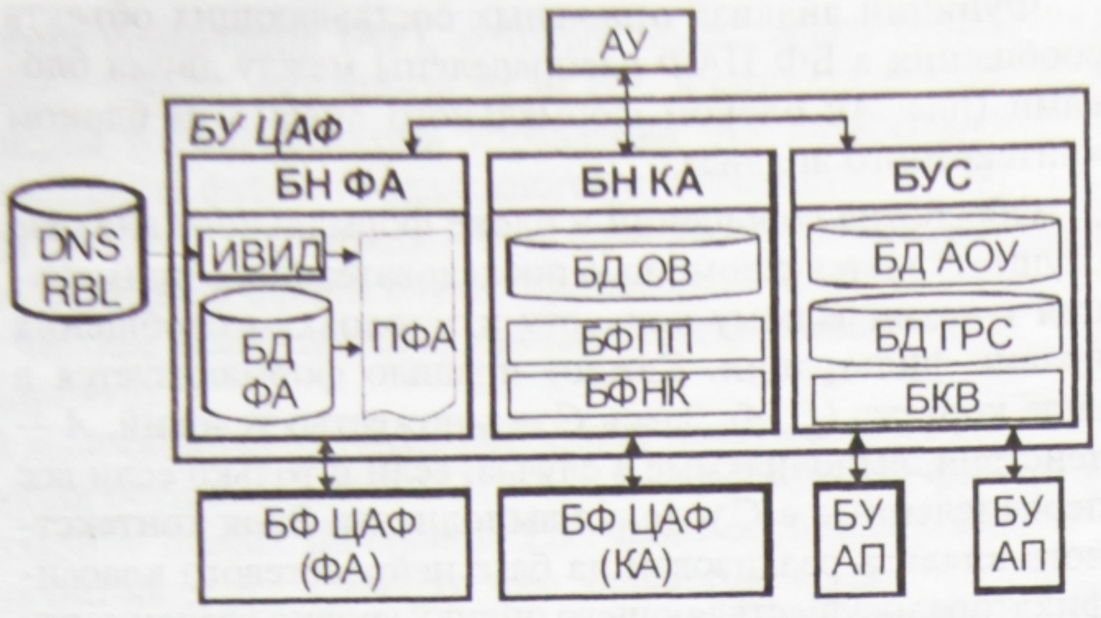

Рис. 5. Взаимосвязь БУ ЦАФ с другими элементами АСФ

Блок настройки формального анализа предоставляет функции настройки БФ ЦАФ. Эти функции доступны только для администратора через агента управления и непосредственное влияние на них со стороны пользователей системы не допускается. Среди функций, предоставляемых данным блоком, имеются функции редактирования профиля ФА, изменение различных локальных БД ФА (черные и белые списки), а также настройка интерфейса с внешними источниками данных (ИВИД). Через ИВИД к АСФ НР могут быть подключены такие источники, как БД RBL или DNS. БН ФА имеет непосредственное влияние на алгоритмы, применяемые в БФ ЦАФ. При настройке системы администратор использует информацию, предоставляемую БУС.

Блок настройки контекстного анализа отвечает за функции настройки контекстного анализа БФ ЦАФ. В составе этого блока имеется блок формирования пространства признаков (БФПП) и блок формирования нейросетевого классификатора (БФНК). Первый блок отвечает за функции составления словаря значимых слов и словосочетаний, а также формирования на их основе векторного представления сообщений. БФНК отвечает за синтез нейросети с переменной структурой. Оба блока работают на основании данных, предоставляемых базой данных, хранящей обучающую выборку (БД ОВ).

Формирование обучающей выборки осуществляется по принципу *FIFO*-буфера. В обучающей выборке одновременно не может находиться более N СНР и более M обычных пользовательских сообщений. Числа N и M задаются администратором АСФ НР. В том случае, если число сообщений превысит одно из заданных значений, то из БД ОВ вытесняется наиболее ранние сообщения с тем же статусом, что и поступившее (СНР или пользовательские).

Занесение сообщения в БД ОВ осуществляется в момент получения сообщения, не имеющего идентификатор сообщения в БД ГРС. БД ОВ представляет собой реляционную таблицу, содержащую следующие домены: идентификатор сообщений, текст сообщения, дата поступления сообщения в базу данных.

