А.М. Терентьев

КОРПОРАТИВНЫЙ ВАРИАНТ ТЕХНОЛОГИИ ИСПОЛЬЗОВАНИЯ АНТИВИРУСНЫХ ПАКЕТОВ DRWEB В НАУЧНЫХ УЧРЕЖДЕНИЯХ

Монография

Чебоксары 2018

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

А.М. ТЕРЕНТЬЕВ

Корпоративный вариант технологии использования антивирусных пакетов DrWeb в научных учреждениях

Монография

Чебоксары 2018

УДК 004.42 + 004.49
ББК 32.973.5
Т35

Рецензенты:

Дадян Эдуард Григорьевич, канд. техн. наук, доцент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»

Дыканалиев Калыбек Мукашевич, канд. техн. наук, доцент,
заведующий кафедрой Кыргызского государственного технического
университета им. И. Раззакова, Кыргызстан

Терентьев, А. М.

Т35 Корпоративный вариант технологии использования антивирусных пакетов DrWeb в научных учреждениях : монография / А. М. Терентьев. – Чебоксары: ИД «Среда», 2018. – 100 с.

ISBN 978-5-6040294-5-9

В данной работе описана оригинальная технология снабжения антивирусными средствами коллектива пользователей научной единицы на примере Федерального государственного бюджетного учреждения науки Центрального экономико-математического института Российской академии наук и известного отечественного антивирусного средства «Доктор Веб».

Технология базируется на выделенном Антивирусном сервере и ряде разработанных автором программных средств. В числе пользователей присутствуют ПК общемировой сети Интернет, внутренней локальной сети, в том числе её выделенных сегментов, а также пользователи сегмента DialUp.

Данная технология реализована в ЦЭМИ РАН с 2003 г. и успешно эксплуатируется более 15 лет. Максимальное число пользователей превышало 200 ПК и серверов.

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

ISBN 978-5-6040294-5-9
DOI 10.31483/a-15
DOI 10.31483/r-11245

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Использование персональных компьютеров практически во всех сферах деятельности, в том числе в научных исследованиях, в связи с известными реалиями требуют обязательного использования антивирусных средств (АВ-средств) [1]. Современный рынок предлагает ряд различных пакетов, как целенаправленно антивирусных, так и совмещающих сугубо АВ-средства с другими средствами информационной безопасности: антиспамовой проверкой почтовых отправлений, брандмауэрами с различными расширенными свойствами, коррекцией представляющих повышенную опасность функций операционной системы и многими другими.

Задействование АВ-средств в организациях и учреждениях, конечно, существенно зависит от структуры используемых в организации технических средств, особенностей функционирования её компьютерной сети, характера использования ПК в данной организации. Важную роль играют также такие трудно формализуемые факторы, как профиль стандартного пользователя и оснащённость IT-персоналом. В полной мере это относится и к научным учреждениям, которые, как будет показано, имеют и последовательно сохраняют в течение многих лет свою устойчивую специфику по этим аспектам.

Разумеется, задействуемые АВ-средства должны допускать модификацию в целях адаптации к условиям коллективного использования.

Крупные научные учреждения, как правило, имеют собственную систему сетевых сервисов в виде электронной почты, удалённого доступа (Dialup) и других, развитую систему технических средств управления общей вычислительной сетью учреждения (организации). Сама сеть при этом может представлять собой исторически сложившуюся совокупность разнородных фрагментов с разной степенью защиты пользователей, разным уровнем технического обеспечения и даже разной пропускной способностью. Всё это в полной мере относится к ЦЭМИ РАН.

Выбор АВ-средств и технологий их внедрения и использования, таким образом, существенно зависит не только от качеств выбранного средства и финансовых критериев учреждения, но, в гораздо большей степени, от характерных особенностей эксплуатирующей

организации по «профилю» её пользователей и доступных IT-специалистов. Вендоры ведущих антивирусных продуктов, со своей стороны, отнюдь не стараются учесть все изложенные особенности, по понятным причинам ориентируясь, в основном, на коммерческие эксплуатирующие организации. Поэтому проблема создания, развития и использования технологии антивирусной защиты пользователей сложно структурированной корпоративной вычислительной сети научного учреждения в современных условиях, несомненно, актуальна.

По устоявшимся правилам совокупность самих сетевых кабелей, обеспечивающих работу локальной сети технических сетевых устройств (маршрутизаторы, коммутаторы, свитчи, хабы и пр.), административных средств управления сетью, включенных в сеть рабочих станций и серверов принято в целом называть корпоративной сетью учреждения (КВС) [2]. Соответственно, единые правила функционирования корпоративной сети и правила работы пользователей естественно назвать корпоративными правилами, а АВ-средства, единые для корпоративной сети с совокупностью соответствующих сетевых сервисов поддержки – корпоративными антивирусными средствами.

Таким образом, **объектами данного исследования** являлись, с одной стороны, наличествующие на момент создания системы АВ-средства, и, с другой стороны, особенности эксплуатации ПК в научном учреждении на примере ЦЭМИ РАН.

В процессе работы проводились научные исследования по созданию, развитию и коллективному использованию информационно-сетевой среды для поддержки АВ-средств на базе существующей и модифицируемой локальной вычислительной сети (ЛВС). **В результате исследований** было выбрано адекватное антивирусное средство и достигнута **цель работы** – создан комплекс программно-технических и организационных решений, обеспечивающий снабжение пользователей института обновляемыми антивирусными средствами. Достигнута желаемая **степень внедрения** – результаты проведенных исследований нашли практическое внедрение в институте и других научных организациях. **Итоги внедрения** – результаты исследований используются для научных экономических исследований на базе созданных в институте единого информационного пространства и информационно-сетевой среды.

Возможная **область применения** работы – распространение созданного технического решения на другие организации – достигнута в ходе разработки. Проведены опытные работы по внедрению созданных корпоративных средств в соседнем Институте проблем рынка РАН, студии «Мосфильм» и других организациях. Следует отметить, что из-за организационно-финансовых проблем долговременного внедрения в этих местах добиться не удалось не по вине автора.

Экономическая эффективность работы – установлена в процессе исследований и включает в себя как экономию внешнего Интернет-трафика, так и повышенную комфортность работы пользователей за счёт получения антивирусных обновлений с внутриинститутского сервера, а не с серверов вендора. Важным является также полное окружение пользователя средствами сопровождения на русском языке.

В данной работе описаны предпосылки создания оригинальной технологии использования антивирусных пакетов серии «Doctor Web» [5] в качестве корпоративного АВ-средства, практическая реализация и итоги внедрения. Аккумулированы особо важные итоги работы автора в этой области за 2003–2018 гг.

ГЛАВА 1. АНАЛИЗ И ПОСТАНОВКА ПРОБЛЕМЫ

Выбор, установка и сопровождение антивирусного средства в организации со средним числом пользователей (50–200) неизбежно связаны с рядом типовых, подлежащих решению проблем. В случаях, когда организация является научным учреждением, к обычному кругу решаемых проблем добавляется ряд специфических вопросов.

1.1. СТРУКТУРА СЕТЕЙ ЦЭМИ РАН

Существовавшая к началу разработки (2003 г.) структура сети ЦЭМИ РАН исторически сложилась достаточно сложной. Функционируя на базе популярных ***Ethernet-II/10-100Base-T***, что означает по стандартным соглашениям принадлежность к классу **01h** (***Etherhet/IEEE802.3***) и типу интерфейса **1Ch** (***D-Link 16 bit***), в ней определён основной стандарт циркулируемых пакетов как мультиплексирование ***Ethernet-II*** и ***IEEE-802.3*** [3]. В структуру сети включены несколько различных сетей класса **C**, имеется ряд выделенных сегментов различного ранга с внутренней адресацией, DialUp. Адресное пространство сети, поддерживаемое в 2003 г. Узлом ЦЭМИ РАН, состояло из трёх сетей класса **C** с различной топологией и нескольких фрагментов сети, выделенных в самостоятельные сегменты. Впоследствии значительное число пользователей переведено во внутренний сегмент сети.

В основной сети **193.232.194.*/24**, помимо компьютеров ЦЭМИ РАН, присутствовало заметное число ПК других организаций. Их снабжать антивирусными средствами не требовалось.

Доступ к антивирусным услугам из основных частей структуры КВС, разумеется, должен быть беспарольным. Для некоторых выделенных сегментов, Интернета и DialUp допускаются пароли. Часть сети ЦЭМИ РАН предоставлена другим организациям, которые не должны иметь доступа к ряду сетевых сервисов, в том числе к антивирусной поддержке.

В развитых сетях с достаточным числом локальных пользователей, как правило, используется одно типовое для данной организации (фирмы, учреждения) АВ-средство. Лицензионная политика

дилеров предусматривает существенные скидки при приобретении увеличивающегося числа комплектов. Дополнительная выгода образуется от единообразия наработанных приёмов манипулирования АВ-пакетом.

1.2. ПРОФИЛЬ ПОЛЬЗОВАТЕЛЕЙ ЦЭМИ РАН

Рассмотрим особенности эксплуатации ПК пользователями в научном учреждении на примере ЦЭМИ РАН. Режим эксплуатации большинства ПК нельзя назвать ни офисным, ни круглосуточным, хотя в общей массе сетевых ПК присутствует часть и тех, и других.

В связи с академическими условиями работы, включение компьютера исполняется далеко не каждый день; более того, значительная часть ПК может не включаться несколько недель. Причиной тому является не только частое отсутствие пользователя на рабочем месте; значительная часть пользователей (около 40%) имеет в запасе второй, более старый ПК, который включается только тогда, когда с новым «что-то происходит».

Особо следует отметить поведение пользователей. По разным причинам, которые нет необходимости здесь анализировать, большинство пользователей не мотивированы в серьёзном освоении компьютера и тонкостей операционной системы, тем более таких «непрофильных» для ученых-экономистов пакетов, как антивирусные. Практика наблюдения более чем 800 установок за 8 лет в ЦЭМИ РАН показывает, что приблизительно в 20% случаев пользователь при установке пакета ошибается хотя бы в одном из действий либо пропускает его, что влечёт за собой невозможность или некорректность установки пакета.

Около 30% вычислительных установок в момент установки АВ-средств по разным причинам оказываются неподготовленными к этому процессу. В частности, предварительное удаление остатков старой версии, рабочих файлов и проверка корректности логической структуры локальных томов не исполняются большинством пользователей. Мало кто из них проверяет наличие достаточного места на системном диске, а уж об удалении ненужных рабочих файлов и дефрагментации не стоит и говорить.

В целом, отношение пользователей к компьютерным системным средствам, к которым, без сомнения, относятся АВ-средства,

во многом сформированное нежеланием и неумением вникать в детали, подробно рассмотрено ещё в 1998 году [4]. К сожалению, эти тенденции сохранились до настоящего времени, хотя столь вопиющих примеров уже не наблюдается

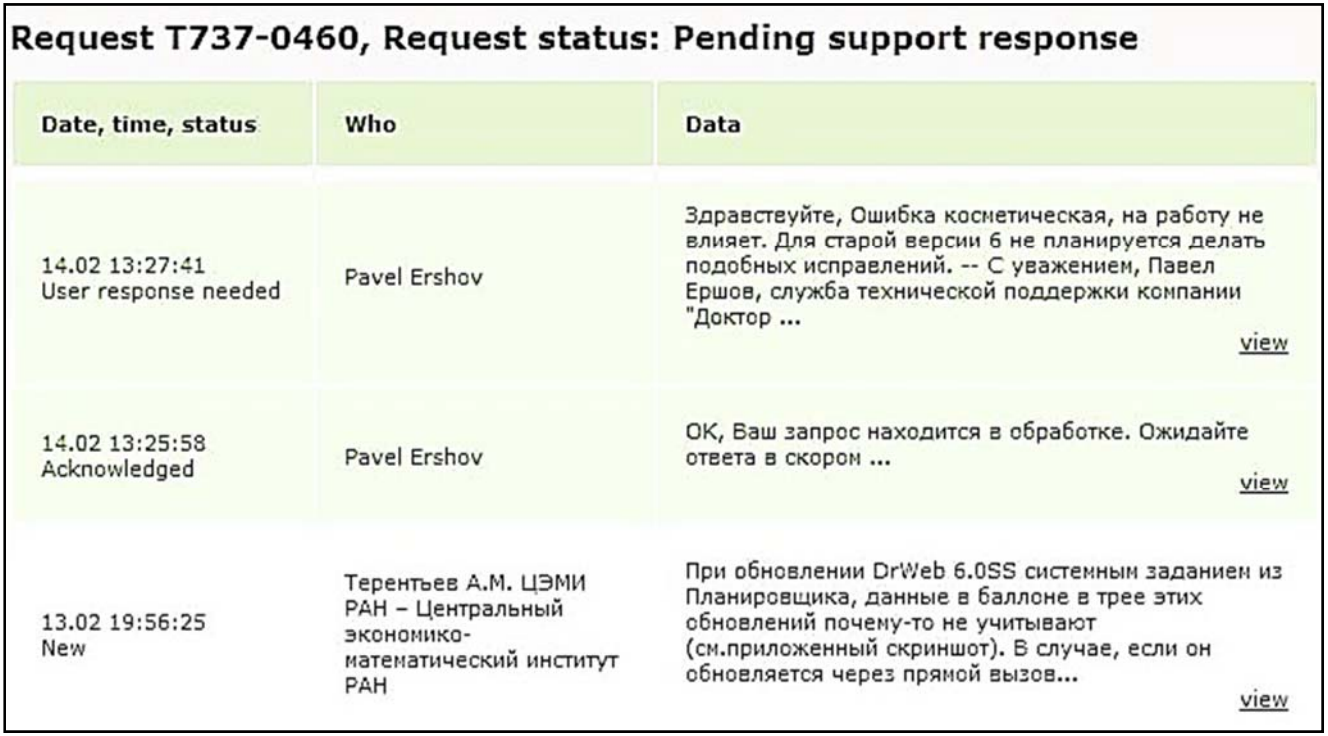
Забегая несколько вперёд, следует сказать, что автор отдал предпочтение продуктам вендора ООО «Доктор Веб» (далее сокращённо DrWeb) [5]. Поэтому, несмотря (или благодаря) давнему предпочтению автором именно этих продуктов [6] [7] [8], помимо позитивных, ряд негативных примеров также взят также из практики эксплуатации этих АВ-средств. Подробно основания выбора именно продуктов DrWeb будут изложены ниже.

Возвращаясь к отношению пользователей, в результате, при попытке установки из стандартного дистрибутива вендора порой возникает ситуация, когда пользователь уже ответил на ряд вопросов, но начавшийся процесс установки неожиданно прерывается с выдачей маловразумительного сообщения (на английском языке или русском профессиональном жаргоне программистов), а порой и без такового. Характерным примером может служить сообщение «**Диск X: не определён**» с прерыванием установки из стандартного дистрибутива, причём дискового тома с означенной буквой на компьютере, действительно, нет. Что означает это сообщение, можно понять только из длинных пояснений, позвонив в техническую службу поддержки. В приведенном примере с антивирусом «Доктор Веб для Windows» причиной появления сообщения являлось отсутствие в момент установки подключённого сетевого диска с указанной буквой, ссылки на который сохранились в некоторых частях системного реестра. Зачем и почему стандартный дистрибутив пакета DrWeb это проверяет, осталось загадкой для автора данной работы. Характерно, что при подобной ошибке при установке пакета в silent-режиме текст подобного сообщения помещался в файл со scratch-именем, который было весьма нелегко обнаружить.

Полного списка возможных ошибок, прерывающих работу стандартной установки, нет ни в одном свободно распространяемом документе по АВ-пакетам всех вендоров. Естественно, в такой ситуации пользователь не осознаёт степень своей вины в части неподготовленности ПК к установке и предпочитает говорить о ненадлежащем качестве программного средства.

Такой вывод пользователя-непрофессионала, между прочим, представляется вполне правомерным, поскольку в идеальном случае программному пакету следовало бы сначала проверить все условия установки, и лишь затем приступать к действиям. К сожалению, подобная желаемая структура программ требует программистского подхода совершенно иной профессиональной школы, что для подготовки современного класса программистов нетипично и практически нигде, кроме специальных организаций, не встречается. Целевая установка современной школы программирования требует «сделать, чтобы работало в большинстве случаев», но вовсе не «сделать, чтобы было понятно и удобно *каждому* конечному пользователю-неспециалисту». Вдобавок, пресловутое выражение Э. Дейкстры «программ без ошибок не бывает» в последние несколько десятилетий, к сожалению, приобрело силу аксиомы и тем самым даёт фактически индульгенцию на некачественную работу, порождая бесконечные патчи, изменения в уже распространённых антивирусных базах, а порой и полное обновление состава исполняющих модулей и уж, конечно же, постоянные отклонения сопровождающей документации от реальных свойств пакета.

Свою роль играет и вынужденная тенденция ориентации программных средств на маркетинговые ходы руководства вендоров вопреки критериям целесообразности и удобства с точки зрения конечного пользователя. Дело доходит до того, что отдельные ошибки, в течение ряда лет мешающие нормальной эксплуатации особо инновационных идей разработчиков пакетов DrWeb, порой поспешно объявляются «косметическими» техподдержкой (рис. 1). Справедливости ради следует отметить, что в описанном на рис. 1 случае автору всё же удалось прийти к нормальному подробному рассмотрению проблемы.



Request T737-0460, Request status: Pending support response

Date, time, status	Who	Data
14.02 13:27:41 User response needed	Pavel Ershov	Здравствуйте, Ошибка косметическая, на работу не влияет. Для старой версии 6 не планируется делать подобных исправлений. -- С уважением, Павел Ершов, служба технической поддержки компании "Доктор ... view
14.02 13:25:58 Acknowledged	Pavel Ershov	OK, Ваш запрос находится в обработке. Ожидайте ответа в скором ... view
13.02 19:56:25 New	Терентьев А.М. ЦЭМИ РАН – Центральный экономико-математический институт РАН	При обновлении DrWeb 6.0SS системным заданием из Планировщика, данные в баллоне в трее этих обновлений почему-то не учитывают (см.приложенный скриншот). В случае, если он обновляется через прямой вызов... view

Рис. 1. Один из характерных запросов в DrWeb об устранении ошибок

Указание недостатков, проведённое выше и сделанное ранее [9], разумеется, существенно не влияет на заслуженно высокий статус пакетов DrWeb, одного из лидеров отечественного рынка АВ-средств, и её разработчиков. Именно вследствие неоспоримых достоинств DrWeb и был выбран в 1999 г. и остаётся до настоящего времени базовым АВ-средством ЦЭМИ РАН. Исследование же взаимодействия различных служб DrWeb и тем более частных мнений менеджеров лежит вне сферы данной работы.

1.3. РАЗВЕРТКА, УСТАНОВКА, НАСТРОЙКА ПАКЕТОВ

Рассматривая подробно ввод в эксплуатацию АВ-средства, как и любого программного пакета, можно выделить ряд этапов его использования: подготовка, установка, настройка, эксплуатация.

Подготовка к установке включает желательное исполнение ряда типовых процедур и соблюдение ряда обязательных правил. Должна быть удалена предыдущая версия пакета или альтернативное АВ-средство[1] и, возможно, ряд иных программ, мешающих работе антивируса (напр., Norton Unerase Wizard и ряд других). Должны отсутствовать логические ошибки на системном томе; должно быть выделено необходимое место для установочного комплекта дистрибутива, его развертки (это отдельное пространство) и конечного состава. В ряде случаев необходимо исполнение ряда обновлений (напр., для Windows' 2000 должны быть установлены Service Pack 4 и Rollup Update 1). Вход в систему в целях установки АВ-средств для современных Windows'2000/XP/Vista/7/+ должен быть выполнен с правами Администратора… Приведена лишь часть основных требований, полный же перечень значительно шире.

Стандартный дистрибутив «Doctor Web для рабочих станций Windows» не предусматривает развёрнутых объяснений возможных некорректных условий установки. В большинстве случаев истинную причину ошибки в установке можно узнать только после

[1] Одновременная работа нескольких антивирусных средств на одном компьютере столь же уместна, как вырезание опухоли одновременно несколькими независимыми хирургами. Существуют комплексные антивирусные средства, включающие несколько ядер известных разработчиков, но этот вариант ввиду его ресурсоёмкости, дороговизны и сложности в обслуживании находится вне рамок рассмотрения данной работы.

обращения в службу технической поддержки DrWeb, приложив журнал установки (если он вообще был получен, если его удалось найти пользователю, если пользователь оказался достаточно умел, чтобы сформировать автоматический запрос в службу поддержки на сайте DrWeb с постоянно меняющимися правилами). Таким образом, проверка условий установки, предложенная пользователям в стандартном дистрибутиве, далека от оптимальной.

Собственно установка пакета в стандартном случае включает поиск нужного дистрибутива, запуск его и исполнение ответов на широкий перечень вопросов, начиная от языка установки и до таких специальных, как логин и пароль для прохода через прокси-сервер. При поиске и запуске дистрибутива, помимо скачивания значительного объёма информации (более 150 Мб), также приходится отвечать на ряд вопросов. Время на ответы не ограничено, но возможны ошибки по вине пользователя. Между тем, в корпоративных условиях на многие вопросы следуют стандартные ответы. Заранее их предусмотрев, можно сильно сократить время установки пакета и избегнуть возможных ошибок.

Завершение ввода в эксплуатацию, непосредственно следуя за настройкой, включает создание ряда специфических условий, облегчающих работу с АВ-пакетом. Прежде всего, это удаление остатков развёртки дистрибутива (150–180 Мб), чего, к сожалению, не делает сам инсталлятор пакета.

Далее, т.к. давность оригинального дистрибутива может быть весьма велика (оригинальные дистрибутивы пакетов DrWeb на сайте DrWeb в последние годы могут не меняться несколько лет), следует сразу же после установки DrWeb вызвать текущее обновление антивирусных баз, которое, в свою очередь, скорее всего вызовет очередную перезагрузку Windows из-за появившихся с момента выпуска дистрибутива многочисленных так называемых критических обновлений, включающие изменённые низкоуровневые драйверы, саму программу обновления (Апдейтер) и ряд других модулей. В последних версиях пакетов DrWeb (5.0, 6.0) стала, наконец, корректно проверяться необходимость перезагрузки в этих случаях. Однако, и в версии 5.0 в этом месте присутствует ряд ошибок, поэтому перезагрузку в этой версии приходится исполнять вручную. Только начиная с версии 6.0 корректно определяется автоматически необходимость перезагрузки ПК после получения

обновлений. В этом случае имеет смысл изменить принятую в оригинальном дистрибутиве по умолчанию процедуру запроса пользователю о перезагрузке системы на принудительную.

