А.М. Терентьев

СЕТЕВОЙ МОНИТОРИНГ. РАЗВИТИЕ И ПРИМЕНЕНИЯ

ТОМ 2

Федеральное государственное бюджетное учреждение науки
«Центральный экономико-математический институт РАН»

А.М. ТЕРЕНТЬЕВ

Сетевой мониторинг. Развитие и применения. Том 2

Монография

Чебоксары
Издательский дом «Среда»
2020

УДК 004.42
ББК 32.973.5
Т35

Рецензенты:

Хрусталёв Евгений Юрьевич, д-р экон. наук,
г.н.с. ФГБУН «Центральный экономико-математический институт РАН»

Тельнов Юрий Филиппович, д-р экон. наук,
зав. кафедрой прикладной информатики
и информационной безопасности ФГБОУ «Российский экономический университет им. Г.В. Плеханова»

Терентьев А.М.

Т35 **Сетевой мониторинг. Развитие и применения. Т. 2**: монография / А.М. Терентьев. – Чебоксары: ИД «Среда», 2020. – 108 с.

ISBN 978-5-907313-11-8

В данной работе описана оригинальная технология круглосуточного отслеживания сетевых пакетов, циркулирующих в локальной сети.

Технология базируется на выделенной рабочей станции, работающей в MS-DOS и принимающей все доступные пакеты. Агрегированные данные передаются на соседний Windows-компьютер через serial-соединение. Мониторная программа на этом Windows-ПК способна отследить заражённые ПК и выполнить действия по отключению их от локальной сети. Эта функция исполняется с помощью коммутатора Cisco.

В данном томе описываются различные научно-практические исследования, позволившие создать профессиональный пакет сетевого мониторинга, а также важнейшие его результаты, опробованные и внедрённые в институте.

За проведённые исследования по данной тематике в 2003 г автор удостоен учёного звания “Doctor of Philosophy” Европейской Академии информатизации (Брюссель).

Монография рекомендована к печати Учёным советом Федерального государственного бюджетного учреждения науки ЦЭМИ РАН.

ISBN 978-5-907313-11-8
DOI 10.31483/a-147

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Использование персональных компьютеров (ПК) практически во всех научных и производственных единицах немыслимо без задействования специальных средств их объединения в единую локальную вычислительную сеть (ЛВС) предприятия. Общение через ЛВС каждого ПК, сервера или иного сетевого устройства требует наличия в нём сетевого адаптера – специальной платы с характеристиками, соответствующими типу сетевых соединений. Сетевое устройство с сетевым адаптером (ПК, сервер, сетевой принтер, каждый сетевой выход коммутатора и т.п.) будем называть нода[1].

Современные средства организации ЛВС могут также включать различные сетевые устройства, организующие ЛВС и выход в Интернет – коммутаторы, маршрутизаторы, хабы, свитчи и др. Эти устройства делают для каждой ноды возможность иметь доступ к другим.

Обмен информацией по ЛВС подробно рассмотрен в томе 1 данной работы [1]. Показано, что по умолчанию сетевые адаптеры настроены так, чтобы принимать либо сетевые пакеты, адресованные «всем» (broadcasting), либо данной ноде-устройству. Для этого, каждый сетевой адаптер имеет свой, уникальный в мире, технологический MAC-адрес (Media Access Control Address), используемый на нижних уровнях модели ISO-OSI. Для идентификации ноды на верхних уровнях ISO-OSI используется IP-адрес (Internet Protocol Address), уникальный внутри ЛВС или во всём мире.

Особенности организации локальных сетей также рассмотрены в [1]. Там же определён термин корпоративная сеть учреждения (КВС), введённый автором ранее [2]. Далее было показано, что принципиально возможно техническое решение, при котором некоторый ПК, называемый Наблюдающей станцией (НС), принимает *все* пакеты, циркулирующие в сети. На базе этого решения создан прототип сетевого мониторинга – программы, наблюдающей проходящие пакеты, с возможностью дампировать все или избранные из них на HDD для последующего подробного анализа.

[1] Этот термин, как и множество других (E-Mail, смайлик и пр.) пришёл в Интернет из самодеятельной международной сети FIDOnet (1985 г). Вместо IP-адреса там был общемировой аналог, например, автор данной работы известен, в частности, под адресом **2:5020/614.13**.

Физический обмен данными осуществляется с высокой скоростью, от 10Мбит/с до 1Гбит/с. В обычной работе, конечный пользователь не имеет возможности просмотреть конкретное содержимое пакетов во время обмена и проанализировать все уровни соглашений модели ISO-OSI. Однако, созданная разработка даёт такую принципиальную возможность.

Программа сетевого мониторинга создавалась и отлаживалась на невысоких сетевых скоростях и ПК со слабыми по отношению к настоящему моменту ресурсными характеристиками (Pentium-90, AMD-DX4/120 и т.п.). Для обеспечения нормальной работы требовалось превратить созданный прототип в мощную полнофункциональную программу. Под это направление автором был получен грант РФФИ 04-07-90260в, и с 2004 по 2006 гг был выполнен ряд существенных преобразований пилотного проекта в высокопрофессиональный пакет. Эти преобразования рассмотрены в Главе 1.

С течением времени, схема подключения компьютеров и структура локальной сети ЦЭМИ РАН несколько раз изменялась. Средства сетевого мониторинга обязаны были быть адаптированными к актуальным изменениям.

Данный том работы посвящен созданию профессиональных средств сетевого мониторинга на основе существующего прототипа и их адаптации к модификациям существующей в ЦЭМИ РАН КВС.

Таким образом, **объектами данного исследования** являлись, с одной стороны, развивающиеся глобальная и локальные вычислительные сети института, и, с другой стороны, особенности эксплуатации НС в этих сетях.

Достигнутые результаты излагаются в последовательности их получения. В данном томе сосредоточены сведения о развитии структуры ЛВС, научные исследования по созданию, развитию и оптимизации технических средств сетевого мониторинга на базе существующей и модифицируемой корпоративной вычислительной сети. **В результате исследований** были созданы необходимые технические средства, модифицированы необходимые программные средства и достигнута **цель работы** – создан полноценный комплекс программно-технических и организационных решений, обеспечивающий круглосуточное наблюдение и регистрацию биллинговых параметров исследуемой сети. Достигнута желаемая **степень внедрения** – результаты проведенных исследований нашли практическое применение в институте. **Итоги внедрения** – результаты исследований

использовались в широком спектре, как для биллинговых статистических исследований, так и для реформирования корпоративной вычислительной сети института.

Возможная **область применения** работы – распространение созданного технического решения на другие организации – достигнута в ходе разработки. Проведены опытные работы по внедрению созданных средств мониторинга в других организациях.

Экономическую **эффективность** работы – не представляется возможным определить вследствие уникальности проведённых исследований и выполненных работ. Сама возможность фиксировать реально протекающие с большой скоростью процессы в локальной сети и впоследствии детально выполнять отложенный их анализ представляет качественно новый метод исследования сетевых потоков.

Сфера практического применения весьма разнообразна, от выявления некорректно настроенных компьютеров с возможностью их автоматического отключения до фиксации сетевых атак и необходимости реорганизации локальной сети. Большинство применений сетевого мониторинга рассмотрено в данном томе, возможность автоматического отключения будет рассмотрена позднее в Томе 3.

ГЛАВА 1. РАЗВИТИЕ СЕТЕВОГО МОНИТОРИНГА

Выбор и нацеленность средств сетевого мониторинга заявлены в программной работе [3]. К таковым можно отнести следующие.

1. Оптимизация построения корпоративной сети:

- Постоянный замер общего трафика, выявление пиковых нагрузок.
- Выявление наиболее загруженных участков сети, возможно, тормозящих общий трафик.
- Выявление «зацикливаний» при передаче пакетов в сети.

2. Экономические (биллинговые) приложения:

- Учёт трафика интересующей группы ПК.
- Суммарный учёт Интернет-трафика, возможно, по подразделениям организации (института).
- Учёт трафика, специализированного по нужному критерию (SQL-сервер, ресурсные системы Интернета, локальная почта и т. д.).

3. Информационная безопасность:

- Выявление некорректно настроенных ПК и/или серверов.
- Выявление некорректно работающих сетевых устройств.
- Выявление вирусной активности в сети с определением источника.
- Индикация неработоспособности («падения») серверов.
- Отслеживание попыток взлома, нерегламентированных доступов, хакерских атак.

Описанные задачи представляются наиболее интересными и не исчерпывают, разумеется, всех возможностей сетевого мониторинга. Значительную часть поставленных задач удалось решить в ходе разработки и внедрения этого программного средства. Для корректного решения поставленных задач, представляется, система аудита и мониторинга должна отвечать следующим требованиям.

- Она должна быть способна принимать не только корректные и «логичные», но именно все сетевые пакеты, включая коллизионные и ошибочные. Информация о некорректно настроенных сетевых устройствах крайне важна в практической работе сетевых администраторов.

▪ Задача аудита должна решаться круглосуточно, без перерывов, поставляя периодические отчеты без прекращения своей основной работы.

▪ Технические и программные средства решения задач мониторинга/аудита не должны зависеть от работоспособности прочих сетевых устройств, в том числе серверов. Функциям аудита не должны мешать прочие задачи, исполняемые на тех же технических средствах.

▪ Задача мониторинга не должна быть зависима от текущего состояния сети, и сама не должна использовать внутрисетевые средства передачи информации.

Основываясь на указанных ограничениях, был создан прототип системы мониторинга корпоративной сети. Созданный прототип, как показано в [1], успешно решал задачи мониторинга при невысоких сетевых скоростях порядка Vcp^2 30-50 КБ/с.

Однако, число отказанных к обработке пакетов нелинейно возрастало с повышением этой скорости. Актуальной задачей создания полноценного функционального пакета стала необходимость резкого повышения его эффективности. Данная глава посвящена проблеме превращения пилот-проекта в полнофункциональное, оптимизированное в работе средство.

1.1. Подбор средств программирования в программе мониторинга

IBM PC сравнительно редко избирается для решения задач обработки данных в реальном времени. Огромное большинство созданных приложений либо ориентировано на интерактивную обработку данных (таковы все приложения, включенные в Microsoft Office), либо, в крайнем случае, снабжаются макросами или скриптами автоматического выполнения, причем задача скорейшего их выполнения в смысле соответствия асинхронным процессам попросту не ставится. Соответственно этому, многочисленные развивающиеся программные средства создания программных приложений целенаправленно не ориентированы на скорейшее выполнение операций, компиляторы с языков высокого уровня известных коммерческих фирм часто функционально не рассчитаны на задачи

[2] Все обозначения введены в [1] и подробно описаны там же.

реального времени, а входящие в их состав подключаемые библиотеки не оптимизированы по коду.

На практике, рекомендации по обеспечению задач реального времени сводятся к повышению мощности процессора и увеличению объёма оперативной памяти. Подобные рекомендации представляются недостаточно обоснованными в случаях, когда одним из существенных требований к проектируемой системе реального времени есть снижение стоимости обеспечивающих средств. Ниже в данной главе показано, что повышение мощности процессора далеко не всегда приводит к увеличению скорости потребных арифметических операций. Особенно ярко это видно на сравнении процессоров E8400 и E8500, когда последний, казалось бы, более быстрый, проигрывает по скорости вычислений. Возможной причиной является лучшее сопряжение с памятью у комплекта с E8400.

Автор считает, что резкое повышение мощности разрабатываемых систем реального времени можно осуществить за счет исправления функциональных недочетов среды разработки.

Типичным представителем описанного выше подхода является алгоритмический язык PowerBASIC [4] [5], развиваемый «PowerBASIC Inc.» с 1989 г. С 1993 г. появилась весьма удобная версия 3.00 компилятора, с 1995 – полнофункциональная версия 3.20 под MS-DOS, с 2000 г. поддерживается версия PowerBASIC 32-bit DLL Compiler и с 2002 г. – PowerBASIC for DOS 3.5, а также PowerBASIC 32-bit GUI Compiler. Особенностью всех указанных версий является наследование известного компилятора TurboBASIC фирмы «Borland International» (1987) по синтаксису и семантике, очень быстрые алгоритмы компиляции, принцип полуавтоматического подключения библиотек системных функций и процедур, постоянная работа над совершенствованием среды разработчика. Такая длительная (свыше 20 лет!) забота о классе «своих» пользователей встречается весьма редко и заслуживает высокой оценки.

Однако, практически всем рассмотренным (после Borland) версиям компиляторов свойственен ряд типичных программистских недочетов. Среди них – возложение функций по реструктуризации внутренних буферов переменных, в особенности текстовых, и «уборке мусора» на аппаратное прерывание по таймеру INT08;

отсутствие полновесных возможностей доступа к памяти переменных (типа оператора EQUIVALENCE), не всегда корректная работа с целочисленными словными переменными и неоптимальность форматных преобразований. Все эти недостатки, кроме первого из названных, могут быть обойдены при практическом программировании. Ряд усилий предпринимает сама фирма – например, начиная с версии 3.20 компилятора для DOS, введены аппараты пойнтеров и flex-строк. Недочеты в «уборке мусора» в целом не влияют на производительность, хотя мешают разработкам систем реального времени. А вот последний из названных недостатков может серьезно снизить производительность таких систем.

Автору пришлось непосредственно столкнуться с подобной проблемой при разработке средств мониторинга ЛВС в MS-DOS. Обрабатывающая программа, получая из сети пакеты информации асинхронно, обязана справляться с их обработкой, не допуская необработанных пакетов. При этом, после обработки каждого пакета корректируется ряд цифровых показателей на текстовом экране. Исследование временных затрат в рабочем цикле показало, что при средних скоростях 50-100 КБ/с (типовая скорость в малых и средних локальных сетях) отключение вывода на экран повышает скорость обработки принимаемых пакетов с 200-600 рабочих циклов в секунду до 2000-8000, в зависимости от типа процессора.

Такие данные однозначно свидетельствуют о том, что преимущественные затраты времени в цикле обработки программы-прототипа связаны с форматными преобразованиями в ходе преобразования числовых значений в текстовый вид.

Автором была исследована возможность построения собственных программ форматных преобразований (из внутреннего вида в символьный) при следующих ограничениях:

– предельная разрядность числа заведомо известна;

– лидирующие нули заполняют всю длину результирующего поля.

Разумеется, при предложении пользователям того или иного компилятора фирмы не предоставляют сведений о характеристических признаках и методологии своих разработок. В связи с этим, кроме прочего, были исследованы некоторые операции языка, навлекшие подозрения относительно качества их реализации в

компиляторах фирмы «PowerBASIC Inc». В этих целях проведены следующие исследования:

– определялась корректность предлагаемой фирмой-разработчиком замены оператора сложения в конструкциях вида C=C+I на оператор INCR для некоторых типов данных;

– определялась сравнительная скорость создания строковых элементов различных типов и ряда операций с ними;

– определялись сравнительные скорости исполнения циклов операций сравнения текстового образца с массивом текстовых строк и предложенной фирмой-разработчиком заменяющей операции ARRAY SCAN по трем типам текстовых объектов языка PowerBASIC.

Все исследования выполнялись на 11 типах персональных компьютеров[3] в среде MS-DOS 6.22 без файлов конфигурации. Замеры времени выполнены с помощью встроенного в синтаксис языка PowerBASIC for DOS микротаймера (оператор MTIMER), который, по заявлению разработчиков PowerBASIC, работает с точностью 20мс. Все проверки выполнялись в циклах, количество которых подобрано с целью получения удобных репрезентативных значений.

Выполненные в 2004 г исследования опубликованы ранее в [6]. При подготовке данной работы к этим исследованиям добавлены современные процессоры Intel Pentium E7300, E8400 и E8500.

1.1.1. Исследования временных характеристик операторов сложения

Определялись времена исполнения операций **C=C+I**, **INCR C,I**, **W=W+I** и **INCR W,I**, где **C** – целочисленный операнд двойной точности (4 байта), **I** – целочисленный операнд обычной точности (2 байта), **W** – беззнаковый целый операнд обычной точности (2 байта). Выбраны фиксированные «средние» начальные значения операндов. Выполнялось по 2000 циклов соответствующих операций. Упрощенный фрагмент программы, исполняющий соответствующие циклы операций, представлен на рис. 1.

[3] В более поздних исследованиях взяты ещё 3 процессора; в таблицах данной главы приведены обобщённые результаты.

```
DEFWRD W: DEFBYT B: DEFLNG C: DEFINT I-N: DEFSTR F,P,Q,R,S,T,U,Z
IR=1342: C1=237486: W1=237486: C2=237486: W2=237486
Q=" C=C+I        INCR C,I       W=W+I     INCR W,I": ? Q
MTIMER: for i=1 to 2000: C1=C1+IR: NEXT i: KX=MTIMER: ?#1,KX,: ? KX,
MTIMER: for i=1 to 2000: INCR C2,IR: NEXT I: KY=MTIMER: ?#1,KY,: ? KY,
MTIMER: for i=1 to 2000: W1=W1+IR: NEXT I: KZ=MTIMER: ?#1,KZ,: ? KZ,
MTIMER: for i=1 to 2000: INCR W2,IR: NEXT I: KT=MTIMER: ?#1,KT: ? KT
```

Рис. 1. Фрагмент программы с тестом времени исполнения операций сложения

Полученные результаты представлены на рис. 2. Легко видеть, что несмотря на известные несоответствия полученных данных скоростям процессора, оператор **INCR** реализован явно не лучшим образом, и рекомендуемое фирмой-производителем PowerBASIC его использование не может быть принято во внимание на рассматриваемых задачах.

Тип персонального компьютера			Сумма времен исполнения 2000 циклов			
№	Тип процессора	F [MHz]	C=C+I	INCR C,I	W=W+I	INCR W,I
1	Pentium-I	90	507	551	529	529
2	AMD DX4-100	100	518	635	596	576
3	Pentium-MMX	166	262	285	274	273
4	Pentium-MMX	200	205	224	214	214
5	Celeron-MMX	266	126	201	201	201
6	AMD-K6-2-300	300	118	164	164	164
7	AMD-Duron-600	600	41	58	49	50
8	Intel Pentium-III	666	50	78	78	78
9	Intel Pentium-III	733	48	74	73	73
10	Athlon-1000	1000	25	35	30	29
11	Intel Pentium-4	1500	69	72	72	72
12	Intel Pentium E7300	2660	10	21	21	21
13	Intel Pentium E8400	3000	8	18	18	18
14	Intel Pentium E8500	3160	11	21	21	21

Рис. 2. Замеры времен исполнения операций суммирования

1.1.2. Исследования работы со строковыми переменными

В рассматриваемой задаче сетевого мониторинга для быстрого определения источника датаграммы приходится сравнивать его MAC-адрес с хранящейся в памяти таблицей. В силу специфики программы, наиболее экономное хранение этих данных исполняется в массивах текстовых переменных. Длина MAC-адреса в Ethernet – 6 байтов. В языке PowerBASIC могут быть определены три типа текстовых переменных: строки фиксированной длины,

строки переменной длины и так называемые flex-строки (всегда фиксированной длины).

В этой связи основной интерес представляют операции присвоения значения текстовой переменной и исполнение поиска до первого совпадения. Стандартный метод поиска реализуется циклом **FOR...NEXT**, однако язык PowerBASIC имеет операторы обработки массивов, и в том числе оператор поиска в массиве по образцу **ARRAY SCAN**. В первых версиях программы мониторинга для хранения таблицы MAC-адресов были использованы массивы текстовых строк фиксированной длины, а поиск реализовывался стандартным циклом **FOR...NEXT** с прерыванием цикла после нахождения. Однако, после успеха прототипа пилот-системы, при построении реальной программы для точного выбора соответствующей языковой поддержки следовало провести необходимые тесты. Это и было сделано соответствующим блоком тестовой программы, аналогичным рассмотренному выше. Для заметного сравнения времен каждая операция исполнялась в цикле 200 раз. Соответствующий фрагмент тестовой программы приведен на рис. 3.

Полученные на той же группе ПК, что и вышеприведенные данные, результаты приведены на рис. 4.

Первые же замеры показали, что априорный выбор фиксированных строк при реализации пилот-системы оказался наихудшим из возможных. Именно операция присваивания уже занимает заметно большее время для строк фиксированной длины, чем для строк переменной длины (!). Этот результат показывает, что практическая реализация аппарата поддержки текстовых строк фиксированной длины в компиляторе с языка PowerBASIC оставляет желать лучшего по ресурсным характеристикам. В то же время, неожиданным и приятным сюрпризом явился быстрый алгоритм реализации **ARRAY SCAN**, который давал хоть и несколько большее время на flex-строках (что вполне понятно каждому практическому программисту на Ассемблере), однако это единственное преимущество строк фиксированной длины не могло повлиять на выбор конструктивного элемента хранения MAC-адресов в пользу flex-строк.

```
Q="Времена обработки (200ц) в различных текстовых объектах": ?#1,Q: ? Q
MAP MacR$$*6: MAP MacN$$()*6: DIM MacN$$(200): MacR$$="::*:::"
DIM SN(200) AS STRING*6: DIM SR AS STRING*6: SR="**:***"
DIM ST$(200): SK$="&&:&&&"
Q="     Flex$$    Fixed*6      Vary$":
Q=" =  :": ?#1,Q;: ? Q;
MTIMER: for i=1 to 200: MacN$$(i)=MacR$$: NEXT i: KX=MTIMER
MTIMER: for i=1 to 200: SN(i)=SR: NEXT I: KY=MTIMER
MTIMER: for i=1 to 200: ST$(i)=SK$: next i: KZ=MTIMER
? KX,KY,KZ
for i=1 to 200: SR=REPEAT$(6,CHR$(i))
  MacN$$(i)=SR: SN(i)=SR: ST$(i)=SR: next i
Q="Find:":? Q;
MTIMER: FOR I=1 TO 200
  IF MacN$$(I)=MacR$$ THEN J=1
NEXT I: KX=MTIMER:
MTIMER: FOR I=1 TO 200
  IF SN(I)=SR THEN J=1
NEXT I: KY=MTIMER:
MTIMER: FOR I=1 TO 200
  IF SK$=ST$(I) THEN J=1
NEXT I: KZ=MTIMER:? KX,KY,KZ
Q="Scan:":? Q;
MTIMER: ARRAY SCAN MacN$$(), =MacR$$, TO J1: KX=MTIMER
MTIMER: ARRAY SCAN SN(), =SR, TO J2: KY=MTIMER
MTIMER: ARRAY SCAN ST$(), =SK$, TO J3: KZ=MTIMER
? KX,KY,KZ
```

Рис. 3. Фрагмент программы проверки работы со строками и массивами строк

Результаты даны на рис. 4. Стоит обратить внимание на строку 6 рассматриваемой таблицы, соответствующую AMD-K6-2-300. Величина **1010** в шестой колонке отнюдь не является ошибкой эксперимента или неточностью. Выше уже говорилось о том, что результирующая программа, полученная после компиляции строк языка PowerBASIC, периодически исполняет процедуру «сборки мусора» именно в отношении текстовых переменных, причем этот процесс сделан неуправляемым для программиста. В рассматриваемый интервал как раз и попал цикл такой процедуры, что привело к несуразному значению микротаймера 1010 в этом месте (естественным было бы значение порядка 500-600).

Тип ПК		Времена текстовой обработки различных объектов (200 циклов)								
		Присвоение			Поиск в цикле			Поиск ARRAY SCAN		
№	MHz	Fix	Var	Flex	Fix	Var	Flex	Fix	Var	Flex
1	90	1032	704	372	1810	551	473	124	171	176
2	100	1855	1224	607	3262	830	853	227	337	370
3	166	586	452	204	1073	231	219	64	86	88
4	200	485	464	156	894	179	175	40	57	60
5	266	505	329	248	810	289	286	81	89	94
6	300	575	347	160	1010	151	159	36	47	52
7	600	183	131	103	318	126	126	30	28	34
8	666	194	121	91	323	111	111	30	31	31
9	733	180	114	86	293	104	104	30	32	31
10	1000	110	81	58	188	76	77	18	17	21
11	1500	244	167	109	414	133	131	23	31	32
12	2660	50	34	28	87	37	37	5	6	6
13	3000	43	29	24	76	33	32	3	5	5
14	3160	46	32	27	79	35	35	7	8	8

Рис. 4. Замеры различных операций со строками и массивами строк разных типов

1.1.3. Исследования операций форматирования данных

Выше было уже отмечено, что весьма значительная доля времени обработки каждого полученного сетевого фрейма в задаче сетевого мониторинга тратится на операции форматных преобразований пересчитанных после получения пакета характеристик сети. Количество таких постоянно меняющихся параметров составляет несколько десятков, и даже самые грубые подсчеты показали, что время собственно обработки пакета в сотни раз меньше времени отражения результатов этой обработки. В этих условиях уделение особого внимания исследованиям различных возможностей оптимизации форматных преобразований при создании результирующей наблюдающей программы представляется вполне оправданным.

За незначительным исключением, программа сетевого мониторинга выводит результаты в виде десятичных целых неотрицательных значений. Однако, ряд отладочных данных и часть оперативной информации (например, MAC-адреса) имеют вид 16-ричных чисел, без которых обойтись невозможно. Поэтому исследования форматных преобразований начаты именно с шестнадцатиричных форматов, которые могут быть сведены к двум основным: байтному и словному.

Синтаксис языка PowerBASIC предлагает стандартную функцию **HEX$(...)** для получения 16-ричного вида числа. Однако, эта функция в зависимости от конкретного значения аргумента может иметь результат разной длины. Так, HEX$(13) есть 1 символ "**D**", в то же время HEX$(31313) есть 4 символа "**7A51**". Как видим, лидирующие нули не выдаются, а лидирующие пробелы исключаются из вывода. Такое форматирование неудобно, а в ряде случаев (например, при выводе пословно MAC-адресов) недопустимо. На стадии пилот-программы соответствующие действия выполняла процедура-функция на языке PowerBASIC наподобие приведенной на рис. 5.

```
DEF FNH4$(R??)
  LOCAL SR$
  SR$=LTRIM$(HEX$(R??))
  DO WHILE LEN(SR$)<4: SR$="0"+SR$: LOOP
  FNH4$=SR$
END DEF
```

Рис. 5. Процедура форматирования слова в 4-символьный 16-ричный вид

В качестве замены двух процедур 16-ричного форматирования была написана программа на Макроассемблере, отдававшая результат вместо строки переменной длины во flex-строки с фиксированными

длинами 2 и 4 байта для исходных байта и слова соответственно. Операторы обращения к процедурам-функциям языка PowerBASIC были заменены обращениями к процедурам на Макроассемблере.

