Технология представления результатов сетевого мониторинга в Интернете. Результаты

Терентьев Александр Макарович, кандидат технических наук, PhD
Центральный экономико-математический институт Российской академии наук (г.Москва)

Аннотация. *В статье показаны результаты применения программ системной службы и управления системной службой web-сервера, созданных на языках высокого уровня PowerBASIC для передачи информации сетевого мониторинга на общедоступный web-сервер. Статья продолжает предыдущий опубликованный материал.*

Ключевые слова: *сетевой мониторинг, информационная безопасность, UDP, web-сервер, системная служба.*

Идея круглосуточного низкоуровневого (на канальном уровне ISO/OSI) сетевого мониторинга с использованием постоянно работающей наблюдающей станции (НС) в качестве одного из основных средств информационной безопасности [1] была высказана автором сразу после реализации пилотного проекта [2] программных средств.

Возможность дампировать в реальном режиме времени на жёсткий диск НС наблюдаемые сетевые пакеты и затем спокойно разбираться побайтно с их составом сразу же очертила сферы многочисленных возможных приложений сетевого мониторинга [3] локальной вычислительной сети (ЛВС). После доведения программных средств до уровня промышленной разработки [4-6], были поставлены многочисленные разноплановые эксперименты [7-14], подробнее см. [26]. Развитие системы сетевого мониторинга в ЦЭМИ РАН помогло решить целый ряд крупных задач, в том числе дефрагментацию ЛВС [7], внедрить автоматическое исключение зараженных ПК из ЛВС с помощью управления коммутатором Cisco Catalyst [15] и корпоративный вариант технологии снабжения пользователей научных учреждений антивирусными средствами [16-18].

Финальный вариант был описан в [6] и [15]. Особенности мониторинга в условиях, когда центральный хаб заменён на современный коммутатор Cisco Catalyst, приведены в [19]. Некоторые проблемные следствия этого изменения показаны в [14]. Дополнительные действия в связи с решением проблем освещены в [22].

Данный цикл статей посвящён проблеме создания эффективного средства передачи данных по ЛВС от ПК с Мониторной программой (МП) к web-серверу.

Первый вариант связи МП↔Сервер с помощью UDP описан в [21]. В этот момент серверную часть исполняло обычное Windows-приложение. Такое решение неоптимально для сервера: для начала работы обычного приложения необходимо выполнить процедуру входа в систему пользователя (Logon), что не отвечает требованиям информационной безопасности сервера, он становится общедоступным для физически находящегося рядом с ним персонала и случайных посетителей. Поэтому, опираясь на уже сделанную работу, встала задача обеспечить взаимосвязь между компьютером с МП и сервером на новом, закрытом от пользователей и случайных людей, уровне.

Для исполнения этого, на web-сервере реализованы 3 программы:

– системная служба TAM LAN Server Service, исполняющая UDP-связь с МП и периодически сбрасывающая актуальную информацию на диск в виде текстового файла определённого формата [26];

– программа управления вышеуказанной системной службой TAM LAN Server Control, являющаяся обычным Windows-приложением и работающая только после исполнения входа в систему (Logon) администратора [27];

– CGI-программа формирования выходной формы по состоянию текстового файла на диске, оставшаяся от прежнего варианта связи МП↔Сервер.

Преимущество такой схемы состоит в том, что системная служба начинает работу сразу же при загрузке сервера, до выполнения процедуры Logon, обеспечивая связь с МП. Программа управления системной службой может быть не загружена, что не мешает работе системной службы и исполнению передачи оперативных данных на сервер. Таким образом, функционирование сервера уже не зависит от места его установки.