Наконец, практика показала, что пользователи в целом весьма небрежно относятся к обновлениям АВ-средств, нередко забывая своевременно выполнить эту процедуру. Для ПК, работающих в офисном режиме, естественным представляется совмещение получения обновлений с включением компьютера. Для ПК круглосуточного режима необходимо создавать специальные задания для Планировщика, исполняющие обновления в определённое время. Начиная с версии 5.0, вендор включает в стандарт поставки задание на обновление, однако оно сформировано, разумеется, без логина и пароля, которые требуются в ряде случаев в корпоративных условиях, а также с требованием исполнения каждые 30 минут, что категорически неприемлемо для условий ЦЭМИ РАН. Такое задание приходится удалять после установки, заменяя его заданием на обновление при включении ПК для офисного режима, либо заданием на обновление 1 раз в сутки для постоянно включённых ПК и серверов.

Настройка антивирусного пакета «Doctor Web для рабочих станций Windows» версий 4.31/33/44 представляла собой гибкий, но весьма трудоёмкий процесс. Достаточно сказать, что число настраиваемых параметров пакета свыше 50, причём далеко не все они могут быть выполнены через экранные меню. Ряд тонких, но важных возможностей требовали ручной коррекции файла настроек DRWEB32.INI[2]. Исполнение всех целесообразных настроек оказывалось не под силу даже пользователям средней квалификации из-за обширного объёма требуемой для усвоения документации (сотни страниц), необходимости знания деталей работы АВ-средств и, к сожалению, порой допущенных в этом средстве ошибок. В сочетании с постоянными и, представляется, мало оправданными переделками в АВ-пакетах DrWeb указанных версий, грамотная настройка этого средства на нужный формат работы

[2] В версиях 5.0/6.0/6.0SS число настраиваемых параметров сильно сокращено, однако сохранены возможности управления многими настройками через файл DRWEB32.INI.

всегда была отдельной существенной проблемой для пользователей.

В частности, характерной проблемой DrWeb версий до 4.44 была нежелательность использования встроенного эвристического анализатора, как из-за его недоработанности и весьма сильного замедления работы маломощных компьютеров, так и вследствие весьма малого эффекта (число реально обезвреженных анализатором вирусов составляло доли процента). При этом, пользователи-непрофессионалы плохо представляют себе, какие конкретные действия нужно выполнять в ситуациях, в которых на какие-либо файлы, порой хорошо им знакомые пакеты, вдруг проявлялась реакция эвристика о том, что это «Возможно, вирус». В связи с этим, для внутриинститутской Антивирусной службы ЦЭМИ РАН проще заблокировать работу эвристика почти во всех возможных случаях, чем разъяснять каждому из 200 непрофессиональных пользователей длинную цепь необходимых действий при появлении таких ситуаций. Это далеко не единственная установка, которую следует, по мнению автора, изменить как умалчиваемую при настройке пакетов.

Конечно же, следует отметить также необходимость изменения некоторых установок «по умолчанию» в целях корпоративной специфики применения АВ-средств. Так, например, в условиях сложной многосегментной корпоративной сети при получении обновлений с внутреннего АВ-сервера бывает необходимо передать АВ-серверу логин и пароль. Соответственно, задание на обновление на Рабочем столе ряда пользователей должно быть сформировано с рядом отличий от стандартного.

Таким образом, на этапе установки и ввода в эксплуатацию антивирусных пакетов DrWeb целесообразно применение средств автоматизации, проверяющих допустимость установки пакета, устраняющих многочисленные ответы пользователя, а также корректирующих настройки пакета.

1.4. ЭКСПЛУАТАЦИЯ ПАКЕТОВ

Серьёзной проблемой эксплуатации пакетов DrWeb стало назойливое стремление разработчиков постоянно осведомлять пользователей о наличии новой версии. Сообщения об этом прихо-

дят во время обновлений, причём само обновление порой блокировалось до выбора пользователем одной из нескольких возможностей («Напомнить завтра» / «Напомнить через 3 дня» / «Через 2 недели»), что, на наш взгляд, не соответствует условиям эксплуатации ПК в научном учреждении, имеющем Антивирусную службу. Более того, в ряде случаев такие сообщения серьёзно затрудняют работу. Так, к примеру, ПК автора работает в режиме постоянной включённости, а обновления осуществляются в 1 час ночи, когда, естественно, за ПК никого нет. Появление подобных сообщений фактически блокирует нормальную работу ПК.

Аналогичные напоминания начинают следовать за месяц до истечения срока действия ключевого файла. При использовании пакетов в научном учреждении, где за обновлением ключевых файлов следит специальная Антивирусная служба, появление подобных напоминаний является лишним. Особо мешают в работе подобные напоминания в случаях эксплуатации пакетов «Doctor Web для файловых Windows-серверов». Сервера, по своей сути, эксплуатируются без постоянного присутствия пользователей; многие из них не имеют ни постоянно подключённой клавиатуры, ни постоянно подсоединённого монитора[3]. Появление подобных напоминаний в этих условиях является поистине медвежьей услугой, поскольку в течение многих недель на экран сервера администратор вполне может не заглядывать.

До конца 2010 г., до обращения автора данной публикации в техническую службу DrWeb, невозможно было корректно обновлять файловые сервера в версиях 5.0/6.0 в случаях, когда не выполнена процедура входа в систему пользователя (Logon). Учитывая, что общепринятым и рекомендуемым является эксплуатация серверов именно без выполнения процедуры Logon, автору этих строк вообще непонятно, кем и как могло эксплуатироваться средство «DrWeb для файловых серверов Windows» до исправления этого недочёта.

В ЦЭМИ РАН среди пользователей популярны ноутбуки. По условиям корпоративной политики, на таковых запрещено осуществлять

[3] Для управления подобными постоянно включёнными серверами уже давно эксплуатируется специальное средство, когда на целую группу серверов используется один комплект «клавиатура + мышь + экран». Амбиции ООО «Доктор Веб» явно не соответствовали современному оснащению технического рынка.

обновления через Интернет. Поэтому, типовая методика установки должна предусматривать, помимо включения задания на обновление в папку **Автозагрузка**, создание аналогичного задания на Рабочем столе пользователя с инструкцией о том, что на ноутбуках из папки **Автозагрузка** задание на обновление следует удалить.

Приведённые замечания показывают, что эксплуатация поставляемых разработчиком стандартных АВ-пакетов DrWeb страдает рядом серьёзных недостатков, нетерпимых в условиях корпоративной эксплуатации.

1.5. ЗАКЛЮЧИТЕЛЬНЫЙ АНАЛИЗ

Всё сказанное выше свидетельствует о ряде дополнительных проблем при непосредственной установке АВ-пакетов DrWeb корпоративными пользователями-непрофессионалами и, в результате, отнимает значительное время и порождает негативные эмоции пользователей.

Таким образом, предложенные вендором стандартные процедуры развертки, установки, настройки и ввода в эксплуатацию антивирусных пакетов DrWeb не рассчитаны на неопытного пользователя, требуют значительного объёма ручных операций и проверки целого ряда условий, а в целом – отнимают заметное время (от 40 минут и более, в зависимости от состояния компьютера и типа предполагаемой эксплуатации).

Следует отметить, что разработчики прекрасно об этом осведомлены. Для корпоративных целей они предлагают иную версию пакета, «Enterprise Suite». Однако, не вдаваясь в многочисленные подробности, отметим, что в предложенном виде этот вариант применительно к условиям ЦЭМИ РАН требует:

– установки, настройки и ввода в эксплуатацию намного более мощного антивирусного сервера, причём на современных операционных системах (Windows'2008+) с дорогостоящими процессорами Xeon, ОЗУ 8 Гб и дорогим аппаратным Raid-массивом в целях повышения скорости чтения;

– установки, настройки и ввода в эксплуатацию SQL-сервера, также оснащённого аппаратным Raid-массивом, уже для распределения серьёзной нагрузки по записи протоколов на жёсткие диски;

– освоения IT-персоналом достаточно сложных инструктивных материалов и приобретение практики использования «Enterprise Suite»;

– множества подготовительных операций системного администратора для обслуживания ряда разнохарактерных классов пользователей;

– постоянного внимания системного администратора над процессами, управляемыми сетевым антивирусным центром;

– разработки ряда специальных нетривиальных программ, извлекающих информацию из нестандартных логов «Enterprise Suite», при желании отобразить статистику работ пользователей на имеющемся Антивирусном сайте.

Все эти условия представляются автору данной работы явно чрезмерными.

В варианте «Enterprise Suite» есть и другие недостатки. К примеру, число пользователей ЦЭМИ РАН порядка 180; в таком случае мгновенный перевод всех пользователей с одной версии пакета DrWeb на другую невозможен; реальный же процесс перехода с версии 4.33 на 4.44, к примеру, занял в ЦЭМИ РАН полгода. Позднее, в 2011 г в момент перехода от версии 5.0 к версии 6.0 DrWeb, ряд пользователей продолжал работу на устаревшей версии 4.44 [10], вследствие чего на АВ-сервере некоторое время поддерживалось 6 областей обновления. Однако, «Enterprise Suite» не поддерживает одновременно несколько различных версий на одном и том же сервере.

По ряду этих и других соображений, предлагаемая разработчиком версия корпоративной технологии использования антивирусного пакета в формате «Enterprise Suite» неудобна, требует повышенной технологической оснащённости, выяснения и исследования недокументированной информации, разработки специальных программ и повышенных затрат IT-специалистов.

Из изложенного ясно, что «разрыв» между совокупностью независимых индивидуальных комплектов и жёстко связанным вариантом «Enterprise Suite» создал предпосылки для альтернативного, промежуточного варианта. Основной особенностью этого варианта, названного при создании нами «технологией корпоративной поддержки», является **идея полного концептуального окружения пользователя сопровождающей поддержкой при установке антивирусного средства и получении обновлений**, однако без жёсткого контроля за состоянием заражённости ПК пользователя и

тем более без навязывания ему конкретного времени и частоты проверок сканером.

1.6. УСЛОВИЯ УСПЕХА РАЗРАБОТКИ

В начале анализа проблемы было отмечено, что помимо авторских пристрастий, существуют и объективные условия выбора вендором «ООО «Доктор Веб», а антивирусными пакетами именно «Doctor Web для рабочих станций» и «Doctor Web для файловых Windows-серверов». Теперь, после рассмотрения авторской концепции корпоративных АВ-средств, включая дистрибутив, можно определить необходимые условия к выбираемому базовому АВ-средству и его исходному, стандартному дистрибутиву, для возможности построения корпоративной среды.

1. Выбранное АВ-средство должно допускать настройку, определяющую обращение за обновлениями вместо базового сервера вендора к серверу эксплуатирующей организации.

Применительно к пакетам Doctor Web, таким средством является файл CUSTOM.DRL, который может быть включён в состав пакета. Файл защищён контрольной суммой и изготавливается службой технической поддержки DrWeb специально по заказу эксплуатирующей организации. В ЦЭМИ РАН в разное время использовалось до 7 различных файлов, определяющих доступ к 7 различным областям обновления.

2. Должен существовать способ включения настройки, указанной в п. 1, в стандартный дистрибутив выбранного АВ-средства.

Применительно к пакету «Doctor Web для рабочих станций», файл CUSTOM.DRL «подхватывается», если он существует в каталоге к моменту вызова стандартного дистрибутива. К сожалению, эта возможность не реализована вендором для дистрибутивов «Doctor Web 6.0 для файловых Windows-серверов», поэтому изготовление соответствующего полноценного корпоративного дистрибутива до исправления этой ошибки невозможно.

3. Должен существовать способ включения группы рекомендованных для корпоративного варианта пользовательских настроек в развёрнутый пакет установленного АВ-средства.

Применительно к пакетам DrWeb, используется технология создания файла с пользовательскими настройками DRWEB32.INI заранее в каталоге установки. При существовании такого файла, он не стирается оригинальным дистрибутивом, а корректируется нужным образом.

4. Выдача обновлений на оригинальных серверах должна соответствовать протоколу HTTP, чтобы для раздачи обновлений использовать аппарат стандартной выдачи файлов.

Все пакеты «Doctor Web» включают утилиту обновления, которая использует стандартный протокол HTTP запроса и приёма файлов [11], что позволило для выдачи обновлений использовать тот же аппарат Apache 1.3.23 [12], что и для HTML-файлов web-сайта. Особенно приятно отметить, что утилита обновления формирует правильное Modification Time для принимаемых файлов.

5. Стандартный дистрибутив должен иметь опционный ключ, позволяющий ему запускаться без выдачи каких-либо запросов пользователю. Должен быть однозначно определён способ определения того, был ли успешно установлен АВ-пакет после отработки стандартного дистрибутива.

Все пакеты DrWeb 4.x–6.0 имеют серию опциональных ключей, которые, при их использовании, подавляют все выдаваемые сообщения пользователю. Все пакеты DrWeb имеют возможность однозначного определения того, установлен ли пакет, по содержимому некоторых ветвей системного реестра, а также по коду завершения. Полная информация по этим вопросам является технической спецификацией разработчика ограниченного пользования, однако, доверенной автору данной работы.

6. В составе стандартного дистрибутива должен находиться файл, определяющий исчерпывающим образом список актуальных файлов. Должен существовать алгоритм, позволяющий по каждому файлу области обновления однозначно определить его принадлежность к актуальному комплекту.

Все современные пакеты DrWeb имеют в своём составе файл, содержащий в себе имена и признаки актуальности всех необходимых файлов – DRWEB32.LST. Хотя автор данной работы самостоятельно определил особенности формата и логической структуры данного файла, таковые здесь приведены не будут, поскольку конкретная информация является собственностью вендора. Разработанные автором программы ведения областей обновления учитывают с 2003 г. формат и особенности этого файла, что существенным образом используется для включения в состав корпоративной области обновления собственных файлов корпоративной поддержки.

С апреля 2014 г. авторы DrWeb изменили функцию получения необходимого списка файлов, используя теперь криптографически защищённый файл VERSION.LST, возможно, рассчитывая на то, и что эксплуатируемая в ЦЭМИ РАН разработка будет заблокирована. Однако, автор нашёл возможность сохранить все функции разработки для всех пользователей.

7. Вне зависимости от предназначения дистрибутива для 32- или 64-битной ОС, утилита обновления пакета должна быть исполнена в 32-битном формате для обеспечения возможности успешной работы на любой платформе, включая серверную.

Все пакеты DrWeb используют утилиту обновления, спроектированную как 32-битное приложение.

После данного явного указания списка требований к поддерживаемому разработанной технологией программному АВ-пакету, можно видеть, что **иные АВ-средства, кроме пакетов DrWeb, в момент, когда создавалась начальная версия корпоративных антивирусных средств в ЦЭМИ РАН (2003 г.), не могли быть поддержаны разработанной технологией.**

Итак, для таких организаций, как научные институты, актуальным является создание «промежуточного» варианта между одиночными пакетами и вариантом «Enterprise Suite».

ГЛАВА 2. КОРПОРАТИВНАЯ СРЕДА КАК ПРЕДЛОЖЕННОЕ РЕШЕНИЕ

Альтернативой стандартному решению «Enterprise Suite», впервые предложенной автором данной работы в 2003 г., является создание корпоративной среды установки и поддержки антивирусных пакетов DrWeb, включающей:

– многоцелевой антивирусный сервер, хранящий как области обновлений указанных антивирусных пакетов (в различные моменты 15-летней эксплуатации – до 6 областей одновременно), так и web-сайт, отражающий инструкции, статистику установок и обновлений этих пакетов и другую информацию;

– специально разработанное программное GUI-средство поддержки корпоративных вариантов пакетов установки DrWeb как для рабочих станций, так и для серверов;

– полученные специальным заказом от разработчика файлы переадресации получения обновлений на области антивирусного сервера вместо штатных серверов DrWeb;

– закупаемые ежегодно ключевые файлы пакетов DrWeb, по паре ключевых файлов на каждый вариант пакета (назначение см. ниже);

– сформированные с использованием полученных ключевых файлов, файлов переадресации, дополнительных текстовых файлов, а также стандартных дистрибутивов разработчика – корпоративные дистрибутивы, включающие также собственные программные разработки;

– ряд специально разработанных программных модулей, исполняющихся на антивирусном сервере в целях формирования областей обновления, ведения статистики этих областей и статистики обращений пользователей;

– инструктивные материалы по корпоративной политике эксплуатации антивирусных пакетов DrWeb, установке и использованию этих пакетов.

2.1. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ ПРИ УСТАНОВКЕ

В результате, действия пользователя при установке (описывается для варианта «DrWeb 6.0 Security Space для рабочих станций»)

следующие. Зайдя на Антивирусный сайт, в соответствующей области пользователь щелчком по ярлыку запускает на своём компьютере специально созданный корпоративный дистрибутив. Сразу же следует отметить, что, если у пользователя нет прав использования корпоративного варианта DrWeb, он не сможет получить доступ к дистрибутиву: права на доступ в область Download абсолютно эквивалентны последующим правам на получение обновлений в соответствующей области. В частности, этим методом по IP-адресам отсекаются пользователи сторонних организаций, ПК которые находятся в основной части ЛВС. Подробнее об авторизации на сайте см. ниже.

После старта корпоративного дистрибутива, исполняется его развёртка во временную папку, которая впоследствии будет удалена, а затем автоматически стартует командный файл. При запуске первым срабатывает программный модуль поддержки TAMDRW60.EXE, вызываемый в режиме инсталляции. Автоматически проверяется ПК пользователя на более чем 20 условий соответствия, и при успехе осуществляется подготовка, включающая очистку ПК от старых ярлыков и оставшихся от старой версии файлов, не удалённых деинсталлятором прежней версии. Разумеется, проверяется наличие альтернативных антивирусных программ и старых вариантов пакетов DrWeb (всего около 20 вариантов), которые зачастую забывают удалить. Далее осуществляется подготовка к запуску оригинального дистрибутива: заранее создаются нужные папки, в них – необходимые файлы сопровождения, формируются настройки будущих программных модулей DWeb (DRWEB32.INI). В связи с наличием так называемой «самозащиты» в версии DreWeb 6.0, модули сопровождения и в частности та же программа TAMDRW60.EXE вместе с файлом её кодированных сообщений TAMDRW60.RME заносятся в отдельно создаваемую папку общего доступа \TAMDrWeb в корне системного тома. В этой же папке будет находиться протокол установки DrWeb на данный ПК DRWSETUP.LOG, а также ряд вспомогательных файлов.

На этом этапе также проверяется доступ к Антивирусному серверу. Во-первых, исполняется попытка считывания некоторого файла, всегда доступного для любого пользователя. В случае неполучения файла, выдаётся соответствующая ошибка доступа, и ра-

бота корпоративного дистрибутива на этом заканчивается. В случае получения файла, производится вторая попытка доступа, уже к нужной области обновления (согласно дистрибутиву), и при требовании авторизации у пользователя запрашиваются логин и пароль на доступ к сайту (предоставляются 3 попытки ввода). Корректность введённой пары логин-пароль проверяется по доступу на соответствующую область обновления. Наконец, полученная указанным доступом информация сравнивается с рабочей информацией дистрибутива для определения того, насколько «свеж» используемый дистрибутив: если уже была выпущена новая его версия, работа также блокируется.

После этого запускается оригинальный дистрибутив в режиме минимума запросов пользователю[4], а после его отработки – опять программа поддержки, второй раз, уже в режиме проверки установленного пакета.

Если проверка подтверждает удачу установки, на ПК пользователя добавляются необходимые компоненты; часть сделанных оригинальным дистрибутивом дополнений корректируется или удаляется в соответствии с корпоративной политикой. После этого автоматически вызывается перезагрузка ПК.

После перезагрузки в специальном режиме, до вызова всех прочих программ и даже до показа ярлыков рабочего стола, однако после установления сетевых соединений и начала работы конкретного пользователя, следует ещё один запуск программы поддержки. На этом этапе удаляются рабочие файлы, в ряде версий проводится коррекция сделанной установки. Факт сделанной установки регистрируется на Антивирусном сайте ЦЭМИ РАН для учёта лицензий. Выводится завершающее информационное сообщение пользователю через Блокнот с рекомендацией о его последующих действиях.

Далее, собственно, запускается показ Рабочего стола Windows и сразу же исполняется вариант стандартного задания пакета DrWeb на обновление. После исполнения обновления (возможно, с последующей перезагрузкой для включения полученных при обновле-

[4] В версии 4.33 было 2 запроса пользователю, в 4.44 – 1, в версии 5.0 и 6.0SS вопросов пользователю вообще не задаётся.

нии критически важных файлов в актуальный состав пакета), программный модуль поддержки запускается ещё раз в скрытом режиме для показа корпоративных сообщений и других специальных целей, которые будут рассмотрены в конце раздела.

В случае выявления недопустимости установки по какой-либо причине, либо неисполнения установки из стандартного дистрибутива, пользователь получает развёрнутое чёткое сообщение на русском языке о создавшейся ситуации с её описанием и возможностями последующих действий. Такое сообщение либо выдаётся программой поддержки, либо предусмотрено в BAT-файле как текстовое сообщение, выдаваемое стандартной программой Блокнот (notepad.exe). Варианты таких аварийных сообщений включают широкий спектр возможных действий пользователя, от рекомендации корректно выбрать соответствующий дистрибутив или удалить старую версию до просьбы немедленно обратиться к Антивирусной службе ЦЭМИ РАН из-за нештатной ситуации.

Таким образом, на всём этапе установки пользователь общается только со средствами поддержки, которые практически не выдают запросов, требующих ответа. Единственным исключением является запрос логина и пароля для доступа на Антивирусный сервер ПК, находящихся вне основной части КВС института и составляющих менее 4% от числа всех пользователей.

Схематически работа корпоративного дистрибутива (с некоторыми упрощениями) изображена на рис. 2.

Упрощения включают отсутствие детализации многочисленных проверок при каждом запуске программы поддержки и сведение множества форм и текстов ошибок к двум-трём. В левой части схемы сверху вниз отображены начальные этапы до перезагрузки операционной системы; в правой части показаны исполняемые в завершение установки блоки.

Штрихпунктирной линией выделен собственно корпоративный дистрибутив в том виде, как он получается после развёртки.