Тестовые исследования включали исполнение 1000 циклов каждого преобразования. Более того, замеры исполнялись несколько раз в ходе тестовой программы для исключения вынужденных ошибок вследствие непредсказуемой операции «сборки мусора» текстовых строк, а также для нивелирования различных результатов в серии (видимо, из-за таймерных прерываний, время исполнения которых зависит от абсолютного значения времени суток).

Результаты показаны в таблице на рис. 6 все для тех же 14 типов компьютеров. Вывод очевиден: заменой написанных на языке PowerBASIC процедур форматирования 16-ричных чисел оригинальным программированием на языке низкого уровня можно ускорить почти на порядок (!) исполнение этих операций в результирующей программе.

Тип ПК		Время 16-ричного форматирования объекта (1000 циклов)							
		Преобразование 1байт=>2симв.				Преобразование 2байта=>4симв.			
		П/п PowerBASIC		П/п на ASM		П/п PowerBASIC		П/п на ASM	
№	MHz	Min	Max	Min	Max	Min	Max	Min	Max
1	90	15370	15435	1616	1617	15502	15567	2060	2061
2	100	25166	26430	2507	2511	25882	26187	2977	2979
3	166	7992	8276	857	857	7962	8201	1129	1129
4	200	6908	7057	701	701	6878	7072	928	928
5	266	6785	6895	954	955	6698	6820	1178	1183
6	300	7811	7811	539	540	7811	7840	633	633
7	600	2896	2898	399	399	2882	2896	399	399
8	666	2727	2791	386	386	2690	2750	476	477
9	733	2486	2497	353	354	2445	2461	433	434
10	1000	1736	1745	241	242	1731	1742	281	281
11	1500	4266	4308	695	695	4270	4309	977	977
12	2660	806	811	128	129	804	810	135	135
13	3000	716	719	113	113	714	715	121	121
14	3160	715	716	116	116	715	715	122	122

Рис. 6. Времена форматирования байта и слова различными процедурами

После получения такого результата естественным следствием была попытка заменить и десятичные процедуры форматирования оригинальным программированием. Однако, для десятичного форматирования с заполнением лидирующими нулями язык PowerBASIC имеет специальный оператор **USING$("##...#",...)**. В целях полноты исследования следовало проверить, не является ли этот оператор более экономным по времени исполнения. Результаты (см. рис. 7) показали, что действительно применение этого оператора примерно в 2 раза более эффективно, чем указанная процедура-функция.

Однако, с учетом полученных данных на преобразованиях чисел в 16-ричный вид достигнутый результат представляется явно недостаточным.

Тип ПК			Времена исполнения цикла из 256 обращений	
№	Производительност	MHz	Процедура-функция	Оператор USING$()
1	Pentium-I	90	10904	5840
2	AMD DX4-100	100	18161	8988
3	Pentium-MMX	166	6025	2837
4	Pentium-MMX	200	5206	2395
5	Celeron-MMX	266	4457	2021
6	AMD-K6-2-300	300	5840	2475
7	AMD-Duron-600	600	1874	801
8	Intel Pentium-III	666	1733	793
9	Intel Pentium-III	733	1605	729
10	Athlon-1000	1000	1146	488
11	Intel Pentium-4	1500	2562	975
12	Intel Pentium E7300	2660	493	194
13	Intel Pentium E8400	3000	440	181
14	Intel Pentium E8500	3160	448	178

Рис. 7. Сравнение процедуры-функции форматирования с оператором USING$

Поэтому, в целях исследования была написана соответствующая библиотека процедур на Макроассемблере (для получения OBJ-файла использован MASM версии 5.10 1988 г.). Библиотека включала несколько различных процедур для преобразования десятичных чисел из разных исходных типов данных на PowerBASIC в

соответствующей длины текстовую строку. Тип входного данного каждой процедуры определялся реальными потребностями форматизации. Так, для длинных целочисленных величин, соответствовавших числу пакетов (принятому, отказанному и т.д.) задействован 7-символьный формат вывода; для числа байтов, представляющихся в основной программе сетевого мониторинга, предусмотрен 9-символьный формат[4]. Эта же библиотека включала ранее написанные подпрограммы перевода байтов и слов в шестнадцатиричный вид, а также несколько вспомогательных процедур (в частности, для преобразования ip-адресов в вид их символьного представления).

Тестовая программа на PowerBASIC 3.00 сравнивала времена исполнения процедур-функций преобразования, написанных на языке PowerBASIC, с временами аналогичных преобразований с использованием созданной библиотеки процедур. Для получения значимых результатов сравнивались времена исполнения 1000 циклов тех и других преобразований. Каждое сравнение исполнялось дважды, чтобы компенсировать работу схемы «уборки мусора» внутри этих циклов. Для более ясного понимания техники замеров на рис. 8 приведен фрагмент тестовой программы для случая 5-символьных преобразований (однако, сохранены определения всех входящих на тот момент входов в построенную библиотеку процедур на Макроассемблере).

В реальности, разумеется, одна программа содержала и все проверки, приведенные в предыдущих разделах выше, и ряд проверок, обсуждаемых ниже, а также некоторые дополнительные действия. Все процедуры-функции преобразований (всего 8 штук), послужившие сравнением для написанных оригинальных, построены аналогично приведенной в конце рис. 8 процедуре FND5$, отличаясь в основном типом входного аргумента (целое со знаком 2 байта, беззнаковое целое 2 байта, целое со знаком 4 байта и др.).

Общий объем текста библиотеки форматных преобразований составил 260 строк Макроассемблера. Объем результирующего объектного файла – 874 байта. Все параметры предполагаются переданными по ссылке.

Для облегчения фиксации получаемых в ходе тестирования результатов, они, помимо экрана, дублировались также в выходной файл. Пример полной реальной выдачи тестовой программы приведен на рис. 9.

Небезынтересно, что из анализа рис. 6-7 можно заключить, что результаты сильно зависят от линейки процессоров: AMD и Athlon, в противоположность предыдущим сравнениям, дают результаты хуже, чем Intel Pentium.

[4] Впоследствии 10-символьный.

```
$ERROR NUMERIC-,OVERFLOW+,STACK-,BOUNDS-
$COM 0
$COMPILE EXE "TAMINE.EXE"
$CPU 80386
$DIM ARRAY
$FLOAT NPX
$LIB COM-,LPT-,GRAPH-,IPRINT-
$OPTIMIZE SPEED
$OPTION CNTLBREAK-,GOSUB+
$SOUND 16
$STATIC
$LINK "TAMCNV.OBJ"
DECLARE SUB TAMCWH4(WORD,FLEX)
DECLARE SUB TAMCID4(INTEGER,FLEX)
DECLARE SUB TAMCBD3(BYTE,FLEX)
DECLARE SUB TAMCBD2(BYTE,FLEX)
DECLARE SUB TAMCID5(WORD,FLEX)
DECLARE SUB TAMCBH2(BYTE,FLEX)
DECLARE SUB TAMCLD9(LONG,FLEX)
DECLARE SUB TAMCLD7(LONG,FLEX)
DECLARE SUB TAMCMH6(FLEX,FLEX)
DECLARE SUB TAMCMIP(FLEX,FLEX)
DECLARE SUB TAMCXH2(BYTE,FLEX)
DECLARE SUB TAMCXH4(BYTE,FLEX)
DECLARE SUB TAMCXHC(BYTE,FLEX)
DEFWRD A,W: DEFBYT B: DEFLNG C: DEFINT I-N: DEFSTR F,P,Q,R,S,T,U,Z
W??=&H4321
```

```
OPEN "O",#1,"TAMINE.RPT"
Q="Тест проверки времен исполнения операций (2000)": ?#1,Q: ? Q
LINE INPUT "Тип ПК / процессор: ",SID$:
?#1,"Тип ПК / процессор: ",SID$: ? SID$
Q="Временные характеристики авторских и традиционных процедур (2x1000ц)"
?#1,Q: ? Q
FOR J=1 TO 2: Q="FND5 "
 MTIMER: FOR I=1 TO 1000: CALL TAMCID5(W??,S$$): NEXT I: K1=MTIMER
 MTIMER: FOR I=1 TO 1000:S$$=FND5$(W??):NEXT I:K2=MTIMER:CALL PrK:NEXT J
CLOSE#1
END
SUB PrK
 SHARED Q,K1,K2
 ? Q;K1,K2: ?#1,Q;K1,K2
END SUB
DEF FND5$(R??)
  LOCAL SR$
  SR$=LTRIM$(STR$(R??))
  DO WHILE LEN(SR$)<5: SR$="0"+SR$: LOOP
  FND5$=SR$
END DEF
END
```

Рис. 8. Фрагмент программы сравнения 5-символьных десятичных преобразований

```
Тест проверки времен исполнения операций (2000)
Тип ПК / процессор:          P-MMX-200
 C=C+I         INCR C,I       W=W+I     INCR W,I
 205            224            214          214
Тест преобразований (сумма времен по значениям от 0 до 255)
FNH2$(B)     FND4$(I)   USING$(####,I)
 1836           5206           2395
Времена обработки (200ц) в различных текстовых объектах
     Flex$$     Fixed*6      Vary$
 =  : 156       485           464
Find: 175       894           179
Scan: 60        40            57
Тест проверки работоспособности авторских процедур
XHn=<(67)6667)65666768696A)> MH6=<00A0CD3F0B54> MIP=<193.232.194.015>
ID4 9999##### 9999
BD3 099###### 099
BD2 99####### 99
BH2 63####### 63
ID5 17185#### 17185
LD9 655359999 655359999     LD9 ********* 655360000
LD7 9999999## 9999999       LD7 *******## 10000000
Временные характеристики авторских и традиционных процедур (2x1000ц)
FNH2  701      6908
FNH2  701      7057
FNH4  928      6878
FNH4  928      7072
FND2  634      12095
FND2  634      12461
FND3  733      17992
FND3  733      18398
FND4  828      18367
FND4  828      18715
FND5  1063     12865
FND5  1063     12880
FND7  1925     24851
FND7  1926     24642
FND9  2250     13755
FND9  2224     13351
```

Рис. 9. Реальный файл отчета серии тестовых проверок на Pentium-MMX-200

Сводка результатов замеров форматных преобразований в десятичный вид приведена на рис. 10. Видно, что во всех случаях процедура-функция на языке PowerBASIC более чем на порядок (т.е. в 10 раз!) медленнее, чем аналогичная процедура на Макроассемблере. Вспоминая, что функция **USING$(...)** всего лишь в два раза быстрее процедуры-функции, получаем, что соответствующая подпрограмма из созданной библиотеки более чем в 5 раз эффективнее непосредственного применения конструкций языка PowerBASIC.

Тип ПК		Времена исполнения циклов из 1000 операций (минимум из 2х попыток)									
		2-зн.строка		3-зн.строка		5-зн.строка		7-зн.строка		9-зн.строка	
№	MHz	Bas	Asm	Bas	Asm	Bas	Asm	Bas	Asm	Bas	Asm
3	166	14561	777	20722	896	15055	1285	15654	2716	28843	2327
4	200	12095	634	17992	733	12865	1063	24642	1926	13351	2224
5	266	10756	905	15826	1007	11414	1199	11328	1948	21056	1786
6	300	12481	507	20063	549	12899	746	13198	1308	27048	1168
7	600	4652	402	6648	441	4878	514	4882	892	8801	795
8	666	4305	363	6301	403	4569	480	4491	780	8511	704
9	733	3874	333	5610	369	4127	439	4109	721	7585	642
10	1000	2787	244	4014	245	2926	291	2948	552	5354	482
11	1500	5808	480	8677	521	6046	596	6147	896	11585	814
12	2660	1206	124	1764	133	1263	140	2354	213	1243	227
13	3000	1044	110	1576	119	1110	124	2076	189	1119	200
14	3160	1052	113	1583	121	1131	128	2083	193	1112	204

Рис. 10. Времена процедур форматирования на PowerBASIC и п/п на MASM

В целом, налицо явное преимущество процессоров AMD-K2 и Duron над эквивалентными Celeron и даже Intel Pentium-III в задачах реального времени, решаемых в MS-DOS. К сожалению, и Athlon-1000 показывает явное преимущество перед Intel Pentium 4-1500. В свою очередь, для автора было неожиданным, что Intel Pentium E8500 даёт результаты в целом хуже, чем E8400. Для современной НС выбран именно E8400.

Суммируя, можно сказать, что исследования показали весьма низкую эффективность реализации типовых конструкций языка PowerBASIC перед предложенными процедурами на Макроассемблере. Это тем более странно, если иметь в виду, что реализация типовых конструкций языка (в данном случае **USING$(...)**) выполнена через присоединяемую при компиляции библиотеку типовых процедур. Вероятно, фирма-разработчик создавала свои типовые процедуры на языке более высокого уровня, нежели Ассемблер, особо не утруждая себя оптимизацией по времени.

Предложенная библиотека процедур с успехом используется в актуальных версиях программ, работающих на наблюдающих станциях. Ее внедрение позволило существенно, более чем в 10 раз снизить ресурсные затраты на цикл обработки принимаемых сетевых фреймов в процессе сетевого мониторинга.

Полностью весь синтаксис обращений к библиотеке TAMCNV.OBJ приведён в предыдущем томе 1 [1].

1.2. Оптимизация работы с видеопамятью

Существовавшая до 2004 г в программе сетевого мониторинга практика вывода числовых показателей на экран включала предварительное формирование конечного символьного вида параметра в оперативной памяти (например, оператором “USING$()”) и исполнение операторов типа “SCREEN”, “LOCATE” и далее “PRINT” для вывода в нужное место экрана.

Обратим внимание на то, что при необходимости какого-либо вывода уже известны все необходимые атрибуты: номер видеостраницы NPage, номер строки на странице Nстр и номер позиции Nпоз., начиная с которой следует сделать вывод. Профессиональный компилятор с языка PowerBASIC по каждому из тройки вышеприведённых операторов делает ряд обращений к процедурам BIOS, надёжных, но сравнительно медленных.

Между тем всё, что требуется сделать – переслать символьный вид выводимого параметра на нужное место в видеопамяти, легко вычисляемое как **Apage+Nстр*160+Nпоз-1**[5], где Apage – адрес начала нужной видеостраницы в оперативной памяти.

Первая, точнее, нулевая страница всегда начинается с **B800**h, а смещение очередной видеостраницы, как показали опыты, зависит от используемой видеокарты и может быть определено на

[5] Nстр начинается с **0**, а Nпоз – с **1**, поэтому вычитаем **1**.

начальном этапе работы программы как некоторое фиксированное число байтов.

Алгоритм определения этого смещения следующий. Перед вызовом программы MS-DOS всегда устанавливает нулевую страницу видеопамяти. Операторами “SCREEN 1,0,0,0” для вывода устанавливается следующая, первая страница видеопамяти, и далее операторами “LOCATE 0,1” и “PRINT “--”;” с первой позиции первой строки выводится два минуса. Далее сканируется видеопамять и ищется сочетание “--”. Адрес этого сочетания относительно начала видеопамяти и будет фактической длиной видеостраницы.

Таким образом, легко вычислить точный адрес начала желаемого расположения данных в видепамяти. Остаётся выполнить нужное форматное преобразование, выводя символы последовательно сразу в видеопамять. Этим обходятся, казалось бы, необходимые обращения к BIOS, которые занимают очень много времени по сравнению с пятью арифметическими операциями вычисления места вывода и одного цикла пересылок.

Такой метод применён в программе мониторинга для вывода большинства числовых значений через использование стандартных входов TAMWLDS, TAMWLDA, TAMWLD7, TAMWDD7 в библиотеке конвертации TamCnv.OBJ, как приведено в томе 1.

Результатом таких манипуляций значительно (более чем в 10 раз!) ускорен вывод основной информации на экран программы мониторинга. Вместо 100-600 основных циклов в секунду нормальными значениями на процессоре E7300 стали 11000-32000 циклов, на процессоре E8400 от 16000 до 32767[6] циклов в секунду.

1.3. Увеличение разрядности основных данных

После перехода ЛВС на 100Мбит значительно увеличилось число переносимых данных в сети. Стандартных 9 позиций для общего числа подсчитанных байтов за стандартный 15-минутный период между отчётами перестало хватать.

В этой ситуации пришлось изменить допустимую разрядность числовых показателей с 9 до 10 разрядов (см. строку “Взято” на рис. 11 ниже) на экране, а также соответственно в отчётах. Поскольку места для изображения 10 разрядов не было, добавлен лидирующий знак “+”, чтобы значения соседних граф не сливались воедино.

Соответственно, переделаны алгоритмы библиотеки преобразований TamCnv.OBJ под новый формат данных. Вместо входов TAMCLD9, TAMCDD9 и аналогичных теперь используются TAMCLDA, TAMCDDA и TAMWLDA.

[6] Вместо значений, больших чем 32767, всегда оставляется 32767.

1.4. Расширение показа IP-адресов

Изменение схемы подключения большинства сетевых ПК института, в основном, собранных во внутреннюю локальную сеть 10.0.*.*/16 было вызвано острой нехваткой сетевых адресов основной адресной сети класса С 193.232.194.*/24. Внешняя сеть допускала максимум 254 адреса, в то время как реальная потребность составляет к моменту формирования данной работы более 400 нод, в числе которых были не только ПК, но также виртуальные сервера, управляемые коммутаторы на этажах и другие сетевые устройства.

Сеть 10.0.*.* построена, в основном, по принципу этажности: компьютеры 2го этажа входили в подсеть 10.0.2.*, компьютеры 21-го – в подсеть 10.0.21.*. В связи с этим, третий октет внутренней локальной сети перестал быть однознаковым, поскольку число этажей института – 21, а помимо 21й группы в числе ЛВС находятся также группы 13, 23, 27 и иные, созданные для обозначения Антивирусной службы, Wi-Fi, виртуальных серверов и иных целей.

С этого времени, по необходимости, Антивирусный сервер института [7] имеет два сетевых интерфейса, «внешний» и «внутренний», чтобы обслуживать всех пользователей института, идентифицируя их по IP-адресу.

Однако, пришлось изменить мониторную программу так, чтобы вместо одной цифры предпоследнего октета IP-адреса на экране были бы видны две. Экономия достигнута за счёт совмещения позиции-разделителя и признака отключаемой ноды. Результат показан на рис. 11.

В качестве примечания следует заметить, что зелёным цветом показаны MAC-адреса, отсутствующие в основной таблице нод, но уже известные средствам мониторинга. Главным образом, это адреса центрального коммутатора **00155D17610C**, **00155D175F0C** и схожие. Красным цветом показана нода, впервые включённая в список нод (в данном случае это WiFi-пользователь). Жёлтым цветом выделены ноды, по каким-либо причинам изменившие IP-адреса, но опознанные по их MAC-адресу. Синим цветом (плохо виден на рисунке) показаны хабы на этажах института.

Любопытным стало узнать, что несмотря на значительное увеличение числа ПК института за 19 лет, число одновременно включённых нод по-прежнему практически не превышает пределов экрана (43 строки * 3 столбца = 129 мест).

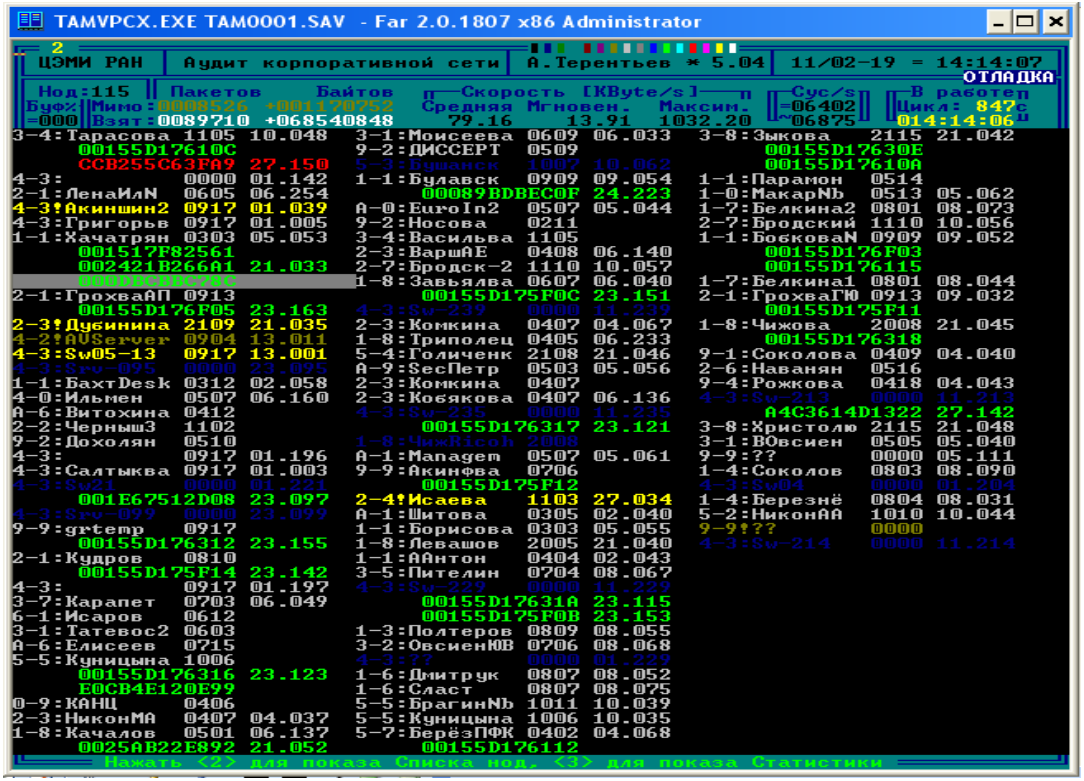

Рис. 11. Современный показ нод «внутренней» ЛВС

ГЛАВА 2. ОСНОВНЫЕ РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ СЕТЕВОГО МОНИТОРИНГА

Предложенный автором метод мониторинга корпоративной сети на основе сплошного неинтерактивного низкоуровневого круглосуточного наблюдения датаграмм с помощью выделенной наблюдающей станции (НС) был реализован в ЦЭМИ РАН с 2000 г. Практически сразу же после внедрения оказалось возможным решить целый ряд актуальных задач: получить полные данные о трафике в сети по ряду первичных показателей (общий объем трафика в пакетах и байтах, средняя и максимальная скорость в сети, процент бродкастинга и др.), выделить Интернет-компоненту трафика, получить данные об относительном распределении TCP/IP-пакетов и пакетов Novell Netware. Оказалось возможным также решать ряд задач по конкретным пользователям: установить время их сетевой активности, определять некорректно настроенные ПК, идентифицировать незаконное появление новых пользователей в сети, по косвенным данным определять возможную зараженность ПК и серверов сетевыми вирусами.

Все эти результаты изложены в Томе 1 данной работы [1].

Однако, переход сетевого мониторинга на новый уровень позволил решать и качественно новые задачи. Данная глава посвящена их рассмотрению.

2.1. Выявление сетевых атак

2003 год запомнился невероятной активностью сетевых вирусов [8]. Многие организации испытали на себе их влияние. В этом году в ЦЭМИ РАН ещё не действовал Антивирусный сайт [9], поэтому точно установить типы вирусного заражения сейчас не представляется возможным. Сетевой мониторинг в это время действовал на базе ПК Pentium-IV Celeron 1500.

«Мода» на сетевые вирусы пришла с развитием локальных сетей по звездообразной схеме через хабы-концентраторы, когда с любого ПК был физически доступен любой, но внутренних локальных сетей с сокрытием адресов ПК в ЦЭМИ РАН ещё не было. В таких условиях достаточным было заражение одного ПК сетевым вирусом, чтобы он, сканируя всю сеть, спокойно заражал все «окрестные» ПК.

В «лучших» традициях вирусописателей, наивысшая их активность в 2003 г проявилась в конце лета, в августе. Соответственно, в сентябре стали проявляться результаты этой активности.

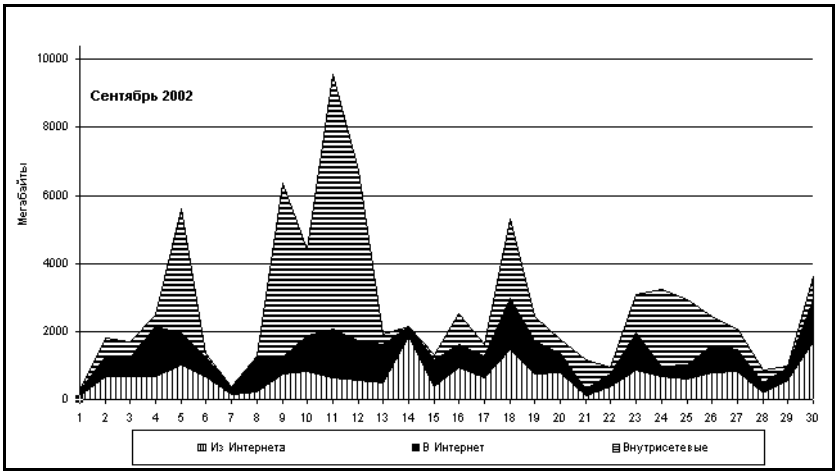

Рис. 12. Сводный трафик за сентябрь 2002 г.