Как системная служба, так и программа управления ею выполнены на хорошо известном мировым профессионалам-программистам языке PowerBASIC [23], позволяющим создавать эффективные приложения как консольного типа (компилятор PowerBASIC Console Compiler, автор использует версию 5.05), так и полноценные GUI-приложения (компилятор PowerBASIC for Windows 9.05). Являясь мощной альтернативой языку среднего уровня C++, PowerBASIC предлагает язык высокого уровня, специфицированный для создания Windows-приложений благодаря встроенной поддержке множества обращений к различным библиотекам Windows [26]. Собственно говоря, все модули сетевого мониторинга с начала его создания (1999г) были написаны на различных диалектах этого языка, при необходимости дополняясь процедурами на Макроассемблере [5]. Так, модули НС были написаны на PowerBASIC for DOS. Все версии компиляторов являются платными (порядка $100 за каждую), лицензирование осуществляется вендором исключительно персонально для каждого пользователя.

Основные информационные потоки, действующие при сетевом мониторинге, отображены на рис. 1. Сплошные линии представляют собой стандартные связи по TCP/IP. Зелёная штрих-пунктирная линия отображает информацию, поступающую по мониторному порту коммутатора на наблюдающие станции (НС), основную и дополнительную. Необходимо отметить, что использование хаба (а не современного свитча) для разделения потоков на этом этапе служит точному мультиплицированию просматриваемых пакетов. Голубые точки от основной НС к рабочему

ПК с МП показывают связь по serial-кабелю НС с МП, исполняемой как Windows-приложение и, стало быть, способной передавать далее данные, используя сетевые технологии Windows. Фиолетовая точечная линия от МП на Антивирусный сервер показывает, собственно, описываемую в данном цикле работ взаимосвязь с системной службой web-сервера, агрегируя исходные данные НС. Красным пунктиром показано управление коммутатором Cisco Catalist 2950 для отключения поражённых компьютеров от локальной сети, исполняемое той же МП в автоматическом режиме.