Применение описанной поддержки снимает ситуации принятия решения пользователем во время процесса установки и исполняет все настройки антивирусного пакета на будущие режимы работы, что существенно экономит время и блокирует возможность ошибок.

Как было показано, в процессе установки АВ-пакета программа поддержки несколько раз в различных целях обращается к Антивирусному серверу (АВ-серверу). Каждое такое обращение оставляет в протоколе работы Антивирусного сервера «след», по которому Антивирусная служба ЦЭМИ РАН легко определяет, с какого адреса поступил запрос на тот или иной этап установки, была ли завершена установка пакета, и если да, то фиксируется ряд сведений о текущем пользователе, в том числе дата и время установки, версия ОС на ПК пользователя, а также персональный код ПК, на который выполнена установка, который был присвоен программой поддержки.

Присутствие указанного персонального кода вызвано следующими причинами. За долгое время с 2003 г. ряд пользователей изменили своё местоположение в институте, либо обменялись своими ПК с коллегами по работе, например, купив на грант новый ПК и передав старый коллеге по указанию администрации института. Таких случаев наблюдались десятки, причём никто из пользователей не удосужился поставить в известность Антивирусную службу института о произошедших изменениях. Пришлось с 2009 г. внедрить индивидуальные номера ПК, генерируемые при каждой установке.

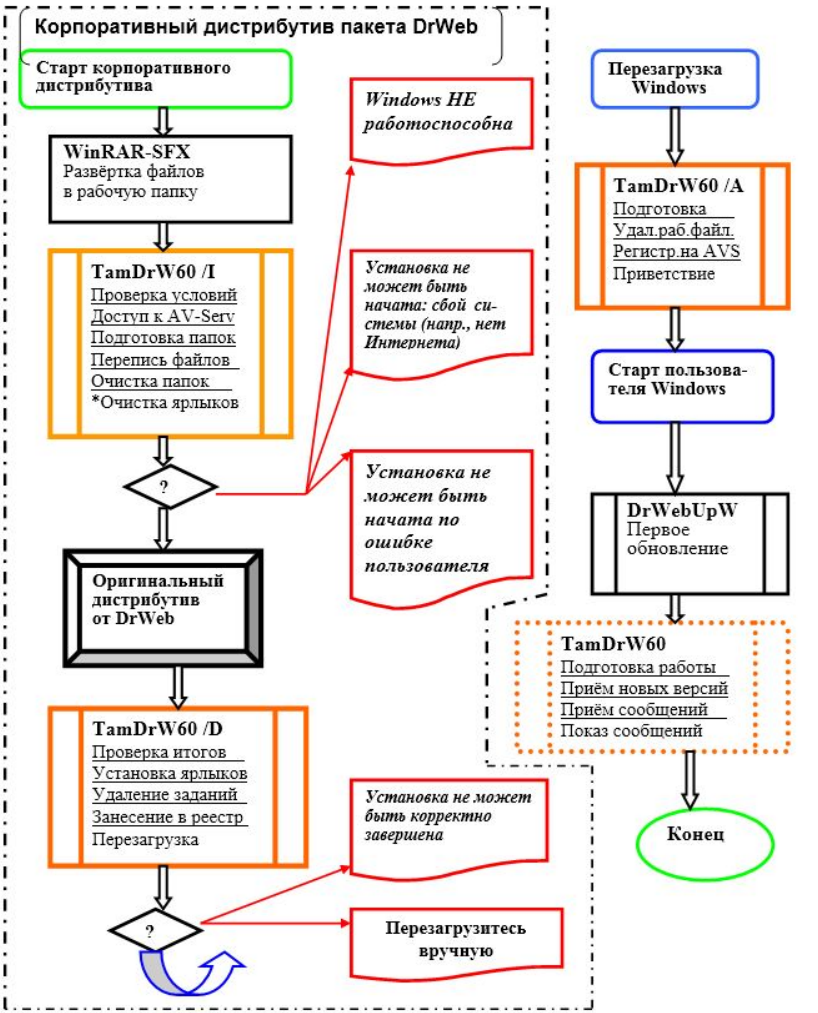


Рис. 2. Упрощенная схема работы корпоративного дистрибутива DrWeb

Далее, с 2007 года начались несанкционированные обращения к АВ-серверу из частных домашних сетей и Интернета. Внедрение индивидуальных номеров показало, что ряд пользователей перенесли за пределы ЛВС института выделенные для них ПК и ничтоже сумняшеся пытались осуществить очередные обновления с

внешних ПК, хотя подобное прямо запрещено утверждённой руководством института Корпоративной политикой использования АВ-средств в ЦЭМИ РАН. За 2008 год выявлено более 30 таких нарушений. К нарушителям применены различные меры воздействия, от простой блокировки АВ-средств до внедрения на ПК под видом обновлений эсплойта, принудительно заставляющего пользователя удалить DrWeb с такого ПК.

2.2. ДАЛЬНЕЙШАЯ ЭКСПЛУАТАЦИЯ ПАКЕТОВ DRWEB

При дальнейшей эксплуатации пакета пользователем обновления антивирусных баз исполняются каждый раз при включении компьютера от лица пользователя, установившего пакет. Обновления исполняются не с сайтов вендора, а из специальной области обновления на Антивирусном сервере. Такая организация работы не только экономит трафик, но и служит гораздо более важным функциям.

Во-первых, многолетняя практика показывает, что не все сеансы обновления завершаются удачно. Бывает разрыв Интернет-связи, иногда наблюдалась перегрузка серверов вендора. За 7 лет отмечены также случаи, когда попытка обновления привела к ошибке вследствие совпадения по времени обновления с процессом реорганизации области на сервере обновления (часть файлов обновилась, часть – нет). В противоречие с многократными заверениями DrWeb в том, что у них постоянных ошибок по связи и обновлениям не бывает, очередной такой случай произошёл совсем недавно, 23.06.2018 в 17:08:54 (в распоряжении автора имеется лог). Наконец, при отсутствии Интернета из-за жары в июле 2010 г., разумеется, сеансы обновлений с антивирусных серверов не проходили, однако это не сбивало работу основной части пользователей: поскольку Антивирусный сервер находится в помещении института, отсутствие Интернет-связи не влияет на работу пользователя, который получает всегда корректные обновления от Антивирусного сервера. Вероятность обрыва связи в этом случае также пренебрежимо мала. Вот и в описанном случае пользователи «не заметили» создавшейся ситуации; они просто не получили новых обновлений 26.05.2010 (область обновления не была изменена).

Во-вторых, скорость обновления пользователей через внутренний сервер резко выше, чем через Интернет. Если в ходе большинства Интернет-соединений с серверами DrWeb скорость зачастую не превышает 50 КБ/с, то при связи с Антивирусным сервером 300–900 КБ/с.

В-третьих, сам факт обновления каждого пользователя с Антивирусного сервера регистрируется специальной программой в конце суток, и на веб-странице Статистики в общедоступной форме содержится список пользователей с датами обновления. Таким образом, обслуживающему IT-персоналу нет необходимости обзванивать или обследовать вверенных их попечению пользователей: все данные об их активности видны на сайте.

В-четвертых, создание своей, корпоративной области обновления позволило избавить пользователей от ряда неудобных сообщений вендора, рекламирующего очередную версию, в ряде случаев – от напоминаний о приближающемся сроке истечения ключевого файла и т. д. К сожалению, эти процедуры организованы «ООО «Doctor Web» с точки зрения корпоративного варианта далеко не лучшим образом: при очередной попытке обновления вдруг появляется соответствующее напоминание, и утилита обновления пакета DrWeb «зависает», ожидая ответа от пользователя (версия 4.33). Более того, если пользователь в течение определённого времени не ответит, обновление вообще не исполняется (версия 4.44). Такая политика нежелательна для корпоративных пользователей рабочих станций и, представляется, недопустима для серверов (обновления которых исполняются, как правило, ночью в отсутствие администраторов). В «своей», корпоративной области обновления, соответствующие приказы до пользователей не доходят.

В-пятых, исследования показали, что через стандартный аппарат обновления пакетов DrWeb можно пересылать также собственные, корпоративные файлы. Антивирусная служба ЦЭМИ РАН с успехом использует эту возможность для рассылки внутрикорпоративных сообщений, которые могут быть адресованы как конкретному пользователю (по его IP-адресу или логину), так и всем сразу. В частности, за месяц до рассылки пользователям новых ключевых файлов все они предупреждаются о необходимости включить *все* имеющиеся ПК в критический период.

В-шестых, наконец, в целях полного исключения возможности контрафактного использования ключей вне ЦЭМИ РАН, корпоративный вариант обновления с 2008 г. предусматривает работу своих пользователей с особыми, заблокированными у вендора, ключевыми файлами. Такая блокировка не мешает работе компонентов антивирусного пакета и обновлений на АВ-сервере, однако не позволит провести обновление с серверов вендора. Антивирусный же сервер ЦЭМИ РАН контролирует IP-адреса пользователей либо связку «логин – пароль», и «свои» пользователи успешно обновляются даже с заблокированными ключами. Естественно, сам Антивирусный сервер использует разблокированный ключ для получения обновления от вендора; отсюда необходимость заказа у вендора именно пары ключей для каждого варианта DrWeb (отдельно для серверов и отдельно для рабочих станций). Такое решение весьма существенно для вендора: оно позволяет быть уверенным в нераспространении ключевых файлов, возлагая всю ответственность на организацию работы Антивирусной службы эксплуатанта.

Следует отметить, что вариант с двумя ключевыми файлами был разработан далеко не сразу [13]. С 2000 г. исследовались различные схемы, пока не был выбран этот метод.

Несколько упрощённая схема потоков информации при формировании корпоративных областей обновления для одного пакета одной версии приведена на рис. 2. Упрощения касаются отсутствия детализации таблиц формируемой статистики, число которых в настоящее время достигает 7. Также не указано, что возможна одновременная обработка нескольких протоколов обновления утилиты DrWeb, накопленных в результате несрабатывания по той или иной причине утилиты поддержки обновлений.

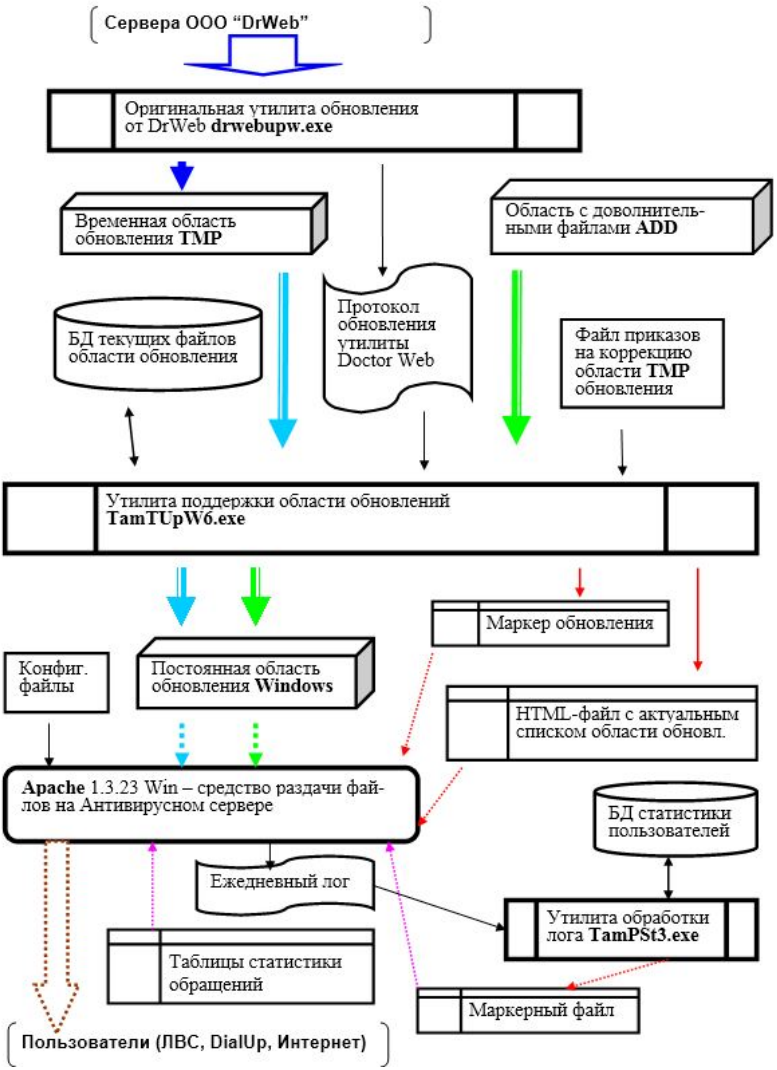


Рис. 3. Схема потоков информации при обновлении DrWeb

Из представленной схемы легко видеть, что скачивание с серверов вендора исполняется в буферную область TMP, представляющую точное зеркало области обновления на сайте вендора. Далее все манипуляции, формирующие область обновления пользователей, исполня-

ются с предварительной многоэтапной проверкой результата, а реорганизация области пользователей исполняется во время, когда раздача обновлений отключена. Этим достигается полная корректность области обновления, предлагаемой пользователям.

Алгоритм формирования конечной области (WINDOWS, имя выбрано вендором) сложен. Он включает анализ корректности её текущего состава, одного или более протоколов, принятых от серверов DrWeb обновлений, учёт управляющих приказов утилиты, фильтрацию приказов на обновление в соответствии с корпоративными правилами[5] и др. По каждой области обновления хранится своя текстовая база данных с рядом характеристик включённых файлов. Такой алгоритм был выработан после ряда вариантов [14].

2.3. ПРИМЕР ОБНОВЛЕНИЯ DRWEB НА СЕРВЕРЕ И РАБОЧЕМ ПК

Рассмотрим примеры обновления DrWeb на сервере (область «***Doctor Web для рабочих станций Windows 6.0 Security Space x86***») и рабочем компьютере (Microsoft Windows'XP Professional SP3) Антивирусной службы.

На рис. 4 представлен экран работы программы обновления соответствующей области обновления АВ-сервера 14.05.2018. Утилита TAMTUPW6 версии 6.06 лаконично показывает получение обновлений для 9 файлов области, а также успешное формирование рабочей формы HTML и маркера обновления для web-сайта TAMTUPW5.MRK.

На рис. 5 представлен собственно протокол работы утилиты обновления (Апдейтера) DrWeb на АВ-сервере, обновляющего нужную область. На рисунке не отражены данные, составляющие коммерческую тайну, а также длинные строки, не имеющие значения для отражения процесса. Легко видеть, что для пользователя (Администратора сети) данные утилиты TAMTUPW6 более лаконичны и информативны, чем протокол работы Апдейтера. Последняя из строчек консольного вывода на рис. 4 отображает обратный отсчёт программы TAMWAIT, удерживающей изображение на экране ровно 10 секунд.

[5] Так, например, файлы *.FLG никогда не попадут в результирующую область обновления. Также предусмотрены специальные меры для ограждения внутрикорпоративных файлов от возможных попыток их удаления приказами исходного файла DRWEB32.LST.

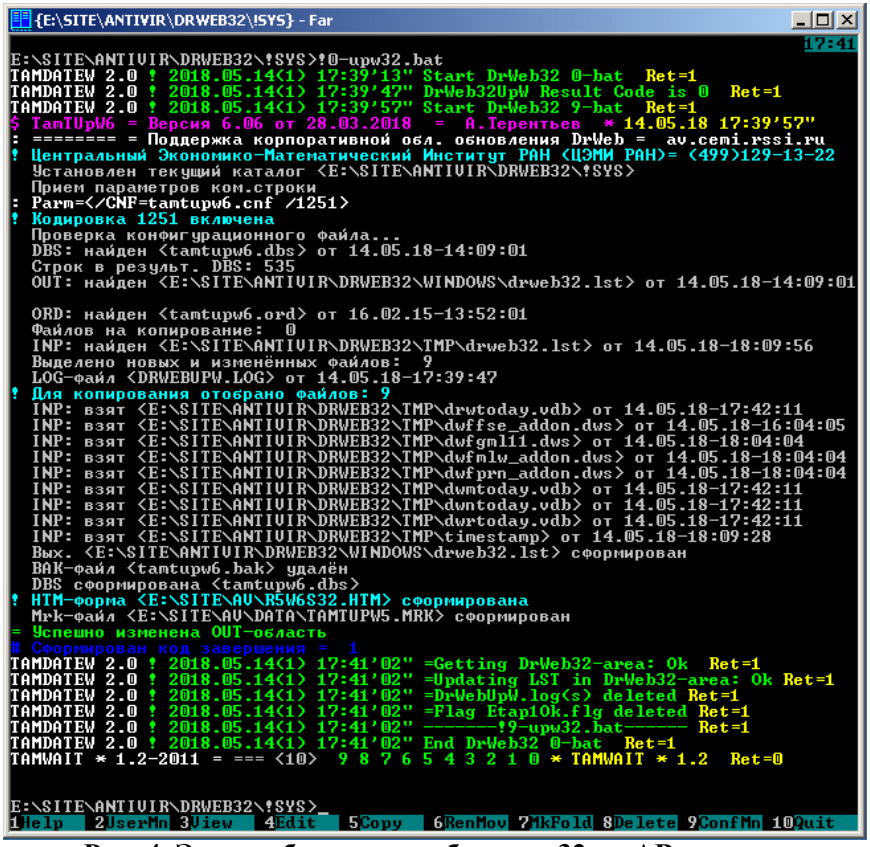


Рис. 4. Экран обновления области x32 на АВ-сервере

```
2018-05-14, 17:39:13  ============================
2018-05-14, 17:39:13  Dr.Web Updater for Windows
   v6.00.18 (6.00.18.04230)
2018-05-14, 17:39:13  (c) Doctor Web, Ltd., 1992-
   2012
2018-05-14, 17:39:13  User: [AVSERVER][Administra-
   tor]
2018-05-14, 17:39:13  Command line: E:\SITE\ANTI-
   VIR\DRWEB32\UPW\drwebupw.exe /GO /QU
   /DIR:E:\SITE\ANTIVIR\DRWEB32\TMP /RP+E:\SITE\AN-
   TIVIR\DRWEB32\!SYS\drwebupw.log /UA /URM:disable
2018-05-14, 17:39:13  Path to log: E:\SITE\ANTI-
   VIR\DRWEB32\!SYS\drwebupw.log
2018-05-14, 17:39:13  Mirroring update area
2018-05-14, 17:39:13  Operating system: Windows
   Server 2003 Standard x86 (Build 3790), Service
   Pack 2
2018-05-14, 17:39:13  ============================
2018-05-14, 17:39:13  License file name::
   E:\SITE\ANTIVIR\DRWEB32\UPW\drweb32.key
2018-05-14, 17:39:13  License key number::
   **********
2018-05-14, 17:39:13  Owner:: ФГБУН ЦЭМИ РАН
2018-05-14, 17:39:13  Activation date:: 2017-02-14
2018-05-14, 17:39:13  Expiration date:: ****-**-**
2018-05-14, 17:39:14  DRL file parsed (E:\SITE\ANTI-
   VIR\DRWEB32\TMP\update.drl, 9 URLs)
2018-05-14, 17:39:14  Create network session
2018-05-14, 17:39:14  Connecting to host:
   http://87.242.75.131/x86/600/sspace/windows/
   (87.242.75.131)
2018-05-14, 17:39:14  Searching timestamp...
2018-05-14, 17:39:14  Transferring timestamp...
2018-05-14, 17:39:14  timestamp transferred
2018-05-14, 17:39:14  Searching drweb32.flg...
2018-05-14, 17:39:14  Transferring drweb32.flg...
2018-05-14, 17:39:14  drweb32.flg transferred
2018-05-14, 17:39:14  Searching version.lst.lzma...
2018-05-14, 17:39:14  Transferring ver-
   sion.lst.lzma...
2018-05-14, 17:39:14  version.lst.lzma transferred
2018-05-14, 17:39:31  Searching drweb32.lst.lzma...
2018-05-14, 17:39:31  Transferring
   drweb32.lst.lzma...
2018-05-14, 17:39:31  drweb32.lst.lzma transferred
2018-05-14, 17:39:34  Searching dwffse_ad-
   don.dws.lzma...
2018-05-14, 17:39:34  Transferring dwffse_ad-
   don.dws.lzma...
```

```
2018-05-14, 17:39:34  dwffse_addon.dws.lzma trans-
   ferred
2018-05-14, 17:39:35  Searching dwfgml11.dws.lzma...
2018-05-14, 17:39:35  Transferring
   dwfgml11.dws.lzma...
2018-05-14, 17:39:36  dwfgml11.dws.lzma transferred
2018-05-14, 17:39:37  Searching dwfmlw_ad-
   don.dws.lzma...
2018-05-14, 17:39:37  Transferring dwfmlw_ad-
   don.dws.lzma...
2018-05-14, 17:39:37  dwfmlw_addon.dws.lzma trans-
   ferred
2018-05-14, 17:39:40  Searching dwfprn_ad-
   don.dws.lzma...
2018-05-14, 17:39:40  Transferring dwfprn_ad-
   don.dws.lzma...
2018-05-14, 17:39:40  dwfprn_addon.dws.lzma trans-
   ferred
2018-05-14, 17:39:42  Searching dwmtoday.vdb...
2018-05-14, 17:39:42  Transferring dwmtoday.vdb...
2018-05-14, 17:39:43  dwmtoday.vdb transferred
2018-05-14, 17:39:43  Searching dwntoday.vdb...
2018-05-14, 17:39:43  Transferring dwntoday.vdb...
2018-05-14, 17:39:44  dwntoday.vdb transferred
2018-05-14, 17:39:44  Searching dwrtoday.vdb...
2018-05-14, 17:39:44  Transferring dwrtoday.vdb...
2018-05-14, 17:39:44  dwrtoday.vdb transferred
2018-05-14, 17:39:44  Searching timestamp...
2018-05-14, 17:39:44  Transferring timestamp...
2018-05-14, 17:39:44  timestamp transferred
2018-05-14, 17:39:47  Searching drwtoday.vdb...
2018-05-14, 17:39:47  Transferring drwtoday.vdb...
2018-05-14, 17:39:47  drwtoday.vdb transferred
2018-05-14, 17:39:47  Files transferred
2018-05-14, 17:39:47  Updating files...
2018-05-14, 17:39:47  Disconnected
2018-05-14, 17:39:47  ============================
```