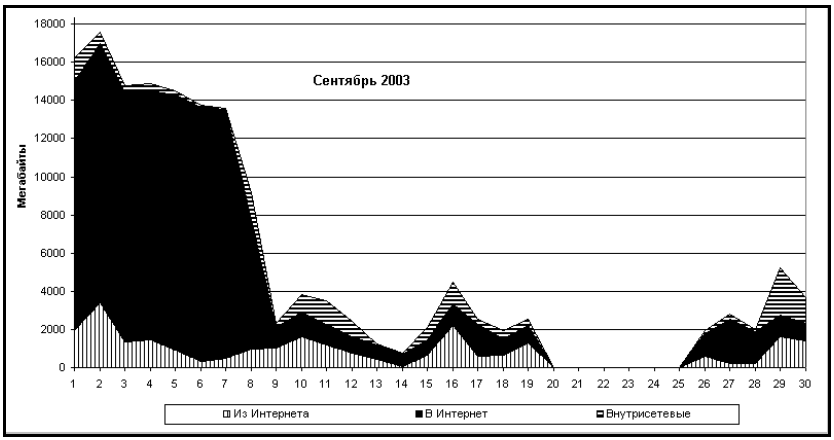

Рис. 13. Сводный трафик за сентябрь 2003 г.

Существенно важным индикатором массового сетевого заражения в ЦЭМИ РАН оказалась возможность исследования внутрисетевого трафика. На рис. 12 представлены для сравнения результаты биллинга за сентябрь 2002 г, а на следующем рис. 13 – за сентябрь 2003 г. Явно видна выраженная активность пересылок пакетов вовне

в период с 1 по 8 сентября 2003 г. При сплошной антивирусной проверке выяснилось, что более 40 ПК были заражены сетевыми вирусами (Nimda), инициирующими множественные обращения к компьютерам внутри сети для заражения соседних ПК.

Таким образом, оказалось найденным ещё одно полезное приложение биллинговой функции сетевого мониторинга.

2.2. Выделение части ЛВС в самостоятельный сегмент

С весны 2002 г. пользователи ЛВС ЦЭМИ РАН начали испытывать регулярные затруднения в работе с сетевыми сервисами. Особенно заметным было замедление работы в Интернете, участились жалобы на самопроизвольные обрывы связей с внешними серверами.

Анализ существующих информационных потоков в ЛВС ЦЭМИ РАН, проведенный с помощью системы сетевого мониторинга, показал явные неравномерности в средней скорости передачи информации в сети (рис. 14) в основном за счет внутрисетевых пересылок информации. Одновременно стало заметным число сетевых коллизий, причем они явно совпадали с пиками трафика.

Так, для примера рис. 14 левая часть сдвоенного пика соответствует интервалу 13÷14 часов, в течение которого из Интернета получено 84,6 МБ, а от ряда ПК внутри сети – значительно больше: отдельные ПК бухгалтерии дали свыше 30 МБ, а бухгалтерский сервер 421,5 МБ. Второй пик в этот же день в 19 часов образован излучением: Интернет 54 МБ, бухгалтерский сервер 55,4 МБ, сотрудник бухгалтерии 82,4 МБайт.

Однако, оставалась неясной направленность этих пересылок, поскольку структура отчетов существующего на тот момент аудита давала суммарную информацию по объемам, испускаемым различными ПК, но отсутствовала информация об адресатах передачи. Существующая к этому моменту технология мониторинга зафиксировала также совпадение резкого увеличения числа сетевых коллизий с моментами достижения предельно высоких скоростей в ЛВС. Так, для приведенного выше примера число коллизионных пакетов увеличивалось в 50 раз (с 28 до 1012 за 15 минут).

В связи с этим, в очередной версии 4.14 наблюдающей программы были существенно расширены функции аудита, в которые **впервые была добавлена возможность полного слежения за трафиком ряда конкретных ПК, включая регистрацию внутрисетевых получателей с фиксацией составляющих трафика по ним**.

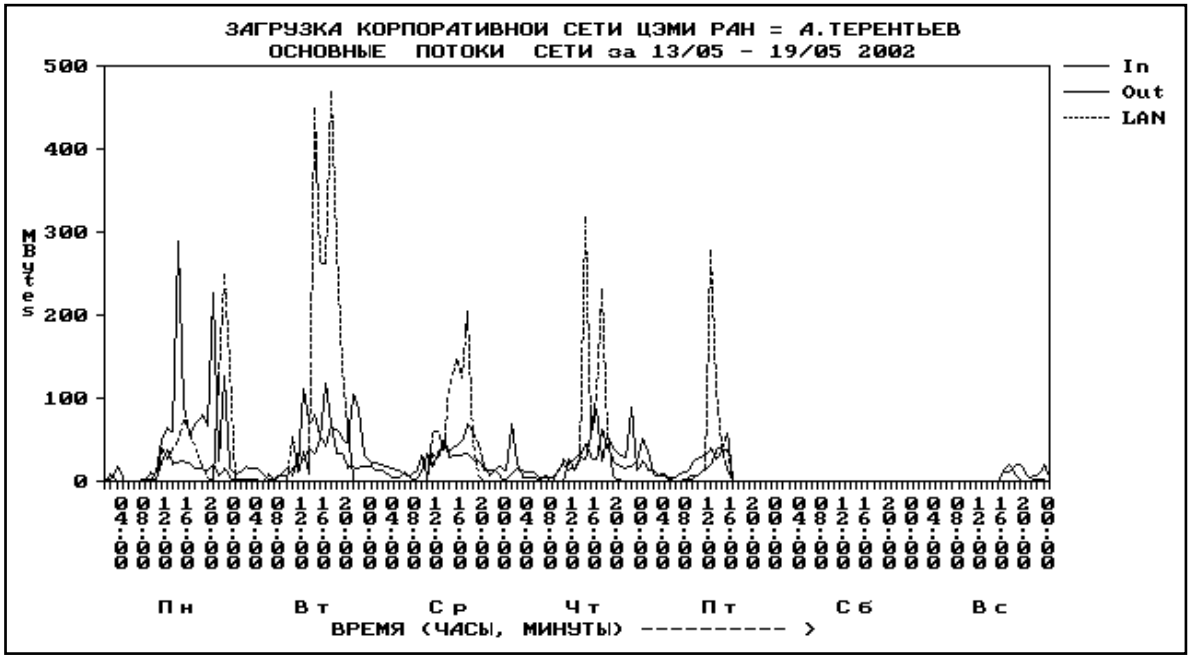

Рис. 14. Пример выраженных пиков внутрисетевых (пунктир) пересылок

Надо сказать, что отслеживание трафика N компьютеров плюс Интернета занимает 4*4*(N+1) байт оперативной памяти, в то время как полный веер (от каждого ПК к каждому) – 4*4*(N+1)*N, что при N=230 с учетом уже задействованных объемов далеко выводило наблюдающую программу за ресурсные рамки MS-DOS. Поэтому было принято решение отслеживать не более чем M компьютеров одновременно плюс Интернет. Оказалось возможным [10] обеспечить максимум M=10. В число этих 10 выделенных ПК вошли, в первую очередь, те, которые показали наиболее высокий излучаемый трафик.

Регулярное наблюдение трафика отдельных ПК после первых же недель наблюдений выявило причину сетевых отказов. В большинстве случаев этой причиной явились внутрисетевые пересылки, в первую очередь на сервер и с сервера бухгалтерии. Необычно высокий трафик периодически отмечен также на серверах других лабораторий.

Консультации с сотрудниками административно-финансовой группы и изучение их работы выявило, что в соответствии с методикой своей работы как сотрудники непосредственно бухгалтерии, так и группы ее математического обслуживания и сопровождения исполняют постоянные пересылки обрабатываемого ими фрагмента БД для фиксации состояния (объем всей БД порядка 1 ГБ) несколько раз в течение рабочего дня. Безусловно, подлинной причиной подобного является, как уже не раз отмечалось, системная и проектная отсталость всей концепции разработки обеспечивающей бухгалтерской системы VIK. Вместо современных SQL-транзакций основой доступа к бухгалтерской БД еще из MS-DOS с механическим перенесением в Windows являлся файловый метод. Поэтому, для обеспечения синхронности в обработке сотрудники после работы с БД попросту копируют фрагмент БД, относящийся к их конкретной задаче (а главбух – БД полностью!) на сервер… и таких пересылок особенно много под конец рабочего дня сотрудников бухгалтерии, что, как неоднократно отмечалось [2], совпадает по времени с пиком использования Интернета научными сотрудниками ЦЭМИ.

Вероятно, не лишне в этом месте еще раз напомнить, что ЛВС устроена так, что каждый испускаемый пакет виден всеми ПК сети, и в один и тот же момент времени может быть передан только один пакет одним из всего множества ПК. Поэтому высокий трафик

внутрисетевых пересылок по технологии Microsoft Network «забивал» остальные датаграммы TCP/IP, исчерпывая время их жизни и разрывая соединения с Интернетом.

Этим объясняется отмеченное многими сотрудниками ЦЭМИ неоправданно выросшее число отказов сетевых служб (в первую очередь, почты и DNS) и число сетевых коллизий. К концу 2002 г. стало очевидным, что в ЛВС ЦЭМИ начали проявляться факторы, блокирующие работу части сетевых служб на время, сравнимое со временем жизни пакетов TCP/IP и «сбивающие» таким образом работу TCP/IP.

На рис. 15 приведены фрагменты одного из отчетов сетевого мониторинга (оставлены главным образом те строки, данные по которым резко выделяются среди прочих). Начальные секции отчета показывают пересылку 99’118’273 байт за 15 минут. Всего же, судя по всем отчетам (здесь не приведены), в сети за этот час передано около 500МБ. По секциям строк **#60-#62**, дающим в приведенном отчете сводные показатели за весь час, легко видеть, что основной трафик был между административно-бухгалтерским сервером и ПК госпожи Железновой: 134,7 МБ было получено и 191МБ – закачано обратно на сервер.

В этих условиях естественной рекомендацией было принятие неотложных мер по обособлению административно-финансовой группы в выделенный сегмент ЛВС, что и было предложено впервые администратором Узла ЦЭМИ РАН Ляпичевой Н.Г. и автором данной работы.

Следует отметить, что топологическое решение проблемы было очевидным. К этому моменту на протяжении ряда лет в ЦЭМИ РАН в рамках действующей ЛВС успешно работали два выделенных сегмента, в которых их группы ПК образовывали собственные сегменты за роутерами, функционирующими на основе Windows NT 4.0 и Windows 2000 Server.

```
#00 ЦЭМИ РАН *  Аудит корпоративной сети * 4.14 = А.Терентьев
#05 Текущее время      30/05-02 = 18:00:00, работает     10781с
#10 Взято пакетов: 236664,       Байтов: 99118273
#11 Мимо пакетов:    5434,       Байтов:  1500677
#13 Ошиб.пакетов:     764,       Байтов:     6996
#12 Скорость максимальная: 1107.71 Kb/s;   Средняя: 107.64 Kb/s
#14 БД:  231,  ПК в работе:   81
#15 Ц/с в среднем -- Всех:   4818;  полезных:     263;  коротких:     113
#17     Всего циклов минимально:    1851;    максимально:    5291
#18 Ситуаций пропуска пакетов:    4098   макс.буферов: 64%
#20  =              К О М П О Н Е Н Т Ы   Т Р А Ф И К А
#20  =           По типу трафика       В т.ч. широковещательные
#20  =          Пакетов   Байтов          Пакетов   Байтов
#21 EtherII-IP:   235459 99015102             355    47289
#22 EtherII-ARP:     284    17040             169    10140
#25 IEEE802.3IPX      87     7759              87     7759
#28 Не опознаны:     497    32318               0        0
#30  =     Структура внутрисетевого трафика
#31 InterNetFrom:  21095 11396997
#32 InterNetTo:    27476  9079454
#33 IntroLAN:     188123 78653627
#50 - - - - - - - - - -
#60  = Сведения о выделенных нодах и их трафике И С П У Щ Е Н О  П Р И Н Я Т О
#61 002. 000652324406 194.059/0F:CiscoNew0921{ 122148 86811702 133498 40612755
#62 .006 0800207BFBB8 194.051/42:IS1-Srvr0921{   2423  1234574  20331  1621806
#62 .011 0002B32D849A 194.091/39:Лейб-NT 0203{   2823  1887765   5198   520307
#62 .038 00C0262C11B7 194.067/42:Ляпичева0902{   7376  3398941   7811  1009628
#62 .041 008048FB3835 194.070/16:Дмитрук 0807{   2785  2202865   2561   353574
#62 .051 0000C0ABFCC2 194.084/17:Шоломицк0801{   2618  2056401   2232   252953
#62 .052 00104B289D3F 194.085/44:Дыбенко 0907{  13784  2650289  18009 20669503
```

```
#62 .054 0050BA5CA260 194.087/11:ААнтон2 0909{  22345 32811341  12309   804673
#62 .090 00A0CC54D44A 194.130/22:Гаврилец1108{   3628  1785993   3557   321487
#62 .105 0030F1019F61 194.145/30:ВОвсиенк0604{   2616  2130602   1990   212324
#62 .118 00A00C45AB32 194.157/1A:Пляскин 0917{   7797  2474178   7409  1285227
#62 .171 004005409F98 194.209/44:Exch    0907{   8950  4786081   9017  1343267
#62 .174 00A0CC54D468 194.214/37:Карапет.0703{  11818  7537704  12460  1989579
#62 .188 004005411AA8 194.228/94:Кузн-ва 0209{  11492 12627039   8367   731390
#61 005. 0090271D849A 194.097/41:ADMSrvr20302{ 427275170173043 414951196077276
#62 .039 0000C0CE4BF8 194.068/94:Желез-ва0214{ 388896134696768 386114191630251
#62 .094 00400540FBE3 194.134/41:Парини  0411{  10271  2172379  10651  2440810
#62 .101 0000C0A746F8 194.141/41:Учитель 0411{  24436 31812152  14685  1306698
#62 .147 00C0262C1325 194.188/41:Ю.Ким   0302{     70     6120     85     7275
#62 .188 004005411AA8 194.228/94:Кузн-ва 0209{   3571  1480956   3416   692242
#61 006. 0800207BFBB8 194.051/42:IS1-Srvr0921{  22336  2704335   4199  1477021
#62 .002 000652324406 194.059/0F:CiscoNew0921{  20331  1621806   2423  1234574
#80  = Сведения о всех нодах и их трафике          И С П У Щ Е Н О
002.000652324406 193.232.194.059/0F:CiscoNew0921{ 122148 86811702  0B49
003.00D0B7A95849 193.232.194.239/43:Server3 0917{   6322  3743625  0311
005.0090271D849A 193.232.194.097/41:ADMSrvr20302{ 427275170173043  2311
006.0800207BFBB8 193.232.194.051/42:IS1-Srvr0921{  22336  2704335  0311
011.0002B32D849A 193.232.194.091/39:Лейб-NT 0203{   5531   551267  0383
014.08002007D17D 193.232.194.057/42:SS1-Srvr0921{   5892   834294  0311
030.000628FEA700 193.232.194.055/42:LtStream0921{    418    40560  0941
038.00C0262C11B7 193.232.194.067/42:Ляпичева0902{   7881  1014638  0301
039.0000C0CE4BF8 193.232.194.068/94:Желез-ва0214{ 386115191630311  0301
086.004005411AA6 193.232.194.126/42:Терент-в0904{    359    26925  0111
Конец отчета <TAMC2315.LST>
```

Рис. 15. Основные строки отчета аудита на 18:00 30.05.2002

Роутеры этих сегментов исполняют также функции внутренних серверов сегментов с рядом различных сетевых служб. Так, в одном из указанных случаев дополнительной функцией роутера была поддержка службы DialUp. В обоих случаях роутер использовался также как файлсервер, поддерживая используемые сотрудниками лабораторий общие файловые области.

Однако, при создании сегмента административно-финансовой группы наблюдался ряд существенных отличий в условиях функционирования по сравнению с указанными сегментами. Во-первых, в выделенных ранее в самостоятельные сегменты лабораториях рабочие места непосредственно соседствовали друг с другом, занимая 1-2 смежные комнаты, и максимальное число рабочих мест в любом из сегментов не превышало 5. К ПК административно-финансовой группы, пользующимся одним и тем же сервером, следовало отнести различные рабочие места бухгалтерии и плановиков, отдела кадров, а также рабочие места сотрудников сопровождения бухгалтерской системы, в своем конечном виде 18 рабочих мест, распределенных по 10 помещениям на 3-х разных этажах здания. Группировка ПК в близлежащие помещения под формируемый сегмент представляла собой самостоятельную непростую организационную задачу, с решения которой собственно и началась практическая реализация ранее теоретически проработанного и согласованного проекта.

Вторым отличием от ранее существовавших сегментов ЛВС являлась необходимость обеспечить сотрудникам в их работе усиленные нормы информационной безопасности, в частности, авторизованный доступ к общеинститутским антивирусным средствам. Ранее устоявшейся практикой обновлений, в соответствии с рекомендациями авторов используемой антивирусной программы, было обращение к антивирусной области файлсервера как к сетевому ресурсу с использованием протоколов сетевой службы Microsoft Network [11]. Как известно, эта технология не обеспечивает в изолированных рабочих группах за роутерами авторизованную связь с внешними серверами. Вдобавок пользователи ЦЭМИ РАН, являясь весьма недисциплинированными в целом (см., напр., [12]), постоянно забывали исполнять обновление антивирусных средств. Включение заданий на обновление в автоматически стартуемые задачи при включении ПК, как выяснилось, также не решает проблему, поскольку ряд пользователей не выполняет

идентификационную процедуру (попросту нажимают клавишу <**Esc**> вместо ввода пароля) и таким образом блокирует работу приложений в Microsoft Network. Следовало найти и обеспечить необходимую технологию авторизованного доступа к антивирусному серверу изнутри выделенного сегмента, гарантирующую автоматическое обновление антивирусных средств.

Далее, в процессе изучения использования информационных сервисов ЦЭМИ РАН, результаты которого отражены в [13], были зарегистрированы попытки доступа из Интернета к административному серверу, никаких сервисов для Интернета не предоставляющему. В частности, за неделю 06-13.03.2002 к ip-адресу административного сервера зарегистрировано 1217 пресеченных попыток обращения. Неоднократно административный сервер заражался сетевыми вирусами. Следовало обеспечить его информационную безопасность.

Следующим отличием формируемого административно-финансового сегмента сети от предыдущих, полностью основанных на использовании протоколов TCP/IP, являлось использование протокола IPX между бухгалтерскими ПК и административным сервером.

Последним отличием административно-финансового сегмента сети от ранее имевшихся сегментов было желание не допустить в ЛВС побочные технологические ip-адреса, испускаемые во внешнюю сеть роутером. По заявлениям ряда системных администраторов, эта проблема «чистоты» ЛВС представляется неразрешимой (до настоящего времени ряд серверов на основе Windows 2000/2003+ Server испускает побочный технологический адрес). Нам, однако, представлялось, что решение все же возможно, но лежит вне Windows-технологии и связано с разделением функций роутера и файлсервера между двумя различными ПК, а главное – с использованием на ПК-роутере операционных систем клонов UNIX (Linux, FreeBSD, SCO UNIX и т.д.). Последующая реализация, описываемая далее, подтвердила нашу правоту.

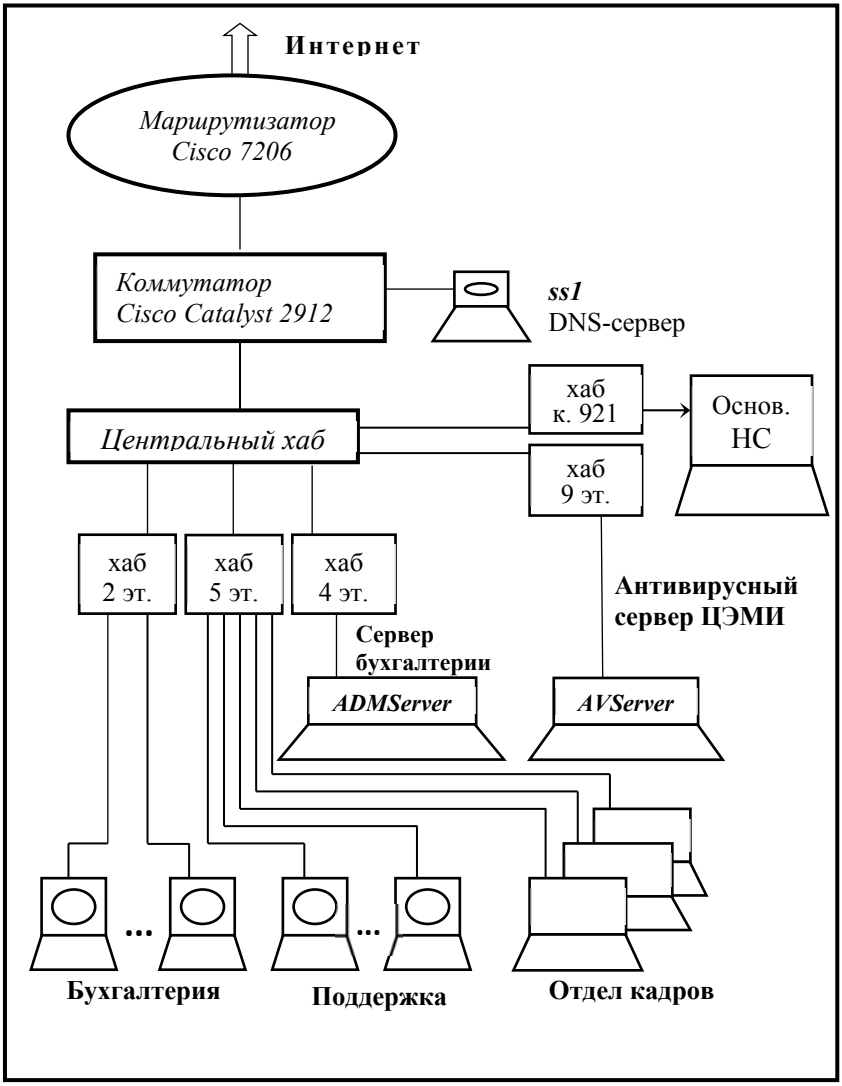

Рис. 16. Прежняя схема подключения административно-финансовой группы ПК

В связи с организационными трудностями, загруженностью другими работами и иными причинами выработка окончательного проектного решения была сильно задержана. За это время был получен ряд ценных дополнительных данных о внутрисетевом

трафике. Изменилась и общая структура ЛВС: вместо центрального хаба был установлен коммутатор Cisco Catalyst-2924 [14]. Была проведена полная реорганизация работы административного сервера с исключением использования протокола IPX в бухгалтерских приложениях.

Авторами всей этой работы [15] было выработано проектное решение по формированию выделенного сегмента ЛВС в составе роутера, 15 рабочих станций и нового административного сервера. К концу 2003 г. это решение было реализовано (число РС увеличено до 18) под непосредственным руководством руководителя Отделения экономической информатики М.Д.Ильменского. Прежняя и новая схемы соответствующих групп ПК изображены на рис. 16 и 17 соответственно.

Роутер выделенного сегмента сети функционирует на маломощном ПК Pentium-MMX-200[7] с объемом оперативной памяти 64Мб. Для связи с внутренним хабом сегмента и внешней частью ЛВС используются два сетевых PCI-адаптера со стандартной для ЛВС ЦЭМИ возможностью работы со скоростями 10 и 100 Мбит/сек. Операционной средой роутера является FreeBSD 5.1pl11, функционирующая в текстовой моде (для повышения эффективности графический интерфейс не устанавливался). Стоит сказать, что использование FreeBSD повышает быстродействие в отличие от Linux, в которой ядро хранит только таблицы. В качестве обеспечения режима маршрутизации и предотвращения сетевых атак на сегмент на роутере использован FireWall FreeBSD. В качестве NAT (трансляция сетевых адресов) [16] используется **natcd** на пользовательском уровне. Внутренние адреса выделенного сегмента определены как 192.168.2.x. Прямой доступ к ПК сегмента сети извне невозможен, равно как и опознавание источника исходящих пакетов: после выхода за роутер все пакеты несут MAC-адрес внешней сетевой карты роутера и его ip-адрес 193.232.194.4. С точки зрения адресного пространства ЛВС, весь выделенный сегмент сети представлен одним ip-адресом роутера. Внутренний трафик сегмента извне незаметен. Однако, по инициативе любого ПК сегмента возможно выборочное общение с общеинститутскими сетевыми службами и Интернетом по протоколам, разрешенным при трансляции адресов, видимое извне как активность роутера сегмента.

[7] В настоящее время, разумеется, более мощный.

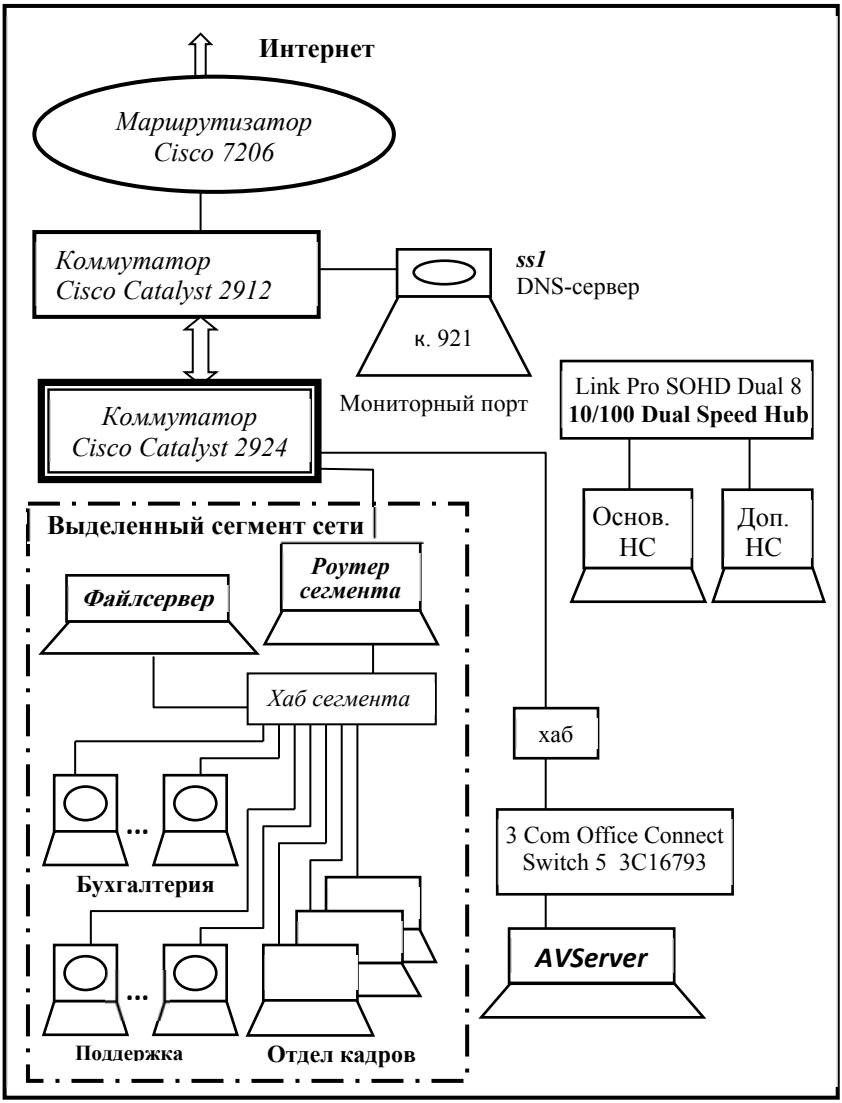

Рис. 17. Итоговая схема выделенного адм.-финансового сегмента ЛВС

В качестве обеспечивающих средств административного сервера имен Windows (WINS) в сегменте задействовано приложение Samba версии 2.8, предназначенное для объединения файловых систем UNIX и Windows [17], использованное с целью резкого

сокращения широковещательных пакетов (broadcasting). Для внешнего администрирования роутера используется SSH-сервер (Secure Shell), для чего требуется транспарентность пакетов по порту 22 между Интернетом и роутером сегмента. Доступ к БД административно-финансовых данных обеспечивается выделенным административным сервером, реализованным на Windows NT 4 (ServicePack 6).