Для формирования обучающей выборки используются математические методы, позволяющие определить статус сообщения даже в том случае, когда отсутствует указание администратора. Статус при этом рассчитывается как результат голосования пользователей с учетом их квалификации.

Блок управления сообщениями ЦАФ реализует функции управления множеством сообщений, обрабатываемых в АСФ НР. Регистрация всех действий с сообщениями происходит в БД ГРС, представляющей собой реляционную таблицу, в которой каждая строка отвечает некоторому идентификатору сообщения. Если в АСФ НР поступает сообщение, которое не было ранее внесено в БД ГРС, то для него заводится новая строка.

В целях предотвращения бесконечного разрастания БД ГРС она периодически очищается от строк, соответствующих сообщениям, которые с большой долей уверенности можно отнести к обычным пользовательским сообщениям. Строка записи о сообщении может быть удалена из БД ГРС в случае выполнения следующих условий: во-первых, соответствующее сообщение должно быть получено однократно, во-вторых, только одним пользователем, в-третьих, не должно быть вручную отнесено к НР, в-четвертых, должно быть удалено, в-пятых, после его удаления должно пройти заданное администратором время (несколько дней). Аналогичная процедура устанавливается также для сообщений, полученных группой пользователей (по одному на каждого пользователя), однако интервал времени ожидания здесь должен быть более длительным. Поскольку вся необходимая для проверок информация сохраняется в режиме on-line в БД ГРС, то их проверка не вызывает никаких технических затруднений.

БД ГРС содержит информацию о результатах обработки сообщения во всех агентах АСФ НР. В таблице приводится структурный состав и пример заполнения нескольких строк БД ГРС.

Первый столбец содержит идентификатор сообщения (*ИС*), второй и третий — результат обработки сообщения в БФ ЦАФ. Далее следуют различные информационные поля, такие как дата, время получения сообщения и пр. Следующий важный столбец — *Email*, где со-

Структура и пример заполнения БД ГРС

ИС	G_F	G_C		*Date*	*Email*	*RelayIP*	*N*	*S*	*User #1*		*User #2*	
0f...1	10	50	...	15.03.04	user@yahoo.com	232.1.1.3	3	U	SA	ER	ND	- -
0f...b	20	30		22.06.04	spam@spammer.com	195.1.19.3	10	S	SM	E -	SM	E-
...												
1e...2	10	70		23.07.04	user@legal.org	213.22.1.1	1	H	HA	- -	ND	- -

храняется email-адрес отправителя данного сообщения (если сообщение было получено из нескольких источников, сохраняются все возможные варианты). Столбец *RelayIP* сохраняет IP-адреса SMTP-серверов, с которых было получено данное сообщение. Столбец *N* содержит число принятых сообщений, столбец *S* — ГСС сообщения. Далее в таблице приведены данные по отдельным пользователям (как и на рис. 2, рассматривается вариант с двумя пользователями). Эти данные включают, во-первых, ЛСС, во-вторых, локальные атрибуты сообщения (*E* — сообщение удалено, *R* — прочитано).

Другой важной базой данных БУС является база данных административной очереди уведомлений (БД АОУ). БД АОУ содержит уведомления, которые должны быть доставлены в различные агенты АСФ НР, но по каким-либо причинам не могут быть доставлены моментально. Невозможность доставки уведомлений может быть вызвана занятостью ресурсов, которые обслуживают данные уведомления.

В административной очереди уведомлений могут храниться уведомления следующих типов:

- уведомление администратору, направленное от пользователя, с просьбой включить в черный (или белый) список тот или иной адрес;
- уведомление от агента пользователя в агент управления (к администратору), направляемое в случае, когда ЛСС какого-либо сообщения меняется на SM;
- автоматическое уведомление от различных элементов АСФ НР к администратору о происшествиях, инцидентах, ошибках и пр.;
- уведомление от БУ ЦАФ к БУ агента пользователя, направляемое при изменении записи ЛСС в БД ГРС, инициированное каким-либо другим агентом пользователя;
- уведомление от БУ ЦАФ к БУ агента пользователя, направляемое при изменении записи ГСС в БД ГРС, инициированное администратором.