Рис. 5. Протокол обновления области x32 на АВ-сервере

Следующие 2 рисунка отображают обновление на рабочем ПК сразу же после исполнения обновления области на сервере.

```
2018-05-14, 17:44:25  ============================
2018-05-14, 17:44:25  Dr.Web Updater для Windows
   v*.**.** (*.**.**.*****)
2018-05-14, 17:44:25  © ООО «Доктор Веб», 1992-20**
2018-05-14, 17:44:25  User: [TRENTY-904][trenty]
```

```
2018-05-14, 17:44:25  Командная строка: G:\Program
   Files\DrWeb\DrWebUpW.exe /GO /QU /URM:noprompt
2018-05-14, 17:44:25  Path to log: G:\Documents and
   Settings\trenty\DoctorWeb\DrWebUpW.log
2018-05-14, 17:44:25  Операционная система: Windows
   XP Professional x86 (Build 2600), Service Pack 3
2018-05-14, 17:44:25  ============================
2018-05-14, 17:44:25  Имя файла лицензии:: G:\Pro-
   gram Files\DrWeb\drweb32.key
2018-05-14, 17:44:25  Номер ключа:: **********
2018-05-14, 17:44:25  Владелец:: ФГБУН ЦЭМИ РАН
2018-05-14, 17:44:25  Дата активации:: ****-**-**
2018-05-14, 17:44:25  Дата окончания:: ****-**-**
2018-05-14, 17:44:25  DRL-файл обработан (G:\Program
   Files\DrWeb\custom.drl, 1 URL)
2018-05-14, 17:44:25  Create network session
2018-05-14, 17:44:25  Подключаемся к хосту:
   http://av.cemi.rssi.ru/antivir/drweb32/windows/
   (193.232.194.11)
2018-05-14, 17:44:25  Поиск timestamp...
2018-05-14, 17:44:25  Принимаем timestamp...
2018-05-14, 17:44:25  timestamp принят
2018-05-14, 17:44:25  Поиск drweb32.flg...
2018-05-14, 17:44:25  Поиск drweb32.lst.lzma...
2018-05-14, 17:44:25  Поиск drweb32.lst...
2018-05-14, 17:44:25  Принимаем drweb32.lst...
2018-05-14, 17:44:25  drweb32.lst принят
2018-05-14, 17:44:26  Поиск dwffse_addon.dws...
2018-05-14, 17:44:26  Принимаем dwffse_addon.dws...
2018-05-14, 17:44:28  dwffse_addon.dws принят
2018-05-14, 17:44:28  Поиск dwfgml11.dws...
2018-05-14, 17:44:28  Принимаем dwfgml11.dws...
2018-05-14, 17:44:30  dwfgml11.dws принят
2018-05-14, 17:44:30  Поиск dwfmlw_addon.dws...
2018-05-14, 17:44:30  Принимаем dwfmlw_addon.dws...
2018-05-14, 17:44:31  dwfmlw_addon.dws принят
2018-05-14, 17:44:31  Поиск dwfprn_addon.dws...
2018-05-14, 17:44:31  Принимаем dwfprn_addon.dws...
2018-05-14, 17:44:32  dwfprn_addon.dws принят
2018-05-14, 17:44:32  Поиск dwmtoday.vdb...
2018-05-14, 17:44:32  Принимаем dwmtoday.vdb...
2018-05-14, 17:44:32  dwmtoday.vdb принят
2018-05-14, 17:44:32  Поиск dwntoday.vdb...
2018-05-14, 17:44:32  Принимаем dwntoday.vdb...
2018-05-14, 17:44:33  dwntoday.vdb принят
2018-05-14, 17:44:33  Поиск dwrtoday.vdb...
2018-05-14, 17:44:33  Принимаем dwrtoday.vdb...
2018-05-14, 17:44:33  dwrtoday.vdb принят
2018-05-14, 17:44:33  Поиск timestamp...
2018-05-14, 17:44:33  Принимаем timestamp...
```

```
2018-05-14, 17:44:33  timestamp принят
2018-05-14, 17:44:33  drwebaf.sys - не установлен -
   пропущен
2018-05-14, 17:44:33  drwebaf_w2k.sys - не установ-
   лен - пропущен
2018-05-14, 17:44:33  drwebpf.sys - не установлен -
   пропущен
2018-05-14, 17:44:33  drwebpf_w2k.sys - не установ-
   лен - пропущен
2018-05-14, 17:44:33  frwl_db.bin - не установлен -
   пропущен
2018-05-14, 17:44:33  frwl_notify.exe - не установ-
   лен - пропущен
2018-05-14, 17:44:33  frwl_set.exe - не установлен -
   пропущен
2018-05-14, 17:44:33  frwl_svc.exe - не установлен -
   пропущен
2018-05-14, 17:44:33  Поиск drwtoday.vdb...
2018-05-14, 17:44:33  Принимаем drwtoday.vdb...
2018-05-14, 17:44:35  drwtoday.vdb принят
2018-05-14, 17:44:35  Файлы приняты
2018-05-14, 17:44:35  Обновление файлов...
2018-05-14, 17:44:37  EXEC(G:\Program
   Files\DrWeb\drwreg.exe) = 1 (rc = 0)
2018-05-14, 17:44:37  Отключены
2018-05-14, 17:44:37  ============================
```

Рис. 6. Протокол обновления DrWeb на рабочем ПК

Рис. 6 отображает протокол обновления рабочего ПК Антивирусной службы сразу же после обновления на сервере (можно проверить имена обновляемых файлов). После исполнения программы-Апдейтера DrWeb автоматически вызывается уже известная программа TAMDRW60.EXE со специальной целью отразить на АВ-сервере прошедшее обновление компьютера с персональной идентификацией «0000FFFFF» и операционной системой 513 (что означает Windows'XP Service Pack 3). Перед этим программа запускает созданный BAT-файл, который в данном случае пуст. В других случаях в нём могут находиться вызовы Блокнота с нужными сообщениями, адресованными всем или конкретному пользователю. Сообщения зашифрованы, так что хотя каждое из них физически рассылается на каждый ПК, пользователи прочесть сообщения непосредственно не смогут.

Рис. 7 показывает протокол работы программы TAMDRW60.EXE, сохраняемый и накапливаемый в папке \TamDrWeb, находящейся в корне системного диска пользовательского ПК.

```
14/05-18 = 17:44:37.== Start TAM DrWeb60 Corporate
   Support Program, v.6.51
14/05-18 = 17:44:37.$$Путь загрузки G:\TAMDrWeb\
14/05-18 = 17:44:37.! Работа в режиме Update
14/05-18 = 17:44:37.! Ожидание завершения Апдей-
   тера... xT= 63877.359
14/05-18 = 17:44:39.! Ожидание Апдейтера завершено
14/05-18 = 17:44:43 ! Программа не изменена
14/05-18 = 17:44:46 ! Help не изменен
14/05-18 = 17:44:49 ! Прошлые рабочие Msg удалены
14/05-18 = 17:44:49 ! Job {G:\Documents and Set-
   tings\trenty\DoctorWeb\tamdrx.bat} started, res= 1428
14/05-18 = 17:44:50 ! TCP5 Удачн. фикс.Обн на AV-
   сервере {?WV=513&SC=0000FFFF}, Попытка 1
14/05-18 = 17:44:51 ! Результат фиксации на сервере: 1
14/05-18 = 17:44:59 ! Время ожидания исчерпано
14/05-18 = 17:44:59 x End TAM DrWeb60 Corporate Sup-
   port Program, RetCode = 0
```

Рис. 7. Протокол работы утилиты TAMDRW60.EXE после обновления

Формально, строка, помеченная «**14/05-18 = 17:44:50**», соответствует затребованию с АВ-сервера некоего доступного файла при указанных параметрах. Программа обработки ежедневного лога «видит» такие обращения и фиксирует факт обновления, IP-адрес, версию ОС и персональный код.

Часть протокола (лога) программы выдачи web-информации АВ-сервером Apache, соответствующая процессу обновления рабочего ПК, представленного выше, отражена на рис. 8. Видны затребованные файлы, коды успешности/неуспешности получения и завершающая строка, показывающая идентификацию компьютера и версию ОС.

Обращаем внимание, что затребуемый автоматически программой обновления флаг **drweb32.flg** не присутствует в рабочей области обновления, хотя был получен от вендора (рис. 5). Благодаря этому блокируются не нужные пользователю сообщения разработчика.

```
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:31 +0400] "GET /anti-
   vir/drweb32/windows/timestamp HTTP/1.1" 200 10
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:31 +0400] "GET /anti-
   vir/drweb32/windows/drweb32.flg HTTP/1.1" 404 746
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:31 +0400] "GET /anti-
   vir/drweb32/windows/drweb32.lst.lzma HTTP/1.1"
   404 746
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:31 +0400] "GET /anti-
   vir/drweb32/windows/drweb32.lst HTTP/1.1" 200 18393
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:33 +0400] "GET /anti-
   vir/drweb32/windows/dwffse_addon.dws HTTP/1.1"
   200 270180
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:36 +0400] "GET /anti-
   vir/drweb32/windows/dwfgml11.dws HTTP/1.1" 200
   2233452
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:37 +0400] "GET /anti-
   vir/drweb32/windows/dwfmlw_addon.dws HTTP/1.1"
   200 170841
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:37 +0400] "GET /antivir/drweb32/win-
   dows/dwfprn_addon.dws HTTP/1.1" 200 44537
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:38 +0400] "GET /anti-
   vir/drweb32/windows/dwmtoday.vdb HTTP/1.1" 200 109610
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:38 +0400] "GET /anti-
   vir/drweb32/windows/dwntoday.vdb HTTP/1.1" 200 36509
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:38 +0400] "GET /anti-
   vir/drweb32/windows/dwrtoday.vdb HTTP/1.1" 200 29141
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:38 +0400] "GET /anti-
   vir/drweb32/windows/timestamp HTTP/1.1" 200 10
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:40 +0400] "GET /anti-
   vir/drweb32/windows/drwtoday.vdb HTTP/1.1" 200 81337
193.232.194.13 c194-13.cemi.rssi.ru -
   [14/May/2018:17:45:56 +0400] "GET /ANTI-
   VIR/DRWEB32/DIST/tamdrw60.idu?WV=513&SC=0000FFFF
   HTTP/1.1" 200 41
```

Рис. 8. Протокол выдачи обновлений программой Apache AB-сервера

ГЛАВА 3. WEB-САЙТ НА АНТИВИРУСНОМ СЕРВЕРЕ

Начиная с 2003 года, года запуска Антивирусного сервера, параллельно с процессами, обеспечивающими получение антивирусных обновлений от вендора и раздачу их пользователям, в ЦЭМИ РАН велась разработка web-сервера в виде Антивирусного сайта (АВ-сайта). На первых шагах это был внутренний технологический сайт, предназначенный исключительно для хранения и предоставления пользователям инструктивных материалов по используемым антивирусным средствам.

Поскольку автор данной работы в 2004 г. получил грант на разработку промышленного варианта системы низкоуровневого круглосуточного сетевого мониторинга [15] [16] [17], эту разработку по условиям гранта следовало отразить в Интернете. В связи с этим, был создан специальный раздел сайта, посвящённый сетевому мониторингу, а весь сайт был открыт для всеобщего доступа из Интернета.

С тех пор сайт постоянно развивается и совершенствуется. Инструкции по антивирусным продуктам приводятся в соответствие актуальным поддерживаемым версиям антивирусных пакетов, открываются новые функции и сервисы.

После вызова открывается начальный вид сайта (рис. 9). В верхней части размещены 3 заголовка: наименование института, лаборатории и службы. При щелчке по этим заголовкам можно получить вход на главный сайт института, описание Лаборатории на главном сайте института и, соответственно, официальные сведения об авторе, руководителе Антивирусной службы.

Сайт имеет фреймовую структуру. Под заголовком размещены 2 поля – левое, с оглавлением разделов сайта и некоторой дополнительной информацией, и правое, представляющее основное поле сайта. Ниже имеется горизонтальное поле завершителя сайта (даунера), в котором помещены сведения о разработчиках сайта, дате последнего изменения сайта и счётчик обращений с данного IP-адреса.

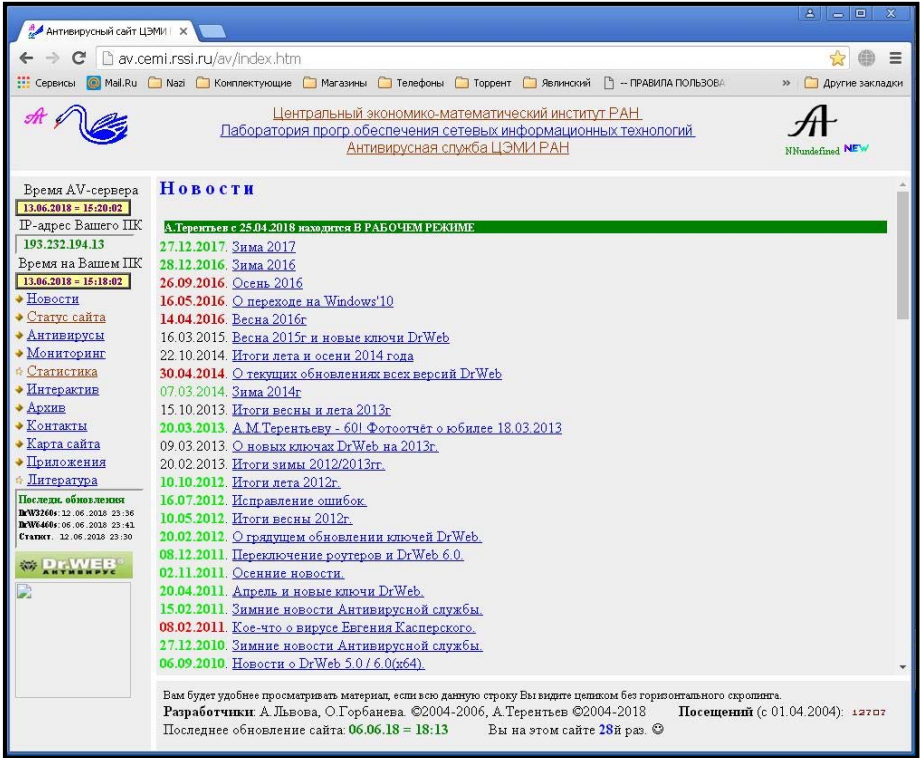


Рис. 9. Общий вид Антивирусного сайта

Рекомендуем обратить внимание, что в левой части приведены 3 важных показателя: IP-адрес обращающегося к сайту, текущее время на АВ-сервере и текущее время на ПК пользователя (меняются каждую секунду). Эти сведения незаменимы для быстрой проверки ПК пользователя, исполняемой перед установкой антивирусных средств.

Под этими сведениями размещаются наименования основных разделов Антивирусного сайта. При обычном вызове сайта в основном поле показывается первый раздел **Новости**. Далее, при щелчке на наименовании раздела, в основном поле сайта показывается начало содержимого заданного раздела.

Под названиями разделов размещён совмещённый информер о состоянии антивирусных областей сервера, точнее, даты их последних обновлений и дата получения последней статистики обращений пользователей (существует с 2008 г.). На приведённом рисунке, в частности, показана текущая дата 13.06.2018, нормальная дата обновления антивирусной области DrWeb32 12.06.2018, но явно ненормальная дата обновления антивирусной области DrWeb64 – 06.06.2018. Это означает, что 07.06.2018 при обновлении этой области произошёл сбой, который был зафиксирован сервером, и более эта область не обновлялась (конечно, это было впоследствии устранено).

Следует отметить, что стандартный вызов АВ-сайта допускается заменять на имеющий параметры. Например, http://av.cemi.rssi.ru?3 после загрузки сайта автоматически переведёт на раздел **Антивирусы**, а вызов http://av.cemi.rssi.ru?4,2 – на раздел **Литература**. Это стало возможным на сайте фреймовой структуры благодаря специальной технологии обращения с глобальными переменными [18].

Движущийся GIF-файл в левом верхнем углу символически отображает инициалы автора сайта и уничтожение червяков (вирусов). Монограмма автора в правом верхнем углу служит входом в специальную область сайта, предназначенную для управления сайтом, и другими целями.

Далее будут кратко рассмотрены все основные области сайта.

3.1. НОВОСТИ

Эта область обычно является стартовой и содержит текущую информацию с датами объявлений об изменяющейся обстановке с АВ-обеспечением в ЦЭМИ РАН, модификациями сайта, существенно важными новостями об антивирусной обстановке в мире

и т. п. При нажатии на заголовок каждой новости в основном окне следует переход на эту новость. На момент подготовки данной работы на сайте содержится 94 новостных раздела.

3.2. СТАТУС САЙТА

Данный раздел содержит основополагающие условия существования сайта. В частности, подчёркивается, что сайт создан и поддерживается по личному желанию автора и не подвержен критике со стороны любых лиц.

Отмечено, что сайт создан для браузера Internet Explorer, и, хотя за время его существования был сделан ряд адаптаций для прочих браузеров, часть функций может быть выполнена некорректно (в частности, показ слайдов в некоторых новостях).

3.3. АНТИВИРУСЫ

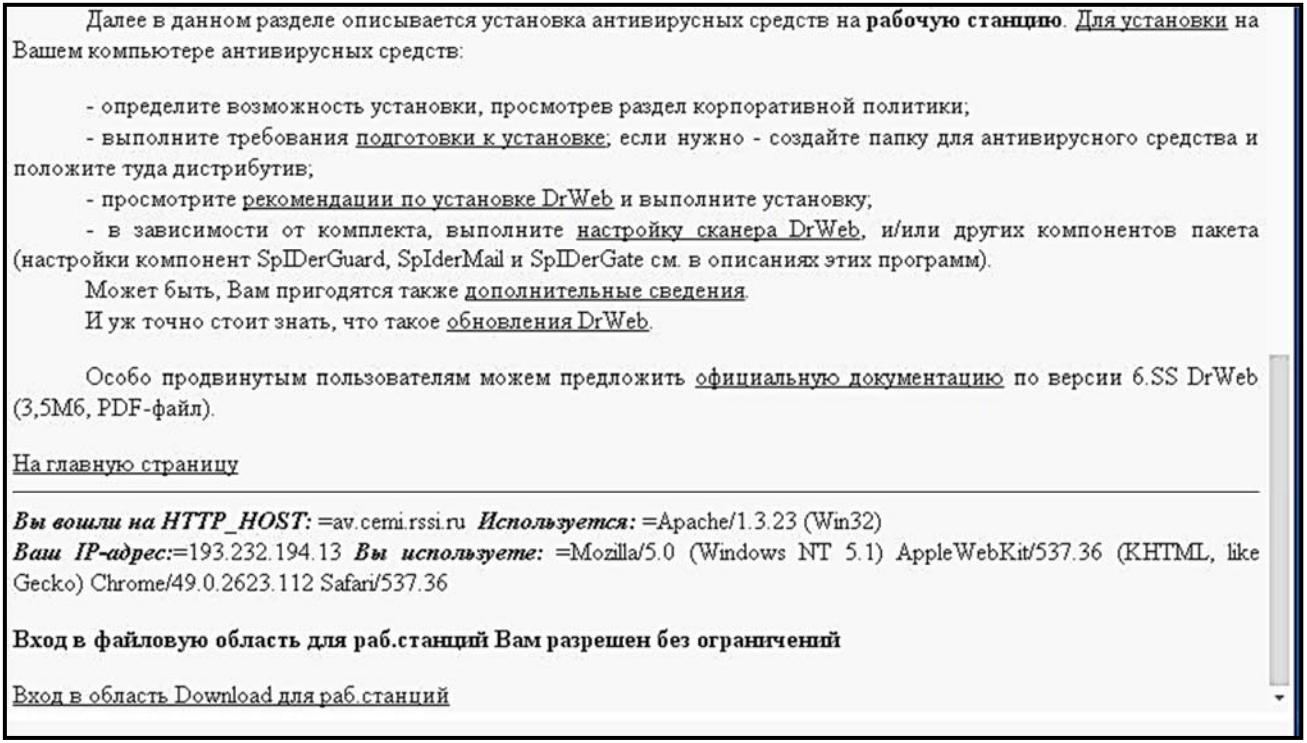
Данный раздел содержит общие данные об используемых АВ-средствах, а также многочисленные ссылки на вторичные документы сайта: инструкции по подготовке и настройке ПК, по установке АВ-средств, по их эксплуатации, а также справочные данные о различных функциях и составе актуальных АВ-средств.

В конце данного раздела содержится вход в область Download для рабочих станций. Для стандартных пользователей АВ-сервера (рис. 10) там содержится фраза о разрешении входа в файловую область Download.

Начало текущего вида области Download показано на рис. 11. Нужно отметить, что после показанной части следует довольно большой перечень различных общеупотребительных программ – как общецелевых программных средств для удаления конкретных вирусов, так и вспомогательных средств для различных операционных систем.

Разумеется, содержание этой области постоянно корректируется: создаются новые дистрибутивы, заменяющие старые, а также включаются новые версии обецелевых программных средств (например, Far).

Для внешних пользователей, а также пользователей управляющей внутренней сети, вход в область Download предоставляется по логину и паролю, если они имеются. Для пользователей основной сети, не являющихся сотрудниками института, вход запрещён. Такие три уровня разграничений сформированы оригинальной программной поддержкой [19] автора на языке Perl [20] [21].


Далее в данном разделе описывается установка антивирусных средств на **рабочую станцию**. Для установки на Вашем компьютере антивирусных средств:

- определите возможность установки, просмотрев раздел корпоративной политики;
- выполните требования подготовки к установке; если нужно - создайте папку для антивирусного средства и положите туда дистрибутив;
- просмотрите рекомендации по установке DrWeb и выполните установку;
- в зависимости от комплекта, выполните настройку сканера DrWeb, и/или других компонентов пакета (настройки компонент SpIDerGuard, SpIderMail и SpIDerGate см. в описаниях этих программ).

Может быть, Вам пригодятся также дополнительные сведения.

И уж точно стоит знать, что такое обновления DrWeb.

Особо продвинутым пользователям можем предложить официальную документацию по версии 6.SS DrWeb (3,5M6, PDF-файл).