Поскольку в описанное время центральный хаб института был уже заменён коммутатором Cisco Catalyst-2924, для включения ветви с выделенным сегментом в ЛВС института на коммутаторе был выделен специальный порт, питающий исключительно роутер выделенного сегмента. На этом порту был обеспечен Secure-режим, допускающий использование единственного сетевого устройства через этот порт – роутера сегмента сети. В целях обеспечения внешнего администрирования роутера сегмента через Cisco-7206 был разрешен пропуск пакетов TCP/IP по порту 22.

Заслуживает внимания схема снабжения членов выделенного сегмента сети дополнениями к антивирусной БД и обновлениями антивирусных версий. Как уже было отмечено выше, ни по виду пакетов, ни по ip-адресу отличить одну ноду сегмента от другой внутри ЛВС невозможно. В то же время, текущая политика лицензирования пакета Doctor Web для Windows, проводимая в описываемое время ЗАО «ДиалогНаука», требовала четкой идентификации ПК, на котором установлены антивирусные средства. В целях однозначной идентификации Антивирусным сервером (АВ-сервером) поступающих с одного и того же ip-адреса запросов на обновление были выполнены следующие работы:

- в настройках Apache антивирусного сервера среди ip-адресов всей локальной сети 194 выделена область адресов, запросы которых требуют парольного доступа для исполнения антивирусного обновления и пополнения БД;
- ip-адрес роутера выделенного сегмента переведен в означенную область;
- каждому ПК выделенного сегмента присвоен свой логин, для удобства соответствующий внутреннему ip-адресу в сегменте (к примеру, для 192.168.2.4 назначен логин BU04) и пароль;
- список логинов и паролей ПК выделенного сегмента сети введен в парольный файл доступа к области обновления антивирусных средств на Антивирусном сервере;

• указанные логин и пароль прописаны в настройках утилиты обновления пакета Doctor Web для Windows каждого ПК в выделенном сегменте;

• разработана программа учета доступа к антивирусной области сервера для выполнения генерации специальной формы учета по выделенному сегменту сети;

• скорректирован раздел Статистика Антивирусного сервера для показа текущей учетной формы выделенного сегмента сети;

• скорректированы пакеты ежедневно исполняющихся учетных заданий для добавочной обработки учетной формы выделенного сегмента сети.

Последние три из названных пунктов подробно освещены отдельно [7].

При поступлении с некоторого ПК выделенного сегмента от утилиты обновления через http запроса на обновление антивирусных средств, антивирусный сервер, определив по ip-адресу необходимость затребования логина и пароля, запрашивает их и, проверив, осуществляет требуемое обновление. Одновременно в логе работы Apache появляется запись с привязкой ко времени о парольном обращении соответствующего пользователя. Учетная программа, анализируя лог и видя логин указанного типа, соотносит его с внутренней БД пользователей выделенного сегмента и корректирует учетную информацию. Для всех ПК выделенного сегмента автоматический запрос на обновление антивирусных средств, согласно ранее разработанной методике [18], стоит в папке «Автозагрузка» и исполняется автоматически при включении ПК. Таким образом фиксируется последнее время включения каждого ПК выделенного сегмента сети, несмотря на то, что он находится за роутером.

На рис. 18 показано состояние четвертой таблицы раздела «Статистика» Антивирусного сервера. Эта информация, доступная через обычный браузер как часть антивирусного сайта [9], дает возможность оперативно отслеживать работоспособность компьютеров выделенного сегмента или потерю связи с Антивирусным сервером и таким образом осуществлять дистанционный контроль для принятия при необходимости оперативных мер.

Статистика * Антивирусная область

Обращения из выделенного фрагмента сети

Предыдущая Следующая	Данные БД	
Login и фамилия	**Послед. дата**	**Обращений**
BU02/Вегнер	00/00-0=00.00	00000
BU03/Беленова	31/08-4=16:02	00061
BU04/Ким	01/09-4=17:50	00134
BU05/Воеводина	31/08-4=14:49	00068
BU06/Рыбина	01/09-4=15:37	00114
BU07/Парини	01/09-4=15:26	00121
BU08/Учитель	01/09-4=17:01	00124
BU10/Егорова	26/08-4=17:34	00214
BU11/Кузнецова	01/09-4=09:51	00201
BU12/Хрестина	01/09-4=16:42	00073
BU13/Перова	01/09-4=11:13	00131
BU14/Илюшкина	01/09-4=13:13	00237
BU15/Железнова	01/09-4=11:31	00267
BU16/Бизюк	27/08-4=09:50	00184
BU17/Денисюк	01/09-4=10:22	00127
BU18/Исарова	01/09-4=14:37	00094
BU19/Герко	31/08-4=10:23	00169
BU20/Бурилина	27/08-4=15:03	00144
BU21/Григорьева	27/08-4=15:32	00157

Рис. 18. Статистика доступа из выделенного сегмента сети к АВ-серверу

Уже в первые дни после начала работы выделенного сегмента сети, по данным мониторинга наблюдающих станций, сбалансировался процент внутрисетевых пересылок (см. рис. 19) в основной части ЛВС, снизились пиковые значения максимальной скорости в

сети и число коллизий уменьшилось до допустимой нормы. При этом, для сотрудников выделенного сегмента сохранены все основные преимущества: электронная почта, Интернет (замедления связи не отмечалось), антивирусная поддержка.

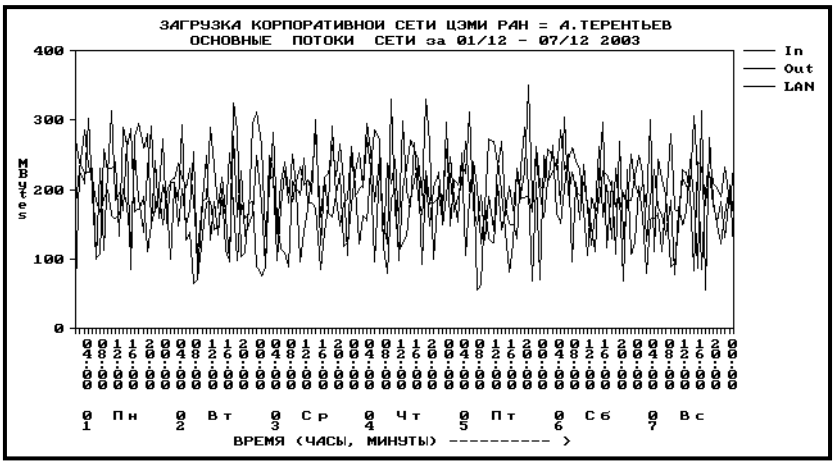

Рис. 19. Пример сбалансированных внутрисетевых пересылок в ЛВС

Таким образом, вычлененная на основе анализа информационных потоков группа ПК с учетом организационной структуры, действующих комплексов задач и общности данных синтезирована в самостоятельно функционирующий сегмент локальной сети института. Построенный описанным образом выделенный сегмент ЛВС снабжается необходимыми общесетевыми услугами (Интернетом, почтой и антивирусной поддержкой) и отвечает требованиям функционирования в общей среде локальной сети института.

В целом были выполнены следующие работы.

- С учетом опыта существующих выделенных сегментов сети предложена схема типового сегмента ЛВС на базе роутера, внутреннего сервера и ряда рабочих мест.
- Определены технические данные, платформа, конфигурация и необходимое программное обеспечение роутера и сервера, позволяющие вписать выделенный сегмент в имеющуюся структуру ЛВС с сохранением независимых логических подключений к внутренней почте и Интернету. Программное обеспечение роутера

выбрано с минимальными затратами на техническую часть (выполнено В.А.Вегнером).

▪ Разработана методика и реализовано индивидуальное подключение членов сегмента к общеинститутским информационным ресурсам, в том числе антивирусным средствам на базе современной технологии web-сервера с возможностью автоматического обновления и автоматического периодического сканирования дисков рабочих станций.

▪ Проведена настройка поддерживающих проект аппаратно-программных средств и перенастройка сетевых сервисов.

Реализованный проект решил задачу построения типового выделенного сегмента ЛВС и может быть рекомендован для масштабирования в рамках ЛВС института. В ходе работы над проектом получены конкретные данные, рекомендующие реализовать аналогичный проект нескольким подразделениям института.

Впоследствии типовая реализация проекта была использована для подключения во внутреннюю часть ЛВС сторонних организаций.

2.3. Исследование почтовых сеансов

Электронная почта, или E-Mail, в корпоративных сетях является одним из наиболее известных пользователям сетевых сервисов. Общение с помощью электронной почты стало одной из самых давних базовых услуг Интернета, нисколько не снизившей своих функций с быстрым его развитием. Качество функционирования E-Mail во многом определяет успешность и стиль работы организации. С точки зрения сетевого администрирования, в средних и крупных сетях обычно имеется несколько поддерживающих почтовых серверов с распределенными функциями. В небольших сетях, как правило, эти функции объединены на одном почтовом сервере, служащем и как транспортный агент и как пользовательский сервер, а также обеспечивающем процедуры антивирусной и противоспамовой обработки электронной почты. Как правило, транспортные серверы работают по стандартным протоколам обмена электронной почтой (SMTP, ESMTP), а получение почты пользователями из ящиков производится посредством различных протоколов, как давно известных (POP2/POP3, IMAP), так и более современных, включающих в себя шифрование (POPS, IMAPS) и других вариантов клиентских и прокси протоколов: hybrid-pop, ironmail и т.д. Здесь, в основном, рассматривается **получение** почты по

протоколу POP3 [19] (порт 110) с почтового сервера клиентом по инициативе последнего.

Поясним для неспециалистов, что имеются в виду сеансы связи с помощью почтовых программ-клиентов типа Microsoft Outlook, Outlook Express, The Bat!, причем только получение почты, но не отправка. Интерактивная работа с почтовыми ящиками через браузеры (по протоколу http) здесь не рассматривается.

Процесс приема почты является весьма удобным для рассмотрения сетевым сервисом по следующим причинам. Данный сервис существует практически в любых сетях, известен и многократно описан. Он интуитивно понятен пользователям-непрофессионалам. Функциональная нагрузка этого сервиса напрямую зависит от осознаваемой активности пользователей и уровня их знаний в настройке собственного ПК.

Получение пользователями корпоративной сети ЦЭМИ РАН пришедших писем осуществляется по следующей схеме (см. рис. 20). Основная прибывающая почта после обработки на шлюзе ***smtprelay.cemi.rssi.ru*** передается на основной транспортный сервер (Mail Relay) ***is1*** 193.232.194.51 (на рис. 20 ip-адреса обозначены своими двумя последними компонентами). Далее почта частично переносится на основной сервер локальной сети ***Server1***, а часть поступает непосредственно пользователям, имеющим почтовый ящик на ***is1*** (например, большинство пользователей DialUp имели ящики на этом сервере).

В схеме рис. 20 изображение несколько опережает текущее изложение материала: вместо хабов установлены коммутаторы Cisco (рассматриваются в последующем томе данной работы), что, однако, не мешает пониманию смысла изложенных процессов.

Таким образом, стандартно пользователи КВС обращаются за почтой на ***Server1***. Однако, в КВС присутствует также ряд почтовых серверов, получающих почту своих пользователей самостоятельно. Ряд пользователей обращается за почтой именно к этим серверам (быть может, в дополнение к основному серверу).

Наконец, у ряда пользователей КВС существуют почтовые ящики на внешних (в основном бесплатных) серверах в Интернете, куда они также периодически обращаются за почтой.

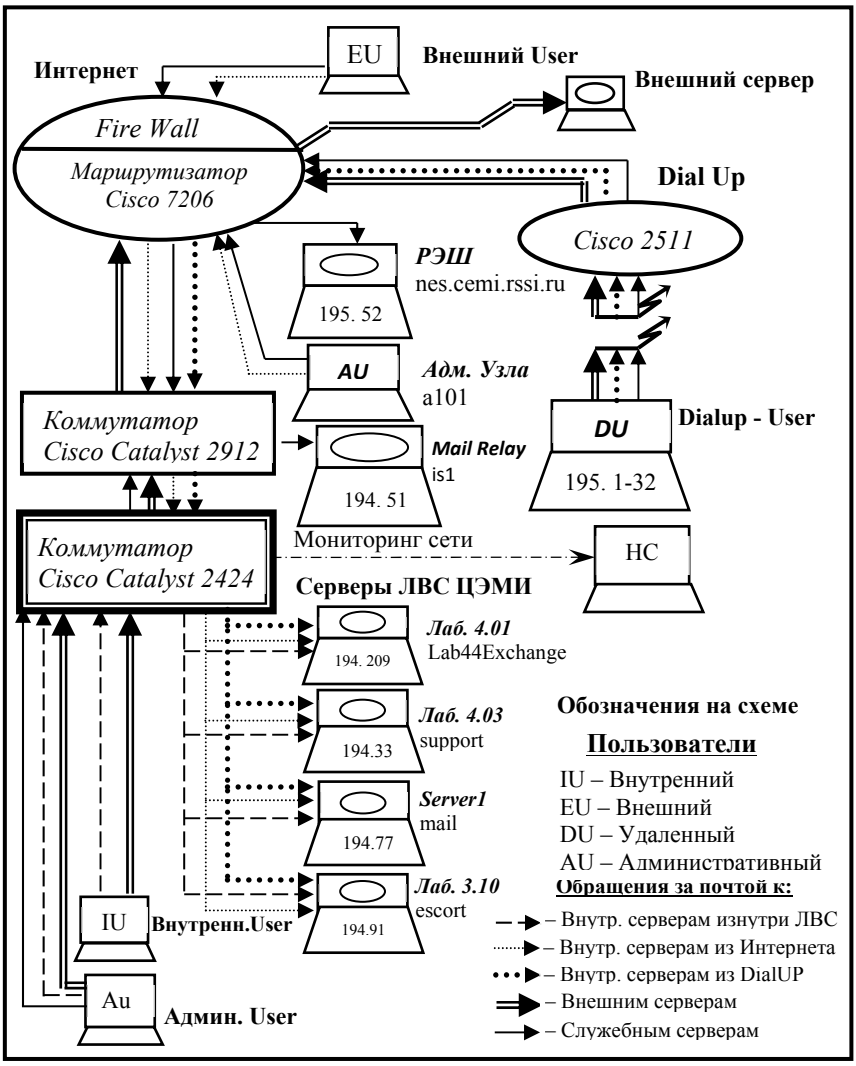

Рис. 20. Схема получения почты с почтовых серверов в КВС ЦЭМИ РАН

Рассматривая пользователей-клиентов электронной почты по местоположению ПК, с которого производится обращение, можно условно выделить «*внутренних*» пользователей по отношению к рассматриваемой КВС и «*внешних*». В свою очередь, из

«внутренних» можно выделить «удаленных» (получающих доступ по телефонным каналам через сервер удаленного доступа) и «административных», имеющих доступ на сервер ***is1***. Таким образом, «внутренние» пользователи могут получать почту как с различного ранга серверов КВС, так и с внешних серверов. «Удаленные» и «административные» пользователи также имеют возможность получения почты как с административного или общего сервера, так и с прочих внутриинститутских, а также внешних серверов. Наконец, «внешним» пользователям из Интернета также открыт доступ для приема почты со всех означенных серверов.

Такая схема сложилась исторически. Ряд научных коллективов, разрабатывая актуальные когда-то проекты, построили свои внутриинститутские почтовые сервера со своим коллективом пользователей, которые продолжают действовать даже после окончания проекта или ухода сотрудников. Разумеется, и ряд сотрудников института, бывая в командировках, получает почту с указанных серверов через Интернет.

Вообще говоря, вопросы правомерности идентификации пользователей и количество отказов в доступе почтовым клиентам могут быть протоколированы на почтовых серверах. Кроме того, каждый пользователь имеет возможность включить протоколирование работы почтового клиента в своем ПК и собрать соответствующую статистику (пример протокола почтового клиента Outlook Express на отдельном ПК см. на рис. 21): Однако, аналитические данные по отдельным почтовым серверам и ПК, входящим в КВС ЦЭМИ РАН, не были опубликованы.

Рассмотренные виды статистики, представляется, имеют один общий недостаток. Представленные данные носят односторонний характер, в силу чего их трудно сопоставить с общей обстановкой в КВС. Отсутствие сравнительных данных не дает возможности строить эффективную системную политику в отношении почты как сетевой сервисной услуги пользователям, не позволяет говорить о приоритетах и не вскрывает возможные недостатки.

```
Outlook Express 5.00.2417.2000
POP3 Log started at 03/26/2004 11:38:45

Outlook Express 5.00.2417.2000
POP3 Log started at 04/01/2004 13:50:10
POP3: 13:53:54 [rx] +OK cemi.rssi.ru POP MDaemon 6.8.5 ready
      <MDAEMON-F200404011357.AA5750967MD8050@cemi.rssi.ru>
POP3: 13:53:54 [tx] USER a103
POP3: 13:53:54 [rx] +OK a103... Recipient ok
POP3: 13:53:54 [tx] PASS
POP3: 13:53:57 [rx] -ERR access denied
```

Рис. 21. Фрагмент протокола Outlook Express на пользовательском ПК

Как было показано в [1], метод комплексного сетевого мониторинга с конца 2001 г. включил в себя исследование почтовых сеансов POP3. Там же подробно показаны основания, по которым отбираются транзакции почтовых сеансов, без восстановления стэков TCP/IP и тем более прикладного уровня. Однако, в ходе исследований было установлено, что инициирующая начало почтового сеанса по протоколу POP3 транзакция формируется всегда в виде *отдельного* сетевого пакета, имея в теле TCP строку вида "**USER xxx.x**" с именем пользователя. Аналогично, если сервер подтвердил открытие POP3-сессии с указанным именем пользователя, после положительного ответа сервера запрашивающий сессию абонент подает второй *отдельный* сетевой пакет со строкой "**PASS yyy...y**".

Практически с начальной версии программное обеспечение наблюдающей станции начало фиксировать эти пакеты для определения фактов установления почтовых сессий в протоколе работы. С тех пор данные о точном отображении инициации сеанса неоднократно менялись. Так, выяснилось, что ряд особым образом настроенных почтовых программ, осуществляющих групповые запросы на прием почты, посылает только одну строку "**USER**", соответствующую нескольким сеансам связи, поэтому истинно состоявшиеся сеансы следует фиксировать только по строкам "**PASS**". Далее, оказалось, что аналогичные строки используются не только в сеансах POP3, но и в протоколе FTP, поэтому среди отобранных строк следует осуществлять фильтрацию по номеру порта 110. Соответственно этому, в процессе совершенствования сетевого мониторинга неоднократно менялся формат регистрации клиентских запросов в логе, и в настоящем виде эти сообщения имеют вид, показанный на рис. 22 (пароли POP3 заменены звездочками).

```
!20041008:143001= List 8700 formed at 14:30:01 [01]
!20041008:143009$ 194.067.023.102<193.232.194.033/00110:USER andrewiooo
!20041008:143009$$009027370F50 194.067.023.102<193.232.194.033:PASS ***
!20041008:143018$ 193.232.194.033<212.057.107.094/00110:USER api
!20041008:143018$$000652324406 193.232.194.033<212.057.107.094:PASS ***
!20041008:143046$ 193.232.194.033<194.085.216.050/00110:USER eg
!20041008:143046$ 193.232.194.077<193.019.082.007/00110:USER zak
!20041008:143046$$000652324406 193.232.194.033<194.085.216.050:PASS ***
!20041008:143046$$000652324406 193.232.194.077<193.019.082.007:PASS ***
!20041008:143134$ 193.232.194.033<212.057.107.094/00110:USER api
!20041008:143134$$000652324406 193.232.194.033<212.057.107.094:PASS ***
!20041008:143145$$00C026A64B4B 063.247.135.234<193.232.194.093:PASS ***
!20041008:143145$$00C026A64B4B 063.247.135.234<193.232.194.093:PASS ***
!20041008:143149$ 193.232.194.077<062.118.057.194/00110:USER genkey
!20041008:143149$$000652324406 193.232.194.077<062.118.057.194:PASS ***
!20041008:143200$ 145.249.012.021<193.232.194.103/00021:USER anonymous
!20041008:143200$$004005407E97 145.249.012.021<193.232.194.103:PASS IE40user@
!20041008:143222$ 193.232.194.033<212.057.107.094/00110:USER api
!20041008:143222$$000652324406 193.232.194.033<212.057.107.094:PASS ***
!20041008:143223$ 193.232.194.209<212.119.108.078/00110:USER sergep
!20041008:143325$ 193.232.194.077<193.232.194.088/00110:USER kogalov
!20041008:143325$$0050DA3884EC 193.232.194.077<193.232.194.088:PASS ***
!20041008:143325$ 193.232.194.077<193.232.194.088/00110:USER ecoins98
!20041008:143325$$0050DA3884EC 193.232.194.077<193.232.194.088:PASS ***
!20041008:143330$ 193.232.194.077<212.092.101.006/00110:USER alex
!20041008:143330$$000652324406 193.232.194.077<212.092.101.006:PASS ***
```

Рис. 22. Фрагмент лога наблюдающей станции с контактами по POP3 и FTP

Анализ приведенного фрагмента протокола позволяет сделать ряд выводов.

- Ряд пользователей обращается за почтой *ежеминутно*, существенно увеличивая трафик в КВС и загружая POP3-серверы, что приводит к задержкам доступа к ним других пользователей.
- Ряд пользователей (строка от 14:32:42 приведенного фрагмента протокола, пользователь **sergep** – Сергей Поляк, ко времени обращения оставивший работу в ЦЭМИ РАН) обращается за почтой *незаконно*, не являясь сотрудниками ЦЭМИ РАН.
- Некоторые ПК (строки от 14:30:09 и от 14:30:18), получая почту с различных внешних серверов, сами являются внутренними почтовыми серверами, в том числе для внешних пользователей (т.е. на таких ПК установлены и POP3-клиент, и POP3-сервер для внешних пользователей).
- В ряде случаев при высокой загрузке сети строки "**USER**" и "**PASS"** могут не обязательно следовать друг за другом непосредственно: между ними могут появиться прочие строки протокола НС (строки от 14:30:46).
- Поскольку мониторинг сети не обязательно является сплошным, и всегда существует возможность пропуска отказанных к обработке пакетов (подробнее см. в [1]), не говоря уже о существующих технологических перерывах мониторинга для фиксации текущих данных, то полной уверенности в отражении в протоколе абсолютно всех состоявшихся сеансов быть не может (строки от 14:31:45).
- Подтверждено наличие хакерских попыток подбора паролей или организации атак типа dDoS на почтовый сервер ЛВС ЦЭМИ по широко известным логинам (строка от 14:33:30 – идентификатор **alex** был удален 26.08.2004, а почту не получал с 25.03.1998).

Совокупный анализ ряда протоколов за сентябрь 2004 г позволил также обнаружить попытку сканирования всех доступных почтовых серверов по логину **root**, обычно обладающему административными правами, с возможной целью взлома. Источник действовал из США через Verizon Internet Services, с ip-адреса 68.163.44.42.

Как видим, попытки фиксации почтовых сеансов данным методом имеют неопределенности и обладают определенной погрешностью. Поэтому, обсуждение результатов, полученных ниже, должно проводиться с пониманием того, что они являются зафиксированным минимумом состоявшихся почтовых сеансов, число

которых в реальности может быть несколько больше. Проведенный далее анализ развития трафика почтовых сеансов выполнен на основе совокупного взаимосвязанного подсчета строк "**USER**" и "**PASS**" в протоколе и является более точным, чем моментальное отображение сеансов на экранах наблюдающей станции [1], исполняемое только на основании пакетов "**USER**".

Далее, как указано в [1], не всякий сеанс POP3 в КВС ЦЭМИ может быть отслежен. Сводная таблица возможности мониторинга различных типов пользователей с разными серверами дана на рис. 23.

Сервера	**Пользователи, получающие почту по протоколу POP3**			
	Внутренние	**Администрат.**	**Удаленные**	**Внешние**
Служебные	**Да**	**Да** (кроме Адм. Узла)	**Нет**	**Нет**
Внутренние	**Да**, кроме обращений из того же фрагмента сети	**Да**	**Да**	**Да**
Внешние	**Да**	**Да** (кроме Адм. Узла)	**Нет**	**Нет**

Рис. 23. Возможность мониторинга POP3-контактов к серверам КВС

При разработке статистической программы обработки логов учтены указанные выше особенности. Объединяя внутренних и административных пользователей, а также внутренние и служебные сервера, имеем 4 основные группы регистрируемых почтовых сеансов:

- от внутренних пользователей к внутренним и служебным серверам;
- от внутренних пользователей к внешним серверам;
- от удаленных[8] пользователей к внутренним и служебным серверам;
- от внешних пользователей к внутренним и служебным серверам.