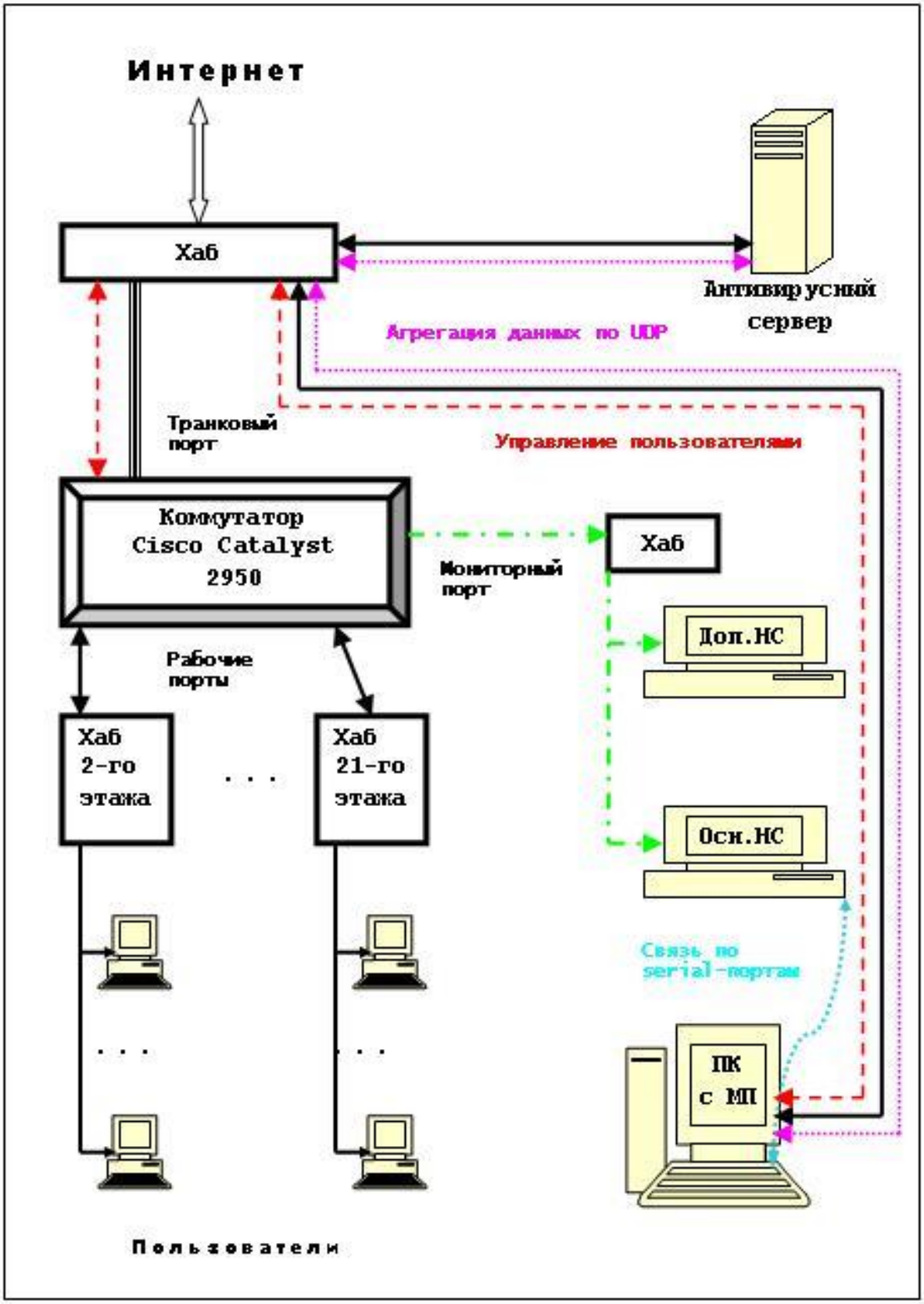

Рис. 1. Информационные потоки при сетевом мониторинге

Рис. 2. Вид окна мониторной программы

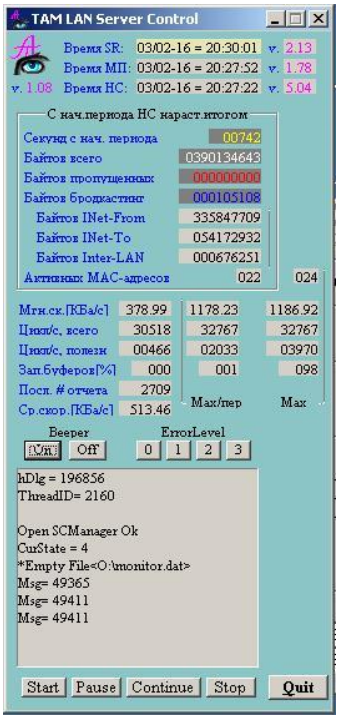

Рис. 3. Вид окна программы управления серверной службой TamObSsC

Мониторная программа, принимающая информацию от НС, исполняется как полнооконное (GUI-) приложение на рабочем компьютере. Современный вид её окна приведён на рис. 2. Поскольку МП обменивается информацией как с НС, так и с серверной службой, есть возможность отображения в блоке служебной информации текущего времени НС и текущего времени сервера.

Вид окна программы управления серверной службой показан на рис. 3. Изображения рисунков 2 и 3 сняты с небольшим интервалом по времени. Легко заметить сходность основных наблюдаемых показателей.

В процессе своей работы, серверная служба создаёт изменяемый при каждой новой пришедшей порции данных файл на рабочем диске. В целях экономии ресурсов, этот рабочий диск O: является виртуальным и создаётся в оперативной памяти, чтобы не перегружать дисковую систему сервера. При вызове соответствующей функции Антивирусного сервера, запускается CGI-программа, которая считывает текущее состояние этого рабочего файла и отображает в виде HTML-кода. Сокращённый текст CGI-программы показан на рис. 4. Обратите внимание на оператор <meta http-equiv="Pragma" content="no-cache"> и последующий, благодаря которым формируемое изображение берётся не из кэша браузера, а запрашивается с web-сервера заново каждые 5 секунд с новыми данными.

Окно, появляющееся в браузере при просмотре агрегированных данных, также слегка изменено по сравнению с приведённым в [21, рис. 15] и в настоящее время имеет вид рис. 5.