На главную страницу

Вы вошли на HTTP_HOST: =av.cemi.rssi.ru ***Используется:*** =Apache/1.3.23 (Win32)
Ваш IP-адрес:=193.232.194.13 ***Вы используете:*** =Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36

Вход в файловую область для раб.станций Вам разрешен без ограничений

Вход в область Download для раб.станций

Рис. 10. Вход в область Download Антивирусного сайта

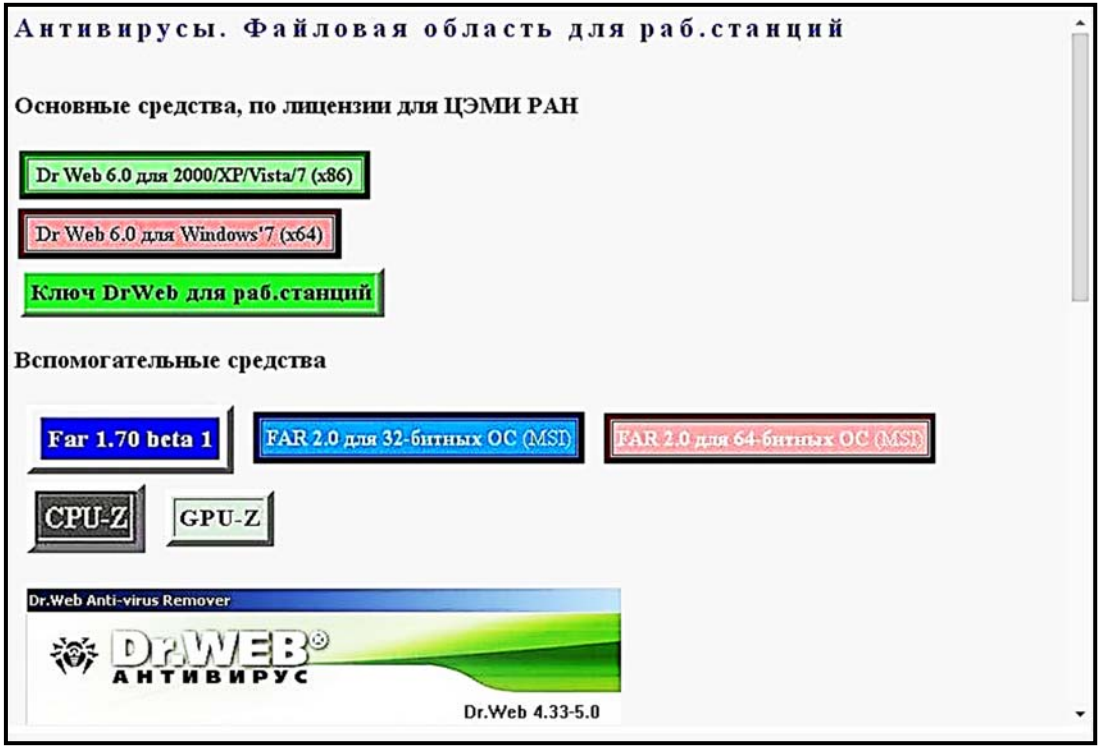


Рис. 11. Область Download Антивирусного сайта

3.4. МОНИТОРИНГ

Данный раздел посвящён низкоуровневому круглосуточному сетевому мониторингу ЛВС [15], развитие которого является самостоятельным проектом и научным направлением, предложенным автором для разработки в ЦЭМИ РАН в 1999 г. [2] [22]. Как уже отмечалось, по условиям гранта 04-07-90260в РФФИ, результаты промышленной разработки обязаны были быть размещены в Интернете, что и было исполнено данным разделом сайта. На рис. 12 показана принципиальная схема потоков информации при сетевом мониторинге к моменту завершения промышленной разработки (2006 г.).

Как можно видеть из рис. 12, персональный компьютер с мониторной программой (МП), регулярно получая данные от наблюдающей станции (НС) по serial-кабелю, исполняет агрегацию данных и посылает через локальную сеть результаты на АВ-сервер [23] [24] [25] [26]. Этот случай является примером функционала, работающего на АВ-сервере помимо антивирусных дополнений.

В этом разделе описана также HTML-форма, вызвав которую можно получить обновляемую каждые 5 секунд сводку о состоянии ЛВС. Этот пример также описывает дополнительный функционал АВ-сервера [27].

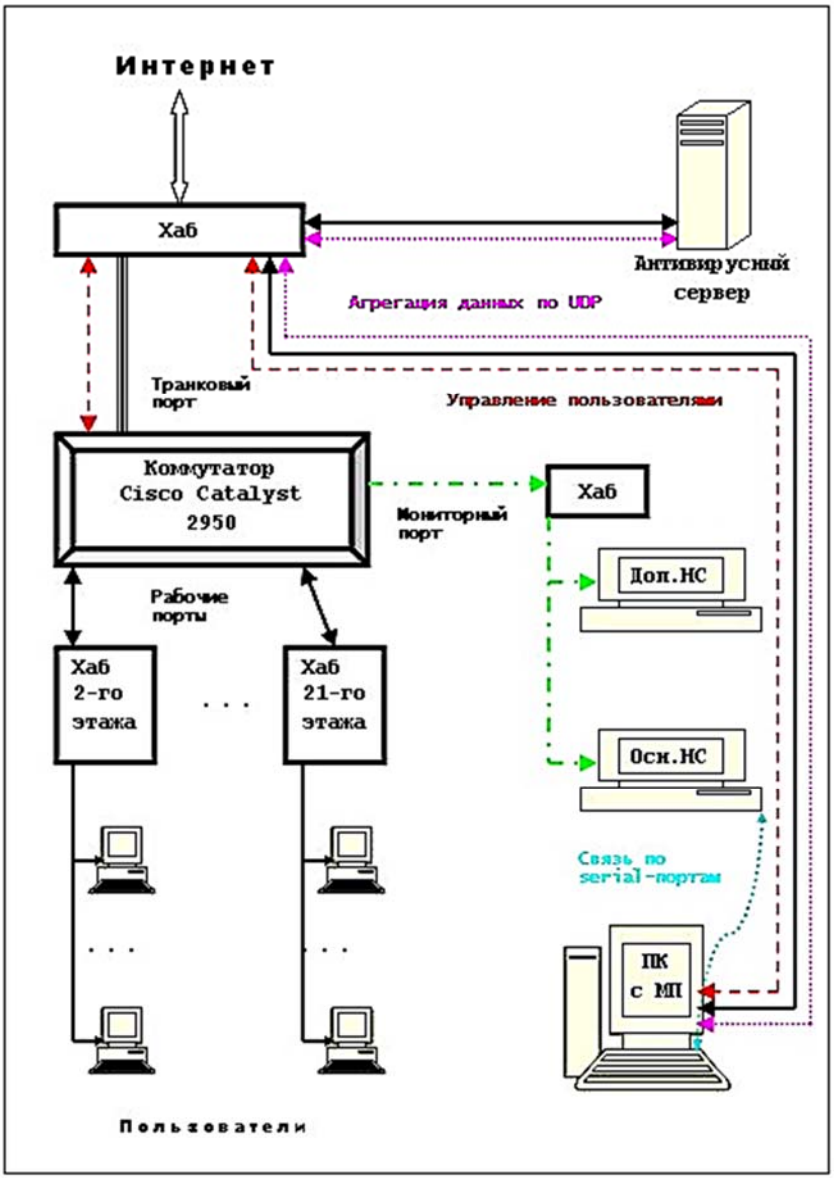


Рис. 12. Схема сетевого мониторинга в 2006 г.

3.5. СТАТИСТИКА

Данная область является, пожалуй, наиболее развитой на АВ-сайте. Помимо статистических данных о состоянии антивирусных областей обновления (вид одной из них приведён на рис. 24) и различного рода статистических таблиц задействования обновлений пользователями (рис. 23), получаемых при ежедневном срабатывании утилит, описанных ниже, в данной области размещены также дополнительные статистические материалы.

Статистика электропитания узла Интернет по запросу пользователя выдаёт сведения о качестве электропитания АВ-сервера (который электрически запитан от Сетевого информационного центра). Форма запроса приведена на рис. 13, форма результатов – на рис. 14.

Подробнее эти вопросы освещены в работах [28] [29].

Статистика скоростей сети 194 ЦЭМИ РАН предусматривает возможность запросов на выдачу средней и максимальной скоростей за интересуемый период (текущий день, текущий месяц, прошлый месяц и пр.). Эта информация относится к агрегации данных сетевого мониторинга и лежит вне рамок тематики данной работы.

Статистика запросов пользователей к DrWeb введена в текущем году и предусматривает возможность подсчёта числа обращений к АВ-серверу за антивирусными обновлениями в различные дни. Подсчёт ведётся на основе учёта обращений к файлу **drweb32.lst** в различных каталогах, независимо от успешности завершения обращения. На рис. 15 приведена форма запроса о числе обращений пользователей за 7 дней, начиная с понедельника 14 мая 2018 г.

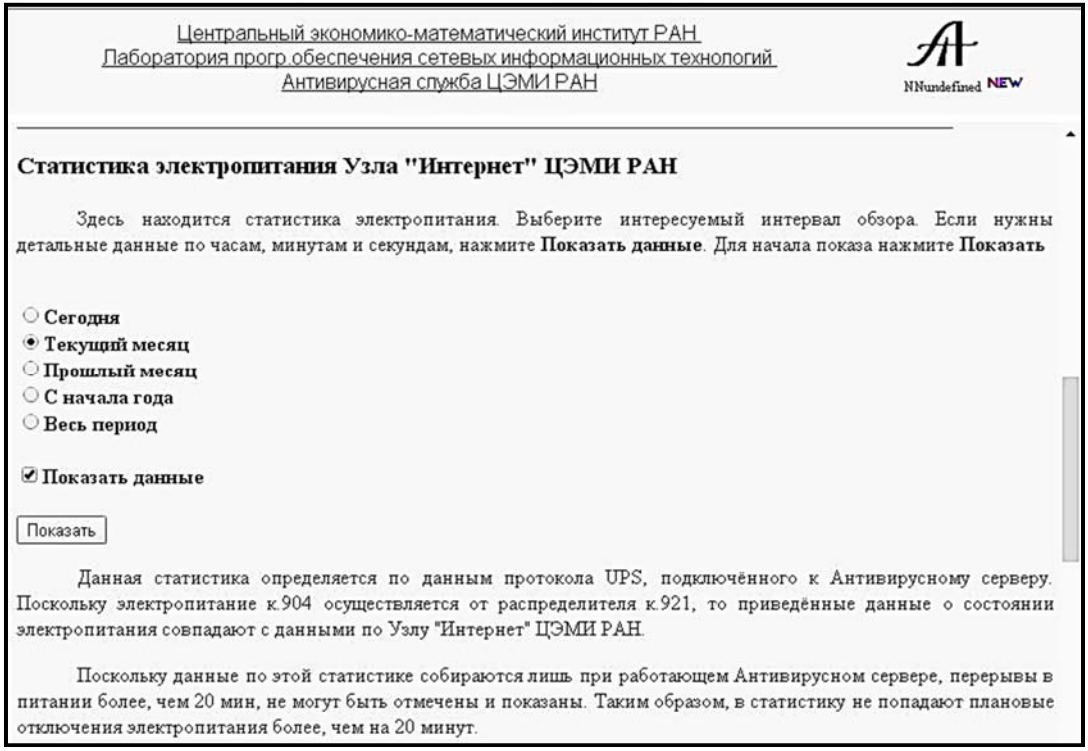


Рис. 13. Форма запроса электропитания в разделе Статистика

Рис. 14. Выходная форма запроса электропитания в разделе Статистика

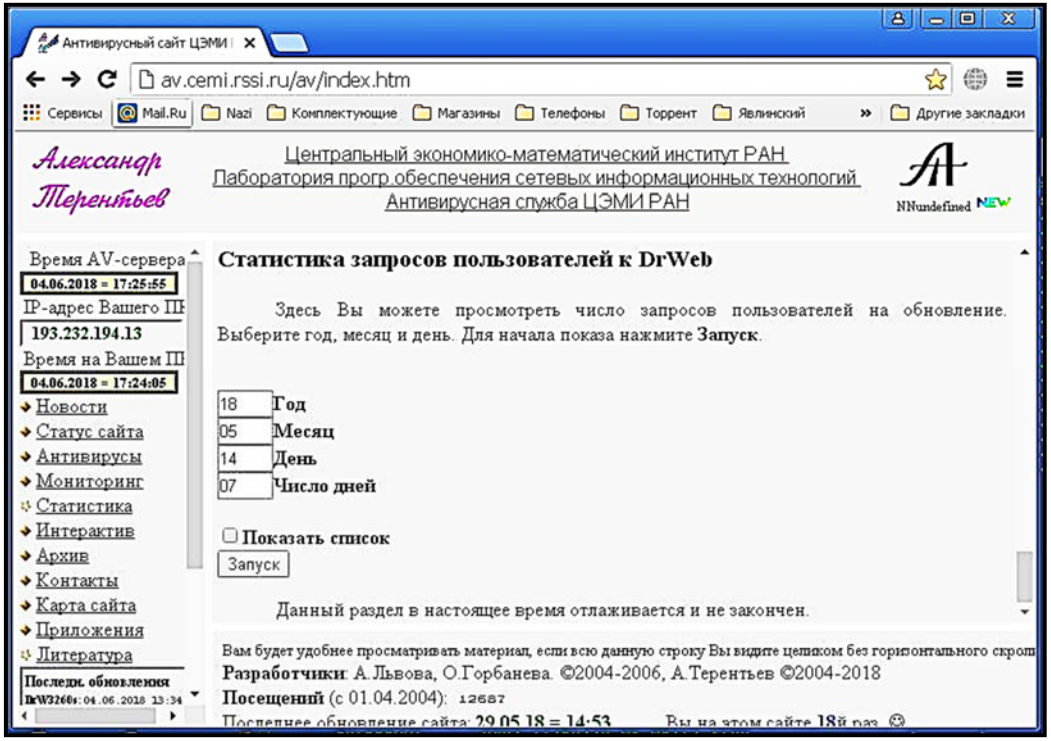


Рис. 15. Запрос по обращениям пользователей в разделе Статистика

Можно видеть (рис. 16), что в различные дни число обращений резко различается. Кроме того, согласно тем же данным, реальное число различных ПК, от которых поступали запросы, существенно меньше, чем общее число запросов за день.

Так, за понедельник 14.05.2018 отмечено 65 различных ПК, которые выполнили 101 обращение за антивирусными обновлениями. Как было разъяснено выше, обращение за обновлением антивирусных баз исполняется, как правило, при включении ПК. Вероятно, ряд компьютеров включался за этот день более одного раза.

Можно видеть, что максимальное число ПК включалось в понедельник и четверг, в остальные дни значительно меньше. В целом, такие данные соответствуют давно известным автору [2] распределению рабочей нагрузки ПК в локальной сети ЦЭМИ РАН.

Отдельный вопрос возникает о значительном числе зафиксированных обращений к АВ-серверу в воскресенье, 20.05.18. Для исследования этого вопроса было выполнено добавочное обращение к этой же форме Статистики, с заданием только этого воскресного дня, но затребованием показа деталей. Результат показан на рис. 17.

Можно видеть, что один из ПК (с IP-адресом 10.0.10.57) обратился 5 раз за антивирусными обращениями. Этот адрес является адресом администратора одной из лабораторий института, который бывает на работе в неурочное время и поэтому до сих пор на нём не скорректировано стандартное задание Планировщика об обновлении каждые полчаса.

Адрес 193.232.194.13 является адресом рабочего ПК Антивирусной службы и автоматически обновляется в 00:30 каждый день. Прочие адреса сети 10.0.*.* принадлежат различным ПК пользователей внутренней части ЛВС, вышедшим на работу в выходной день. Адрес 46.188.27.174 является внешним, домашним адресом Интернета автора данной работы. Обновлялись все 3 компьютера автора, так что ничего необычного здесь нет.

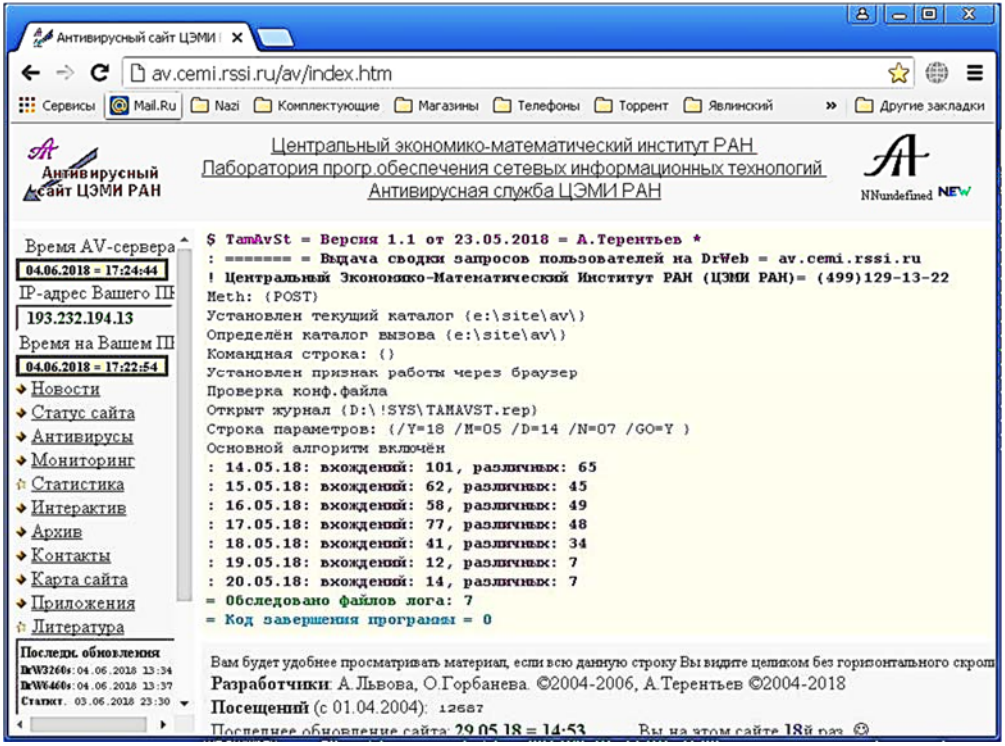


Рис. 16. Выход запроса пользователей DrWeb в разделе Статистика

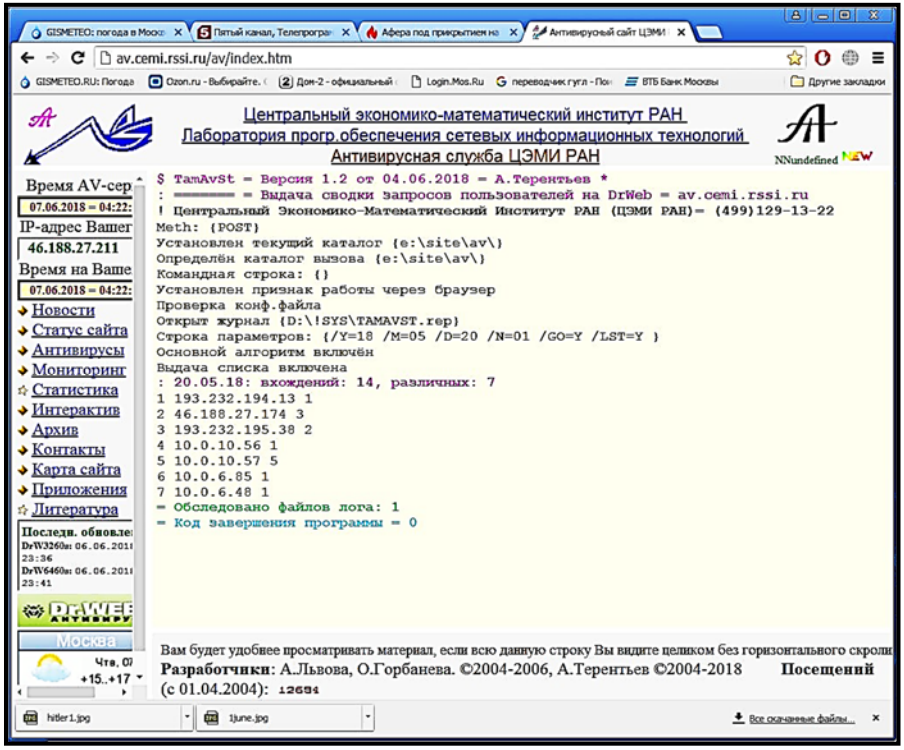


Рис. 17. Выходная форма детального запроса о пользователях DrWeb

3.6. ИНТЕРАКТИВ

Данный раздел, созданный в 2007 г., предполагал развитие возможностей интерактивной работы с сайтом.

Проверка антивирусных средств на ПК пользователя сайта предусматривает попытку скачивания заведомо вирусного файла с АВ-сервера на ПК пользователя. Разумеется, в качестве такового файла используется безвредный, однако внесённый во все антивирусные базы всех антивирусных средств тестовый файл [30]. Если АВ-средство на ПК пользователя действенно, оно должно дать реакцию, как на завирусованный файл, и блокировать скачивание. На страничке сайта конкретно пояснено, какая реакция должна быть у DrWeb.

Предусмотрена возможность проверки не только прямого скачивания заражённого файла, но и нахождение его в составе ZIP-архива, RAR-архива, а также двойного архива (ZIP-архив внутри RAR-архива). Тем самым проверяется качество антивирусной защиты ПК пользователя любым антивирусным средством.

Другая страница Интерактива предусматривает **набор тестов на знание ПК и антивирусной защиты пользователем**. Автор гордится тем, что Антивирусный сайт ЦЭМИ РАН был первым в РФ, где появился подобный вариант интерактивного обучения пользователей [31]. В настоящее время многие сайты переняли эту возможность с различными успехом и полнотой, соответствующий раздел появился даже на официальном сайте DrWeb.

Ещё несколько страничек раздела Интерактив намечено для использования в будущем. Планируется запустить Измеритель скорости Интернета, сбор мнений о сайте и др.

3.7. АРХИВ

В данном разделе размещены сведения о формировании и развитии Антивирусной службы института с 2000 года. Включены ссылки на нормативные документы, принятые Дирекцией или Научно-техническим Советом института по информационной безопасности и антивирусной проблематике.

3.8. КОНТАКТЫ

По установившемуся соглашению с администрацией ЦЭМИ РАН, системное обслуживание всех 5-ти Отделений института исполняется

выделенными системными администраторами. В данном разделе приведены сведения обо всех системных администраторах Отделений.

Разумеется, присутствует и контакт автора данной работы как руководителя Антивирусной службы.

3.9. КАРТА САЙТА

В данном разделе присутствует перечень наиболее существенных частей контента web-сервера, значимого для пользователей. Даны даты последних версий этих документов.

