средств параллельной обработки. В основе системы лежат подходы автоматической сегментации, бинаризации и векторизации объектов, автоматизированное построение схем обработки и анализ результата оператором, после чего осуществляется корректировка вычислительной схемы. Использование объектно-ориентированного подхода, параллельной обработки, внутреннего представления, сочетание ручной и автоматической обработок в совокупности обеспечивают эффективную обработку топологии ИС.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Система цифровой обработки изображений слоев интегральных микросхем / А.А. Дудкин [и др.] // Идентификация образов; под ред. Р.Х. Садыхова. – Минск, 2001. – Вып. 2. – С. 72-87.
2. Дудкин, А.А. Реализация параллельной обработки изображений в системах технического зрения на базе MPI и многоагентной архитектуры / А.А. Дудкин, А.В. Отвагин // // Вестник Брестского государственного технического университета. Физика, математика, информатика. – 2006. – № 5 (41). – С. 2-8.

Материал поступил в редакцию 20.09.08

DOUDKIN A.A. Main approaches to implementation integrated circuits layout processing in computer vision systems for design and production of electronic devices

The system is described to automate integrated circuits layout restoring during integrated circuits re-design and production inspection. An automatic segmentation, binarization and vectorization, computer-aided development of processing scenarios and analyses procedures are in the basis of the system. An effective layout processing is provided by implementation of object-oriented approach, parallel realization, using inner representation and combination of manual and automatic processing.

УДК 004.8.032.26

Головко В.А., Безобразов С.В., Меленчук В.В.

НЕЙРОСЕТЕВОЙ ПОДХОД ДЛЯ ОБНАРУЖЕНИЯ ЭЛЕКТРОННОГО СПАМА

Введение. С развитием компьютерных наук и компьютерной техники общество столкнулось с проблемой развития киберпреступности. Сегодня киберпреступники используют не только средства угрозы компьютерной информации, такие как компьютерные вирусы и сетевые атаки, но и рассылку спама [1]. Спамом принято называть — массовую рассылку писем любого вида корреспондентам, не желающим их получать. К спаму причисляют рассылки коммерческой, политической рекламы и антирекламы, а также мошеннические письма и письма, содержащие в себе угрозу информации, например вирусы. Спам приобрёл широкое распространение в системах электронной почты, т.к. стоимость отправки электронных писем крайне низкая, в отличие от обычной бумажной корреспонденции. Например, за один день, по некоторым данным рассылается более 55 миллиардов писем [2], классифицированных как спам.

На сегодняшний день разработано много методов обнаружения и блокировки спама, однако это не спасет ситуацию. Киберпреступники постоянно разрабатывают новые методы обхода существующей защиты, и пользователи по всему миру продолжают получать огромное количество нежелательной почты каждый день.

В данной статье рассмотрен нейросетевой подход для классификации электронной почты. В первом разделе статьи представлен обзор наиболее популярных методов обнаружения электронного спама. Второй раздел содержит описание нейросетевого подхода классификации электронного спама. В третьем разделе представлены результаты проведенных экспериментов, выявлены недостатки и преимущества разработанного метода.

1. Эволюция методов борьбы с нежелательной корреспонденцией. Задача любой системы фильтрации спама — разделение потока входящей корреспонденции на спам и нормальную почту. Эта задача может решаться на разных этапах доставки писем: на почтовом сервере или на компьютере клиента.

Для анализа письма годятся любые его признаки, но на практике чаще всего используют следующие:

- IP-адрес отправителя;
- e-mail адрес отправителя и адрес для ответа;
- тема и текст сообщения;
- совокупность прочих признаков, таких как почтовый клиент, время отправки, отметки промежуточных узлов доставки и др.

Рассмотрим подробнее каждый из перечисленных методов.

Фильтрация по IP-адресам. Первые методы фильтрации спама были весьма простыми. Например, ведение «чёрных списков» IP-адресов, откуда запрещена доставка корреспонденции [1]. Т.е. на почтовом сервере проверяются все адресаты, от которых идет корреспонденция. Если адрес отправителя находится в «черном списке», то такое письмо блокируется и не доходит до конечного адресата. Составлением «черного списка» может заниматься как отдельная всемирная организация, так и создатели почтового сервера. К плюсам данного подхода можно отнести надёжность. Надежность блокирования нежелательных писем обуславливается определением на основе статистики «мест» распространения спама, и в итоге письма блокируются еще до доставки конечному пользователю. К недостаткам данного метода можно отнести слабую эффективность в настоящий момент. Для отправки спама сейчас широко используются бесплатные открытые почтовые службы, а также заражённые вредоносными программами компьютеры обычных пользователей, так называемые зомби-сети [3]. Таким образом, блокировка IP-адресов, с которых рассылается большой поток нежелательных писем, скажется на обычных пользователях, не подозревающих, что их компьютеры заражены.

