УДК 004.492

КОРПОРАТИВНЫЙ ВАРИАНТ РЕАЛИЗАЦИИ АНТИВИРУСНЫХ ПАКЕТОВ DOCTOR WEB В НАУЧНЫХ УЧРЕЖДЕНИЯХ: ПРЕДПОСЫЛКИ

А. М. ТЕРЕНТЬЕВ,
кандидат технических наук,
ведущий научный сотрудник
E-mail: tam@cemi. rssi. ru
Центральный экономико-математический институт РАН

В статье освещены вопросы корпоративного использования популярных отечественных антивирусных пакетов «Доктор Веб». Исследованы процессы установки, настройки и эксплуатации упомянутых средств. Показана неэффективность пакетов, рассчитанных на единичного пользователя, в корпоративных условиях. Определены недостатки стандартного корпоративного средства Doctor Web Enterprise Suite.

Ключевые слова: *антивирусный пакет, Доктор Веб, пользователь, корпоративный вариант, стандартное корпоративное средство, IT-персонал, лицензия, дилер.*

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

Задействование АВ-средств в организациях и учреждениях, конечно, существенно зависит от таких параметров, как характер использования ПК в данной организации, особенности организации и функционирования ее компьютерной сети, структуры используемых в организации технических средств. Важную роль играют также такие трудно формализуемые факторы, как профиль стандартного пользователя и оснащенность 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.

Крупные научные учреждения, как правило, имеют собственную систему сетевых сервисов в виде электронной почты, удаленного доступа (Dialup) и других, а также 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, с разным уровнем технического обеспечения и даже с разной пропускной способностью. Все это в полной мере относится к Центральному экономико-математическому институту РАН (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» ее 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***. 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***.

В данной статье описаны предпосылки создания оригинальной технологии использования антивирусных пакетов серии Doctor Web [1] в качестве корпоративного АВ-средства. Практическая реализация будет освещена в последующем, в серии статей будут аккумулированы особо важные итоги работы автора в этой области за 2003–2011 гг.

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.

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 приемов манипулирования АВ-пакетом.

Дальнейшее рассмотрение постановки проблемы во многом ориентировано на выбранное АВ-средство – серию пакетов, вендором которых является ООО DoctorWeb (далее кратко – DrWeb). Помимо давней (примерно 15-летней) приверженности автора именно к этим средствам [2–4], имеется весьма актуальная причина сделанного выбора, что будет разъяснено позднее.

Развертка, установка, настройка пакетов. Рассматривая подробно ввод в эксплуатацию АВ-средства, как и любого программного пакета, можно выделить ряд этапов его использования: подготовку, установку, настройку, эксплуатацию.

Подготовка к установке включает желательное исполнение ряда типовых процедур и соблюдение ряда обязательных правил. Так, должна быть удалена предыдущая версия пакета или альтернативное АВ-средство[1] и, возможно, ряд иных программ, мешающих работе антивируса (например, 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 (например 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. Следует иметь в виду, что приведена лишь часть основных требований, полный же перечень значительно шире.

Стандартный дистрибутив «Doctor Web для рабочих станций Windows» не предусматривает развернутых объяснений возможных некорректных условий установки. В большинстве случаев истинную причину ошибки в установке можно узнать только после обращения в службу технической поддержки DrWeb, приложив журнал установки (если он вообще был получен, если его удалось найти пользователю, если пользователь оказался достаточно умелым, 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.

[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 ресурсоемкости, дороговизны и сложности в обслуживании находится вне рамок рассмотрения данной работы.

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 объема информации (в настоящее время около 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 избежать 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 развертки дистрибутива (100–180 Мб), чего, к сожалению, не делает сам инсталлятор пакета.