Как пояснено в начале данной главы, к некоторым разделам сайта существует быстрый вызов. В карте сайта приведены сведения о таких вызовах.

Карта сайта существует с конца 2004 г.

3.10. ПРИЛОЖЕНИЯ

Данный раздел создан для хранения различных нормативных документов и внутренней документации системных администраторов. Раздел имеет парольный вход для доступа к внутренней документации.

Раздел был актуален в период становления комплексов информационной безопасности в институте (2000–2004 гг.).

3.11. ЛИТЕРАТУРА

За годы работы автора в Отделении экономической информатики был выпущен ряд сборников по тематике информационной безопасности и смежных. Был также выпущен ряд статей автора и сотрудников Отделения по той же тематике. В 2015 г. были аккумулированы все сведения о различных сборниках Отделения и помещены в эту область.

В настоящее время область содержит актуальные сведения о публикациях основных сотрудников Отделения с 1998 года и насчитывает свыше 50 наименований отдельных публикаций и сборников.

Начиная с 2016 года, на АВ-сервере регулярно, не реже раза в квартал, запускается специальное приложение, регистрирующее запросы к различным материалам данного раздела с 01 апреля 2004 года по настоящий момент. Теперь под данными о каждой публикации находятся текущие сведения о числе затребований данного файла из Интернета – как общем, так и отдельно поисковыми ботами. По состоянию на момент написания данной работы, лидеры имеют от 5000 до 9000 запросов.

ГЛАВА 4. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ПРЕДЛОЖЕННЫХ РЕШЕНИЙ

В ЦЭМИ РАН автором велась разработка предложенного варианта в течение 15 лет. Фактически, в течение всех лет эксплуатации постоянно исполнялась та или иная доработка программ, BAT-файлов, инструкций пользователю, внешнего вида сайта и его контента [32].

Внедрён в эксплуатацию антивирусный сервер, хранящий корпоративные области обновления пакетов «Doctor Web» в различных вариантах: «Doctor Web для Windows x86» (2004–2018 гг.), «Doctor Web для Windows x64» (2004–2018 гг.) и «Doctor Web для файловых Windows-серверов» (1999–2012 гг.), инструктивные материалы по эксплуатации этих пакетов (2004–2018 гг.), Антивирусный сайт (2004 г.) с полной поддержкой статистики получения обновлений пользователями (начиная с 2005 г.), корпоративный дистрибутив (2006 г.). Создание программы поддержки развёртки и ввода в эксплуатацию для версий 4.33 (2008 г.), 4.44 (2009 г.), 5.0 (2010 г.), 6.0 (2011 г.), 6.0SS (2012 г.), применяемой многократно внутри корпоративного дистрибутива, завершает логический цикл полного концептуального окружения пользователя-непрофессионала при работе с указанными АВ-средствами.

Техническим средством, использованным для практической реализации предложенной методики корпоративной поддержки антивирусных пакетов, первоначально являлся сервер на основе Pentium-III/600GHz, Microsoft Windows Server'2000 и Apache 1.3.23. Впоследствии эта конфигурация была обновлена до Intel Pentium4 / 3,0 GHz / 2Gb / Raid1:2*80Gb, что оказалось вполне достаточным для раздачи обновлений, поддержки Антивирусного сайта и выполнения ряда других операций реального времени. Однако, и в настоящее время модернизированный вариант прежнего Антивирусного сервера, несмотря на его значительное физическое и моральное устаревание, с успехом используется для раздачи обновлений при профилактических работах на основном Антивирусном сервере.

Сравнение задействованных технических средств с приведёнными ранее требованиями поддержки «Enterprise Suite» показывает, что в рамках предложенной технологии корпоративной поддержки оказалось возможным задействовать гораздо меньшие ресурсы и технические средства, чем при использовании «Enterprise Suite».

Базовыми программными средствами АВ-сервера являются Microsoft Windows Server 2003 R2 Service Pack 2, Apache 1.3.23, Perl. Внутри ряда областей сервера разрешена поддержка CGI и EXEC-модулей. АВ-сайт сформирован полностью вручную с использованием HTML и CGI, а также анимированного GIF на заставке сайта.

Первоначально при создании АВ-сервера использовалась технология поддержки АВ-средств с использованием вспомогательного рабочего ПК Антивирусной службы [14]; в настоящее время все сопровождающие процессы сосредоточены непосредственно на АВ-сервере.

Внедрение в эксплуатацию предложенного корпоративного варианта антивирусных пакетов DrWeb фактически представило собой использование средств автоматизации, что позволило существенно интенсифицировать процесс обслуживания пользователей. Число сотрудников, занятых антивирусным обслуживанием пользователей, сократилось в 3 раза.

Выше показана неэффективность использования стандартных предлагаемых вендором вариантов использования антивирусных пакетов Doctor Web в научных учреждениях и сформулирована авторская концепция корпоративной поддержки этих пакетов в указанных условиях. Технические и базовые программные средства реализации предложенной концепции описаны здесь.

4.1. ТЕХНОЛОГИЧЕСКИЙ АНТИВИРУСНЫЙ СЕРВЕР

Как уже было упомянуто, АВ-сервер, помимо операционных средств и программного комплекса Apache+Perl, реализующего web-сервер, включает в своей рабочей области ряд групп каталогов, каждая из которых составляет одну область обновления того или иного пакета DrWeb. Формирование каждой области обновления исполняется 1 раз в сутки в период, когда web-сервер отключён (23:30 – 00:05 MSK). Задания на реформирование областей обновления автоматически запускаются Планировщиком Заданий

АВ-сервера с интервалом в 10 минут. Отдельно запускается задание на подведение ежедневных итогов работы АВ-сервера «**!accnt-1.bat**» с учётом работы всех пользователей при получении обновлений и информации web-сайта.

На рис. 18 показан BAT-файл **!accnt-1.bat**, исполняющийся ежедневно в 23:30. Он содержит команду останова Apache, запись ежедневного лога в служебный каталог и запуск процедуры ежедневного учёта. Этот BAT-файл включает два внутренних BAT-файла, показанные на рисунках 19 и 20.

```
ECHO OFF
REM !accnt1.bat = Catch Apache access log - Part1
REM ----------  For daily activate upon 23:30
tamdatew "accnt-1 bat-file issues OK" >>accnt.log
if exist accname.$$ DEL accname.$$>>accnt.log
tamdatnw accname.$$ a
REM Maybe need testing...
"D:\Program Files\Apache Group\Apache\Apache.exe" -w -n
   "Apache" -k stop
if exist access.log del access.log>>accnt.log
ECHO F|XCOPY "D:\Program Files\Apache Group\Apache\logs\ac-
   cess.log" E:\STAT\SITE\access.log /Y /F>>accnt.log
copy /b acc1.ba + accname.$$ + acc2.ba accnty.bat
call accnty.bat
del "D:\Program Files\Apache Group\Apache\logs\access.log" >>ac-
   cnt.log
IF NOT EXIST "D:\Program Files\Apache Group\Apache\logs\ac-
   cess.log" GOTO OkDel
tamdatew =!!= Accnt-1 Current Apache log IS NOT delet-ed!>>ac-
   cnt.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=Accnt1_Flag_is_NOT_Present
goto No
:IssueX
```

```
if exist accessx.log del accessx.log >>accnt.log
copy /b access.log accessx.log >>accnt.log
call accntx.bat
:No
tamwait 10
```

Рис. 18. BAT-файл завершения дневной работы Apache

```
ECHO F|XCOPY access.log E:\STAT\LOGS\A180612.LOG /Y
   /F>>accnt.log
```

Рис. 19. BAT-файл копирования лога дневной работы Apache accnty.bat

```
REM =accntx.bat= Execute Statistics on the ACCESSX.LOG
tamdatew =-= Statistic issued. Begin-of-accntx.bat>>accnt.log
IF NOT EXIST tampst3.flg GOTO NoStat
tampst3.exe /cnf=tampst3
REM /ALLIP
IF ERRORLEVEL 2 GOTO ErrStat
ECHO =Statistics Results are acceptable >>accnt.log
ECHO F|xcopy r51s.htm E:\SITE\ANTIVIR\STAT\r51s.htm /Y /N
   /F>>accnt.log
ECHO F|xcopy r51w.htm E:\SITE\ANTIVIR\STAT\r51w.htm /Y /N
   /F>>accnt.log
ECHO F|xcopy r52t.htm E:\SITE\ANTIVIR\STAT\r52t.htm /Y /N
   /F>>accnt.log
ECHO F|xcopy r53t.htm E:\SITE\ANTIVIR\STAT\r53t.htm /Y /N
   /F>>accnt.log
ECHO F|xcopy r54t.htm E:\SITE\ANTIVIR\STAT\r54t.htm /Y /N
   /F>>accnt.log
ECHO F|xcopy r55t.htm E:\SITE\ANTIVIR\STAT\r55t.htm /Y /N
   /F>>accnt.log
ECHO F|xcopy r56t.htm E:\SITE\ANTIVIR\STAT\r56t.htm /Y /N
   /F>>accnt.log
ECHO F|xcopy r57t.htm E:\SITE\ANTIVIR\STAT\r57t.htm /Y /N
   /F>>accnt.log
DEL accname.$$>>accnt.log
DEL accessx.log >>accnt.log
tamdatew All Statistics are Ok>>accnt.log
GOTO EndStat
```

```
:ErrStat
tamdatew =*= Statistics Results are UNacceptable!>>accnt.log
tamsmtp /GO /TXT=Statistics_are_Unacceptable
GOTO EndStat
:NoStat
tamdatew *** Flag is NOT exist. Statictics are blocked
:EndStat
tamdatew === End-of-accntx.bat >>accnt.log
tamwait 10
```

Рис. 20. BAT-файл подсчёта ежедневной статистики accntx.bat

```
ECHO OFF
REM !accnt2.bat = Catch Apache access log - Part2
REM ----------   For daily activate after 00:00
tamdatew "accnt-2 bat-file issues OK" >>accnt.log
"D:\Program Files\Apache Group\Apache\Apache.exe" -w -n
   "Apache" -k start
tamdatew "Apache Started >>accnt.log
ECHO ------------- >>accnt.log
tamwait 10
```

Рис. 21. BAT-файл начала работы Apache !accnt2.bat

Отметим, что в случае неожиданных ситуаций при подсчёте статистики убирается флаговый файл **tampst3.flg**, вследствие чего в последующие дни до принятия оперативных мер Администратором копирование ежедневных логов исполняется, но ежедневная статистика не подсчитывается. В таких ситуациях посылается E-Mail-извещение Администратору.

В начале очередных суток, исполняется активация Apache с помощью BAT-файла **!accnt2.bat**, показанного на рис. 21.

Таким образом, организуются ежедневные завершение работы web-сайта и его инициация в начале следующих суток.

В целях уменьшения износа HDD, задействована утилита организации виртуального диска сравнительно небольшого объёма[6], внедрённая в ядро Windows'2003 Server с постоянной буквой вир-

[6] ©Qsoft RAMDisk Enterprise, объёмом 32 Мб.

туального логического диска. Первоначально это средство использовалось для ежесекундной записи промежуточных пакетов в составе средств сетевого мониторинга и их отображения на сайте; но впоследствии в эту область оказалось удобным перенести ряд оперативно формируемых в процессе поддержки АВ-средств файлов.

Важной является поддержка присоединённого к серверу UPS с помощью PowerChute [28] [29]. Бесперебойное питание выдерживает 30 минут отключения питания, после чего исполняется программное завершение работы сервера. Восстановление работы исполняется автоматически через 10–30 минут после восстановления питания.

На АВ-сервере специальная область выделена под контент Антивирусного сайта [32]. Эта область основного контента Антивирусного сайта всегда доступна всем классам пользователей. Помимо обслуживания пользователей антивирусных средств, контент сайта имеет и другие задачи.

Корпоративные дистрибутивы и ряд вспомогательных средств размещены в областях Download ограниченного доступа. Средства разграничения доступа спроектированы так, что одни и те же конфигурационные файлы разрешают/запрещают доступ к области Download web-сервера и одновременно к областям обновлений АВ-средств. Доступ 96% пользователей института (как с внешними, так и с внутренними IP-адресами) к этим областям беспаролен.

Таким образом, для определения возможности установки пакета DrWeb достаточно с данного ПК попробовать войти в нужную область Download. При этом применено авторское расширение обычной бинарной альтернативы до «Доступен» – «Доступен по паролю» – «Не доступен» [19].

В целях статистики и контроля работы пользователей, web-сайт АВ-сервера (или просто «АВ-сайт») содержит ряд ежедневно формируемых HTML-таблиц. Так, одна из четырёх сводных таблиц показана на рис. 22. Её содержание не нуждается в комментариях.

Установки и обновления DrWeb для раб.станций

Данная статистика получена утилитой обработки лога программы Apache ***TamPSt3 3.50 * 01.05.2012***.

Утилита выполнена **05.03.13 23:30'03"**.

Всего актуальных пользователей: **169**, в т. числе:

пользователей версии 5.00: **23**,

пользователей версии 6.0SS (x32): **125**,

пользователей версии 6.0SS (x64): **21**,

Предыдущая Следующая		Вчера, 05.03.2013			Март 2013		
		Обновл	Устан	Объем [Kb]	Обнов.	Уст.	Объем [Mb]
Внутренние пользователи ЛВС ЦЭМИ	**Реальные IP**	8	0	48094.89	28	0	163.92
	Виртуал. IP	89	0	458396.33	250	1	1500.89
	Бухгалтерия и кадры	3	0	23189.32	7	0	58.43
Внешние пользователи	**DialUp**	0	0	0.	0	0	0.
	Internet	6	0	36301.9	29	0	163.07
Всего		106	0	565982.44	314	1	1886.3

Рис. 22. Одна из сводных таблиц Статистики АВ-сайта

Помимо сводных таблиц, АВ-сайт содержит ряд таблиц с детальными сведениями о пользователях. Небольшая часть одной из таких таблиц, содержащая обращения пользователей ЛВС ЦЭМИ РАН, показана на рис. 23. В этой таблице показано, на каком ПК с какой ОС какая версия пакета и когда была установлена, когда было последнее обновление. Так, «**513»** означает Microsoft Windows XP SP3; «**y**» соответствует пакету «DrWeb 6.0 SS x86». В реальной HTML-форме содержится полная расшифровка всех обозначений.

Помимо статистических таблиц по обслуживанию пользователей, на АВ-сайте присутствуют также сведения об областях обновления. Примером может служить фрагмент такой таблицы для DrWeb 6.0SSx86 (рис. 24).

Предыдущая Следующая		Антивирусная область					
IP-адрес	П/р, Фам., Комн.	Обновление	Всего	Устан.	Win	О/У	Перс.код
010.000.002.042	11:Козырев /0316	05/03-13=13:41*	0219	14/05-12-	513	y/y	4F8FC487
010.000.002.034	11:Козырев2 /0316	05/09-12=09:58-	0079	23/05-12-	513	y/y	59DB88E0
010.000.002.036	11:КозыревNb /0316	26/02-13=11:36-	0130	23/05-12-	611	z/z	28EE5F8E
010.000.005.054	11:Бекларян /0303	27/02-13=16:08-	0098	18/10-10-	512	w/w	7D5007FE

Рис. 23. Внутренние пользователи АВ-сервера (фрагмент таблицы)

Статистика * Антивирусная область

Область обновления DrWeb для раб.станций 6.0 SS-32bit

Данная таблица получена утилитой оценки результатов исполнения обновления пакета Doctor Web *TamTUpW5 * 5.15, 21.10.2012 (C)A.Терентьев*.

Утилита выполнена **05.03.13 23:35'42"**.

Имя файла	Длина	Дата образования	CRC32	Получен
timestamp	00000010	05.03.13-22:43:30*	085F0715	130305233601*
drwtoday.vdb	00147606	05.03.13-22:42:58*	696BBEAD	130305233601*
drwdaily.vdb	00025854	05.03.13-00:17:04*	52AE80C3	130305233601*
dwrtoday.vdb	00018986	05.03.13-22:42:17*	EEFF86CD	130305233601*
dwntoday.vdb	00045118	05.03.13-22:42:45*	F82DE3A5	130305233601*
vrcpp.dll	02931392	05.03.13-20:51:09*	592C8C7D	130305233601*

Рис. 24. Состояние одной из областей обновления (фрагмент)

Ежедневное состояние всех таблиц доступно на АВ-сайте.

В момент выхода данной работы на АВ-сервере ЦЭМИ РАН действует 2 области обновления для различных АВ-пакетов DrWeb:

– для пакета «DrWeb для p/c 6.0 SS x64» (только для Windows'7);

– для пакета «DrWeb для p/c 6.0 SS x86» (основная область для раб. станций с 32-битными ОС).

Следует отметить, что работа АВ-сайта на АВ-сервере отнюдь не являлась беспроблемной. Неожиданно выяснилось, что наличие внутреннего сетевого интерфейса на область ЛВС с внутренними адресами 10.0.*.*/16 периодически создаёт проблемы, разрывая связь с роутером, при которой сбрасываются таблицы локальных статических маршрутов [33], и сервер становится недоступным для пользователей внутренней ЛВС. Решение этой проблемы было найдено в периодическом пинговании [34] роутера и новой прокладки маршрутов с помощью BAT-файла. Более подробно о конструкции ЛВС и принятых решениях см. в [35] [36] [37] [38].

Другой проблемой явились постоянные атаки [39] на АВ-сервер. К счастью, периметр основной корпортивной сети 193.232.194.*/24 надёжно перекрыт маршрутизатором [39] [40] [41], но бесконечные HTTP-атаки хоть и нерезультативны, но загружают Apache и загромождают его логи.

4.1.1. КОРПОРАТИВНЫЙ ДИСТРИБУТИВ

Корпоративный дистрибутив организован в виде саморазвёртываемого EXE-файла, содержащего в себе все необходимые компоненты для установки пакета DrWeb на ПК пользователя. Корпоративный дистрибутив ориентирован на операционную систему пользователя, поэтому одновременно на АВ-сервере присутствует ряд различных дистрибутивов. Стандартными в течение ряда лет являлись корпоративные дистрибутивы пакетов DrWeb версий 5.0, 6.0SSx86, 6.0SSx64 и 6.0 для файловых Windows-серверов. Каждый из них включал в себя соответствующий стандартный дистрибутив пакета DrWeb и набор вспомогательных файлов, в том числе ключевой файл drweb32.key (заблокированный у вендора), файл настройки DrWeb на АВ-сервер **custom.drl**, файл **drweb32.ini** с начальными установками нужного пакета и ряд других.

В процессе создания корпоративных дистрибутивов использована лицензионная версия программы WinRAR 3.61 с необходимыми наборами вспомогательных текстовых файлов, управляющих созданием нужных дистрибутивов.

Упрощённая схема работы корпоративного дистрибутива была приведена на рис. 2. Во время своей работы корпоративный дистрибутив удаляет остатки старых версий и установок, модифицирует ряд заданий для Планировщика заданий, созданных оригинальным дистрибутивом. Так, например, стандартное задание Планировщика на обновление с повтором каждые 30 минут отменяется и заменяется заданием в папке Автозагрузка, либо (при нескольких пользователях на данном ПК) заменяется на задание с триггером запуска при включении ПК для гарантированного получения обновлений даже при работе пользователей без административных прав. В атрибуты задания на обновление включаются при необходимости логин и пароль к АВ-серверу.

Корпоративный дистрибутив при своей работе на разных этапах неоднократно использует TCP/IP-соединение с АВ-сервером, поэтому перед его вызовом необходимо убедиться в наличии устойчивого соединения с Интернетом и отключить возможные блокирующие соединение или задающие вопросы программы типа ZoneAlarm или файерволов.

Важное свойство корпоративного дистрибутива – возможность быть запущенным на ПК, где помимо основного пользователя с правами администратора системы есть и другие пользователи. В этом случае несколько меняется схема получения обновлений: вместо ярлыка в папке **Автозагрузка** на обновление DrWeb создаётся задание Планировщика заданий на обновление от имени системной учётной записи. Такое задание исполняется в скрытом режиме при входе любого пользователя. Для показа возможных текстовых циркулярных сообщений Антивирусной службы дополнительно создаётся задание на специальный запуск утилиты поддержки корпоративного режима **TamDrW60** у каждого пользователя.

Для запуска корпоративного дистрибутива в многопользовательском режиме достаточно скопировать его во временную папку на ПК и вызвать с параметром «**/M**».

4.2. СПЕЦИФИЧЕСКИЕ ПРОГРАММНЫЕ СРЕДСТВА

Программные средства корпоративной поддержки включают в себя две группы программных компонентов. Одна из них включает ряд программных модулей, блоков и текстов, составляющих в совокупности корпоративный дистрибутив, поставляемый пользователям в виде исполняемого файла. Эти модули рассмотрены в разделе «Корпоративный дистрибутив».

Вторая группа программных средств включает набор утилит, находящихся и исполняемых на АВ-сервере; эти утилиты рассмотрены ниже. Общим для всех утилит является то, что они написаны на мощном развитом алгоритмическом языке PowerBASIC [42] [43] [44] и созданы либо компилятором PoweBASIC for Windows 9.05 (GUI-утилита), либо PowerBASIC Console Compiler 5.05 (утилиты консольного типа).

4.2.1. УТИЛИТА ПОДДЕРЖКИ КОРПОРАТИВНОГО СОПРОВОЖДЕНИЯ TAMDRW60

GUI-программа **tamdrw60.exe** предназначена для сопровождения установки АВ-пакетов «DrWeb 6.0 SS» как для рабочих станций, так и для серверов в составе специально созданных для конкретной организации корпоративных дистрибутивов, используемых в локальной сети эксплуатанта. Задействование программы позволяет выполнить установку и настройку пакета полностью в автоматическом режиме. Программа исполняет более 40 функций, краткое представление о которых можно получить из рис. 25.