Уведомления, направляемые администратору, извлекаются последними в ручном режиме, что может приводить к модификации правил фильтрации или ГСС в ГРС. Блок координирования взаимодействия (БКВ) обеспечивает прием от агента пользователя уведомлений об изменении ЛСС или атрибутов сообщений и осуществляет, во-первых, модификацию БД ГРС, во-вторых, определение всех заинтересованных в данном событии агентов АСФ НР и помещение в АОУ уведомлений на их адрес. Кроме этого, если удаляются какие-либо сообщения, то это может привести к необходимости изменения, во-первых, БД ГРС, во-вторых, БД обучающей выборки. Ответственность за выполнение операций такого рода несет БКВ.

Возможна ситуация, при которой могут возникать петли управления. Например, модификация ЛСС в одном из агентов пользователя может приводить к модификации ЛСС в другом. Последнее событие снова порождает уведомление, которое в общем случае может снова приводить к изменению ЛСС в первом агенте пользователя. Поэтому одной из функций БКВ является фиксация подобной ситуации и запрещение бесконечных циклов перехода ЛСС. Это осуществляется с помощью введения ограничения на число изменений ЛСС в заданный интервал времени (не более 10 за минуту). Если заданное значение превышено, БКВ генерирует уведомление об ошибке в системе администратору и прекращает постановку уведомлений в АОУ.

Агент пользователя

Блок фильтрации агента пользователя (АП) осуществляет функции фильтрации от имени пользователя данного АП. Так же, как и в случае БФ ЦАФ, поступление сообщения в БФ АП сопровождается расчетом его ИС. Далее проводится регистрация сообщения в локальном реестре сообщений (ЛРС). ЛРС является структурой, область действия которой ограничена данным АП. В том случае, если необходимо организовать обмен данными между различными АП или между АП и ЦАФ, то это достигается при использовании ГРС. Основной задачей, в которой применяется ЛРС, является обеспечение синхронизации при работе пользователя и функциональных блоков (ФБ) АП с сообщениями, имеющими одинаковый ИС. Управление ЛРС осуществляется из блока управления АП.

В том случае, если сообщение с данным ИС уже имеется в БД ЛРС, то поступающее сообщение наследует все свойства имеющегося в АП дубликата, а его фильтрация в БФ АП не проводится. Такое сообщение сразу передается в БП АП, где оно помещается в ту же папку, что и другие сообщения с аналогичным содержанием.

В том случае, если сообщение является новым в данном АП, то оно поступает в блоки фильтрации. В отличие от БФ ЦАФ, в БФ АП не реализовано разделение блоков формального и контекстного анализа. Вместо этого все функции анализа осуществляются унифицированным методом на основе системы правил вида $\langle C, A \rangle$.

Среди условий, которые могут фигурировать в множестве *C* каждого правила, могут быть условия по результатам фильтрации в БФ ЦАФ и условия, связанные с результатами обработки в других АП. В результате фильтрации в БФ АП сообщению назначается ЛСС, и оно может быть либо уничтожено, либо направлено в одну из папок блока предоставления АП.

Блок предоставления АП предоставляет доступ пользователю к сообщениям, переданным в АП. Пользователь получает возможность открывать сообщения, просматривать их и отвечать на них. Сообщения хранятся в системе папок. Одна часть папок содержит сообщения СНР, другая — обычные пользовательские сообщения. Если пользователь осуществляет перенос сообщений между папками, содержащими сообщения разного статуса, то это приводит к генерации сигнала изменения статуса, который направляется в блок управления, где и происходит дальнейшая обработка этого события.

В случае, если сообщение в блоке предоставления АП меняет локальные атрибуты (в случае прочтения пользователем сообщения, удаления сообщения, генерации ответа на сообщение и т. д.) в блок управления АП направляется сигнал, позволяющий координировать подобные действия пользователя.

В своих разработках мы использовали собственную почтовую программу, однако возможно применение стандартных клиентских программ на базе систем *The-Bat!*, *Microsoft Outlook* и т. д.