Таким образом, способ с использованием «белого списка», антипод «черного списка», годится лишь в исключительных случаях закрытых сообществ, например, для организации корпоративной почты.

Фильтрация по ключевым словам. Тема письма и его текст являются важным признаком для анализа спама. Как правило, текст спама отличается от текста нормальной корреспонденции, так как спам несет в себе отличную от простой переписки функцию: заманивание пользователей посетить Интернет-сайт или купить какую-нибудь вещь, оглашение коммерческой или политической информации и др. Фильтрация по ключевым словам и фразам является еще одним методом обнаружения спама [1]. Метод имеет ряд преимуществ, связанных с простотой его реализации – достаточно занести в базу данных запрещенные ключевые слова или фразы и в дальнейшем проверять наличие этих ключевых слов в тексте письма. Однако метод имеет и ряд существенных недостатков:

- правильно настроить подходящие ключевые слова достаточно

***Безобразов Сергей Валерьевич**, старший преподаватель кафедры «Интеллектуальные информационные технологии» Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.
***Меленчук Василий Васильевич**, инженер-программист представительства компании «CIB Software GmbH» (ФРГ) в Республике Беларусь.*

сложно, т.к. неосторожное включение популярного слова в «чёрный список» приведет к классификации нормального письма как спам;

- список ключевых слов может быть индивидуальным и неприменимым в общем случае на промежуточных и конечных серверах;
- спамеры, т.е. люди, занимающиеся рассылкой спама, зачастую умышленно допускают грамматические ошибки в словах с целью обмана таких фильтров.

Байесовская фильтрация. Более сложным методом для анализа темы и текста письма является использование наивного байесовского классификатора, основанного на теореме Байеса со строгими предположениями о независимости [1]. У фильтра имеется словарь с вероятностными оценками для каждого слова, которые выставляются индивидуально в процессе обучения фильтра. Если общая вероятность для всех слов текста превышает пороговое значение — то письмо классифицируется как спам.

Данный метод является достаточно гибким и эффективным по сравнению с использованием обычных фильтров по правилам. Основным плюсом байесовского фильтра является возможность его настройки на конкретного пользователя с учётом индивидуальных особенностей приходящей корреспонденции.

Однако, как уже отмечалось ранее, методы рассылки спама постоянно эволюционируют, и злоумышленники научились обходить байесовский фильтр путём добавления в тело письма текстового «шума» — бессмысленного набора слов, имеющих высокие вероятностные показатели как нормального письма [4].

И все же, на сегодняшний день Байесовский фильтр для обнаружения спама является надежным методом защиты и имеет точность обнаружения спама, равную примерно 92,2% [5].

Фильтр Маркова. В отличие от байесовского фильтра, который анализирует лишь слова, фильтр на основе цепей Маркова анализирует цепочки слов и пытается предсказать следующие слова во фразе [6].

На практике по причине значительных системных требований используются фразы длиной не более четырех - шести слов. Разработчиками конкретных систем, например CRM114 [7], афишируется точность в 99,9%, тем не менее, конкретные тесты выявляют эффективность таких фильтров, равную примерно 95,4% [5].

Цепочка слов, по мнению ряда исследователей, должна быть не менее четырех – шести слов, и не более пятнадцати, т.к. короткие фразы увеличивают вероятность определения корректных писем как спам, что недопустимо и является существенной проблемой данного фильтра.

Альтернативные методы борьбы со спамом. Помимо перечисленных методов борьбы со спамом с разной степенью эффективности применяются и другие методы, из числа которых можно выделить следующие: проверка контрольных сумм писем по базам данных спама в Интернете (методы Distributed Checksum Clearinghouse [8], Vipul's Razor [9], Recurrent Pattern Detection [10]); проверка сервером отправителя письма; методы, использующие модифицированные версии транспортных протоколов передачи почты.