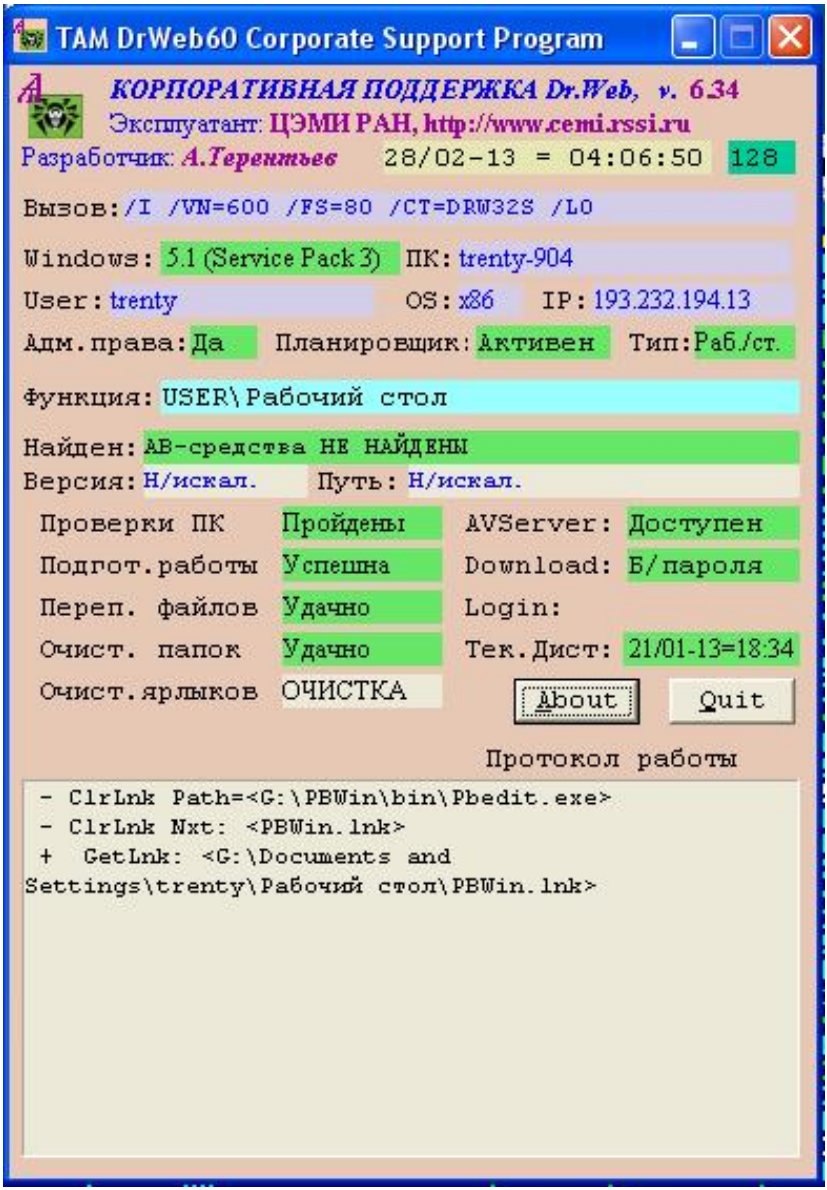


Рис. 25. Экран программы корпоративной поддержки

После установки пакета, программа в скрытом режиме вызывается каждый раз при обновлении АВ-средств пользователя, связываясь с АВ-сервером для передачи ему персонального кода пользователя, а также организует выдачу циркулярных и персональных рассылочных сообщений службы поддержки.

Программа написана на языке PowerBASIC for Windows 9.05, объём исходного текста – 257 КБ (5365 строк). Версия 6.33 утилиты зарегистрирована в ФИПС в 2012 г. Текущая актуальная версия – 6.51.

4.2.2. УТИЛИТА РЕФОРМИРОВАНИЯ ОБЛАСТИ ОБНОВЛЕНИЯ TAMTUPW6

Эта утилита предназначена для реформирования области обновления с созданием статистической HTML-формы для АВ-сайта со сведениями о текущем состоянии нужной области обновления АВ-сервера.

Схематически формирование каждой области обновления приведено на рис. 3. BAT-файл реорганизации области обновления сначала запускает процедуру обновления соответствующей TMP-области, а затем, в зависимости от успеха работы утилиты обновления DrWeb (Апдейтера), запускает и реформирование области WINDOWS.

Предусмотрена возможность многократного запуска Апдейтера перед реформированием области (например, для случаев, когда по тем или иным причинам распределение до области WINDOWS скачанных в область TMP файлов не выполнено).

В случае нарушения структуры базы данных области обновления или иных критических ситуаций предусмотрен флаговый файл для блокирования последующего запуска обновления и автоматического создания E-Mail-сообщения о крахе обновления.

```
@ECHO OFF
ECHO ------------------------->>!xcopy.rc
tamdatew Start DrWeb32 0-bat >>!xcopy.rc
IF EXIST etap1ok.flg DEL etap1ok.flg
:NoDel
IF EXIST etap1.flg GOTO Go
ECHO *** Flag ETAP1.FLG is NOT setting! >>!xcopy.rc
```

```
GOTO Ok
:Go
E:\SITE\ANTIVIR\DRWEB32\UPW\drwebupw.exe /GO /QU
   /DIR:E:\SITE\ANTIVIR\DRWEB32\TMP /RP+E:\SITE\ANTI-
   VIR\DRWEB32\!SYS\drwebupw.log /UA /URM:disable
IF ERRORLEVEL 255 GOTO Ex255
IF ERRORLEVEL 128 GOTO Ex128
IF ERRORLEVEL 64 GOTO Ex64
IF ERRORLEVEL 32 GOTO Ex32
IF ERRORLEVEL 16 GOTO Ex16
IF ERRORLEVEL  8 GOTO Ex8
IF ERRORLEVEL  4 GOTO Ex4
IF ERRORLEVEL  2 GOTO Ex2
IF ERRORLEVEL  1 GOTO Ex1
tamdatew DrWeb32UpW Result Code is 0 >>!xcopy.rc
CALL !3.bat
CALL !9-upw32.bat
GOTO Ok
:Ex1
tamdatew DrWeb32UpW Result Code is 1 >>!xcopy.rc
GOTO ExU
:Ex2
tamdatew DrWeb32UpW Result Code is 2-3 >>!xcopy.rc
GOTO ExU
:Ex4
tamdatew DrWeb32UpW Result Code is 4-7 >>!xcopy.rc
GOTO ExU
:Ex8
tamdatew DrWeb32UpW Result Code is 8-15 >>!xcopy.rc
GOTO ExU
……
:Ex255
tamdatew DrWeb32UpW Result Code is 255 >>!xcopy.rc
GOTO ExU
:ExU
tamsmtp /GO /TXT=UpW32_Errors
:Ok
tamdatew End DrWeb32 0-bat >>!xcopy.rc
tamwait 10
```

Рис. 26. Текст BAT-файла !0-upw32.bat обновления области x86

В случае успешного обновления области, создаётся HTML-форма содержания области (видна на рис. 9) и маркерный файл со временем обновления для отражения в левой части Антивирусного сайта в блоке «Последние обновления».

```
@ECHO OFF
REM 2nd Etap of DrW32 Correction = !9-upw32.bat
tamdatew Start DrWeb32 9-bat >>!xcopy.rc
tamtupw6.exe /CNF=tamtupw6.cnf /1251
IF ERRORLEVEL 255 GOTO Cod255
IF ERRORLEVEL 128 GOTO Cod128
IF ERRORLEVEL 64 GOTO Cod64
IF ERRORLEVEL 32 GOTO Cod32
IF ERRORLEVEL 16 GOTO Cod16
IF ERRORLEVEL 8 GOTO Cod8
IF ERRORLEVEL 4 GOTO Cod4
IF ERRORLEVEL 2 GOTO UpW
IF ERRORLEVEL 1 GOTO Main
tamdatew --- The Result TamTUpW5 Code is 0. No needed.
   >>!xcopy.rc
GOTO Endbat
:UpW
tamdatew !NO Updating DrWebUpW-utility >>!xcopy.rc
rem xcopy E:\SITE\ANTIVIR\DRWEB32\TMP\drwebupw.exe
   E:\SITE\ANTIVIR\DRWEB32\UPW /F /Y /N >>!xcopy.rc
:Main
tamdatew =Getting DrWeb32-area: Ok >>!xcopy.rc
tamdatew =Updating LST in DrWeb32-area: Ok>>!xcopy.rc
DEL drwebupw.log>>!xcopy.rc
tamdatew =DrWebUpW.log(s) deleted>>!xcopy.rc
DEL etap1ok.flg>>!xcopy.rc
tamdatew =Flag Etap1Ok.flg deleted>>!xcopy.rc
goto Endbat
:Cod255
tamdatew XXX Getting Process Aborted by TAMtUpw6 - Ret=255
   >>!xcopy.rc
goto Endbat
:Cod128
tamdatew XXX Getting Process Aborted by TAMtUpw6 - Ret=128
   >>!xcopy.rc
```

```
goto Endbat
:Cod64
tamdatew XXX Getting Process Aborted by TAMtUpw6 - Ret=64
   >>!xcopy.rc
goto Endbat
:Cod32
tamdatew XXX Getting Process Aborted by TAMtUpw6 - Ret=32
   >>!xcopy.rc
goto Endbat
:Cod16
tamdatew XXX Getting Process Aborted by TAMtUpw6 - Ret=16
   >>!xcopy.rc
goto Endbat
:Cod8
tamdatew XXX Getting Process Aborted by TAMtUpw6 - Ret=8
   >>!xcopy.rc
goto Endbat
:Cod4
tamdatew XXX Getting Process Aborted by TAMtUpw6 - Ret=4
   >>!xcopy.rc
goto Endbat
:Nobat
tamdatew XXX Process Aborted by me>>!xcopy.rc
tamsmtp /GO /TXT=UpW32_Aborted
:EndBat
tamdatew -------!9-upw32.bat------>>!xcopy.rc
```

Рис. 27. Текст BAT-файла !9-upw32.bat обновления области x86

```
@ECHO OFF
REM 1st Etap of Drw32 Addition: Store current log to Logs
IF NOT EXIST E:\SITE\ANTIVIR\DRWEB32\LOG\drwebupw.lgs
   tamdatew --- New Logs DrWeb32 --- >E:\SITE\ANTI-
   VIR\DRWEB32\LOG\drwebupw.lgs
copy E:\SITE\ANTIVIR\DRWEB32\LOG\drwebupw.lgs /a +
   E:\SITE\ANTIVIR\DRWEB32\!SYS\drwebupw.log /a
   E:\SITE\ANTIVIR\DRWEB32\LOG\drwebupw.lgs /a >>!xcopy.rc
```

Рис. 28. Текст BAT-файла !3.bat обновления области x86

Основные BAT-файлы формирования области обновления DrWeb32 показаны выше на рисунках 26, 27 и 28. Следует обратить

внимание на то, что помимо сообщений Администратору сайта через E-Mail в случае критических ситуаций, все действия фиксируются в файле **!xcopy.rc**, так что впоследствии можно проследить все этапы формирования области.

Эта консольная утилита исполняется во всех BAT-файлах, запускаемых для формирования нужных областей обновления по расписанию. Во время работы всех этих BAT-файлов раздающий процесс Apache отключен, хотя утилиту можно запускать и при работающем Apache.

Версия 5.15 утилиты зарегистрирована в ФИПС в 2012 г. Текущая версия утилиты – 6.06.

4.2.3. УТИЛИТА СТАТИСТИЧЕСКОГО УЧЁТА ОБНОВЛЕНИЙ ЗА ДЕНЬ TAMPST3

Эта утилита обсчитывает все обращения пользователей за антивирусными обновлениями за сутки. Утилита ведёт внутреннюю базу пользователей с учётом их обращений за текущий день и получения 7 отчётных HTML-форм по итогам рабочего дня.

Статистические формы по областям обновления (отдельно для каждой из поддерживаемых версий DrWeb), как показано на рис. 24, содержат учётную информацию о каждом рассылаемом модуле из области обновления (имя, момент образования, длина, контрольная сумма CRC32, признаки). Эта информация редко используется в практике, главным образом для проверки работы сервера.

Статистические формы по итогам рабочего дня включают:

– «Установки и обновления DrWeb для файловых Windows-серверов»;

– «Установки и обновления DrWeb для рабочих станций» (рис. 22);

– «Статистика обращений к антивирусному сайту»;

– «Сводка обращений за прошлый месяц»;

– «Обращения из Административно-финансового сегмента сети»;

– «Обращения пользователей ЛВС ЦЭМИ РАН» (рис. 23);

– «Обращения DialUp- и внешних пользователей»;

– «Отказы в обращениях пользователей».

Программа ведения статистики использует самостоятельно накапливаемые базы данных в текстовом формате и протоколы работы других программ –соответственно, протокол работы утилиты обновления DrwebUpw.exe пакета DrWeb и протокол Apache, сформированный в специальном пользовательском формате:

LogFormat «%a %h %u %t \"%r\" %s %B» trentylog

Формат форм определяется шаблонами, для генерации форм используется свыше 50 определяемых и реализованных утилитой макровызовов.

Программа TAMPSt3 сформирована с помощью компилятора «PowerBASIC Console Compiler 5.05», занимая объём 97 Кбайт (2170 строк). Утилита версии 3.50 зарегистрирована в ФИПС в 2012 г. Текущая версия утилиты – 3.70.

4.2.4. УТИЛИТА ПОСЫЛКИ E-MAIL TAMSMTP

Данная утилита исполняет посылку от имени фиктивного E-Mail-адреса на предопределённый E-Mail-адрес предопределённого текста сообщения с предопределённым заголовком. Предопределения находятся в конфигурационном файле, расположенным в каталоге размещения утилиты. Большинство предопределений могут быть изменены параметрами обращения.

Конфигуратор сохраняет также адрес E-Mail-сервера.

Фиктивный E-Mail-адрес должен быть известен для Mail Transport Agent E-Mail-сервера, к которому исполняется обращение.

В случаях AB-сервера password не применяется, разрешение на SMTP-операцию прописано в списке IP E-Mail-сервера института.

4.2.5. УТИЛИТА ФОРМИРОВАНИЯ ИМЕНИ ФАЙЛА TAMDATNW

Эта утилита предназначена для формирования в указанном файле имени некоторого файла из первой буквы и текущей даты. Так, например, обращение «**tamdatnw.exe accname.$$$ A**» сформирует в новом файле с именем **accname.$$$** текстовую строку длиной ровно 7 символов «**A**yymmdd», где yy, mm и dd – соответственно, по две цифры года, месяца и дня, а первый символ определён вторым параметром вызова программы.

Утилита применяется в BAT-файле **accnty.bat**, который сам формируется в процессе работы BAT-файла «**!accnt-1.bat**», для

формирования имени файла, с которым будет скопирован ежедневный лог в архивную папку.

4.2.6. УТИЛИТА ОТОБРАЖЕНИЯ ТЕКСТА TAMDATEW

Эта утилита предназначена для отображения на экране и занесения в файл текстового параметра, дополненного текущей датой и временем. Так, например, вызов «TAMDATEW.EXE Text>>stdo.txt», выполненный, к примеру, 13.06.2018 в 18:23, вызовет помещение в конец файла stdo.txt строки:

! 2018.06.13(3) 18:23'42" Text

а также на экран консольного вывода строки:

! 2018.06.13(3) 18:23'42" Text Ret=3

где код завершения утилиты показан в виде «**Ret=3»** (3й день недели, среда).

Во всех случаях исполняемые утилиты реформирования области обновления (рис. 4), обновления статистики и др. создают консоль вывода на экран аналогично Коммандеру CMD. Указанная утилита выводит текст в этот консольный вывод через STDOUT в разной цветовой гамме, что значительно облегчает оперативный просмотр исполнения процессов.

Одновременно данная утилита позволяет организовывать BAT-файлы с выделением процессов согласно нужным дням недели.

4.2.7. УТИЛИТА ЗАДЕРЖКИ ОТОБРАЖЕНИЯ ВЫВОДА TAMWAIT

Данная утилита создаёт ежесекундно пополняющуюся строку на экране в течение нескольких секунд, число которых задаётся параметром утилиты. Это помогает задержать на экране отображение в консоли вывода в течение нужного времени для спокойного просмотра полного изображения.

Иллюстрацией применения этой утилиты служит рис. 4, где последняя строка поэтапно сформирована описываемой утилитой.

ГЛАВА 5. ДОСТИГНУТЫЕ РЕЗУЛЬТАТЫ

Взаимосвязь с пользователями ЦЭМИ РАН ведётся с учётом существующей структуры пользователей. Локальная сеть ЦЭМИ РАН включает ряд абонентов с прямыми международными адресами в нескольких сетях класса С, ряд сегментов одной из этих сетей за собственными серверами-роутерами подразделений института, а также обширный сегмент сети, включающий 95% всех пользователей с внутренними адресами (т.н. «внутренние пользователи»). Один из фрагментов сети (административно-финансовый) исторически выделен самостоятельной строкой в сводных таблицах статистики.

АВ-сервер имеет два сетевых интерфейса: на внешний и внутренний сегменты сети. Все пользователи этих сегментов имеют прямой беспарольный доступ к АВ-серверу. Незначительное количество пользователей, находящихся за собственными серверами (в том числе административно-финансовый сегмент) или в других сетях, имеют парольный доступ.

Регулярная раздача обновлений по антивирусным пакетам DrWeb началась с сентября 2003 г. и первоначально включала только область обновления для рабочих станций. Впоследствии к ней была добавлена область обновления для серверов. За всё время существования АВ-сервера последовательно сменились несколько эксплуатируемых версий пакетов DrWeb. В настоящее время закончен переход с версии 6.0 на 6.0 Security Space, начатый несколько лет назад.

Сводные данные о числе выполненных запросов пользователей за обращениями к антивирусным областям за всё время существования АВ-сервера представлены в таблице 1.

Таблица 1

Статистика удовлетворения запросов пользователей

Год	Обновлений		Обращений к сайту	
	Число раз	Мб	Число раз	Мб
2004	***21876***	***2099,86***	***1196***	***73,48***
2005	***25755***	***1970,82***	***1808***	***158,69***
2006	***31940***	***3984,74***	***1295***	***209,63***
2007	***30984***	***2397,98***	***1399***	***340,12***
2008	***33207***	***9384,13***	***3195***	***773,16***
2009	***24280***	***10180,87***	***1944***	***899,28***
2010	***23844***	***16106,61***	***14509***	***642,07***
2011	***22199***	***15877,56***	***37953***	***831,29***
2012	***22629***	***54724,17***	***43324***	***902,75***
2013	***23234***	***131258,68***	***50143***	***3106,50***
2014	***17047***	***137294,97***	***53386***	***4085,81***
2015	***27159***	***150829,37***	***51567***	***4628,63***
2016	***23436***	***194795,11***	***43173***	***6293,93***
2017	***15571***	***166040,32***	***31715***	***6851,49***

Примечания. Начиная с июля 2007г, в объём выполненных обращений включены также объёмы скачанных дистрибутивов с Антивирусного сайта.

С 2010 г. хакерские http-атаки [39] включены в число и объёмы обращений к сайту.

С 2013 г. на сайте появился полный список Литературы автора с 1998 г.

Итого, за 14 полных лет обслужен **343161** запрос пользователей на обновления DrWeb, по которым пользователям предоставлено **875,92** ГБайт информации. Принимая, что количество пользователей АВ-сервера в эти годы было в пределах 130–190, экономия Интернет-трафика по обращениям к АВ-средствам практически совпадает с объёмами, скачанными пользователями с АВ-сервера, т.е. более **875** Гб.

В приведённую выше статистику до сентября 2010 г не включены необслуженные (отказанные) запросы, а также многочисленные попытки хакерских обращений к АВ-серверу. Разумеется, при-

ведённая статистика не отражает также прочих функций АВ-сервера, например, поддержку сетевого мониторинга в реальном режиме времени, и ряд других.

Основная часть контента Антивирусного сервера ЦЭМИ РАН доступна с 2013 г для поисковых роботов; во всех поисковых системах по запросу «антивирусный сайт» ссылка на него выдаётся в числе первых.

Рассмотрим подробнее выгоды от внедрения описанной системы.

5.1. ВЫГОДЫ ПОЛЬЗОВАТЕЛЕЙ АВ-СЕРВЕРА ЦЭМИ РАН

Установка и настройка корпоративных средств может исполняться самостоятельно. Созданные корпоративные дистрибутивы осуществляют полное концептуальное окружение пользователя, выдавая ему в случае неуспеха необходимую диагностическую информацию на русском языке.

В процессе работы, циркулярные сообщения Антивирусной службы ЦЭМИ РАН, а также новые ключевые файлы доставляются пользователю на рабочее место автоматически.

Наличие АВ-сайта увеличивает степень информированности пользователей о текущем состоянии АВ-средств, их возможностях и возникших проблемах.

При сбоях и отказах Интернета АВ-сервер остаётся доступен, и пользователи не испытывают неудобств в получении обновлений. В случаях некорректности конкретных сеансов обновлений с серверов вендора, пользователи этого не замечают и не испытывают неудобств.

Скорость обновления с внутреннего сервера намного превышает скорость обновления через Интернет.

5.2. ВЫГОДЫ АВ-СЛУЖБЫ И СИСТЕМНЫХ АДМИНИСТРАТОРОВ ЦЭМИ РАН

Установка и настройка корпоративных средств исполняется полностью автоматически за 5–10 минут, в то время как индивидуальная настройка отнимала значительно больше времени (в некоторых версиях DrWeb более 40 минут). Наличие информационно-статистических сводок позволяет точно знать задействованное

число лицензий и отслеживать персональные ситуации, в том числе переход пользователей с одной версии DrWeb на другую.

Наличие АВ-сайта позволяет мгновенно установить IP-адрес пользователя и тип доступа к АВ-средствам. Присутствие шестнадцатеричного идентификационного кода позволяет осуществить однозначную идентификацию перенесённого на другое рабочее место ПК, что в условиях независимой работы научных подразделений института иногда бывает незаменимым. Этот же код позволяет установить факт несанкционированного выноса ноутбуков за пределы института.

5.3. ВЫГОДЫ АДМИНИСТРАЦИИ ЦЭМИ РАН

Внедрённая система позволяет легко (в течение часа) подключать новых пользователей, оперативно реагируя на изменение состава пользовательских ПК.

Предложенное техническое решение минимально по ресурсным требованиям и некритично в обслуживании.

Свободный доступ к таблицам статистики позволяет легко установить действующее число лицензий, а также распределённость установленных АВ-средств по Отделениям института. Поскольку получение корпоративных АВ-средств связано с включением ПК, легко установить последнее включение ПК того или иного пользователя на рабочем месте.

За счёт централизованного получения обновлений достигнута значительная экономия Интернет-трафика.

5.4. ВЫГОДЫ ВЕНДОРА ООО «ДОКТОР ВЕБ»

Реально используемое число лицензий можно в любой момент проконтролировать по статистическим таблицам АВ-сайта.