Верхние три строки показывают текущее время на Антивирусном сервере, ПК с Мониторной программой и наблюдающей станции. Небольшое расхождение времени вполне естественно, хотя бы по причинам, отмеченным в [2].

Следующий блок информации показывает данные очередного 15-минутного периода наблюдения: сколько прошло секунд с начала периода и сколько различных типов информации обработано (например, из Интернета скачано 47,652,028 байтов из обработанных 64,304,570). Тут же указан последний номер сформированного НС текстового отчета. Пожалуй, это самые информативные показатели для стороннего пользователя.

Третий блок информации содержит только один показатель – среднюю скорость в сети, рассчитанную с начала периода. В данном примере значение 84.86 килобайтов в секунду – очень низкая скорость, что вполне понятно из-за времени суток снятия скриншота.

Последний блок информации содержит ряд интегральных данных по трём позициям (столбцам): за последнюю секунду, за последний 15-минутный период и за всё время последнего включения НС с начала суток. Максимальная мгновенная скорость 1184.7 показывает практически полное насыщение ЛВС в текущих условиях наблюдения [19] через мониторный порт коммутатора. Максимальное количество полезных циклов в секунду 2883 при том, что за 1 цикл обрабатывается 1 датаграмма (пакет) длиной не более 1500 байт, показывает максимальный объём обработанной информации в секунду.

Максимальный за сутки процент задействования буферов НС (15%) показывает, что станция имеет значительный резерв нагрузки. Нули в графе «Пропущено» второго блока подтверждают этот тезис.

Наконец, число активных устройств в ЛВС в ночное время фактически равно числу серверов и постоянно включенных ПК. Обратим внимание на то, что сутки начались в 00:00:00, т.е. 3 часа назад по отношению ко времени получения скриншота, поэтому 20 устройств – вполне реальное число, учитывая два антивирусных сервера, рабочий ПК антивирусной службы с МП, ряд коммутаторов, имеющих собственный IP-адрес, 3 роутера сегментов сети, дежурные компьютеры Сетевого информационного центра ЦЭМИ РАН и прочие серверы.

Получение информации в МП от НС идёт ежесекундно. Соединение МП↔Сервер срабатывает каждые 5 секунд.

```
#!/perl/bin/perl
#r4mon.cgi
################
$LOCK_EX=2;
$LOCK_UN=8;
$datafile="O:/monitor.dat";
#########
 open(DATA,"+<$datafile");
 flock(DATA,$LOCK_EX);
 $Dat=<DATA>;
 chop($Dat);
 flock(DATA,$LOCK_UN);
 close(DATA);
####### Распределяем список по элементам и убираем сигнальный символ
 @Var=split(/,/,$Dat,30);
 $Var[6]=substr($Var[6],2);
print "Content-Type: text/html; charset=windows-1251\n\n";
print "<HTML><HEAD>\n";
print '<meta http-equiv="Pragma" content="no-cache">'; print "\n";
print '<meta http-equiv="Refresh" content="5">'; print "\n";
.....
print "<TITLE>Текущий мониторинг ЛВС ЦЭМИ РАН</TITLE>\n";
print "<body bgcolor=#0066FF lang=RU style='font-size:10pt'><center>\n";
.....
print "<TABLE cols=1 border=3 bgcolor=#00CCFF bordercolor=#0099CC>\n";
print "<TR><TD>\n";
print "<table cols=3 border=3 bgcolor=#99CCFF bordercolor=#333399"
print " cellspacing=1 cellpadding=3 rules=rows frame=box width=100%>\n";
print "<col align=left><col align=left><col align=right>\n";
.....
print "<tr><th align=left rowspan=3 width=25%><small>"
print "Текущ. время, версия</small></th><th><small>Сервер</small></th>";
print '<td style="color:#006600; font-weight:bold; font-size:10pt">';
print "$Var[0]"; print "</td>\n";
.....
print "$Var[20]"; print "</td>\n";
print "</table>\n";
print "</TABLE></CENTER></BODY></HTML>\n";
```

Рис. 4. Текст CGI-программы, отображающей сводные данные ЛВС

Рис. 5. Вид окна агрегации на Антивирусном сервере

Системная служба обновляет рабочий файл на сервере синхронно с получением очередной информации по UDP. Отображение окна рис. 5 обновляется с интервалом в 5 секунд, в чем можно убедиться непосредственно [24].