2. Применение искусственных нейронных сетей для обнаружения спама. Искусственные нейронные сети (ИНС) [11], благодаря своим уникальным вычислительным способностям, прочно вошли в нашу жизнь. Построенные по аналогии с биологическими нейронными сетями, ярким представителем которых является человеческий мозг, они способны решать многие задачи, ранее считавшиеся нерешаемыми или трудно поддающимися решению. Уникальные вычислительные способности ИНС позволяют им не только решать многие, поставленные перед ними задачи, но и способны к самообучению, и, что не маловажно, к адаптации, т.е. адекватно реагировать на изменения окружающей среды. Благодаря своей параллельной архитектуре, ИНС обладают высоким уровнем быстродействия, что послужило причиной использования их в таких трудоемких задачах как прогнозирование, классификация, обнаружения, управления, робототехники т.д. На сегодняшний день трудно себе представить область, где ИНС не нашли свое применение.

Как было отмечено ранее, проблема электронного спама остро стоит перед современным пользователем глобальной сети Internet. Для решения этой проблемы брошено много сил и средств, как технических, так и правовых, однако злоумышленники постоянно находят пути обхода существующих средств защиты и доставляют нежелательные электронные письма на компьютеры пользователей по всему миру.

Для решения проблемы обнаружения спама нами было предложено использовать искусственные нейронные сети, хорошо зарекомендовавшие себя в таких областях защиты информации, как обнаружение вредоносных программ и сетевых атак [12]. При выборе архитектуры нейронной сети мы остановились на обучающемся векторном квантователе [13]. Нейронная сеть для векторного квантования была предложена в 1982 году Кохоненом и называется обучающимся векторным квантователем (learning vector quantization – LVQ) [13]. LVQ-сеть представляет собой двухслойную нейронную сеть (конкурирующий и линейный слои) с прямым распространением сигналов (см. рис. 1).

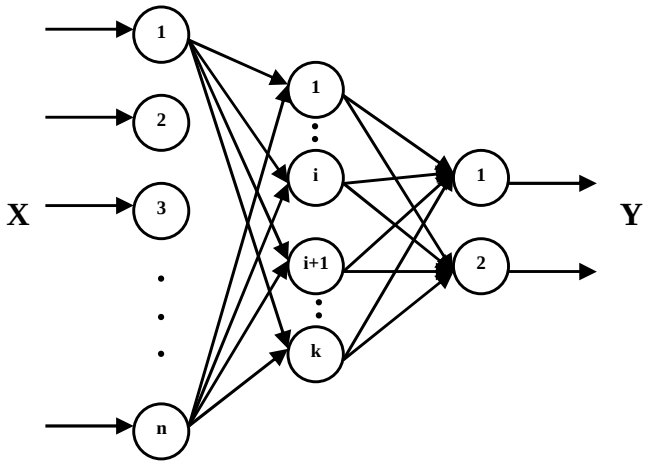

Рис. 1. *Нейронная сеть для векторного квантования*

Оба слоя нейронной сети содержат по одному конкурирующему на каждый кластер и одному линейному нейрону на каждый целевой класс. Конкурирующий слой выполняет кластеризацию векторов, а линейный слой соотносит кластеры с целевыми классами, заданными пользователем [11]. Векторный квантователь обучается в процессе поступления эталонных векторов. В процессе обучения образуются кластеры различных эталонов, каждому из которых соответствует свой нейрон. При поступлении на вход такой нейронной сети неизвестного образа, он идентифицируется в соответствии с мерой близости к эталонным векторам и кодируется на выходе сети номером нейрона. Совокупность кодовых векторов называется кодовой книгой. При поступлении входного вектора на сеть происходит его сравнение с вектором из кодовой книги. В процессе этого выбирается такой кодовый вектор, который наилучшим образом аппроксимирует входной вектор, и его номер используется в качестве кода. В качестве меры близости может использоваться евклидово расстояние.

Обучение LVQ состоит в изменении весов в соответствии с адаптивным правилом обучения и изменении позиции кодового вектора во входном пространстве. Существует большое количество вариантов обучения векторного квантователя [11]. Мы использовали алгоритм конкурентного обучения с одним победителем [11]. При таком обучении в отдельный квант времени только один нейрон может быть победителем.