Блок управления АП (БУ АП) является блоком, который, во-первых, управляет работой прочих функциональных блоков данного АП, во-вторых, регулирует взаимодействие данного АП с прочими агентами АСФ НР (рис. 6). Данный блок находится под непосредственным управлением пользователя данного АП, который определяет поведение БУ АП путем настройки. БУ АП не содержит никаких схем задержки, в нем не реализуются никакие последействия и т. д. Блок работает в режиме стимул — реакция. Стимул определяется внешними сигналами, реакция — ответом БУ на них. При получении внешних сигналов управления выполняются необходимые действия, после чего блок переходит в состояние ожидания до следующей команды из внешних источников. Источниками входных сигналов БУ АП являются:

- БП данного АП;
- БФ данного АП;
- ЦАФ (от АУ — при изменении ГСС);
- ЦАФ (от других АП — при изменении ЛСС).

Обработка сигналов от этих источников в БУ АП позволяет сформировать управление для внутренних функциональных блоков АП, а также выработать сигналы взаимодействия с другими агентами АСФ НР (через ЦАФ).

Со стороны БП АП в БУ АП могут быть направлены сигналы управления, извещающие о том, что пользователь данного АП изменил ЛСС какого-либо сообщения. Со стороны БУ ЦАФ направляются сигналы двух типов:

- сигналы со стороны отдельных АП, уведомляющие о том, что их пользователи изменили ЛСС какого-либо сообщения;
- сигналы со стороны АУ, находящегося под управлением администратора, которые уведомляют о том, что некоторые сообщения изменили ГСС.

При обработке сигналов управления, направленных от БП АП, БУ АП генерирует уведомление о них и передает его в ЦАФ. При изменении статуса (ЛСС) генерируется уведомление изменения ЛСС. БУ ЦАФ в ответ на уведомление изменяет соответствующую запись в ГРС и организует доставку уведомлений во все заинтересованные АП (т. е. в те из них, в которых имеются сообщения с тем же идентификатором сообщения). В том случае, если ЛСС был изменен на SM (признан СНР), то уведомление также направляется администратору АСФ НР для проверки данного сообщения и изменения ГСС в ГРС. Если сигнал управления вызван изменением атрибутов сообщения, то это также приводит к генерации соответствующего уведомления и передачи его в ЦАФ, который определяет реакцию АСФ НР на подобные действия. При получении уведомлений, генерируемых при изменении ГСС, выполняются следующие действия. Если ГСС был изменен на *S*, а сообщение еще не было прочитано, то оно удаляется. Если такое сообщение было прочитано и имеется несколько его копий, то все копии удаляются, остается только один представитель данного сообщения. Если ГСС был изменен на *H*, то никаких действий не проводится.