На рис. 24 [19] показано состояние этих сервисов за месяц. Отчетливо заметны недельные изменения. Лидирующее число запросов было во вторник, 07 числа.

[8] В настоящее время удалённый доступ по модемам в ЦЭМИ РАН закрыт

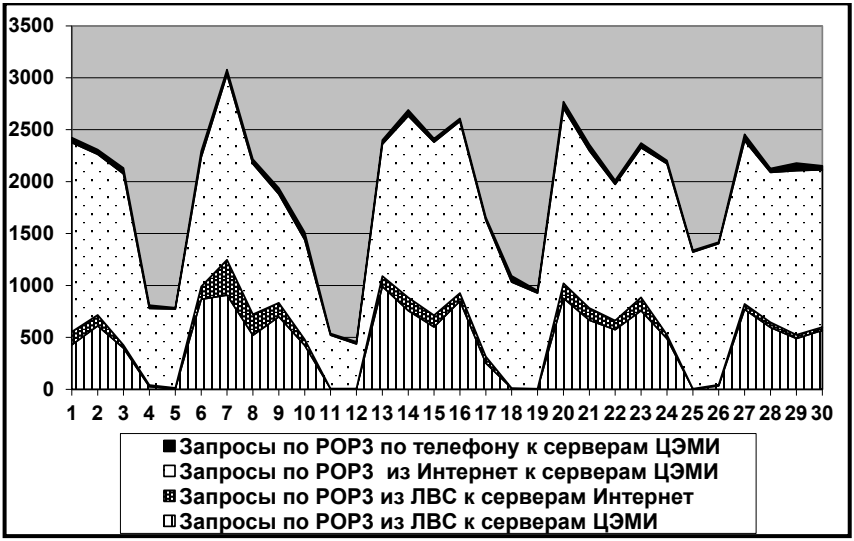

Рис. 24. Запросы POP3-клиентов в КВС ЦЭМИ РАН за сентябрь 2004 г.

Легко видеть, что **число запросов внешних пользователей устойчиво и намного превышает совокупные запросы внутренних и удаленных пользователей**, т.е. тех, для обеспечения которых, в первую очередь, и существует корпоративная сеть института. За годы исследований эти тенденции все более росли.

Другую любопытную особенность вскрывает следующий шаг анализа почтового сервиса. Фиксация строк USER и PASS в ежедневном протоколе наблюдающей станции не могла не спровоцировать нас на вопрос о равномерности потребления почтовых услуг разными пользователями. Увы, и в этом вопросе наблюдалось очевидное, несправедливое и все более увеличивавшееся неравенство: **незначительное число отдельных лиц загружает своими обращениями почтовые сервера в десятки раз больше, чем все остальные пользователи, взятые вместе**. На рис. 25 даны числа обращений различных пользователей к серверам за тот же месяц, что и на рис. 24.

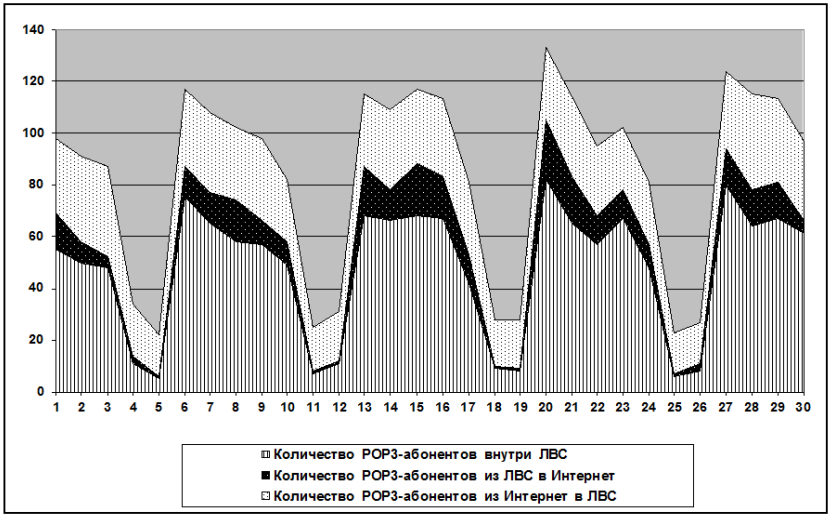

Рис. 25. Количество POP3-абонентов в КВС ЦЭМИ РАН за сентябрь 2004 г

Видно, что из общего числа почтовых ящиков внутри ЛВС ЦЭМИ РАН (не менее 230) используется не более 110 за день (в среднем, 74). Также видно, что число абонентов почтовых ящиков на серверах Интернета составляет в среднем около 20% от числа абонентов внутри ЛВС ЦЭМИ РАН, т. е. каждый пятый активный пользователь имеет дополнительный почтовый ящик в Интернете. Число внешних абонентов (включая и отвергнутые попытки обращения извне к несуществующим пользователям, и доступ сотрудников через Интернет) достигает в среднем 30% от общего числа абонентов.

Из рис. 25 следует, что число внешних абонентов почтовых ящиков внутренних серверов (верхняя область) как минимум в 4 раза ниже прочих. Однако, на рис. 24 ясно видно, что те же внешние абоненты дают более половины всех почтовых сеансов (!). Для лучшего обозрения сказанного приведем таблицей один типичный день (рис. 26, взято также из [19]).

	Варианты типов обращений			
	Внутр. к внутр. серверам	Удаленных к внутр. серв.	Внутр. к внешним серверам	Внешних к внутр. серверам
Попыток обращений	716	11	65	1423
Пользователей	80		17	31
Среднее количество попыток обращений на одного пользователя	**9,1**		**3,8**	**45,9**

Рис. 26. Число зарегистрированных POP3-запросов 04 октября 2004 г.

Как видим, действительно, основную нагрузку на почтовые сервера давали внешние абоненты. Средства сетевого мониторинга позволяют выяснить поименно, кто именно и откуда дает наибольший поток вызовов. Рис. 27 показывает полный список обращений к почтовым серверам за тот же день, агрегированный по числу однотипных обращений одного и того же пользователя к одному и тому же серверу. Список отсортирован в убывающем порядке по числу обращений.

Результаты весьма красноречивы. Максимум обращений выполнен из Интернета, причем первое место держат внешние обращения к неофициальному серверу.

Адрес пользователя	Адрес сервера	Имя абонента	Тип обращ.	Всего обращ.
212.057.107.094	193.232.194.033	api	Извне	530
193.019.082.007	193.232.194.077	zak	Извне	389
212.119.108.078	193.232.194.209	sergep	Извне	115
193.232.195.016	193.232.194.077	kogalov	DialUp	99
193.232.194.088	193.232.194.077	ecoins98	Внутр.	95
194.067.023.103	193.232.194.077	slast	Извне	63
062.118.057.194	193.232.194.077	genkey	Извне	49
195.058.037.192	193.232.194.033	market	Извне	37
194.085.216.050	193.232.194.033	irinats	Извне	35
194.085.216.050	193.232.194.033	eg	Извне	33
193.232.194.087	193.232.194.077	albert	Внутр.	32
193.232.194.212	194.067.023.102	jet999	Наружу	31
193.232.194.224	193.232.194.077	kachalov	Внутр.	27
193.232.194.159	193.232.194.077	elev	Внутр.	25
193.232.194.159	193.232.194.077	ilmensky	Внутр.	25
082.181.029.054	193.232.194.077	peresetsky	Извне	23
194.067.023.103	193.232.194.077	spivak	Извне	22
194.067.023.103	193.232.194.077	efimov	Извне	21
194.067.023.103	193.232.194.077	sotskov	Извне	21
194.067.023.103	193.232.194.077	vl_levin	Извне	21
194.067.023.103	193.232.194.077	danilov	Извне	21

193.232.194.083	193.232.194.077	iger	Внутр.	19
193.232.194.216	193.232.194.077	aspir	Внутр.	18
193.232.194.207	193.232.194.077	lenail	Внутр.	18
193.232.194.218	193.232.194.077	erzink	Внутр.	15
082.142.180.100	193.232.194.033	inter	Извне	15
193.232.194.253	193.232.194.077	ecr	Внутр.	15
193.232.194.107	193.232.194.077	golshtn	Внутр.	12
193.232.194.202	193.232.194.077	varshav	Внутр.	14
193.232.194.097	193.232.194.077	prettyal	Внутр.	14
193.232.194.120	193.232.194.077	shatalin	Внутр.	11
193.232.194.112	193.232.194.077	kozyrev	Внутр.	11
193.232.194.079	193.232.194.077	levashov	Внутр.	11
193.232.194.182	193.232.194.077	verkhovskaya	Внутр.	10
193.232.194.087	062.076.011.151	bakh	Наружу	10
193.232.194.071	193.232.194.077	avdmi	Внутр.	10
193.232.194.182	193.232.194.077	makarov	Внутр.	10
193.232.194.145	193.232.194.077	vovs	Внутр.	10
90 строк опущены			.....	Менее 10
193.232.194.013	193.232.194.051	tam	Внутр.	1

Рис. 27. Сводка POP3-запросов к почтовым серверам 04 октября 2004 г.

Анализируя списки имен пользователей-абонентов почтовых ящиков за заметный период по всем почтовым серверам, можно также видеть неравномерность распределения запросов. Достаточное представление об этом дает приведенная на рис. 28 месячная сводка.

Серверы		Пользователи		Запросов	
Имя	**Адрес**	**Кол-во**	**Из них фальшивых**	**Кол-во**	**%**
Support	194.33	21	2	12329	33,8
is1	194.51	4	0	175	0,5
server1	194.77	143	2	20854	57,2
Escort	194.91	1	1	1	0,0
lab44exchange	194.209	3	0	1446	4,0
Внешние серверы		24	Нет данных	1651	4,5
ИТОГО		**196**		**36456**	**100,0**

Рис. 28. Сводка POP3-запросов к почтовым серверам за сентябрь 2004 г.

Наконец, интерес представляет «почтовая компонента» в общем трафике. В этой связи следует отметить, что собственно трафик POP3 средствами существующей версии сетевого мониторинга возможно выделить только там, где он составляет единственную компоненту взаимосвязи между двумя сетевыми адаптерами с известными MAC-адресами. В мониторируемых ПК, к счастью, есть одна такая составляющая: это пересылки от административного (***is1***) сервера КВС основному почтовому серверу ЛВС (***Server1***), между прочим, соотносимые с трафиком всех POP3-пользователей сервера ***Server1***. Обращаясь к рис. 20, видим, что трафик указанной пересылки является входящим в ЛВС. Поэтому естественно сравнить его с общим потоком поступающей из Интернета информации. Собственно, именно эти два трафика и являются основными входящими в ЛВС, помимо обращений из DialUp к отдельным ПК ЛВС. Почасовой анализ (рис. 29) обоих названных компонент входящего трафика все за тот же день показывает, что трафик основного почтового сервера по протоколу POP3 по своим объемам составляет заметную долю в ЛВС только ночами, при весьма низких абсолютных значениях трафиков.

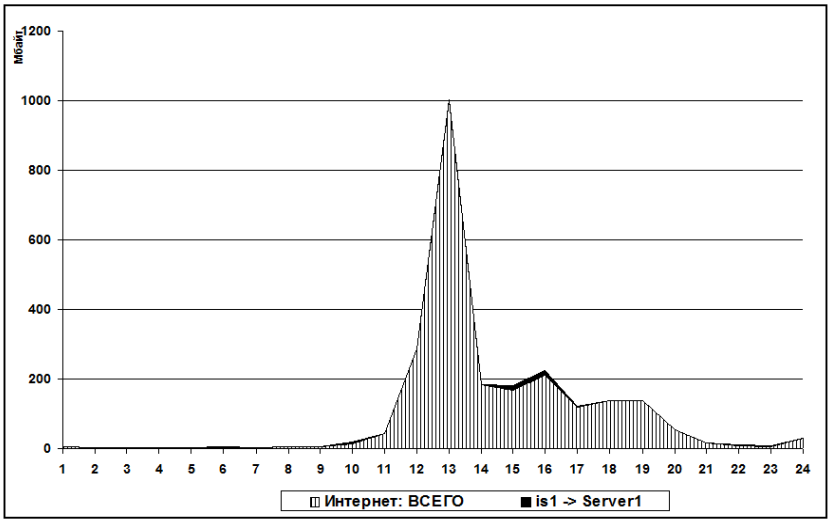

Рис. 29. Общий трафик из Интернета и POP3-трафик Server1 за 04.10.2004 г.

В [19] отмечается, что основным результатом проведенных исследований является назревшая к 2004 г. необходимость выработать и внедрить политику работы пользователей с электронной почтой с учетом аспектов информационной безопасности. При этом предполагалось затронуть следующие аспекты.

- Пересмотреть имеющийся список внешних пользователей всех почтовых серверов с целью постепенного исключения всех ящиков и перевода пользователей на основные почтовые серверы. В перспективе – закрыть все почтовые серверы, кроме административного и основного.
- Резко ограничить или запретить вообще обращения внутренних пользователей к внешним почтовым серверам с целью предотвращения вирусных эпидемий в КВС ЦЭМИ (не выполнено).
- В целях существенного снижения нагрузки почтовых серверов ЛВС ЦЭМИ РАН рекомендовать установить пользователям предельное число обращений к почтовому серверу в сутки (рекомендуемое значение – 12).

2.4. Опыт переносной наблюдающей станции

До настоящего момента вопросы эксплуатации программного обеспечения комплекса сетевого мониторинга и аудита обсуждались применительно к стационарному варианту. Однако, обозначив одну из важных функций сетевого мониторинга как вопрос экономических приложений, до 2004 года автор не имел возможности проверить на реальном опыте многие технологические процессы, сопровождающие развертывание и установку наблюдающих средств на новом месте, особенности их эксплуатации и формирование заключительного отчета.

Между тем, быстрота ввода в эксплуатацию разработанных средств на новом месте представляются одной из важных эксплуатационных характеристик наблюдающей станции.

В августе 2004 г. автору представилась возможность испытать разработку в сфере прикладной экономики. Одна из фирм грузоперевозок с малым числом сотрудников обратилась с просьбой проверить счета, присылаемые на оплату провайдером. По условиям договора, оплачивался только входящий трафик фирмы, причем взималась фиксированная оплата за трафик в рамках договора и существенно повышенная за превышение трафика.

Заказчику представлялось, что в течение нескольких месяцев провайдер существенно завышает их входящий трафик.

Исследованиям подверглась рабочая среда в виде 4х ПК, объединенных в локальную сеть с помощью стандартного 5-портового концентратора типа switch фирмы 3Com. К этому же концентратору подключался разъем от гейта (рис. 30).

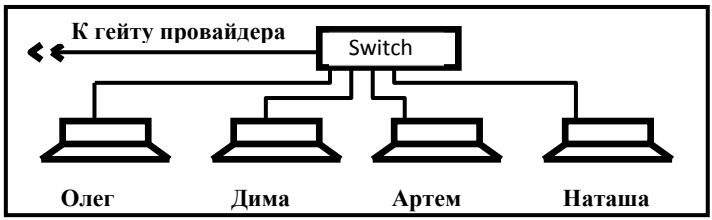

Рис. 30. Исходная схема исследуемой рабочей группы

В качестве средства исследования был использован системный блок мобильной НС на основе Everex Pentium-120[9] с заимствованной на месте клавиатурой. На время настройки был подключен монитор. В целях полноты фиксации всех проходящих в сети пакетов имевшийся концентратор был заменен на Hub Link Pro Dual 8 10/100. Результирующая схема приведена на рис. 31. НС была установлена открыто, но ее функции всем сотрудникам не сообщались. Экран подключался к системному блоку только на период настройки и снятия результатов.

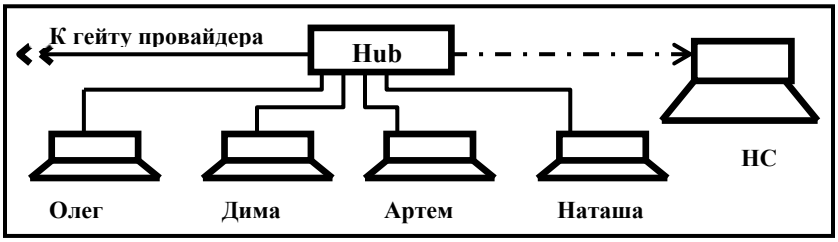

Рис. 31. Схема рабочей группы, модифицированная для измерений

Настройка НС состояла в следующем. Заказчик знал ip-адрес гейта и локальные ip-адреса всех сотрудников, но не мог сообщить MAC-адреса (с которыми работает программное обеспечение НС). Тестовый запуск НС в режиме собирания информации позволил в считанные минуты определить по излучаемому бродкастингу (на экране просмотра пакетов) MAC-адреса всех сотрудников и провайдера.

Далее база была откорректирована в текстовом режиме с помощью Volkov Commander, были сделаны необходимые установки в BAT-файле и запущен рабочий режим. Вся процедура настройки заняла не более 10 минут.

Проверке подлежали следующие гипотезы.

- Априорная оценка заказчика верна; провайдер представляет неверные данные о фактическом входящем в сегмент трафике.

[9] Этот ПК работоспособен до настоящего времени и используется Антивирусной службой ЦЭМИ РАН для отслеживания присутствия сотрудников на рабочих местах.

• Априорная оценка заказчика неверна; провайдер представляет истинные данные о трафике, который повышен вследствие неявной активности сетевых вирусов на смежных ПК соседних сетей (в том же здании их более 40), сканирования ПК наблюдаемой сети, сетевых атак или иных причин.

• Априорная оценка заказчика неверна; провайдер дает верные сведения о трафике; истинное потребление ПК в наблюдаемой сети по каким-либо причинам выше, чем предполагалось в априорной оценке заказчика.

Все ПК сотрудников были протестированы на вирусы современными антивирусными средствами. На 2х ПК были обнаружены вирусы несетевого класса, так что гипотеза о вирусной активности подтверждения не получила. Анализ первых суток работы НС не показал в сети наличия пакетов с посторонними ip-адресами, излучаемыми вне гейта. Не оказалось также излучения UDP- и ICMP-пакетов, характерных для сетевых вирусов. Таким образом, вторая гипотеза отпала.

Замеры исполнялись в течение 3х неполных суток. Для облегчения последующих подсчетов, вследствие сравнительно небольшого трафика НС была сконфигурирована на выдачу 1 полного отчета в час. Пример отчета приведен на рис. 32.

После получения замеров за полный рабочий день был осуществлен сводный подсчет результатов по всем отчетам, и эти данные сравнены с данными провайдера за те же сутки, полученными специальным запросом. Интересуемые данные находились в секции «Сведения о трафике выделенных нод». Непосредственно под строкой “**ПРОВАЙД-Испущено**”, дававшей общий объем выкачанной информации из Интернета, идет раскладка по отдельным ПК, кто сколько скачал. Разумеется, были выделены **все** ноды для получения подробных данных, тем более что один из компьютеров (***Дмитрий***) использовался как базовый ПК для получения почты и вынужденно показывал заметный трафик.

Интересуемые данные за два отчетных дня представлены на рис. 33.

```
#00 ЦЭМИ РАН *  Аудит корпоративной сети * 4.52 = А.Терентьев
#02 Полный, пополняющий файл отчета <TAMC0052.LST>, серия начата с 0039
#04 Программа запущена 10/06-04 в 00:00:05
#05 Текущее время      10/06-04 = 14:00:00, работает     50395с
#06 В цикле    3600сек.; всего   13ч59м55с
#07 Отчет сформирован  по признаку   8
#10 Взято пакетов:  16647,       Байтов:  6291504
#11 Мимо пакетов:       0,       Байтов:        0
#13 Ошиб.пакетов:       0,       Байтов:        0
#12 Скорость максимальная:   84.91 Kb/s;   Средняя:   1.71 Kb/s
#17     Всего циклов минимально:    3065;    максимально:    6957
#18 Ситуаций пропуска пакетов:       0   макс.буферов: 23%
#30  =     Структура внутрисетевого трафика
#31 InterNetFro    0006400 004689878
#32 InterNetTo:    0006554 000713776
#33 IntroLAN:      0003693 000887850
#50 - - - - - - - - - -
#60  = Сведения о трафике выделенных нод      И С П У Щ Е Н О     П Р И Н Я Т О
#61 001. 0007E9473FD7 5.001/0F:ПРОВАЙД 0511{0006400 004689878 0006554 000713776
#62.003  0050BAC0AEEC 5.004/02:Дмитрий 0511{0002126 001887008 0002043 000207740
#62.004  005004C85824 5.008/03:Артем   0511{0000173 000113754 0000200 000025241
#62.005  00055D499C66 5.002/04:Наташа  0511{0004101 002689116 0004311 000480795
#80  = Сведения о всех нодах и их трафике           И С П У Щ Е Н О
001.0007E9473FD7 192.168.115.001/0F:ПРОВАЙД  0511 {0006400 004689878 0319
002.00E018D45012 192.168.115.009/01:Олег     0511 {0000000 000000000 0011
003.0050BAC0AEEC 192.168.115.004/02:Дмитрий  0511 {0003856 000673959 8311
004.005004C85824 192.168.115.008/03:Артем    0511 {0000555 000071005 8311
005.00055D499C66 192.168.115.002/04:Наташа   0511 {0005836 000856662 8311
Конец отчета <TAMC0052.LST>
```

Рис. 32. Отчет наблюдающей станции от 10.06.2004 за 14:00:00

	Объемы скачанной информации (байты)			
Часы за 09.06.2004	**Олег**	**Дима**	**Артем**	**Наташа**
11	0	768724	0	2277310
12	0	527209	727056	3763251
13	1920113	375933	262442	1622836
14	2497396	403974	108616	1687603
15	130477	80900	54197	1966320
16	30686	0	10565	6833770
17	0	30994	77735	2120586
18	0	73216	1221542	202853
19	0	32560	1125771	0
20	0	33432	1916948	0
21	0	0	7656	0
Всего за 09.06.2004	**4578672**	**2326942**	**5512528**	**20474529**
Часы за 10.06.2004	**Олег**	**Дима**	**Артем**	**Наташа**
11		279341		1088888
12		1027253		7785762
13		2338258		2764718
14		1887008	113754	2689116
15		58475	348219	1743218
16	1133531	103569	287644	52713
17	341240	408		339214
18		358		974238
19		352		7982260
20		468		6377578
21		182		352546
Всего за 10.06	**1474771**	**5695672**	**749617**	**32150251**
Итого за 2 рабочих дня	**6053443**	**8022614**	**6262145**	**52624780**

Рис. 33. Сводные данные о закачках от провайдера за 09-10.06.2004

Таким образом, результаты подтвердили последнюю из названных гипотез, причем замеры с помощью НС показали даже несколько большие значения, чем данные провайдера. Существенное (в 4-5 раз) превышение априорной оценки было вызвано неожиданно высоким входным трафиком, поступающим на ПК "***Наташа***" рабочей группы.

Следует сказать, что психологически ни заказчик, ни автор данной работы не были готовы к полученному результату; в априорном обсуждении нам представлялась наиболее вероятной первая из гипотез. В полученном же результате заказчика стал интересовать естественный вопрос, нельзя ли выяснить, какие узлы Интернета вызывались «общительной» сотрудницей и с какой целью.

Надо сказать, что в цели разработки программного обеспечения НС, определенные в 1999 г., не входило отслеживать или каким-либо иным образом протоколировать контакты пользователей с сайтами Интернета. Однако, все же имелось 2 исключения из этого правила. Во-первых, POP3-сеансы получения почты могли и, разумеется, протоколировались в описываемом экспресс-анализе (подробнее см. [20]). Во-вторых, с самого начала разработки имелась технологическая возможность дампирования пакетов, входящих и/или исходящих от определенного MAC-адреса. Вследствие этого, наблюдение по согласованию с заказчиком было решено продлить еще на день, и включить дампинг всех приходящих на интересующий MAC-адрес сетевых пакетов.

В результате были получены неопровержимые доказательства того, что один из сотрудников в рабочее время за счет фирмы занимается посторонней деятельностью, посещает не связанные с его служебной необходимостью сайты и ведет внеслужебную переписку, что приводит к существенным дополнительным расходам фирмы на оплату сверхлимитного трафика.

Заказчику были предоставлены адреса и www-имена сайтов, посещенных сотрудницей; при необходимости могли бы быть предоставлены и фрагменты почтовой переписки. Вся информация была предоставлена исключительно на основании протоколов наблюдения; какой-либо анализ данных в компьютере сотрудницы не проводился. Однако, заказчику было разъяснено, каким образом можно найти нужные материалы на ПК, с которого действовала сотрудница.

Следует отметить, что указанный способ включения НС не являлся единственно возможным [20]. Принятая в данном случае схема учитывала желание автора статьи получить также полные данные о межкомпьютерных пересылках в фирме. Рассмотрение этого вопроса выходит за рамки данной работы, предоставив автору, однако, материал для совершенствования программного обеспечения НС.

Резюмируя, можно сказать следующее.

- Разработанные средства сетевого анализа позволяют провести экспресс-анализ трафика малой сети даже с помощью маломощной переносной наблюдающей станции.
- Этап настройки средств сетевого мониторинга на незнакомую сеть минимален, исполняется полуавтоматически и требует затрат порядка 10+N минут при числе пользователей N.

В целом, имеющееся программное обеспечение НС пригодно для качественного экспресс-анализа локальных сетей даже при использовании на маломощных компьютерах. Для получения количественных показателей с достаточной степенью точности (95% и выше) следует использовать более мощный ПК.

2.5. Получение обновлений DrWeb через AB-сервер

Стандартно, установленные клиенты отечественного антивирусного программного обеспечения “Doctor Web” обязаны получать антивирусные обновления с серверов DrWeb. Однако, автором разработана специальная корпоративная технология снабжения своих внутренних клиентов этого пакета с помощью оригинальных разработанных программ и Антивирусного сервера (AB-сервера) [18].