Структура ИНС и алгоритм ее функционирования разделяет работу детектора, в основе которого лежит ИНС, на две стадии: стадию обучения и стадию обнаружения.

Для обучения детектора необходимо сформировать обучающую выборку. Обучающая выборка должна содержать в себе объекты двух классов: спам-письма и «нормальные» письма. На рисунке 2 представлен типичный представитель класса спам, а на рисунке 3 представлен типичный представитель класса нормальных писем.

Рис. 2. *Электронный спам*

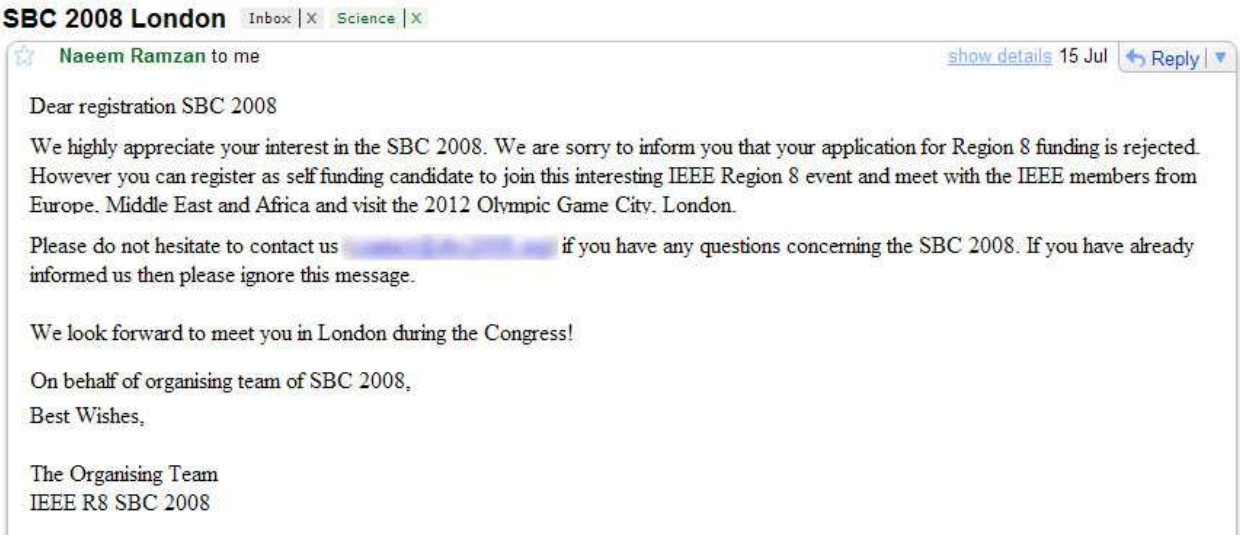

Рис. 3. *«Нормальное» электронное письмо*

На стадии обнаружения обученные детекторы проверяют неизвестные образы (электронные письма) и соотносят их с тем или иным классом. В результате, каждое полученное электронное письмо проверяется на предмет спама, и если нейросетевой детектор классифицирует письмо как спам, оно заносится в специальную папку, а пользователю выдается сообщение о количестве спам-писем. Если же детектор классифицирует новое электронное письмо как нормальное – то оно передается пользователю.

3. Описание экспериментальной системы. Нами была предложена модель системы обнаружения электронного спама на основе ИНС. Механизм функционирования предложенной системы изображен на рисунке 4.

Нейросетевые детекторы обучаются на заранее сформированной выборке, которая состоит из спама и нормальных писем, причем процентное соотношение спма к нормальным письмам равняется 50% / 50%. Обученные нейросетевые детекторы проверяют и классифицируют поступаемые электронные письма. Как было отмечено ранее, нейросетевой детектор разбивает все пространство образов на два класса и соотносит входящий образ к тому или иному классу. В зависимости от результата классификации, электронное письмо попадает либо в ящик «Спам», либо в ящик «Нормальные письма». Для достоверности результатов каждое письмо проверяется несколькими нейросетевыми детекторами. Такой подход позволит минимизировать ошибки, связанные с неправильной классификацией спам-письма как нормального письма.