Использование в корпоративном варианте пользователями заблокированных у вендора ключей блокирует возможность выноса ключевого файла за пределы эксплуатанта и использование его на сторонних ПК.

За время эксплуатации корпоративного варианта DrWeb выявлен ряд ошибок в официальной документации DrWeb и практической работе (рис. 29), найдено несколько новых вирусов (рис. 30), обнаружены ложные срабатывания компонентов DrWeb на некоторых фай-

лах [45] [46] (рис. 31). Исследованы возможности подключения сторонних операционных систем для лечения особо опасных вирусов [47] [48]. Активное участие Антивирусной службы в развитии DrWeb помогает улучшению потребительских характеристик продукта.

Досадными случаями являются выявление фатальных ошибок на двух ПК, эксплуатировавшихся без DrWeb или с его неполным функционалом (отсутствием проверки входящей почты). В обоих случаях пришлось переставлять операционную систему из-за шифрации файлов трояном.

Все сказанное свидетельствует о слаженной работе Службы технической поддержки DrWeb и Антивирусной службы ЦЭМИ РАН.

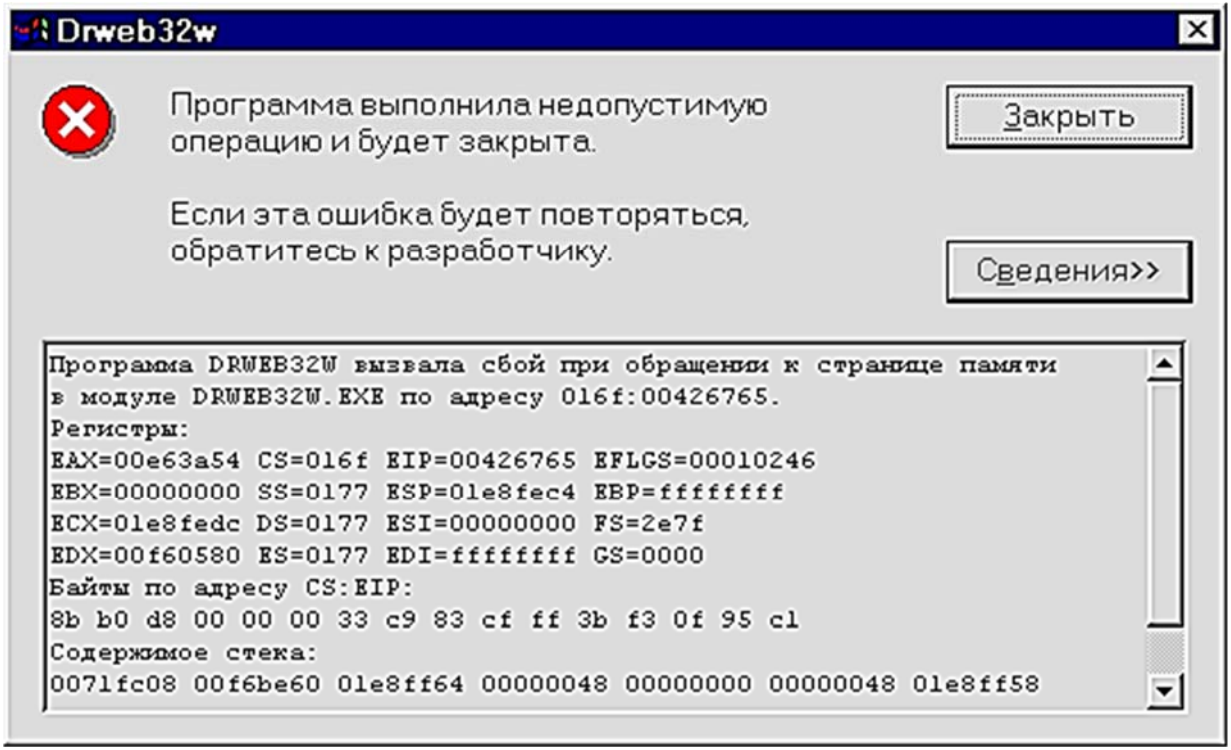


Рис. 29. Скриншот ошибки компонента DrWeb (2006 г.)

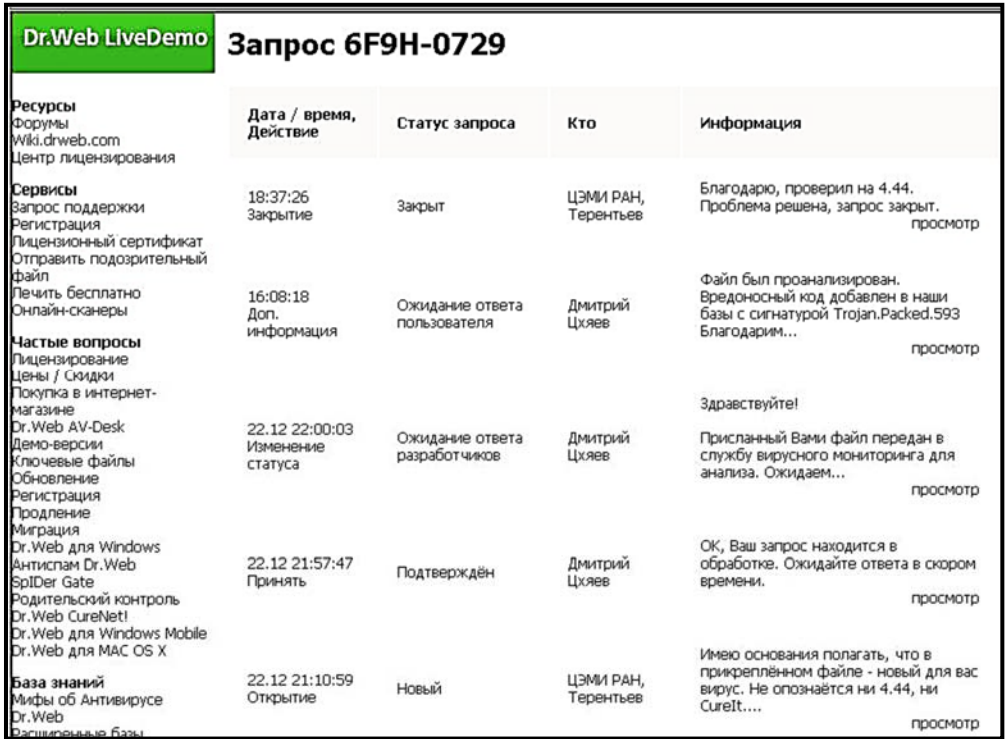


Рис. 30. Скриншот подтверждения нового вируса (2009 г.)

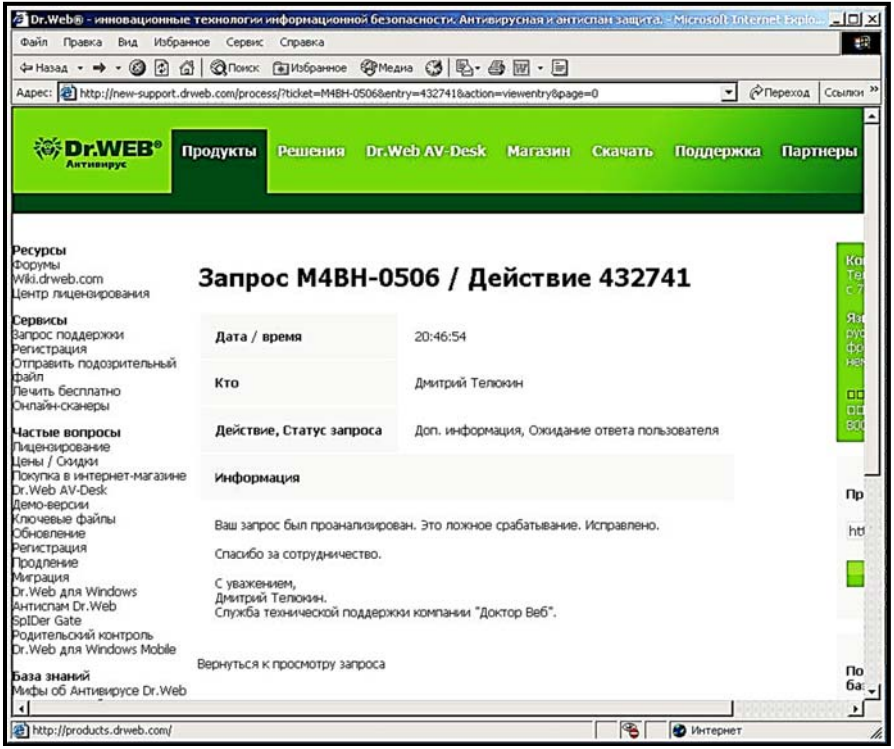


Рис. 31. Скриншот подтверждения ложного срабатывания (2008 г.)

5.5. ВИДИМЫЕ НЕДОСТАТКИ КОРПОРАТИВНОГО ВАРИАНТА

Доступ к обновлениям АВ-средств невозможен в течение 35 минут в день с 23:30 до 00:05 MSK. Однократное ежедневное обновление АВ-средств на АВ-сервере фактически заставляет пользователей эксплуатировать АВ-средства с антивирусными базами, отстающими от поставляемых вендором (обновления от серверов вендора меняются каждый час) на сутки.

5.6. СТЕПЕНЬ НОВИЗНЫ ОПИСАННОГО РЕШЕНИЯ И ЕГО ТИРАЖИРУЕМОСТЬ

Автору к моменту публикации данной работы неизвестны аналоги описанных программно-технических средств корпоративной поддержки установки и сопровождения антивирусных пакетов DrWeb, помимо формата «Enterprise Suite», оговорённого при анализе проблемы.

Представленные средства сравнительно легко могут быть тиражированы для использования в других организациях. Необходимые технические средства для этого гораздо меньшие, чем требующиеся при установке разработанных вендором корпоративных средств на основе фирменного пакета разработчика DrWeb «Enterprise Suite».

При тиражировании отнюдь не является обязательным полное воспроизведение всех функциональных особенностей корпоративной поддержки. Минимальными требованиями являются наличие областей раздачи обновлений через Apache на файловом Windows-сервере и использование утилит автора поддержки этих областей. Весь web-интерфейс не является обязательным и может быть произвольным: формат статистических таблиц во многом определяется эксплуатантом.

Все созданные автором утилиты спроектированы с поддержкой выделенных текстовых конфигурационных файлов, что позволяет их быстро перенастраивать на нужные объекты информационного пространства сервера. Все утилиты являются консольными 32-битными приложениями.

За время эксплуатации описанных средств проведено 2 попытки внедрения в различных организациях: Институте народнохозяйственного прогнозирования (ИНПРАН) РАН и в киноконцерне «Мосфильм». Обе попытки показали быстроту и успешность тестового внедрения. К сожалению, обе организации отказались от промышленной эксплуатации после переговоров о финансировании проектов.

Автор благодарит службу технической поддержки ООО «Доктор Веб» за давние плодотворные консультации и многолетнее терпение, без которых автору реализовать описанную разработку было бы попросту невозможно.

ЗАКЛЮЧЕНИЕ

Успешное внедрение предложенной технологии решает задачу защиты корпоративного пользователя современными антивирусными средствами [49]. Долголетнее активное развитие и использование разработанных средств показывает актуальность выполняемой работы. Использование приёмов системного программирования [50] [51] [52] [53] обеспечивало универсальность разработанных средств применительно к операционным системам.

ПЕРЕЧЕНЬ РИСУНКОВ

ПЕРЕЧЕНЬ ССЫЛОЧНЫХ ДОКУМЕНТОВ

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

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

3. Паркер Т. TCP/IP. Освой самостоятельно. – М.: Бином, 1997. – 448 с.

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

5. Сайт ООО «Doctor Web» [Электронный ресурс]. – Режим доступа: https://www.drweb.ru

6. Терентьев А.М. Противовирусная защита ПК в Windows 95/98/NT / Препринт #WP/99/078. – М.: ЦЭМИ РАН, 1999. – 82 с. (Рус.). – ISBN 5-8211-0070-4

7. Терентьев А.М. Антивирусная защита ПК в Windows 95/98/NT: Методическое пособие по антивирусному комплекту ЗАО «ДиалогНаука». – М.: Перспектива, 1999. – 101 с.: ил. – ISBN 5-86225-488-0

8. Терентьев А.М. Антивирусная защита ПК в Windows 95/98/NT: Методическое пособие по антивирусному комплекту ЗАО «ДиалогНаука». – 2-е изд. – М.: Перспектива, 2000. – 104 с.: ил. – ISBN 5-86225-490-0

9. 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.

10. Терентьев А.М. Информационная безопасность рабочих станций в ЦЭМИ РАН // Отчёт о научно-исследовательской работе «Компьютерные, информационно-телекоммуникационные технологии и инструментальные средства для создания среды коллективного распределённого моделирования сценариев социально-экономического и информационного развития Российской Федерации (заключительный)». – М.: ЦЭМИ РАН, 2012. – №ГР 01.2.00 9 51390, Инв. № ЦИТИС 02201350131.

11. Ляпичева Н.Г. Коррекция ошибок HTTP-соединения в локальной сети ЦЭМИ РАН / Н.Г. Ляпичева, А.А. Акиншин, А.М. Терентьев, П.В. Григорьев // Развитие технологий и инструментальных средств информационной безопасности. Вып. 2: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – С. 49–58. – ISBN 978-5-8211-0615-5

12. Айлебрехт Л. Apache web-сервер. – Мн.: Новое знание, 2002. – 592 с.: ил. – ISBN 985-6516-85-4 (рус.).

13. Антивирусный сайт ЦЭМИ РАН. Новости от 05.05.2007 [Электронный ресурс]. – Режим доступа: http://av.cemi.rssi.ru?1,45

14. 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. Вып. 1: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2004. – С. 47–59. – ISBN 5-8211-0317-7

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

16. 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. Вып. 1: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2004. – С. 75–87. – ISBN 5-8211-0317-7

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

18. Терентьев А.М. Параметрическое управление контентом фреймового сайта / А.М. Терентьев, А.С. Львова // Развитие технологий и инструментальных средств информационной безопасности. Вып. 1: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2010. – С. 62–67. – ISBN 978-5-8211-0543-1

19. Терентьев А.М. Адаптация антивирусного сайта к актуальным пользователям антивирусных средств / А.М. Терентьев, О.Г. Горбанева, А.С. Львова // Развитие и использование средств сетевого мониторинга и аудита. Вып. 2: Сб. статей / Под ред. М.Д. Ильменского. – М.: ЦЭМИ РАН, 2005. – С. 40–53. – ISBN 5-8211-0365-7

20. Пэтчетт К. CGI/Perl: создание программ для Web / К. Пэтчетт, М. Райт; пер. с англ. – К.: Издательская группа BHV, 2000. – 624 с. – ISBN 966-552-010-5

21. Кристиансен Т. Perl: библиотека программиста / Т. Кристиансен, Н. Торкингтон. – СПб.: Питер, 2000. – 736 с.: ил. – ISBN 5-80486-0094-X

22. Терентьев А.М. Методы аудита локальных сетей в MS-DOS / А.М. Терентьев, А.Е. Винокуров // Сборник трудов ЦЭМИ РАН «Вопросы информационной безопасности узла Интернет в научных организациях». – М.: ЦЭМИ РАН, 2001. – С. 60–63. – ISSN 5-8211-0134-4

23. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Системная служба // XXVII Международная научная конференция «Стратегии устойчивого развития мировой науки». Т. 1. – М.: Евразийское научное объединение, 2017. – № 5 (27). – С. 41–46. – ISSN 2411-1899

24. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Управление системной службой // XXVIII Международная научная конференция «Интеграция науки в современном мире». Т. 1. – М.: Евразийское научное объединение, 2017. – №6 (28). – С. 28–33. – ISSN 2411-1899

25. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Результаты. // XXIX Международная научная конференция «Теоретические и практические вопросы современной науки». Т. 1. – М.: Евразийское научное объединение, 2017. – №7 (29). – С. 27–31. – ISSN 2411-1899

26. Терентьев А.М. Технология представления результатов сетевого мониторинга в Интернете. Дополнительные сведения // XXX Международная научная конференция «Научные аспекты современных исследований». Т. 1. – М.: Евразийское научное объединение, 2017. – №8 (30). – С. 37–41. – ISSN 2411-1899

27. Терентьев А.М. Адекватное отображение на технологическом www-сервере событий реального времени / А.М. Терентьев, А.С. Львова // Развитие и использование средств сетевого мониторинга и аудита. Вып. 3: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2006. – С. 50–59. – ISBN 5-8211-0409-2 (978-5-8211-0409-0)

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

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

30. Терентьев А.М. Интерактивная проверка антивирусных средств // Развитие технологий и инструментальных средств информационной безопасности. Вып. 1: Сб. статей / Под ред. А.М. Терентьева. – М., ЦЭМИ РАН, 2010. – С. 56–61. – ISBN 978-5-8211-0543-1

31. Терентьев А.М. Средства интерактивного обучения на Антивирусном сайте ЦЭМИ РАН // Развитие технологий и инструментальных средств информационной безопасности. Вып. 2: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – С. 59–63. – ISBN 978-5-8211-0615-5

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

33. Ляпичева Н.Г. Коррекция ошибок HTTP-соединения в локальной сети ЦЭМИ РАН / Н.Г. Ляпичева, А.А. Акиншин, А.М. Терентьев, П.В. Григорьев // Развитие технологий и инструментальных средств информационной безопасности. Вып. 2: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – С. 49–58. – ISBN 978-5-8211-0615-5

34. Терентьев А.М. Поддержание доступности HTTP-соединения с помощью периодического пингования // XXIV Международная научная конференция «Современные концепции научных исследований». Т. 1. – М.: Евразийское научное объединение, 2017. – №2 (24). – С. 37–39. – ISSN 2411-1899

35. 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, А.М. Терентьев // Развитие и использование средств сетевого мониторинга и аудита. Вып. 1: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2004. – С. 88–101. – ISBN 5-8211-0317-7

36. Терентьев А.М. Корпоративный вариант реализации антивирусных пакетов Doctor Web в научных учреждениях: предпосылки // Национальные интересы: приоритеты и безопасность. – М.: Издательский дом «Финансы и кредит», 2013. – №17 (206). – С. 41–48. – ISSN 2073-2872

37. Терентьев А.М. Корпоративный вариант реализации антивирусных пакетов Doctor Web в научных учреждениях: реализация // Национальные интересы: приоритеты и безопасность. – М.: Издательский дом «Финансы и кредит», 2013. – №19 (208). – С. 40–45. – ISSN 2073-2872

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

39. Терентьев А.М. HTTP-атаки на web-сервер // XXVI Международная научная конференция «Актуальные вопросы развития науки в мире». Т. 1. – М.: Евразийское научное объединение, 2017. – №4 (26). – С. 58–62. – ISSN 2411-1899

40. Кочетова Н.А. Опыт использования сетевого экрана ASA5510 в качестве граничного маршрутизатора корпоративной сети / Н.А. Кочетова, Н.Г. Ляпичева // Развитие технологий и инструментальных средств информационной безопасности. Вып. 2: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – С. 22–33. – ISBN 978-5-8211-0615-5

41. Ляпичева Н.Г. Обнаружение сетевых атак на граничном маршрутизаторе // Развитие технологий и инструментальных средств информационной безопасности. Вып. 2: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – С. 34–48. – ISBN 978-5-8211-0615-5

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

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

44. PowerBASIC [Электронный ресурс]. – Режим доступа: https://www.powerbasic.com

45. Терентьев А.М. О ложных срабатываниях антивирусных пакетов «Doctor Web» // Развитие технологий и инструментальных средств информационной безопасности. Вып. 2: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – С. 64–73. – ISBN 978-5-8211-0615-5

46. Терентьев А.М. Ложные срабатывания антивирусных средств // Национальные интересы: приоритеты и безопасность. – М.: Издательский дом «Финансы и кредит», 2013. – №4 (193). – С. 41–46. – ISSN 2073-2872

47. Терентьев А.М. Антивирусное обеззараживание персональных компьютеров с помощью подключения сторонних операционных систем // Национальные интересы: приоритеты и безопасность. – М.: Издательский дом «Финансы и кредит», 2012. – №37 (178). – С. 45–51. – ISSN 2073-2872

48. Терентьев А.М. Лечение компьютерных вирусов на ПК с помощью подключения внешних операционных систем / А.М. Терентьев, П.В. Григорьев // Развитие технологий и инструментальных средств информационной безопасности. Вып. 2: Сб. статей / Под ред. А.М. Терентьева. – М.: ЦЭМИ РАН, 2012. – С. 6-21. – ISBN 978-5-8211-0615-5

49. Терентьев А.М. Выбор адекватных средств информационной защиты персонального компьютера в России // Национальные интересы: приоритеты и безопасность. – М.: Издательский дом «Финансы и кредит», 2012. – №33 (174). – С. 37–42. – ISSN 2073-2872

50. Граппа П. Windows XP. Трюки – СПб.: Питер, 2005. – 394 с.: ил. – ISBN 5-94723-925-6

51. Харт-Дэвис Г. Microsoft Windows XP Professional. Полное руководство / Пер. с англ. – М.: СП ЭКОМ, 2004. – 816 с.: ил. – ISBN 5-9570-0013-2

52. Хейвуд Д. Внутренний мир Microsoft TCP/IP / Пер. с англ.; Дрю Хейвуд. – К.: ДиаСофт, 2000. – 496 с.

53. Microsoft TCP/IP. Учебный курс / Пер. с англ. – 2-е изд., испр. – М.: Издательско-торг. дом «Русская редакция», 1999. – 344 с. – ISBN 5-7502-0112-0

Для заметок

Для заметок

Для заметок

Научное издание

Терентьев Александр Макарович

КОРПОРАТИВНЫЙ ВАРИАНТ ТЕХНОЛОГИИ ИСПОЛЬЗОВАНИЯ АНТИВИРУСНЫХ ПАКЕТОВ DRWEB В НАУЧНЫХ УЧРЕЖДЕНИЯХ

Авторская монография
Чебоксары, 2018 г.

Редактор *А.М. Терентьев*
Компьютерная верстка и правка *С.Ю. Семенова*
Дизайн обложки *Н.В. Фирсова*

Подписано в печать 20.07.2018 г.
Дата выхода издания в свет 30.07.2018 г.
Формат 60×84/16. Бумага офсетная. Печать офсетная.
Гарнитура Times. Усл. печ. л. 5,8125. Заказ 1409. 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