Создание этой технологии исключительно важно для функционирования всей антивирусной службы института. AB-сервер способен поддерживать одновременно несколько разнотипных антивирусных пакетов, к примеру, “**DrWeb для рабочих станций Windows 32bit Security Space 6.0**“, “**DrWeb для файловых Windows-серверов 32bit 6.0 Security Space**” и ряд других. Он всегда доступен для внутренних пользователей, скорость обновления с него на порядок выше. Вместо ежечасных обновлений, рекомендуемых DrWeb, обновления получают компьютеры при их включении – в общем, учтены различные особенности эксплуатации ПК в научных учреждениях. Число пользователей Антивирусной службы ЦЭМИ РАН с 2004 года (время создания AB-сервера)

менялось в пределах от 25 до 220, во время написания данной работы их число чуть выше 100 вследствие необходимости экономии денег на лицензии. Полная информация о свойствах и особенностях работы такой технологии приведена в [18].

Однако, для построения всей этой технологии важно было проверить принципиальную возможность получения антивирусных обновлений DrWeb с АВ-сервера, раздатчиком файлов на котором является Apache 1.3.23. Эту принципиальную возможность проще всего было проверить с помощью сетевого мониторинга. Соответствующий эксперимент 2004 года воспроизведён специально для данного раздела 06 марта 2019 года, результаты его приводятся ниже.

Для проведения эксперимента, в разрыв кабеля от компьютера автора с адресом 193.232.194.13 к АВ-серверу 193.232.194.11 включён хаб, отвод от которого подсоединён к НС, аналогично рис. 31 предыдущего раздела. Разумеется, при этом стали «видны» через их broadcasting все ПК, подключённые к внешней сети института. Сокращённая БД таковых приведена на рис. 34.

```
000652324406 19 193.232.194.059 0F:CS7206-4 0921/01
0015178D064F 33 193.232.194.005 43:RouN__Sw 0917/05
00104B36E236 31 193.232.194.011 42:AVServer 0904/09
0014854E59CA 21 193.232.194.018 42:AVServ3  0904/00
00508BACF971 31 193.232.194.013 42:Терент-в 0904/00
00A0C9D68CEB 01 193.232.194.033 43:Смитиенк 0917/10
00C0262B1179 01 193.232.194.085 41:Дыб-Alex 0907/12
001CC0589C99 01 193.232.194.131 51:Артамон1 0717/09
00C0F0217135 01 193.232.194.227 81:Селивер. 0817/09
0003472C8158 11 193.232.194.246 41:LIB-Srvr 0711/09
08CC68431B4B 01 193.232.194.010 42:Cisco904 0904/09
```

Рис. 34. Фрагмент БД внешних адресов ЦЭМИ РАН

После настройки НС на дампирование всех пакетов от ПК автора, была осуществлена попытка обновления текущего установленного пакета DrWeb. Первым файлом при этом запрашивается drweb32.flg (он отсутствует на сервере), вторым – файл timestamp, в котором содержится момент создания последней версии области обновления. На рис. 35 показан протокол запроса на этот файл (**Pkt=4**), на рис. 36 – протокол ответа сервера на данный запрос (**Pkt=5**).

Таким образом, запрос и ответ сводятся к обмену тектовыми сообщениями, вкратце показанными на рис. 37. Официальный

протокол утилиты обновления DrWebUpW.exe на этот сеанс показан на рис. 38.

Легко заметить, что для аутентификации утилита обновления использует дополнительные строки "**X-DrWeb**", которые Apache 1.3.23, разумеется, игнорирует. Важно, что принимающая сторона не требует особого подтверждения валидизации, видимо, полагаясь на криптозашифрованный адрес сервера обновления, содержащийся в специальном файле CUSTOM.DRL. Этот файл специально для работы Антивирусной службы ЦЭМИ РАН со своим сервером предоставлен Технической службой поддержки DrWeb по запросу автора.

Сказанное означает, что состояние предъявляемого ключа не влияет на получение файлов. Так, всем пользователям института во время подготовки данной работы распространяется указанный ключ **0133999100**, являющийся *заблокированным* на сайте DrWeb. Это сделано специально для того, чтобы исключить возможность нечестным сотрудникам вынести ключ за пределы института и использовать его на прочих ПК.

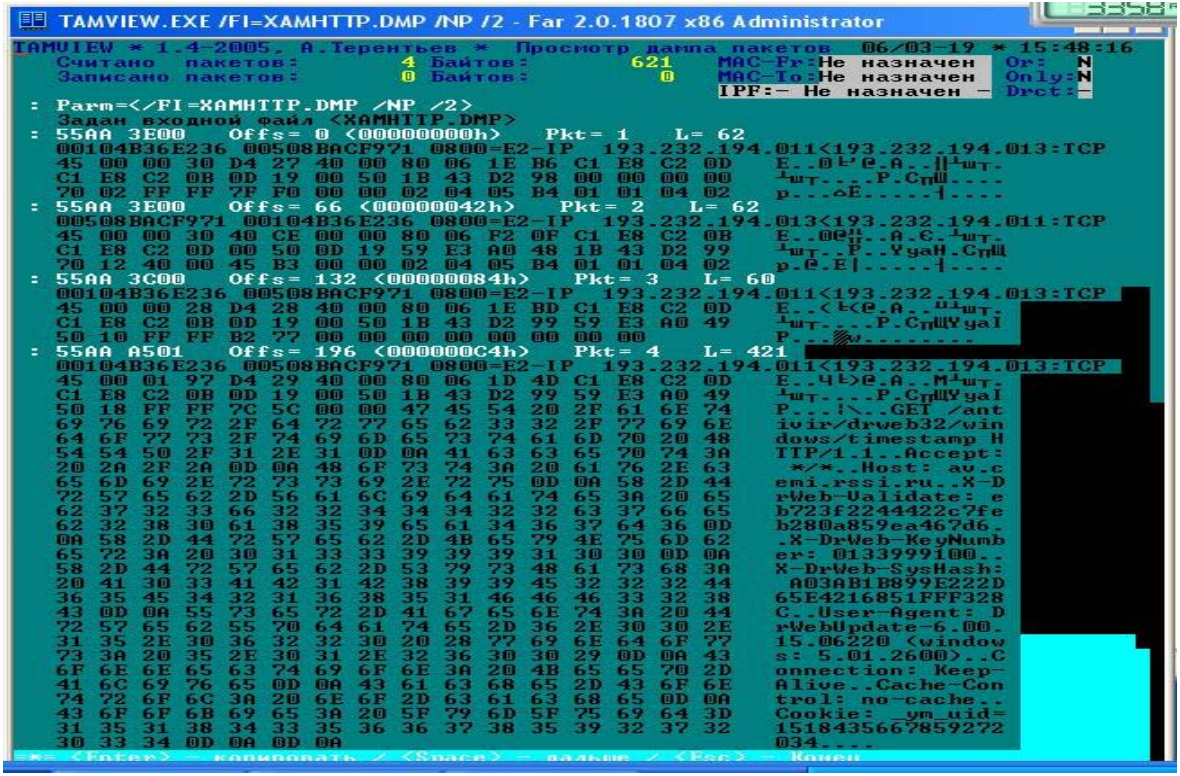

Рис. 35. Протокол запроса файла timestamp (последний)

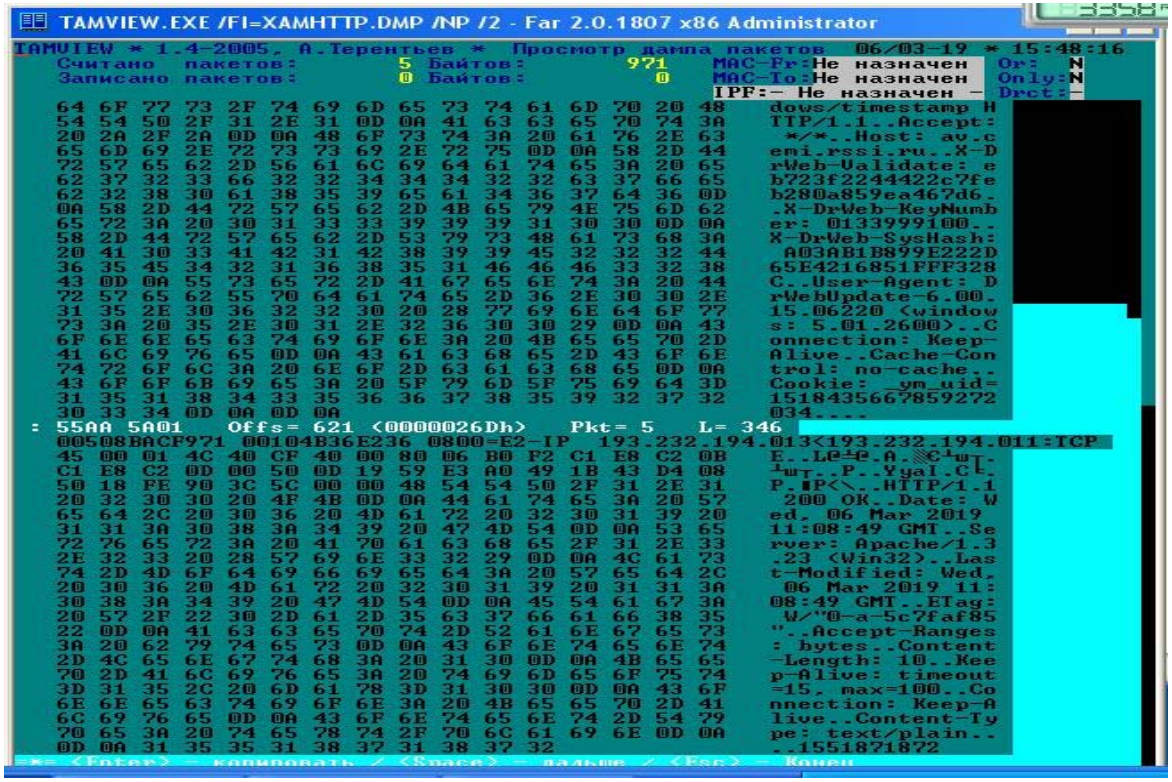

Рис. 36. Протокол ответа сервера на запрос рис. 35

```
ЗАПРОС НА СЕРВЕР
GET /antivir/drweb32/windows/timestamp HTTP/1.1
Accept: */*
Host: av.cemi.rssi.ru
X-DrWeb-Validate:
eb723f2244422c7feb280a859ea467d6
X-DrWeb-KeyNumber: 0133999100
X-DrWeb-SysHash: A03AB1B899E222D65E4216851FFF328C
User-Agent: DrWebUpdate-6.00.15.06220 (windows:
5.01.2600)
Connection: Keep-Alive
Cash-Control: no-cache
Cookie: _ym_uid=1518435667859272034

ОТВЕТ СЕРВЕРА
HTTP/1.1 200 OK
Date: Wed, 06 Mar 2019 11:08:49 GMT
Server: Apache/1.3.23 (Win32)
Last-Modified: Wed, 06 Mar 2019 11:08:49 GMT
ETag: W/"0-a-5c7faf85"
Accept-Ranges: bytes
Content-Length: 10
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text-plain
1551871872
```

Рис. 37. Текстовый вид тегов HTTP запроса и ответа

Следует отметить, что до внедрения подобной технологии регулярно наблюдались попытки различных пользователей скопировать ключ для домашнего использования. Ни убеждения пользователей, ни запреты не действовали. Реально такие попытки прекратились только после предоставления пользователям ЦЭМИ РАН заблокированного ключа.

Принятый файл timestamp содержит символы **1551871872** (Wed, 06 Var 2019 11:31:12 GMT), показывающие момент создания обновления на серверах DrWeb.

Отчёт НС, соответствующий времени обновления, представлен на рис. 39.

```
2019-03-06, 15:07:21  ============================================
2019-03-06, 15:07:21  Dr.Web Updater для Windows v*.**.**
2019-03-06, 15:07:21  © ООО «Доктор Веб», 1992-201*
2019-03-06, 15:07:21  User: [TRENTY-904][trenty]
2019-03-06, 15:07:21  Командная строка: G:\Program Files\DrWeb\DrWebUpW.exe /GO /QU /URM:noprompt
2019-03-06, 15:07:21  Path to log: G:\Documents and Settings\trenty\DoctorWeb\DrWebUpW.log
2019-03-06, 15:07:21  Операционная система: Windows XP Professional x86 (Build 2600), Service Pack 3
2019-03-06, 15:07:21  ============================================
2019-03-06, 15:07:21  Имя файла лицензии:: G:\Program Files\DrWeb\drweb32.key
2019-03-06, 15:07:21  Номер ключа:: 0133999100
2019-03-06, 15:07:21  Владелец:: ФГБУН ЦЭМИ РАН
2019-03-06, 15:07:21  Дата активации:: 2017-02-14
2019-03-06, 15:07:21  Дата окончания:: 2020-04-22
2019-03-06, 15:07:21  DRL-файл обработан (G:\Program Files\DrWeb\custom.drl, 1 URL)
2019-03-06, 15:07:21  Create network session
2019-03-06, 15:07:21  Подключаемся к хосту: http://av.cemi.rssi.ru/antivir/drweb32/windows/
(193.232.194.11)
2019-03-06, 15:07:21  Поиск timestamp...
2019-03-06, 15:07:21  Принимаем timestamp...
2019-03-06, 15:07:21  timestamp принят
2019-03-06, 15:07:21  Поиск drweb32.flg...
2019-03-06, 15:07:21  Поиск drweb32.lst.lzma...
2019-03-06, 15:07:21  Поиск drweb32.lst...
2019-03-06, 15:07:21  Принимаем drweb32.lst...
2019-03-06, 15:07:21  drweb32.lst принят
.....
2019-03-06, 15:07:23  Файлы приняты
2019-03-06, 15:07:23  Обновление файлов...
2019-03-06, 15:07:25  EXEC(G:\Program Files\DrWeb\drwreg.exe) = 1 (rc=0)
2019-03-06, 15:07:25  Отключены
2019-03-06, 15:07:25  ============================================
```

Рис. 38. Протокол утилиты обновления DrWeb (сокращён)

```
#00 ЦЭМИ РАН *  Аудит корпоративной сети * 5.23 = А.Терентьев
#02 Полный, пополняющий файл отчета <TAMC0002.LST>, серия начата с 0001
#04 Программа запущена 06/03-19 в 14:56:09
#05 Текущее время      06/03-19 = 15:05:28, работает       559с
#06 В цикле     328сек.; всего    0ч09м19с
#10 Взято пакетов:   5149,      Байтов:   4908173
#11 Мимо пакетов:    3964,       Байтов:   362077
#13 Ошиб.пакетов:     455,       Байтов:      4758
#12 Скорость максимальная:  706.69 Kb/s;   Средняя:  14.66 Kb/s
#14 БД:   84,  ПК в работе:   11
#15 Ц/с в среднем -- Всех:  11092;  полезных:      17;  коротких:    1013
#17     Всего циклов минимально:    3324;    максимально:   32767
#18 Ситуаций пропуска пакетов:      10   макс.буферов: 86%
#20  =              К О М П О Н Е Н Т Ы   Т Р А Ф И К А
#20  =         По типу трафика         В т.ч. широковещательные
#20  =Тип пакета   Пакетов    Байтов     Пакетов   Байтов
#21 EtherII-IP:    0004626 0004875493    0000039 0000006902
#22 EtherII-ARP:   0000346 0000020760    0000345 0000020700
#23 EtherII-IPX:   0000000 0000000000    0000000 0000000000
#24 EtherII-other: 0000009 0000001230    0000000 0000000000
#25 IEEE802.3IPX:  0000000 0000000000    0000000 0000000000
#26 IEEE802.2SNAP: 0000000 0000000000    0000000 0000000000
#27 802.3/802.2:   0000000 0000000000    0000000 0000000000
#28 Не опознаны:   0000168 0000010690    0000000 0000000000
#30  =     Структура внутрисетевого трафика
#50 - - -
#80  = Сведения о всех нодах и их трафике           И С П У Щ Е Н О   Bits
```

```
001.000652324406 193.232.194.059/0F:CS7206-4 0921 {0000331 0000019971 0319
006.0015178D064F 193.232.194.005/43:RouN__Sw 0917 {0000001 0000000060 8333
010.00104B36E236 193.232.194.011/42:AVServer 0904 {0003401 0004789345 8331
012.0014854E59CA 193.232.194.018/42:AVServ3  0904 {0000001 0000000092 8121
030.00508BACF971 193.232.194.013/42:Терент-в 0904 {0001187 0000079195 8331
037.00A0C9D68CEB 193.232.194.033/43:Смитиенк 0917 {0000001 0000000243 8101
046.00C0262B1179 193.232.194.085/41:Дыб-Alex 0907 {0000001 0000000251 8101
059.001CC0589C99 193.232.194.131/51:Артамон1 0717 {0000015 0000001956 8B01
069.00C0F0217135 193.232.194.227/81:Селивер. 0817 {0000015 0000001752 8101
073.0003472C8158 193.232.194.246/41:LIB-Srvr 0711 {0000014 0000001931 8111
083.08CC68431B4B 193.232.194.010/42:Cisco904 0904 {0000018 0000003537 0301
084.08CC68431B4C  No IP-traffic /00:         0000 {0000164 0000009840 4100
-----
Конец отчета <TAMC0002.LST>
```

Рис. 39. Отчёт НС, соответствующий времени обновления DrWeb

Таким образом, проверка подтвердила принципиальную возможность использования Apache 1.3.23 для срабатывания предложенной технологии получения клиентами института антивирусных обновлений DrWeb. Это заложило основу внедрения корпоративной технологии использования антивирусных пакетов DrWeb в научных учреждениях, предложенную автором.

Следует отметить, что начальный вариант технологии включал предварительное создание образов областей обновления на стороннем ПК [7], и лишь позднее все процессы их формирования были перенесены исключительно на АВ-сервер, что, безусловно, является более помехоустойчивым.

Спроектированная технология получения антивирусных дополнений работоспособна и функционирует с 2003 г по настоящее время. Полное её изложение приведено в [18].

2.6. Исправление маршрутизации АВ-сервера

Данный раздел значительно опережает хронологическое изложение трансформаций ЛВС ЦЭМИ РАН, однако служит характерным примером применения средств сетевого мониторинга для решения конкретной сетевой проблемы.

Локальная вычислительная сеть института к 2012 году включала две неравноценные по числу подключённых вычислительных установок (ВУ) области. В меньшей части имели хождение прямые IP-адреса сети 193.232.194.*/24. В большей части ЛВС установлены внутренние IP-адреса сети 10.0.*.*/24. Интерфейсом между двумя частями ЛВС является роутер с внешним адресом 193.232.194.5 и внутренним 10.0.1.1, сформированный на базе Unix-сервера. Это же ВУ занимается также маршрутизацией внутренней части ЛВС, для чего интерфейс 10.0.1.1/24 имеет алиасы 10.0.2.1/24, 10.0.4.1/24 и т.д., включая 10.0.13.1/24. В целях взаимной изоляции, сеть 10.0.0.0/24 с помощью сетевой маски 255.255.255.0 разделена на несколько подсетей, причём номером подсети является третий октет адреса.

В целях снабжения пользователей института антивирусными пакетами серии “Doctor Web”, в состав сети входит Антивирусный сервер на платформе Microsoft Windows’2003 Server. Раздачу пакетов антивирусных обновлений, доступ к Антивирусному сайту и ряд других функций, как уже говорилось, исполняет Apache 1.3.23. Идентификация пользователей в целях учёта лицензий в этих

условиях возможна либо по IP-адресу, либо по связке логин-пароль. Поскольку установка логинов и паролей на все 200[10] актуальных пользователей АВ-сервера, часть которых находится во внешней ЛВС и часть – во внутренней, трудоёмка, АВ-сервер имеет два сетевых интерфейса, один во внешней части ЛВС (через него закачиваются обновления от вендора и раздаётся информация для «внешних» пользователей), и второй – во внутренней части ЛВС, соответственно с адресами 193.232.194.11/24 и 10.0.13.11/16. При этом, выбор маски 16 был обусловлен необходимостью обслуживания всех внутренних пользователей в различных подсетях сети 10.0.x.0/24.

Внутренняя часть ЛВС к 2012 году была построена по звездообразной схеме с центром в виде коммутатора Cisco Catalist WS-C2924XL. Принципиальная схема сетевой коммутации приведена на рис. 40. В начале эксплуатации показанной схемы, в центральной части внутренней ЛВС находился Switch D-Link, неуправляемый коммутатор уровня 2 модели ISO/OSI. Аналогичные устройства были установлены на всех нижеследующих уровнях древовидной топологии ЛВС. Таким образом, интерфейс АВ-сервера был включён в однородную проводящую среду, с расположенными на ней ПК получателей обновлений.

При этом, широковещательные ARP-запросы для поиска необходимых MAC-адресов беспрепятственно распространялись от АВ-сервера через соответствующий интерфейс на все уровни топологии и были видны сетевым адаптерам ПК получателей. Ответные ARP-пакеты от них таким же образом достигали интерфейс AV-сервера. В результате, ARP-таблицы содержали необходимые списки MAC-адресов для обеспечения передачи пакетов на уровне 2 между AV-сервером и ПК-получателями обновлений [21].

[10] В 2012 году, в настоящее время несколько меньше.

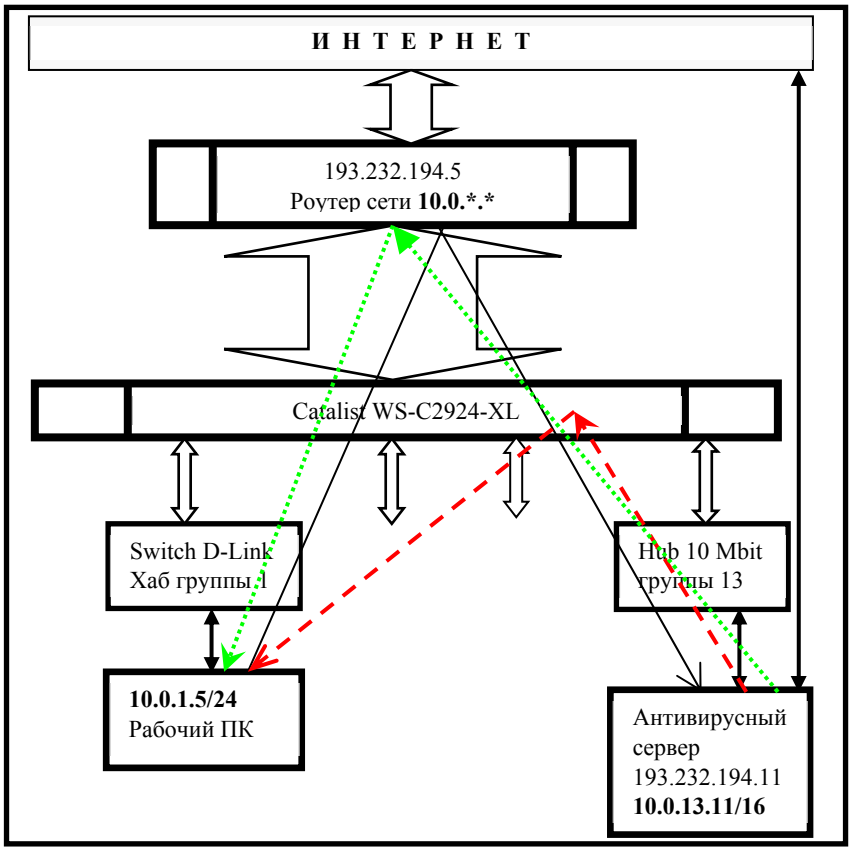

Рис. 40. Схема хождения пакетов во внутренней части ЛВС

Как показали детальные исследования автора с помощью средств сетевого мониторинга (см. предыдущий раздел, а также [21]), антивирусное обновление состоит из ряда обменов пакетами между ПК-получателем и АВ-сервером. От ПК-получателя исходит http-запрос к АВ-серверу на получение файла, затем сервер в ответ высылает получателю множество пакетов, согласно длине запрошенного файла.

Если http-запрос и подавался через роутер, то ответные пакеты к ПК-получателю приходили уже напрямую через коммутаторы, т. к. маршруты на всю сеть у АВ-сервера были определены

напрямую через интерфейс. При затребовании последовательно нескольких файлов, этот процесс повторялся для каждого файла.

При этом, в течение ряда лет пользователи не испытывали каких-либо затруднений ни в доступе к Антивирусному сайту, ни в получении обновлений. Однако, с установкой в центре внутренней ЛВС устройства Cisco Catalyst, ситуация изменилась следуюшим образом.

При небольших объёмах получаемых данных (до 1÷2 Мб) заметных затруднений с получением информации от АВ-сервера не возникало. В эти объёмы вполне укладывалось общение с Антивирусным сайтом, а также получение регулярных обновлений. Однако, при установке из дистрибутивов антивирусных средств на новые ВУ, вследствие значительной разницы между сроком подготовки дистрибутива и текущим состоянием антивирусной области, первое после установки обновление приводило к выкачиванию значительных объёмов информации (50÷400Мб), и в этих случаях появлялись проблемы. В течение первых минут скорость скачивания, как обычно, возрастала до некоторого значения, далее внезапно падала, вплоть до полной остановки процесса и прерывания по таймауту. При этом, каждый конкретный процесс скачивания прерывался на разных этапах, значения скоростей и интенсивность их падения были также разными. На отрезке между Cisco Catalyst и хабом в 10Mbit (длина трассы примерно 50 м) наблюдалось, по данным Cisco Catalyst, заметное число коллизий. Такая неустойчивость поведения процесса скачивания с разными конкретными характеристиками при последовательных пробах с одного и того же конечного ПК наводила на мысль о нерегулярных ошибках в канале передачи информации, свойственных обычно физическим погрешностям канала.