4. Результаты экспериментов. Нами был произведен ряд экспериментов, демонстрирующих работу нейросетевых детекторов для обнаружения спама. Результаты экспериментов отображены в таблице 1 (спам-письма имеют имя *s****, а нормальные письма – *n****). Архитектура отдельного нейросетевого детектора является следующей: количество входных элементов $n = 256$, количество скрытых элементов $k = 10$, количество выходных элементов $l = 2$ (см. рис. 1). Следует отметить, что поскольку количество спам-писем и количество нормальных писем, составляющих обучающую выборку, одинаково, то нейросетевой детектор разбивает все пространство образов наполовину, т.е. первый класс, класс нормальных писем, занимает половину

Рис. 4. *Экспериментальная система обнаружения спама*

Таблица 1. *Результаты классификации электронной почты*

Имя файла / размер файла	Детектор 1 Y_1 / Y_2	Детектор 2 Y_1 / Y_2	Детектор 3 Y_1 / Y_2	Детектор 4 Y_1 / Y_2
n001 / 598 bytes	0,56 / 0,44	0,55 / 0,45	0,57 / 0,43	0,58 / 0,42
n002 / 428 bytes	0,51 / 0,49	0,49 / **0,51**	0,52 / 0,48	0,51 / 0,49
n003 / 1195 bytes	0,64 / 0,36	0,66 / 0,34	0,62 / 0,38	0,88 / 0,12
n004 / 407 bytes	0,52 / 0,48	0,53 / 0,47	**0,50 / 0,50**	0,53 / 0,47
n005 / 563 bytes	0,55 / 0,45	0,56 / 0,44	0,54 / 0,46	0,52 / 0,48
n006 / 265 bytes	0,49 / **0,51**	0,51 / 0,49	0,51 / 0,49	0,49 / 0,51
n007 / 318 bytes	0,56 / 0,44	0,51 / 0,49	0,52 / 0,48	**0,50 / 0,50**
n008 / 1021 bytes	0,61 / 0,39	0,74 / 0,36	0,50 / 0,50	0,79 / 0,21
n009 / 630 bytes	0,59 / 0,41	0,55 / 0,45	0,56 / 0,44	0,54 / 0,46
s001 / 268 bytes	0,42 / 0,58	0,46 / 0,54	**0,55** / 0,45	**0,50 / 0,50**
s002 / 506 bytes	0,45 / 0,55	**0,67** / 0,33	0,44 / 0,56	0,49 / 0,51
s003 / 260 bytes	0,40 / 0,60	0,40 / 0,60	**0,50 / 0,50**	**0,50 / 0,50**
s004 / 1879 bytes	0,19 / 0,81	0,11 / 0,89	0,40 / 0,60	0,07 / 0,93
s005 / 1040 bytes	0,21 / 0,79	0,13 / 0,87	0,10 / 0,90	0,12 / 0,88
s006 / 442 bytes	0,48 / 0,52	0,01 / 0,99	0,48 / 0,52	0,43 / 0,57
s007 / 1526 bytes	0,64 / 0,36	0,23 / 0,77	0,25 / 0,75	0,21 / 0,79
s008 / 458 bytes	0,49 / 0,51	0,48 / 0,52	0,47 / 0,53	0,48 / 0,52
s009 / 577 bytes	0,**51** / 0,49	0,47 / 0,53	0,48 / 0,52	0,46 / 0,54

всего пространства, так же как и второй класс, класс спама занимает вторую половину. Отсюда следует, что необученный нейросетевой детектор при поступлении на его вход неизвестного образа будет соотносить его равновероятно как одному классу, так и ко второму, т.е. на выходах его мы получим значения равные $Y_1 = 0,5$ и $Y_2 = 0,5$. Обученный же нейросетевой детектор для спама будет иметь значение $Y_2 > 0,5$, а для нормального письма $Y_1 > 0,5$.

Анализируя результаты проведенных экспериментов, можно заметить некоторую тенденцию: файлы большего размера классифицируются корректней, чем файлы меньшего размера. С чем это связано? Это связано с принципом работы LVQ нейронной сети. Для того, чтобы найти связь между данными внутри файла и, в зависимости от обнаруженной связи, корректно классифицировать неизвестный образ, LVQ должна иметь достаточное количество данных. А в таких спам-письмах как, например, «посети нашу страницу!» недостаточное количество данных для корректной классификации с помощью ИНС.