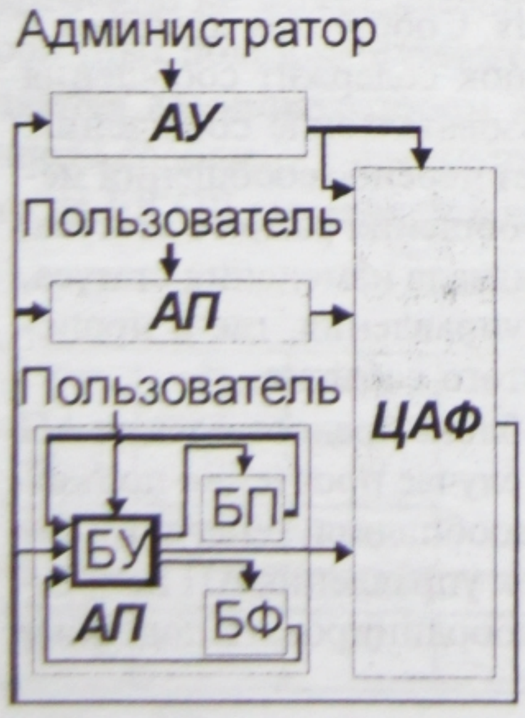

Рис. 6. Функциональная схема взаимодействия БУ АП с другими элементами АСФ НР

При обработке уведомлений, генерируемых со стороны других АП, осуществляется повторный запуск тех правил фильтрации из профиля пользователя, которые в множестве *C* содержат условия совместной фильтрации. Если выполнение какого-либо правила фильтрации приводит к изменению ЛСС, то в БП АП сообщение перемещается в соответствующую папку. Это действие, в свою очередь, заставляет отреагировать БУ АП с помощью передачи уведомления в БУ ЦАФ об изменении ЛСС, что приводит к повторному распространению уведомлений в АСФ НР. Пользователь АП может использовать БУ АП в качестве транспорта, осуществляющего доставку уведомлений на имя администратора АСФ НР. Пользователь может направить уведомления с просьбой включить в базу данных черного (или белого) списков адресов, использующихся в БФ ЦАФ, определенные адреса. Этот же канал может применяться для передачи уведомлений об ошибках АСФ НР, составляемых в письменной форме.

Агент управления

Блок управления агента управления используется только для организации доступа со стороны администратора к БУ ЦАФ с удаленных систем. В случае крупных корпоративных систем это позволяет оперативно управлять несколькими БУ ЦАФ отдельных подразделений с одного терминала и координировать их совместную работу.

Замечание о физической конфигурации системы

В данной статье рассматривается только функциональное построение АСФ НР. Поэтому мы не касаемся подробно вопросов механизмов обмена между отдельными функциональными блоками. Сделаем только несколько замечаний относительно наиболее важных физических конфигураций.

Наиболее просто в изложенной функциональной модели реализуется конфигурация, в которой весь ЦАФ, а также БФ и частично БП всех агентов пользователя реализуются на базе серверного аппаратно-программного комплекса, обслуживающего корпоративную систему

электронной почты режиме 7 × 24. При этом функциональные блоки БП и БУ каждого агента пользователя реализуются на базе отдельного интеллектуального терминала в виде персональной ЭВМ конкретного пользователя. В серверной части БП АП организуется хранилище сообщений (ХС), в которое попадают сообщения после прохождения системы фильтров. В пользовательской части БП АП организуется доступ к сообщениям, хранящимся в ХС, по запросу (например, по протоколу POP3 или IMAP4). При считывании сообщения из ХС предусмотрен вариант, когда сообщение остается в ХС, что позволяет многократно считывать одно и то же сообщение даже в том случае, когда ПЭВМ пользователя отключена (например, пользователю может потребоваться удаленный доступ к сообщениям с портативного компьютера).

Выводы

В статье описана архитектура гибкой многоагентной автоматизированной системы фильтрации, контур настройки которой допускает самоадаптацию в автоматическом режиме на основании результатов голосования пользователей. Систему строят на основе существующей почтовой инфраструктуры, дополняя и расширяя ее для решения задачи коллективной фильтрации нежелательных сообщений, поступающих из внешних сетей.

Предлагаемая архитектура позволяет исключить администратора из контура настройки системы и осуществить оперативное реагирование на ошибки фильтрации в реальном масштабе времени, что дает возможность повысить эффективность работы информационной системы предприятия и сократить непроизводительные расходы на обслуживание нежелательной информации.

Список литературы

1. **Cranor L. F. and LaMacchia B. A.** Spam! Communications of the ACM. 1998. Vol. 41. N 8. P. 74—83.
2. **Why** Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report. Washington: The Center for Democracy and Technology, 2002. 18 p.
3. **Atkins S.** Size and Cost of the Problem // In Proc. of the 56th Internet Engineering Task Force Meeting, San Francisco, March 2003. 31 p.
4. **Raymond, Eric S.** Bogofilter. http://bogofilter.sourceforge.net/
5. **SpamAssassin.** http://spamassassin.org/
6. **Prakash,** Vipul Ved. Vipul's Razor. http://razor.sourceforge.net/
7. **SpamTest**/Kaspersky AntiSpam, http://www.ashmanov.com
8. **Галушкин А. И.** Теория нейронных сетей. Кн. 1: Учеб. пос. для вузов. М.: ИПРЖР, 2000.
9. **Власов А. И., Цыганов И. Г.** Адаптивная фильтрация информационных потоков в корпоративных системах на основе механизма голосования пользователей // Информационные технологии. 2004. № 9. С. 12—19.