Характерно, что описанные проблемы возникали только во внутренней части ЛВС. Все «внешние» пользователи, в том числе Интернет-пользователи, подобных затруднений не ощущали. Поэтапное тестирование сетевой карты, хаба группы 13 и проводного соединения от хаба до Catalyst физических некорректностей не выявило. При подключении к тому же хабу дополнительной рабочей станции, передача информации от АВ-сервера шла без задержек и падения скорости. С другой стороны, описанные выше проблемы наблюдались на всех без исключения ВУ внутренней ЛВС, подключенных к разным портам Cisco Catalyst.

В процессе дальнейшего анализа возникшей ситуации была предложена гипотеза о том, что падение скорости и разрыв связи HTTP-соединения возникает вследствие некорректной коммутации сетевых пакетов устройством Cisco Catalyst из-за логической ошибки роутинга. В самом деле, схема организации внутренней части ЛВС предполагает, что на каждый запрос от пользователя (чёрная сплошная тонкая ломаная линия со стрелкой от рабочего ПК к АВ-серверу на рис. 40) ответный пакет должен приходить сначала на роутер, а уж потом коммутироваться на нужный интерфейс (зелёная прерывистая ломаная линия со стрелкой от АВ-сервера к рабочему ПК). Однако, вследствие того, что используемая АВ-сервером маска сети 10.0 имеет 16, а не 24 бита, ответный пакет не проходит через роутер, непосредственно коммутируясь сразу на нужный порт Catalyst (красная пунктирная ломаная со стрелкой от АВ-сервера к рабочему ПК). Тем самым, HTTP-соединение, базирующееся на TCP/IP-протоколах, «рушится» на роутере по неответу. Различные значения порогового объёма успешно переданных данных зависят в этом случае от текущей загрузки интерфейсной связки роутер/Catalyst.

В целях проверки данной гипотезы, на АВ-сервере был выполнен командный файл, содержащий явные определения статических маршрутов для всех пакетов, отправляемых по всем подсетям сети 10.0, через роутер. Результаты команды `netstat -rn` перед подачей командного файла даны на рис. 41. Конкретные команды этого командного файла представлены на рис. 42. Результаты той же команды после прогона командного файла даны на рис. 43.

```
IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 50 8b 6c bd a4 ...... Compaq NC3120 Fast Ethernet NIC
0x10004 ...00 13 d4 da 26 c5 ...... Marvell Yukon 88E8053 PCI-E Gigabit Ethernet
 Controller
===========================================================================
===========================================================================
Active Routes:
Network Destination     Netmask          Gateway       Interface  Metric
       0.0.0.0         0.0.0.0   193.232.194.59   193.232.194.11      20
     10.0.13.0   255.255.255.0       10.0.13.11       10.0.13.11      10
    10.0.13.11 255.255.255.255        127.0.0.1        127.0.0.1      10
10.255.255.255 255.255.255.255       10.0.13.11       10.0.13.11      10
     127.0.0.0       255.0.0.0        127.0.0.1        127.0.0.1       1
 193.232.194.0    255.255.255.0   193.232.194.11   193.232.194.11      20
193.232.194.11  255.255.255.255        127.0.0.1        127.0.0.1      20
193.232.194.255  255.255.255.255   193.232.194.11   193.232.194.11    20
     224.0.0.0        240.0.0.0        10.0.13.11       10.0.13.11    10
     224.0.0.0        240.0.0.0    193.232.194.11   193.232.194.11    20
255.255.255.255  255.255.255.255       10.0.13.11       10.0.13.11     1
255.255.255.255  255.255.255.255   193.232.194.11   193.232.194.11     1
Default Gateway:    193.232.194.59
===========================================================================
Persistent Routes:
None
```

Рис. 41. Исходная таблица маршрутизации на Антивирусном сервере

```
route add 10.0.1.0 mask 255.255.255.0 10.0.13.1
route add 10.0.2.0 mask 255.255.255.0 10.0.13.1
route add 10.0.4.0 mask 255.255.255.0 10.0.13.1
route add 10.0.5.0 mask 255.255.255.0 10.0.13.1
route add 10.0.6.0 mask 255.255.255.0 10.0.13.1
route add 10.0.8.0 mask 255.255.255.0 10.0.13.1
route add 10.0.9.0 mask 255.255.255.0 10.0.13.1
route add 10.0.10.0 mask 255.255.255.0 10.0.13.1
route add 10.0.21.0 mask 255.255.255.0 10.0.13.1
```

Рис. 42. Содержание командного файла, исправляющего ошибки роутинга

После выполнения данной процедуры, описанные ошибки связи прекратились, скорость передачи информации возросла до 300÷500 Кбит/с. Таким образом, гипотезу можно считать подтверждённой.

```
IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 50 8b 6c bd a4 ...... Compaq NC3120 Fast Ethernet NIC
0x10004 ...00 13 d4 da 26 c5 ...... Marvell Yukon 88E8053 PCI-E Gigabit Ethernet
Controller
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   193.232.194.59   193.232.194.11     20
         10.0.1.0    255.255.255.0        10.0.13.1       10.0.13.11      1
         10.0.2.0    255.255.255.0        10.0.13.1       10.0.13.11      1
         10.0.4.0    255.255.255.0        10.0.13.1       10.0.13.11      1
         10.0.5.0    255.255.255.0        10.0.13.1       10.0.13.11      1
         10.0.6.0    255.255.255.0        10.0.13.1       10.0.13.11      1
         10.0.8.0    255.255.255.0        10.0.13.1       10.0.13.11      1
         10.0.9.0    255.255.255.0        10.0.13.1       10.0.13.11      1
        10.0.10.0    255.255.255.0        10.0.13.1       10.0.13.11      1
        10.0.13.0    255.255.255.0       10.0.13.11       10.0.13.11     10
       10.0.13.11  255.255.255.255        127.0.0.1        127.0.0.1     10
        10.0.21.0    255.255.255.0        10.0.13.1       10.0.13.11      1
   10.255.255.255  255.255.255.255       10.0.13.11       10.0.13.11     10
```

```
        127.0.0.0        255.0.0.0         127.0.0.1         127.0.0.1      1
    193.232.194.0    255.255.255.0   193.232.194.11    193.232.194.11     20
   193.232.194.11  255.255.255.255         127.0.0.1         127.0.0.1     20
  193.232.194.255  255.255.255.255   193.232.194.11    193.232.194.11     20
        224.0.0.0        240.0.0.0       10.0.13.11        10.0.13.11     10
        224.0.0.0        240.0.0.0   193.232.194.11    193.232.194.11     20
  255.255.255.255  255.255.255.255       10.0.13.11        10.0.13.11      1
  255.255.255.255  255.255.255.255   193.232.194.11    193.232.194.11      1
Default Gateway:    193.232.194.59
===========================================================================
Persistent Routes:
  None
```

Рис. 43. Результирующая таблица маршрутизации на AB-сервере

Рассмотрим, что произошло после замены центрального коммутатора ЛВС. Интеллектуальный коммутатор Cisco Catalyst 2950 с наиболее современной из доступных для установки Cisco IOS 12.0(5)WC17 обладает развитыми средствами безопасности, и кроме того коммутирует пакеты на 2-м и 3-м уровнях модели ISO/OSI (9-канальном и протокольном). В качестве анонсированных свойств безопасности на коммутаторе имеются: возможность предотвращения флудинга широковещательными пакетами, запрет повторной отправки через некоторый интерфейс пакета, прибывшего с этого же интерфейса, организация защищённых портов, борьба с подменой ARP-пакетов (когда третья сторона высылает ARP-ответ с подменённым MAC-адресом [22]).

Анализ действующей конфигурации Catalyst показал, что в ней на двух портах командами:

port block unicast
port block multicast

запрещено широковещание и передача ответов на широковещание пакетами 2-го уровня от неизвестных источников в присоединённый к порту сегмент, поэтому на этих портах ограничена работа ARP-протокола [21]. Это обычные меры повышения безопасности портов коммутатора от флудинга и в конечном счёте – против отказа в обслуживании. Такая конфигурация требует обязательности назначения маршрутов для всех сетевых устройств ЛВС (т.е. маршрутизации на 3-м уровне), т.к. основной роутер находится во внутреннем, роутерном сегменте, присоединённом к одному из этих портов и недоступном для обращения на уровне 2.

На всех ПК в ЛВС по умолчанию назначены шлюз, DNS- и WINS сервер на одном и том же адресе – адресе роутера, так что все пакеты, исходящие из ПК сети, без помех проходят через роутер в нужном направлении. Однако, команды ping и tracert (ICMP) от ПК, обращённые в роутерный сегмент, не получают ответа по вышеприведённой причине ограниченности работы на уровне 2. Эти команды, обращённые к ПК на других портах, получают ответы, минуя роутер.

АВ-сервер, в конфигураторе которого шлюз по интерфейсу ЛВС не был указан, нормально отвечал на пришедшие через роутер http-запросы ПК получателей. При этом, ответ высылался уже на канальном уровне 2 непосредственно ПК-получателю, с предварительным использованием ARP-протокола и записью в ARP-таблицу, как было

и до замены коммутатора. Однако, если http-запрос приходил из роутерного сегмента, ARP-протокол инициировался из роутера к АВ-серверу и поэтому отрабатывал нормально.

В то же время, передача файла от АВ-сервера к ПК-получателю исполнялась уже непосредственно на канальном уровне, т.к. у АВ-сервера на внутреннем интерфейсе, естественно, не был указан шлюз «по умолчанию»[11]. В этом случае, подтверждение успешного приёма каждого пакета приходило АВ-серверу до тех пор, пока в ARP-кэше ПК-получателя существовала строка ARP для АВ-сервера. Согласно алгоритму протокола, запись является динамической и удаляется через определённый промежуток времени (обычно 2 минуты). Если файл успел передаться до этого времени, то благополучно запрашивался новый файл (с возобновлением записи об АВ-сервере в ARP-кэше ПК-получателя), и пользователь не видел проблем.

В случае же передачи длинных файлов, требующей более 2-х минут, запись из ARP-кэша ПК-получателя успевает удалиться, и передача прекращается (теряются подтверждения приёма). Если в это время пользователь быстро даст ping на АВ-сервер (а такие эксперименты также были произведены), то после ответа АВ-сервера на эту команду в кэше снова появляется строка ARP для АВ-сервера, и затормозившийся процесс передачи продолжается! Одновременно обнаружено, что при попытке обновлений из роутерного сегмента, скачивание заканчивалось сразу – в этот сегмент не проходили пакеты на уровне 2, он доступен только через шлюз.

Суммируя, можно сделать вывод, что ошибка состояла в незаконченности преобразования ЛВС, связанной с идеологией изолированности сегментов ЛВС при помощи средств коммутатора Catalyst-2950. Абсолютно все ПК (включая АВ-сервер) должны иметь одинаковые методы доступа к сети, через шлюз, с коммутацией пакетов на 3-м уровне, поскольку коммутация на канальном уровне ограничена на одном из основных портов. Поэтому, в описанных условиях и было необходимо назначить статические маршруты с АВ-сервера к получателям обновлений для общей успешности приёма http-обновлений.

Для подробного анализа ситуации проводился сетевой мониторинг интерфейса между «внутренним» сетевым адаптером АВ-

[11] Шлюз АВ-сервера, разумеется, указан на «внешнем» интерфейсе для доступа в Интернет.

сервера и отвечающим ему выводом 10.0.13.1 через уже знакомую читателям схему включения хаба в разрыв цепи с отводом на НС.

Была также написана тестовая программа получения с АВ-сервера файлов различной длины. Пример работы программы представлен на рис. 44. В приведённом примере скачивается с АВ-сервера файл объёмом 10Мбайт на домашний ПК автора через Интернет. Средняя скорость закачки определена как 725 КБ/с, максимальная скорость достигла 2 МБ/с. Время закачки – 13 секунд. Именно эта программа помогала внедрению корпоративной технологии приёма антивирусных пакетов в институте, хотя там в ряде случаев были отмечены скорости на порядок меньше. Подобное средство незаменимо при проверке коннективности ЛВС.

В экспериментах обнаружено, что при закачке файлов выставленный указатель HTTP/1.1 «Конец файла» не является валидным показателем. В приведённом случае, например, согласно рис. 44, в процессе закачки было получено 3 таких выставленных указателя, независимо от истинного конца файла, который должен определяться только по числу скачанных байтов. Такое отступление от стандартов протокола HTTP является полезным знанием для практических программистов.

Возвращаясь к проблеме восстановления статических маршрутов, следует сказать, что интерфейсом между двумя частями ЛВС является роутер, сформированный на базе Unix-сервера. Это же ВУ занимается также маршрутизацией внутренней части ЛВС, для чего интерфейс 10.0.1.1 имеет алиасы 10.0.2.1, 10.0.4.1 и т.д., включая 10.0.13.1. В целях взаимной изоляции, сеть 10.0.*.* фактически разделена на несколько подсетей, причём номером подсети является третий компонент адреса.

Как подробно разъяснено выше, в процессе реорганизации ЛВС обнаружилась проблема хождения TCP/IP-пакетов. Там же разъяснено, что для восстановления нормального прохождения на Антивирусном сервере были проложены статические маршруты к алиасам роутера внутренней части ЛВС. Однако, далее обнаружилось, что периодически (1-2 раза в месяц) доступность Антивирусного сервера по внутреннему интерфейсу стала нарушаться. Замечено, что при этом таблица маршрутизации на Антивирусном сервере стала сбрасываться к начальному состоянию. Причины подобного оставались неясными.

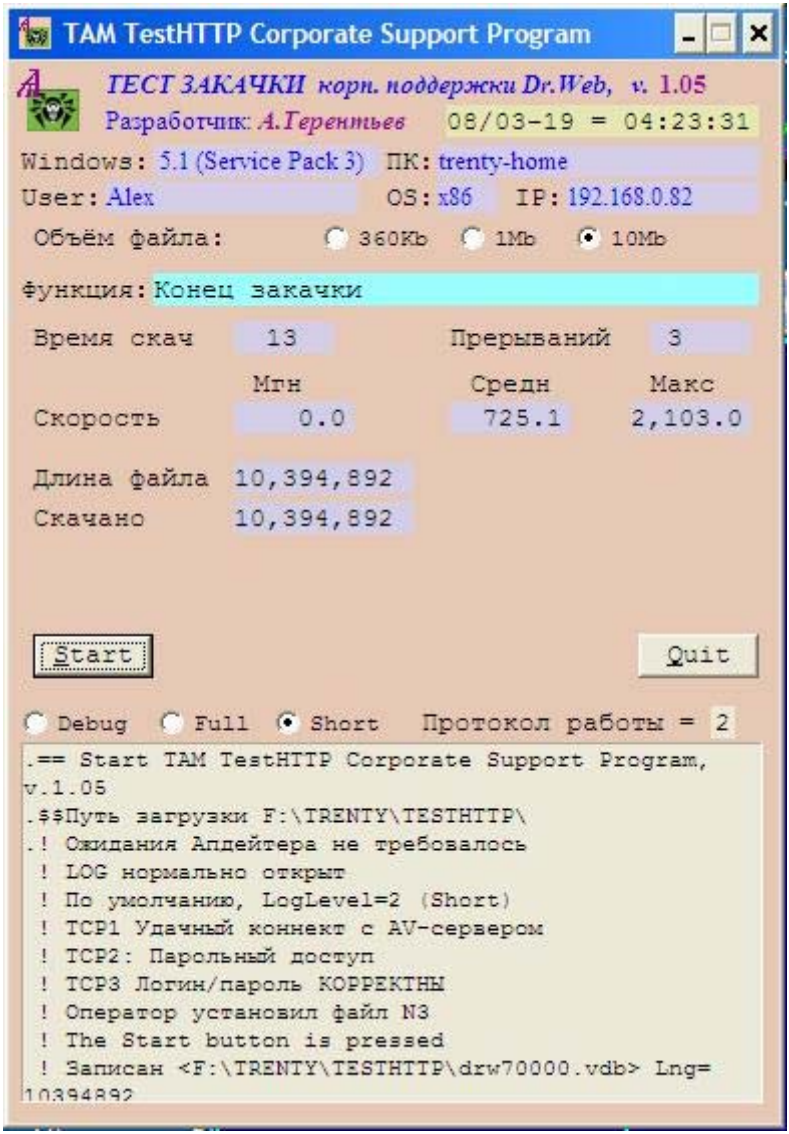

Рис. 44. Пример тестовой программы HTTP-скачивания файлов

Разумеется, потеря статического маршрута к алиасу 10.0.13.1/16 необратима без восстановления маршрутизации на Антивирусном сервере, т.е. исполнения ряда ручных операций по восстановлению

хождения пакетов в локальной сети ЦЭМИ РАН. В то же время, указанная потеря не приводит к прерыванию обслуживания пользователей по первому, «внешнему» интерфейсу Антивирусного сервера, а также получению обновлений на Антивирусный сервер от серверов поставщика антивирусных средств. За время эксплуатации текущей схемы с использованием дополнительных статических маршрутов неоднократно прерывалась связь с алиасом 10.0.13.1, и большинство «внутренних» пользователей переставали получать обновления, в то время как прочие продолжали их получать и этой проблемы не замечали. Обычный контроль за работой Антивирусного сервера, в том числе получение очередных обновлений, исполняется с рабочего ПК Антивирусной службы ЦЭМИ РАН. Однако, этот ПК, имея адрес 193.232.194.13, сообщается с Антивирусным сервером также по «внешнему» интерфейсу, и определить отказ «внутреннего» интерфейса с этого ПК не представляется возможным. В отдельных случаях проходило несколько суток, прежде чем кто-либо из пользователей жаловался на отсутствие обновлений. Конечно, такая ситуация является нетерпимой (в среднем за сутки получают обновления 50÷70 пользователей).

В целях ежедневного контроля доступа к Антивирусному серверу, один из ПК Сетевого операционного центра был переведён из внешней сети во внутреннюю (10.0.9.61), а дежурному оператору было вменено в обязанность дважды в сутки контролировать доступ к Антивирусному серверу с посылкой электронного письма автору в случае наличия проблем. К сожалению, ввиду различных причин, подобный метод контроля не давал надёжной гарантии успеха. Основной причиной, как и во многих других случаях [12], явился человеческий фактор.

Поэтому, встала проблема постоянного контроля наличия связи Антивирусного сервера по «внутреннему» интерфейсу с алиасом 10.0.13.1.

Наилучшим вариантом, по представлению автора, является периодическое пингование (ping) по ICMP-ECHO-протоколу [23] алиаса 10.0.13.1 роутера «внутренней» части ЛВС с Антивирусного сервера по внутреннему интерфейсу. Для этого использована специально написанная программа, которая позволяет оператору ПК

устанавливать проверяемый IP-адрес, начинать и заканчивать период проверки и завершать программу.

На рис. 45 показано окно программы на экране ПК. Виден пингуемый адрес 10.0.13.1, установленный, согласно протоколу, 01 февраля 2016 в 20:19:08, исполнено начало пингования в 20:19:12, получен первый ответ в 20:19:13, и с тех пор до текущего времени (03 февраля, 20:45:54) изменений не было.

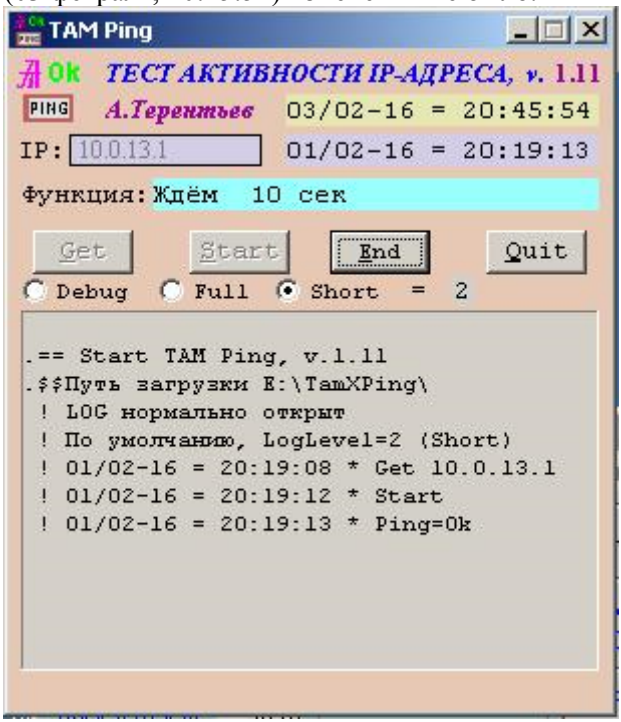

Рис. 45. Окно программы TamIPing Антивирусного сервера

Такой успешный результат наблюдается отнюдь не всегда. Примером служит рис. 46, на котором показано постоянное пингование общедоступного сервера Яндекса **YA.RU**. Легко видеть, что периодически наблюдаются интервалы непрохождения пинга (последний – с 21:17:52), далее, впрочем, восстанавливаемые. Безусловно, это не отказы общеизвестного сервера, а периодические разрывы и/или помехи в работе сети оператора 2COM, являющегося домашним провайдером автора.

Программа составлена так, что пингование исполняется каждые 10 секунд. По результатам пингования значок в верхнем левом углу программы, а также иконка на панели задач изменяется согласно текущему состоянию.

Таким образом, даже убрав окно программы с экрана, по виду значка на панели задач легко видеть текущее состояние (сравните иконки на рисунках 1 и 2): зелёные буквы **Ok** либо косой красный крест.

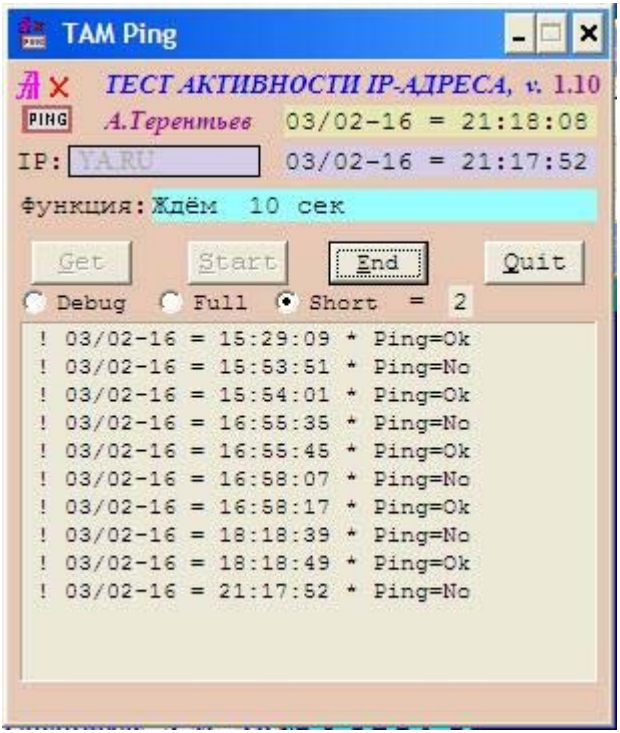

Рис. 46. Окно программы TamIPing домашнего ПК автора

Основная часть алгоритма программы проста. Вызывается стандартное приложение Windows PING.EXE командой

cmd /C PING -n 1 -w 2000 sPing >$TmpFile

где **sPing** – IP-адрес либо URL пингования, **$TmpFile** – временный файл результата. Далее этот файл проверяется на присутствие в нем конструкций “**Reply from**” либо “**Ответ от**” (последнее – в кодировке 866). Присутствие одной из конструкций означает успешное прохождение пинга, отсутствие – неудачу. Изменение

предыдущего состояния, т.е. переход от удачного пингования к неудачному и наоборот, вызывают фиксацию этого в протоколе работы с привязкой ко времени. Таким образом, например, из рис. 46 видно, что все неудачи были одиночными, т.к. через 10 секунд после них следовали удачные пинги.

Следует особо отметить, что временный файл **$TmpFile** на Антивирусном сервере создаётся, как это подробнее рассмотрено в [24], на виртуальном диске, т.е. в оперативной памяти, чтобы не задействовать лишний раз файловую систему, тем более, что она построена на основе зеркального Raid-1-массива. Этот виртуальный диск с постоянной при загрузке Windows буквой поддерживается утилитой "**RAMDrive [Qsoft] Enterprise [x86]**".

Эксперименты, проведённые с помощью указанной программы, показали следующее. Физическое разрывание цепи по внутреннему интерфейсу Антивирусный_Сервер↔Антивирусный_Хаб↔Роутер_ЛВС немедленно (с точностью до 3 секунд) фиксируется пропаданием пинга и сбросом таблицы статической маршрутизации. Восстановление цепи также немедленно вызывает восстановление пинга, но **таблица маршрутизации при этом не восстанавливается**. Для её восстановления достаточно запустить BAT-файл, описанный выше; после вторичного прокладывания статических маршрутов процесс получения обновлений по внутреннему интерфейсу Антивирусного сервера, как показывают эксперименты, автоматически успешно продолжается.

Полученные результаты экспериментов потребовали доработки программы пингования TamIPing. Изменения заключались в следующем.

– Периодичность пингования изменена с 10 секунд до 3 секунд, чтобы наверняка фиксировать даже короткое нарушение физической цепи.

– В программу добавлен блок, который при пропадания пинга немедленно высылает электронное письмо автору с фиксацией ситуации.

– При восстановлении прохождения пинга автоматически запускается BAT-файл прокладки статических маршрутов на сервере, и также может быть выслано подтверждающее электронное письмо.

– Введено автоматическое начало пингования при загрузке программы.

– Введён автоматический старт программы при загрузке сервера.

Программа создана с помощью лицензионного оптимизирующего компилятора PowerBASIC for Windows 9.05. Опции интервала пингования, автозапуска работы после вызова, BAT-файл восстановления статических маршрутов и ряд других размещаются в настраиваемом конфигурационном файле.

Описанная методика поддержки статических маршрутов на сервере с двумя интерфейсами успешно используется на двух серверах в ЦЭМИ РАН более года. На одном из серверов отмечены крайне редкие (несколько раз за год) непрохождения пинга, на другом подобные ситуации встречаются чаще, до нескольких раз за сутки. В обоих случаях отмечено 100%-ное восстановление статических маршрутов с помощью указанных средств.