Выводы. Разработан метод обнаружения нежелательных электронных писем. Классификация производится на основе детекторов, построенных с применением методов искусственных нейронных сетей. Преимуществом такого подхода является высокая точность обнаружения спам-писем благодаря свойству искусственных нейронных сетей находить взаимосвязь между различными данными. К недостаткам разработанного метода можно отнести неспособность к корректной классификации небольших по размеру, содержащих всего несколько слов, писем. Для обнаружения таких нежелательных электронных писем необходимо использовать другие существующие методы, например, каталог запрещенных слов.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Спам // Википедия [Электронный ресурс]. – 2008. – Режим доступа: http://ru.wikipedia.org/wiki - Дата доступа: 20.09.2008.
2. Spammers Continue Innovation: IronPort Study Shows Image-based Spam, Hit & Run, and Increased Volumes Latest Threat to Your Inbox // IronPort [Электронный ресурс]. – 2008. — Режим доступа: http://www.ironport.com/company/ironport_pr_2006-06-28.html - Дата доступа: 18.09.2006.
3. С.В. Безобразов. Применение искусственных иммунных систем для обнаружения вирусов // Вестник БрГТУ. Физика, математика, информатика.-2005.- №5(35).-С.66-70.
4. What is the effect of Bayesian poisoning? // Sunbelt Blog [Электронный ресурс]. – 2008. – Режим доступа: http://sunbeltblog.blogspot.com/2006/08/does-bayesian-poisoning-exist-maybe.html - Дата доступа: 20.09.2008.
5. Spam Filtering II [Электронный ресурс]. – 2005. – Режим доступа: —http://web.archive.org/web/20050307062526/http://sam.holden.id.au/writings/spam2/ - Дата доступа: 19.09.2008.
6. Chhabra, S., Yerazunis, W. S., and Siefkes, C. 2004. Spam Filtering using a Markov Random Field Model with Variable Weighting Schemas. In Proceedings of the Fourth IEEE international Conference on Data Mining (November 01 - 04, 2004). ICDM. IEEE Computer Society, Washington, DC, 347-350.
7. The CRM114 Discriminator // The Controllable Regex Mutilator [Электронный ресурс]. – 2008. – Режим доступа: http://crm114.sourceforge.net/ - Дата доступа: 19.09.2008.
8. Distributed Checksum Clearinghouses [Электронный ресурс]. – 2005. – Режим доступа: http://www.rhyolite.com/dcc/ - Дата доступа: 17.09.2008.

9. Vipul's Razor Homepage [Электронный ресурс]. – 2008. – Режим доступа: http://razor.sourceforge.net/ - Дата доступа: 17.09.2008.
10. Recurrent Pattern Detection Technology (RPD™) // CommTouch [Электронный ресурс]. – 2008. – Режим доступа: http://www.commtouch.com/site/Products/technology.asp - Дата доступа: 18.09.2008.
11. В.А. Головко. Нейронные сети: обучение, организация и применение. Кн. 10: Учеб. пособие для вузов / Общая ред. А. И. Галушкина. - М.: ИПРЖР, 2000. –С.114-129.
12. Е. Касперский. Компьютерное зловредство. – СПб.: Питер, 2007. - 208 с.
13. Kohonen T. Sell-organised formation of topologically correct feature maps// Biological Cybernetics. - 1982. - N43.-P.59-69.

Материал поступил в редакцию 23.09.08

GOLOVKO V.A., BEZOBRAZOV S.V., MELENCHUK V.V. Neural network approach for spam detection

The neural network approach for spam detection is described. The most used up-to-date methods for spam detection is examined. The weaknesses of described method for spam detection are showed. Spam detection system based on artificial neural networks applying is designed. Research results are submitted.

УДК 004.75:004.451

Отвагин А.В., Пынькин Д.А.

СРЕДСТВА СОЗДАНИЯ ВИРТУАЛЬНОГО ОПЕРАЦИОННОГО ОКРУЖЕНИЯ ДЛЯ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Введение. Современный этап развития вычислительной техники и скорость обновления вычислительных ресурсов приводит к тому, что многие организации, предоставляющие коллективный доступ к высокопроизводительным вычислениям, тратят значительные средства на поддержку и эксплуатацию вычислительных и коммуникационных систем. В этих условиях абсолютно необходимо внедрять современные технологии, обеспечивающие снижение расходов на поддержание компьютерной инфраструктуры. Вместе с тем вычислительные центры, организованные на базе различных аппаратных и программных платформ, могут существенно снизить производительность вычислений из-за отсутствия унифицированной вычислительной среды, что приводит к заметному снижению экономического эффекта использования таких центров. По этой причине многие вычислительные центры не стремятся своевременно модернизировать свое оборудование и вводить в эксплуатацию новые мощности.