Актуальные на момент первоначального написания тексты программ зарегистрированы в ФИПС. Следует отметить, что автор не претендует на открытие собственной техники программирования системных служб: часть приведённых программных решений заимствована из многолетних обсуждений на международном форуме программистов по языку PowerBASIC. Конечно, эти решения адаптированы под требования конкретной реализации и использованные версии компиляторов.

Таким образом, основные агрегирующие данные сетевого мониторинга в ЛВС ЦЭМИ РАН сделаны возможными для наблюдения любыми пользователями Интернета. Программные средства реализованы на языке высокого уровня PowerBASIC, имеющем диалекты создания консольных и полнооконных приложений. Работа указанных программ проверена в средах Microsoft Windows 2000 Server и Microsoft Windows Server 2003 R2.

Большинство работ автора, приведённых в списке Литературы, доступны для чтения в разделе «Литература» Антивирусного сайта ЦЭМИ РАН [25].

Литература:

1. Терентьев А.М. Информационная безопасность в крупных локальных сетях. // «Концепции», N1(9)-2002, с.25-30. Свидетельство Роскомпечати 014305.

2. Терентьев А.М. Методы и средства наблюдения загрузки локальных вычислительных сетей на примере ЦЭМИ РАН. / Препринт #WP/2001/110 - М., ЦЭМИ РАН, 2001, - 74с. ISBN 5-8211-0141-7.

3. Терентьев А.М. Задачи полноценного аудита корпоративных сетей // «Концепции», N1(11)-2003, с.94-95. Свидетельство Роскомпечати 014305.

4. Терентьев А.М. Построение и развитие системы сетевого мониторинга. / Развитие и использование средств сетевого мониторинга. Вып.1 Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2004, с.5-23. ISBN 5-8211-0317-7.

5. Терентьев А.М. Ускорение форматных преобразований в системах реального времени, реализованных на языке PowerBASIC для i386+. / Развитие и использование средств сетевого мониторинга. Вып.1 Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2004, с.24-36. ISBN 5-8211-0317-7.

6. Терентьев А.М. Мониторная программа как средство интеграции данных наблюдающей станции в локальной сети. / Развитие и использование средств сетевого мониторинга. Вып.2. Сб. статей под ред. М.Д.Ильменского. — М.: ЦЭМИ РАН, 2005, с.6-13. ISBN 5-8211-0365-7.

7. Вегнер В.А., Ляпичева Н.Г., Львова А.С., Терентьев А.М. Разработка и реализация типового проекта выделенного сегмента ЛВС например ПК административно-финансовой группы ЦЭМИ РАН. / Развитие и использование средств сетевого мониторинга. Вып.1. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2004, с.88-101. ISBN 5-8211-0317-7.

8. Терентьев А.М. Опыт сетевого экспресс-мониторинга с помощью переносной наблюдающей станции. / Развитие и использование средств сетевого мониторинга. Вып.1. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2004, с.41-46. ISBN 5-8211-0317-7.

9. Терентьев А.М. Об одной побочной возможности использования ARP-пакетов. / Развитие и использование средств сетевого мониторинга. Вып.1. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2004, с.37-40. ISBN 5-8211-0317-7.

10. Ляпичева Н.Г., Терентьев А.М. Исследование сетевых сервисов на примере клиентского почтового протокола POP3. / Развитие и использование средств сетевого мониторинга. Вып.1. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2004, с.60-74. ISBN 5-8211-0317-7.

11. Терентьев А.М. Возможность полуавтоматического управления сетевыми коммутаторами Cisco Catalyst. / Развитие и использование средств сетевого мониторинга. Вып.2. Сб. статей под ред. М.Д.Ильменского. — М.: ЦЭМИ РАН, 2005, с.14-27. ISBN 5-8211-0365-7.