Практика использования серверов в большинстве случаев не предусматривает постоянного присутствия человека за клавиатурой и монитором сервера. Во многих случаях это невозможно не только вследствие круглосуточной работы сервера, но и из-за технических особенностей: ряд серверов эксплуатируется вообще без постоянно подключённых монитора и клавиатуры. В полной мере это относится к Windows-серверам, и в том числе к Антивирусному серверу (АВ-серверу) ЦЭМИ РАН.

Между тем, в ряде случаев необходимо совевременное приинятие решений, а зачастую и операторских действий при нештатных ситуациях на сервере. Если относительно сбоев электропитания можно что-то предпринять, например, осуществив резкое увеличение срока поддержки автономного питания [25; 26], то существуют ситуации, когда реагировать нужно незамедлительно.

Одна из такого рода ситуаций стала происходить на АВ-сервере в мае 2018 года, когда при принудительном завершении работы раздатчика web-информации Apache 1.3.23 по непонятным причинам не удалялся текущий протокол работы (лог) программы Apache. Это приводило к тому, что на следующие сутки образовывался не новый протокол работы, а продолжался текущий за предыдущие сутки, причем такой эффект мог быть многодневным. При фиксации этого эффекта, автору работы приходилось ежедневно с 23:30 до 00:00 с помощью программы удалённого доступа Remote Administrator [27] контролировать корректность удаления лога, а в случаях невозможности его удаления (“***Файл access.log занят посторонней программой”***) перезагружать сервер, останавливать автоматически стартовавший при перезагрузке Apache, удалять лог и вновь стартовать Apache. Когда означенная ситуация повторилась в пятый раз за 10 дней, стала очевидной необходимость не только найти выход из

ситуации без перезагрузки сервера, но и предусмотреть способ оповещения о такой ситуации.

Для завершения рассмотрения описанной ситуации следует сказать, что разблокировку лога оказалось возможным быстро осуществлять бесплатной программой ***IoBit Unlocker*** [28], которая показала присутствие пары несанкционированных процессов, запущенных якобы из каталога общего доступа. Каталог был исключён из разрешённых к доступу ботами добавлением строки в файл ROBOTS.TXT, и больше означенная проблема не возникала.

Тем не менее, описанная ситуация навела автора на мысль создать внутри Антивирусной службы института сервис автоматической посылки E-Mail-сообщений с параметрической настройкой темы письма и текста сообщения.

```
ECHO OFF
REM !accnt1.bat = Catch Apache access log - Part1
tamdatew "accnt-1 bat-file issues OK" >>accnt.log
if exist accname.$$ DEL accname.$$>>accnt.log
tamdatnw accname.$$ a
"D:\Program Files\Apache Group\Apache\Apache.exe" -w -n "Apache"
     -k stop
if exist access.log del access.log>>accnt.log
ECHO F|XCOPY "D:\Program Files\Apache
     Group\Apache\logs\access.log" E:\STAT\SITE\access.log /Y
     /F>>accnt.log
copy /b acc1.ba + accname.$$ + acc2.ba accnty.bat
REM Занесение дневного лога с нужным именем в каталог
call accnty.bat
REM Удаление дневного лога
del "D:\Program Files\Apache Group\Apache\logs\access.log"
     >>accnt.log
IF NOT EXIST "D:\Program Files\Apache
     Group\Apache\logs\access.log" GOTO OkDel
tamdatew =!!= Accnt-1 Current Apache log IS NOT deleted!
     >>accnt.log
tamsmtp /GO
GOTO TstFlg
:OkDel
tamdatew =+++= Accnt-1 Current log moved. >>accnt.log
:TstFlg
if exist tampst3.flg goto IssueX
tamdatew Accnt1 - Flag is NOT present ! >>accnt.log
tamsmtp /GO /txt=Flag
goto No
:IssueX
if exist accessx.log del accessx.log >>accnt.log
copy /b access.log accessx.log >>accnt.log
REM Наконец можно выполнить полноценную обработку дневного лога
call accntx.bat
:No
tamwait 10
```

Рис. 47. BAT-файл завершения дневной работы Apache

Такой блок уже был однажды запрограммирован и включён в программу постоянного пингования связи с роутером локальной сети [23]. Теперь этот блок был выделен в самостоятельную программу, к которой возможно обращение из BAT-файла. Большинство параметров (путь создаваемого файла отчёта, адрес (URL) почтового сервера, поля From, To, Subj, Text и Password) обычно хранятся в конфигурационном файле рядом с вызываемой программой в системном каталоге, а изменяемые Subj и/или Text могут дополнительно задаваться параметрами вызова.

Теперь соответствующие строки проверки реального удаления лога Apache вставлены в BAT-файл ежедневного завершения работы Apache (рис. 47). В случае неудаления лога исполняется обращение **tamsmtp /GO**, информирующее о необходимости вмешаться в ситуацию.

Второе обращение, ниже, **tamsmtp /GO /TXT=Flag** предусмотрено для ситуации, когда вследствие некорректной работы блока **accntx.bat** обработки дневного лога в предшествующие дни (например, из-за переполнения таблицы пользователей) оказывается убранным флаг-файл **tampst3.flg**. Конфигурационный файл программы **tamsmtp.exe** показан на рис. 48. Из него видно, что поле Subj содержит текст-идентификацию основного AB-сервера "**[AV_Server_LOG]**", текстом по умолчанию является "**Log_NOT_Deleted_Today**". При втором вызове текст меняется на "**Flag**".

```
' TAMSMTP.CFG - конфигуратор SMTP
FullRepName=TAMSMTP.REP
server=vs1.cemi.rssi.ru
from=avir@cemi.rssi.ru
to=tam@cemi.rssi.ru
subj=[AV_Server_LOG]
text=Log_NOT_Deleted_Today
```

Рис. 48. Конфигурационный файл программы TamSmtp.exe

Для реализации приведённой схемы оказалось необходимым на общеинститутском почтовом сервере создать фиктивный аккаунт **avir**, чтобы существующий Mail Transport Agent (MTA) принимал посланные от этого имени сообщения. Поскольку на сервере **vs1.cemi.rssi.ru** не предусмотрена схема парольного доступа, принимаемые сообщения ограничены не аутентификацией, а разрешёнными фиксированными исходящими IP, включающими все AB-сервера и постоянно включённый рабочий ПК Антивирусной

службы. Адрес назначения **to** является основным адресом администратора АВ-серверов.

Результат реализации значительно сокращает объём работы по администрированию АВ-сервера [29]. В частности, вместо ежедневного дистанционного наблюдения в 23:30 за процессом завершения дневной работы по раздаче антивирусных обновлений достаточно скачать и просмотреть текущую почту.

К настоящему времени проведена работа по модификации всех BAT-файлов АВ-серверов с включением туда оповещений в случае аварийных или критических ситуаций.

Поскольку существуют и другие службы, используемые сервером (например, UPS), которые предусматривают оповещение через E-Mail, теперь возможно их задействовать через тот же аккаунт **avir**, повысив информативность сервера и рабочего ПК в критических ситуациях.

Программа **tamsmtp.exe** написана на языке PowerBASIC Console Conpiler 5.05 [30] и достаточно тривиальна. Однако, уточнённый протокол отправки E-Mail был определён опять же с помощью имеющейся системы наблюдения циркулирующих в локальной сети пакетов.

Внедрение в практику сигнальных E-Mail-сообщений подняло работу администратора АВ-сервера на качественно новый уровень. Замещая необходимость постоянного наблюдения за процессами актуализации областей антивирусных обновлений и ежедневной статистики, такая технология существенно экономит время обслуживания. Наличие конфигуратора в программе отправки E-Mail и самодокументированность программы позволяет легко внедрить описанную технологию на других институтских Windows-серверах.

2.7. Определение некорректной настройки ПК

Ещё в [31] отмечено, что некорректная настройка сетевых параметров одного ПК может существенно повлиять на всех других пользователей данного фрагмента сети. При обсуждении принципов работы ПК в сети в 2003 г. было установлено правило «Один MAC – один IP», которое и соблюдалось в течение ряда лет.

Исключения из этого правила начались после выделения основного количества ПК во внутреннюю сеть в связи с введением Wi-Fi, виртуальных серверов и прочих технологических новинок, но для основных сетевых нод правило продолжало действовать. Однако, с течением времени стали наблюдаться два отклонения от этого правила.

Первое: Windows-сервер, имеющий более одного сетевого интерфейса, как выяснилось, посылает broadcasting-оповещения обо всех своих адресах *по всем интерфейсам*. Иными словами, Антивирусный сервер, имеющий в основной сети адрес 193.232.194.11 и во внутренней сети адрес 10.0.13.11, посылает оповещения в обеих сетях от *каждого* из этих IP-адресов. Причину такого сетевого поведения Windows-сервера установить не удалось, но и устранить оказалось невозможным. Пришлось «приспособить» программу сетевого мониторинга к такому явлению.

Второе: компьютер, подвергшийся успешной вирусной атаке, зачастую, помимо своего основного адреса, излучает сетевые пакеты с другими, фальшивыми IP-адресами, которые могут представлять действующие IP-адреса сторонних организаций. Такое явление оказалось столь частым, что стало использоваться в средствах сетевого мониторинга для определения завирусованных ПК. Подробно эта тематика раскрыта в последующем томе данной работы.

2.8. Вспомогательный показ ПК внутренней сети института

Антивирусное обслуживание пользователей предполагает, в том числе, интерактивное взаимодействие антивирусного администратора с их персональными компьютерами для снятия оперативных проблем.

В связи с академическим стилем работы сотрудников ЦЭМИ РАН [18], для Антивирусной службы особенно важным является определение присутствия того или иного сотрудника на рабочем месте, чтобы оказать техническую помощь.

Нестандартность присутствия пользователей института на рабочих местах заставила иметь вторую, малую НС, подключённую к внутренней ЛВС ЦЭМИ РАН, которая постоянно находится в режиме отладочного показа списка нод (рис. 11). Конечно же, эта НС не получает информационных фреймов unicasting от пользователей института, однако, поскольку каждый включённый ПК института «заявляет» о себе регулярными посылками broadcasting-фреймов, состав включённых ПК за последние 15 минут отчётного периода всегда виден на экране, как разъяснено выше в разделе 1.4.

Благодаря этому нововведению, Антивирусная служба ЦЭМИ РАН всегда имеет перед глазами список актуальных включённых ПК.

2.9. Фиксация сбойных сетевых адаптеров

Наличествующее в ЦЭМИ РАН оборудование, и в первую очередь персональные компьютеры, исторически были приобретены в разное время с заметным интервалом в 10-15 лет. За годы работы часть электронных компонентов, и в том числе сетевые адаптеры, пришла в негодность.

К сожалению, конструктивные особенности сетевых карт таковы, что они не всегда имеют чётко выраженную характеристику «работает» – «не работает», в ряде случаев на формально работающих сетевых адаптерах наблюдаются сбои с различной частотой. Одним из наиболее явных проявлений таких сбоев является «обрезание» первых байтов сетевого фрейма, в результате чего корректное распознавание его делается невозможным, поскольку первые 14 байтов (два MAC-адреса и поле Etype) определяющим образом задают характер всего пакета.

Практически, такое явление до поры до времени проходит незаметно: сбойные пакеты просто отбрасываются всеми адресатами, а через необходимое время сетевые карты повторяют трансляцию пакетов, на которые не получены подтверждения. Разумеется, такое явление засоряло сеть, но оставалось незамеченным до внедрения центрального сетевого коммутатора Cisco Catalyst (об этом – в следующем Томе работы).

Тем не менее, в практике работы программы сетевого мониторинга наличествует специальный режим, когда все «подозрительные» пакеты дампируются. Отбор исполняется по ряду определяемых оператором НС признаков – например, при появлении новой ноды. «Обрезание» фрейма спереди как раз и влечёт сдвиг байтов с фиктивным образованием новых MAC-DA и MAC-SA, что фиксируется программой мониторинга.

Последующий ручной просмотр отдампированных пакетов часто позволяет определить источник искажённых пакетов. Большинство из них принадлежит стандартам TCP/IP, и следовательно можно визуально определить местонахождение поля Etype, а перед ним – MAC-SA (если сдвиг не превышает трёх-четырёх байтов, а так и происходит в большинстве случаев).

Указанный метод за время мониторинга позволил зафиксировать несколько сбойных сетевых адаптеров и указать на их немедленную замену.

ЗАКЛЮЧЕНИЕ

Том 2 данной работы посвящён созданию профессионального варианта сетевого анализатора, основанного на обычном ПК и имевшемся в продаже сетевом адаптере. Работая в круглосуточном режиме и наблюдая все имеющие хождение пакеты в интересуемом участке локальной вычислительной сети, снабжённый процедурами, организующими круглосуточную работу, сетевой анализатор канального уровня является по сути средством постоянного сетевого мониторинга объектов ЛВС.

Для превращения пилот-проекта в профессиональный программный продукт проведён ряд специальных исследований и экспериментов. Проанализированы времена срабатывания различных операторов языка PowerBASIC for DOS и предложена уникальная библиотека конвертации числовых переменных из машинного вида в символьный с получением экономии до 5–10 раз. Предложена схема исключения необязательных «длинных» циклов, сокращающая вывод информации на монитор. Использованы методы системного программирования, в частности, внедрена технология прямого доступа к видеопамяти в MS-DOS в процессе конвертации данных.

Показано, что с помощью синтезированных средств на ПЭВМ невысокой мощности возможно устойчивое наблюдение сетевых пакетов канального уровня, в том числе коллизионных.

Успешное внедрение предложенной технологии позволило решить ряд различных задач, подробно описываемых во второй главе данной монографии.

К их числу, в частности, относятся:

– оптимизация структуры сети ЛВС с выделением сегментов, содержащих ПК с большими объёмами пересылаемых данных, для исключения влияния на основную часть сети;

– выявление сетевой заражённости ПК через биллинговые признаки;

– обеспечение работы Антивирусного сервера для раздачи обновлений антивирусных пакетов “Doctor Web”;

– коррекция работы Антивирусного сервера для поддержания конннективности во внутренней локальной сети;

– исследование почтовых сеансов приёма почты по протоколу POP3;

– создание переносной наблюдающей станции, пригодной для экспресс-анализа сторонних сетей;

– определение присутствия сотрудников института на рабочих местах по факту включённости их компьютеров;

– определение в ряде случаев неработоспособных или сбойных сетенвых адаптеров на ряде сетевых ПК.

В следующем томе данной работы будет продолжено рассмотрение приложений сетевого мониторинга, в частности:

– определение нарушающих правила работы в сети персональных компьютеров или серверов;

– определение точного протокола общения TelNet связи с коммутаторами производства Cisco Catalist для создания блока автоматической связи программных приложений с этими коммутаторами;

– автоматическое отключение от ЛВС устройств, нарушающих правила работы в сети, при использовании централизованного коммутатора Cisco Catalyst.

Предложенная технология работы с сетевым мониторингом опробована в ЦЭМИ РАН и ряде сторонних организаций, в первую очередь из числа входящих в корпоративную сеть ЦЭМИ РАН.

Антивирусный сайт ЦЭМИ РАН [9] в разделе «Литература» включает все опубликованные работы автора с 1988 г. и многие работы коллег Отделения экономической информатики ЦЭМИ РАН по тематике информационной безопасности.

.

ПЕРЕЧЕНЬ РИСУНКОВ

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

1. Терентьев А.М. Сетевой мониторинг. Методы и средства. Т. 1: монография / А.М. Терентьев. – Чебоксары: ИД «Среда», 2019 – 116 с. – ISBN 978-5-6042304-9-7

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

3. Терентьев А.М. Задачи полноценного аудита корпоративных сетей // Концепции. – 2003. – №1(11). – С. 94–95. – Свидетельство Роскомпечати 014305.

4. Zale, Robert S. PowerBASIC Compiler, version 3. User's Guide. – Power-BASIC, Inc. 316 Mid Valley Center. Carmel, CA 93923. – 335 с.

5. Zale, Robert S. PowerBASIC Compiler, version 3. Reference Guide. – Power-BASIC Inc. 316 Mid Valley Center. Carmel, CA 93923. – 335 с.

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

7. Терентьев А.М. Технология антивирусной защиты сетевых ПК с использованием специализированного сервера и ПК-сателлита / А.М. Терентьев, А.С. Львова // Развитие и использование средств сетевого мониторинга и аудита: сб. статей / под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2004. –Вып. 1. – С. 47–59. – ISBN 5-8211-0317-7

8. Ляпичева Н.Г. Обнаружение сетевых почтовых атак // Развитие и использование средств сетевого мониторинга и аудита: сб. статей / под ред. М.Д. Ильменского. – М.: ЦЭМИ РАН, 2005. – Вып. 1. – С. 28–39. – ISBN 5-8211-0365-7

9. Антивирусный сайт ЦЭМИ РАН [Электронный ресурс]. – Режим доступа: http://av.cemi.rssi.ru

10. Терентьев А.М. Построение и развитие системы сетевого мониторинга // Развитие и использование средств сетевого мониторинга и аудита: сб. статей / под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2004. – Вып. 1. – С. 5–23. – ISBN 5-8211-0317-7

11. Терентьев А.М. Антивирусная защита сетевых рабочих станций / Использование и развитие современных информационных технологий в научных исследованиях: сб. статей / под ред. М.Д. Ильменского – М.: ЦЭМИ РАН, 2003. – С. 64–73. – ISBN 5-8211-0262-6.

12. Терентьев А.М. Многопользовательский режим работы на персональных ЭВМ. Средства системной поддержки. Препринт #WP/99/071. – М.: ЦЭМИ РАН, 1998. – 79 с. – ISBN 5-8211-0035-6.

13. Ляпичева Н.Г. Информационные сервисы и обеспечение их защиты от несанкционированного доступа из сети Интернет // Использование и развитие современных информационных технологий в научных исследованиях: сб. статей / под ред. М.Д. Ильменского – М.: ЦЭМИ РАН, 2003. – С. 32–63. – ISBN 5-8211-0262-6

14. Терентьев А.М. Мониторинг корпоративной сети ЦЭМИ РАН в условиях использования коммутатора Cisco Catalyst / А.М. Терентьев, Н.Г. Ляпичева, Н.А. Кочетова // Развитие и использование средств сетевого мониторинга и аудита: сб. статей. / под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2004. – Вып. 1. – С. 75–87. – ISBN 5-8211-0317-7

15. Вегнер В.А. Разработка и реализация типового проекта выделенного сегмента ЛВС на примере ПК административно-финансовой группы ЦЭМИ РАН / В.А. Вегнер, Н.Г. Ляпичева, А.С. Львова [и др.] // Развитие и использование средств сетевого мониторинга и аудита: сб. статей / под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2004. – Вып.1. – С. 88–101. – ISBN 5-8211-0317-7

16. Doyle Jeff, DeHaven Jennifer Carroll. Routing TCP/IP, Volume II (CCIE Pro-fessional Devel-opment) 1st Edition. – Indianapolis: CiscoPress.; April 2001; Pages: 976. ISBN: 1578700892

17. Дунаев С.Б. UNIX-сервер. Настройка, конфигурирование, работа в операционной среде, Internet-возможности: в 2-х т. Т. 2. – М.: Диалог-Мифи, 1999. – 131 с.

18. Терентьев А.М. Корпоративный вариант технологии использования антивирусных пакетов DrWeb в научных учреждениях: монография / А.М. Терентьев. – Чебоксары: ИД «Среда», 2018. – 100 с. – DOI 10/31483/a-15; DOI 10.31483/r-11245. – ISBN 978-5-6040294-5-9

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

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

21. Ляпичева Н.Г. Коррекция ошибок HTTP-соединения в локальной сети ЦЭМИ РАН / Н.Г. Ляпичева, А.А. Акиншин,

А.М. Терентьев [и др.] // Развитие технологий и инструментальных средств информационной безопасности: сб. статей / под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – Вып. 2. – С. 49–58. – ISBN 978-5-8211-0615-5

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

23. А.М. Терентьев. Поддержание доступности HTTP-соединения с помощью периодического пингования // Современные концепции научных исследований: материалы XXIV Международной научной конференции. – М.: Евразийское научное объединение, 2017. – №2(24). – Т. 1. – С. 37–39. – ISSN 2411-1899

24. Терентьев А.М. Корпоративный вариант реализации антивирусных пакетов Doctor Web в научных учреждениях: результаты // Национальные интересы: приоритеты и безопасность. – М.: ИД «Финансы и кредит», 2013. – №20(209). – С. 41–46. – ISSN 2073-2872.

25. Терентьев А.М. Актуальные проблемы бесперебойного электропитания персональных компьютеров и серверов // Национальные интересы: приоритеты и безопасность. – М.: ИД «Финансы и кредит», 2013. – №30(219). – С. 46–53. – ISSN 2073-2872

26. Терентьев А.М. Автоматизация контроля и статистического анализа электропитания серверов (на примере Антивирусного сайта ЦЭМИ РАН) // Национальные интересы: приоритеты и безопасность. – М.: ИД «Финансы и кредит», 2013. – №32(221). – С. 56–60. – ISSN 2073-2872

27. Удалённый администратор [Электронный ресурс]. – Режим доступа: http://www.radmin.ru/

28. Разблокировщик [Электронный ресурс]. – Режим доступа: https://ru.iobit.com/iobit-unlocker.php

29. Терентьев А.М. Использование сигнальных E-Mail сообщений // Вестник ЦЭМИ РАН. – 2018. – Вып. 2. – 6 с. – DOI 10.33276/S0000557-0-1. – ISSN 2658-3887 [Электронный ресурс]. – Режим доступа: http://av.cemi.rssi.ru/av/r4lit58.pdf

30. PowerBASIC Console Compiler [Электронный ресурс]. – Режим доступа: https://www.powerbasic.com

31. Терентьев А.М. Информационная безопасность в крупных локальных сетях // Концепции. – 2002. – №1(9). – С. 25–30. – Свидетельство Роскомпечати 014305.

Для заметок

Для заметок

Научное издание

Терентьев Александр Макарович

СЕТЕВОЙ МОНИТОРИНГ.
РАЗВИТИЕ И ПРИМЕНЕНИЯ.
ТОМ 2

Монография
Чебоксары, 2020 г.

Редактор *А.М. Терентьев*
Компьютерная верстка и правка *А.А. Кузьмина*
Дизайн обложки *Н.В. Фирсова*

Подписано в печать 03.03.2020 г.
Дата выхода издания в свет 05.03.2020 г.
Формат 70×100/16. Бумага офсетная. Печать офсетная.
Гарнитура Times. Усл. печ. л. 6,2775. Заказ 400. Тираж 500 экз.

Издательский дом «Среда»
428005, Чебоксары, Гражданская, 75, офис 12
+7 (8352) 655-731
info@phsreda.com
https://phsreda.com

Отпечатано в ООО «Типография «Перфектум»
428000, Чебоксары, ул. К. Маркса, 52

ISBN 978-5-6042304-9-7

Терентьев Александр Макарович (р.1953) окончил МИЭМ в 1978 г. по специальности «Прикладная математика». С 1980 – зав. Отделом СМО ИВЦ Моспродснаба, с 1982 – ст. научный сотрудник ведущих отраслевых институтов угольной, затем лесной промышленности страны. Кандидат технических наук (1988). Ph.D. Европейской академии Информатизации (Брюссель, 2003). Работает в ЦЭМИ РАН с 1988; в настоящее время – ведущий научный сотрудник Лаборатории программного обеспечения сетевых информационных технологий. Области научных интересов – проблемы информационной безопасности пользователей, рабочих станций и компьютерных сетей. Основной научной деятельностью А.М.Терентьева являются возглавляемые им направления работ: антивирусные средства персональных компьютеров; мониторинг корпоративной сети.

Предложенные А.М. Терентьевым новые для ЦЭМИ РАН направления работ по тематике информационной безопасности были доложены на Научно-технических Советах ЦЭМИ РАН (1999, 2000, 2010 гг.) и на Учёном Совете ЦЭМИ РАН в 2001 г.

Под руководством А.М. Терентьева создана и успешно функционирует Антивирусная служба ЦЭМИ РАН (2001 г.). Для обеспечения антивирусными средствами ПК и серверов ЛВС ЦЭМИ РАН создана и внедрена постоянно совершенствуемая технология корпоративной поддержки пользователей антивирусного пакета DrWeb. Число пользователей антивирусных средств, централизованно поддерживаемых Антивирусной службой, выросло с 15 (1999 г.) до 200 (2008 г.).

Универсальные средства наблюдения трафика корпоративной сети, предложенные в качестве нового направления работ ЦЭМИ РАН в 1999 г., были в необходимом объёме реализованы по гранту РФФИ 04-07-90260 «Система комплексного аудита и мониторинга корпоративной сети» (2004–2006). Реализация выполнена с использованием низкоуровневого круглосуточного сетевого мониторинга с автоматическим отсечением сетевых объектов, нарушающих работу сети.

Автором опубликовано более 80 научных работ (2020 г.). Он регулярно участвует в Программах Президиума РАН, был руководителем этапов госконтракта с Правительством Москвы (2007–2008 гг.). Ряд программных продуктов А.М. Терентьева зарегистрированы в ФИПС (2012–2014 гг.). Работы с его участием многократно отмечались в числе лучших работ Отделения (1999, 2000, 2003, 2005, 2010, 2018 гг.). А.М. Терентьев награждён медалью в память 850-летия Москвы, а также почётной грамотой Президента РАН (2013 г.).

История становления А.М. Терентьева как программиста описана на страницах «Виртуального компьютерного музея» (http://www.computer-museum.ru/articles/prgtales/1606/).

Интересы исследователя не ограничены узким кругом профессиональных работ. А.М. Терентьев являлся редактором первого в России специализированного журнала «КомпАс» по компьютерным играм (1994 г.): http://www.computer-museum.ru/games/compas.htm. Он также выступил модератором конференции FIDONet RU.GAME.STRATEGY (1996 г.). Помимо этого А.М. Терентьев – автор Help'ов к ранним версиям популярных отечественных антивирусных программ Doctor Web для Windows и SpIDer Guard (2001 г.).

На Антивирусном сайте ЦЭМИ РАН (http://av.cemi.rssi.ru) в разделе «Литература» аккумулированы все печатные работы автора, начиная с 1998 г.

Издательский дом «Среда»
Делитесь знаниями
в среде профессионалов!