Одной из перспективных технологий освоения и внедрения новых вычислительных ресурсов является виртуализация. Применение виртуализации позволяет добиться снижения стоимости вычислительных ресурсов, повышения производительности и адаптации имеющихся ресурсов к постоянно изменяющимся запросам пользователей. В настоящее время уже созданы базовые технологии виртуализации, и она становится все более эффективной, гибкой и надежной [1].

Технология виртуализации предназначена для запуска на одной аппаратно-операционной платформе нескольких операционных систем и/или приложений для них в независимых разделах; в этом случае физическая вычислительная система рассматривается как множество виртуальных. Пользователь при этом эксплуатирует свои приложения в собственном независимом разделе под управлением определенной версии операционной системы (ОС), а новые программные средства будут работать в другом разделе под управлением, возможно, другой версии или совершенно отличной по архитектуре ОС. Особенности эксплуатации новых приложений или системного программного обеспечения (ПО) не оказывают влияния на функциональность прежних версий, а необходимость поддержки устаревшего лицензионного ПО или оборудования не ограничивает возможности внедрения новых программных средств. Виртуализация позволяет инкрементальную модернизацию вычислительных средств, не ограничивая общую производительность системы.

Одним из преимуществ виртуализации является также возможность использования ее в качестве средства встраивания существующих вычислительных ресурсов в глобальные информационно-коммуникационные структуры, так называемые ГРИД-системы [2]. В этом случае виртуализация призвана сгладить отличия конкретной технологии организации высокопроизводительных ресурсов и гарантировать единое прозрачное представление ресурса для пользователя.

1. Выбор технологии виртуализации операционного окружения. Виртуализация является основным способом повысить производительность и эффективность использования вычислительных систем без кардинальной замены аппаратного обеспечения. Технология виртуализации основана на применении виртуальных машин (ВМ) – комплекса программных средств, обеспечивающих функционирование ПО, разработанного под конкретную программно-аппаратную платформу, в окружении, создаваемом с помощью ВМ [3, 4]. Основные цели виртуализации и преимущества, предоставляемые ее использованием, - это [5]:

1. Изоляция и абстрагирование аппаратного обеспечения. Предоставляя абстракцию аппаратуры, ВМ одновременно изолируют хостовую (базовую) ОС от реального аппаратного обеспечения, позволяя проводить обновление вычислительных мощностей без потери работоспособности ОС.
2. Использование ПО, ориентированного на уникальные архитектуры и ОС. В настоящее время вывод системного ПО из эксплуатации (например, из-за обновления аппаратной базы), приводит к немедленному прекращению использования программ, разработанных под данную платформу. Технология виртуализации позволяет эмулировать аппаратуру, для которой предназначено устаревшее системное ПО, тем самым обеспечивая его корректное функционирование на новых вычислительных ресурсах.
3. Тестирование нового системного ПО. Установка или адаптация нового системного ПО на вычислительные ресурсы, находящиеся в эксплуатации, прежде всего, требует периода тестирования, позволяющего судить о пригодности выбранных для обновления программных средств. Тестирование может выполняться на ВМ, специально выделенной для испытания нового ПО, тем самым, предохраняя общие вычислительные ресурсы от прекращения их корректного функционирования. Наличие нескольких тестовых ВМ позволяет разделить работу между тестировщиками и ускорить процессы миграции на новое ПО.
4. Экономия энергоресурсов. Вместо выделения отдельных разделов вычислительного центра, предназначенных для решения задач конкретной аппаратно-операционной платформы, виртуализация обеспечивает прозрачную эксплуатацию вычислитель-

***Отвагин А.В.**, старший научный сотрудник Объединенного института проблем информатики НАН Беларуси.*
Беларусь, ОИПИ НАН Беларуси, 220012, г. Минск, ул. Сурганова, 6.
***Пынькин Д.А.**, ассистент Белорусского государственного университета информатики и радиоэлектроники.*
Беларусь, БГУиР, 220013 г. Минск, ул. П.Бровки 6.