12. Терентьев А.М. Консоль управления сетевыми коммутаторами Cisco. / Развитие технологий и инструментальных средств информационной безопасности. Вып.1. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2010, с.6-20. ISBN 978-5-8211-0543-1.

13. Ляпичева Н.Г. Выбор Интернет-провайдера на основе измерения трафика / Развитие и использование средств сетевого мониторинга и аудита. Вып. 3. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2006, с.36-49. ISBN 5-8211-0409-2 (978-5-8211-0409-0).

14. Ляпичева Н.Г., Акиншин А.А., Терентьев А.М., Григорьев П.В. Коррекция ошибок HTTP-соединения в локальной сети ЦЭМИ РАН. / Развитие технологий и инструментальных средств информационной безопасности. Вып. 2. Сборник статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2012. — С.49-58.

15. Терентьев А.М. Автоматическая изоляция некорректных объектов КВС по информации сетевого мониторинга. / Развитие технологий и инструментальных средств информационной безопасности. Вып. 3. Сборник статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2012. — С.6-15. ISBN 5-8211-0409-2 (978-5-8211-0409-0).

16. Терентьев А.М. Корпоративный вариант реализации антивирусных пакетов Doctor Web в научных учреждениях: предпосылки. // «Национальные интересы: приоритеты и безопасность». — М.:Издательский дом «Финансы и кредит», N17(206), 2013, с.41-48, ISSN 2073-2872.

17. Терентьев А.М. Корпоративный вариант реализации антивирусных пакетов Doctor Web в научных учреждениях: реализация. // «Национальные интересы: приоритеты и безопасность». — М.:Издательский дом «Финансы и кредит», N19(208), 2013, с.40-45, ISSN 2073-2872.

18. Терентьев А.М. Корпоративный вариант реализации антивирусных пакетов Doctor Web в научных учреждениях: результаты. // «Национальные интересы: приоритеты и безопасность». — М.:Издательский дом «Финансы и кредит», N20(209), 2013, с.41-46, ISSN 2073-2872.

19. Терентьев А.М., Ляпичева Н.Г., Кочетова Н.А. Мониторинг корпоративной сети ЦЭМИ РАН в условиях использования коммутатора Cisco Catalyst. / Развитие и использование средств сетевого мониторинга и аудита. Вып.1. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2004, с.60-74. ISBN 5-8211-0317-7.

20. Управление сетевой средой Microsoft Windows 2000. Учебный курс MCSA/MCSE/пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2003.

21. Терентьев А.М., Львова А.С. Адекватное отображение на технологическом www-сервере событий реального времени. / Развитие и использование средств сетевого мониторинга и аудита. Вып.3. Сб. статей под ред. А.М.Терентьева. — М.: ЦЭМИ РАН, 2006, с.50-59. ISBN 5-8211-0409-2.

22. Терентьев А.М. Поддержание доступности HTTP-соединения с помощью периодического пингования. // XXIV Международная научная конференция «Современные концепции научных исследований» — М.: «Евразийское научное объединение», N2(24), 2017. Т.1, с.37-39. ISSN 2411-1899.

23. [Интернет-ресурс] Международный сайт языка программирования PowerBASIC: http://www.powerbasic.com.

24. [Интернет-ресурс] Вызов периодически меняющегося отображения результатов сетевого мониторинга в браузер пользователя: http://av.cemi.rssi.ru/av/r4mon.cgi.

25. [Интернет-ресурс] Антивирусный сайт ЦЭМИ РАН: http://av.cemi.rssi.ru

26. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Системная служба. // XXVII Международная научная конференция «Стратегии устойчивого развития мировой науки» — М.: "Евразийское научное объединение", N5(27). 2017. Т.1, с.41-46. ISSN 2411-1899.

27. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Программа управления системной службой. // XXVIII Международная научная конференция «Интеграция науки в современном мире» — М.: "Евразийское научное объединение", N6(28). 2017. Т.1, с.28-33. ISSN 2411-1899.