Следует иметь в виду, что давность оригинального дистрибутива может быть весьма велика (оригинальные дистрибутивы пакетов DrWeb на сайте DrWeb в последние годы могут не меняться несколько лет). Поэтому сразу же после установки DrWeb нужно вызвать текущее обновление антивирусных баз, которое, в свою очередь, может вызвать очередную перезагрузку Windows из-за появившихся с момента выпуска дистрибутива многочисленных так называемых критических обновлений (включающих измененные низкоуровневые драйверы, саму программу обновления и ряд других модулей). В последних версиях пакетов DrWeb стала, наконец, корректно проверяться необходимость перезагрузки в отдельных случаях. Однако и в текущей эксплуатируемой версии 5.0 в этом месте присутствует ряд ошибок, поэтому перезагрузку в этой версии приходится выполнять вручную. Только начиная с версии 6.0, корректно автоматически определяется 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 выполнять 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 определенное время. Начиная с версии 5.0, вендор включает в стандарт поставки задание на обновление. Однако это задание сформировано без логина и пароля, которые требуются в ряде случаев в корпоративных условиях, а также с 30-минутным режимом исполнения, 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 включенных ПК и серверов.

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

В частности, характерной проблемой DrWeb версий до 4.44 была нежелательность использования встроенного эвристического анализатора по причине его слабой работоспособности и весьма сильного замедления работы маломощных компьютеров, а также 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 Антивирусной службы ЦЭМИ РАН про-

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

ще заблокировать работу эвристика почти во всех возможных случаях, чем разъяснять каждому из 180 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.

Эксплуатация пакетов. Серьезной проблемой эксплуатации пакетов DrWeb стало назойливое стремление разработчиков постоянно осведомлять пользователей о наличии новой версии. Сообщения об этом приходят во время обновлений, причем само обновление порой блокировалось до выбора пользователем одной из нескольких возможностей («Напомнить завтра» / «Напомнить через 3 дня» / «Через 2 недели»), что, на взгляд автора, не соответствует условиям эксплуатации ПК в научном учреждении, имеющем Антивирусную службу. Более того, в ряде случаев такие сообщения серьезно затрудняют работу. Так, к примеру, ПК автора работает в режиме постоянной включенности, а обновления осуществляются в 1 ч ночи, когда, естественно, за ПК никого нет. Фактически появление подобных сообщений 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». Серверы, как известно, эксплуатируются без постоянного присутствия пользователей; многие из них не имеют ни постоянно подключенной клавиатуры, ни постоянно подсоединенного 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.

В 2010 г. до обращения автора данной публикации в техническую службу DrWeb невозможно было корректно обновлять файловые серверы в версиях 5.0/6.0 в случаях, когда не выполнен Logon. Учитывая, что общепринятой и рекомендуемой 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 недочета.

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

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

Профиль пользователей ЦЭМИ РАН. Рассмотрим, наконец, особенности эксплуатации ПК-пользователями компьютеров 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 условиями работы включение компьютера исполняется далеко не каждый день; более того, значительная часть ПК может не включаться несколько недель.

Наконец, структура сети ЦЭМИ РАН исторически сложилась достаточно сложной: в нее

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

включены несколько различных сетей[4], имеется ряд выделенных сегментов различного ранга с внутренней адресацией, DialUp. Доступ к антивирусным услугам из некоторых выделенных сегментов, Интернета и DialUp должен быть парольным, из основного же – беспарольным. Часть сети ЦЭМИ РАН предоставлена другим организациям, которые не должны иметь доступа к ряду сетевых сервисов, в том числе и к антивирусной поддержке.

Особо следует отметить ***поведение пользователей.*** По разным причинам, которые нет необходимости здесь анализировать, большинство пользователей не мотивированы в серьезном освоении компьютера и тонкостей операционной системы, тем более таких «не профильных» 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 ошибается хотя бы в одном из действий, что влечет за собой невозможность или некорректность установки пакета. Около 30% вычислительных установок в момент установки антивирусных средств по разным причинам оказываются не подготовленными к этому процессу. В частности, предварительное удаление остатков старой версии, рабочих файлов и проверка корректности логической структуры локальных томов не исполняются большинством пользователей.

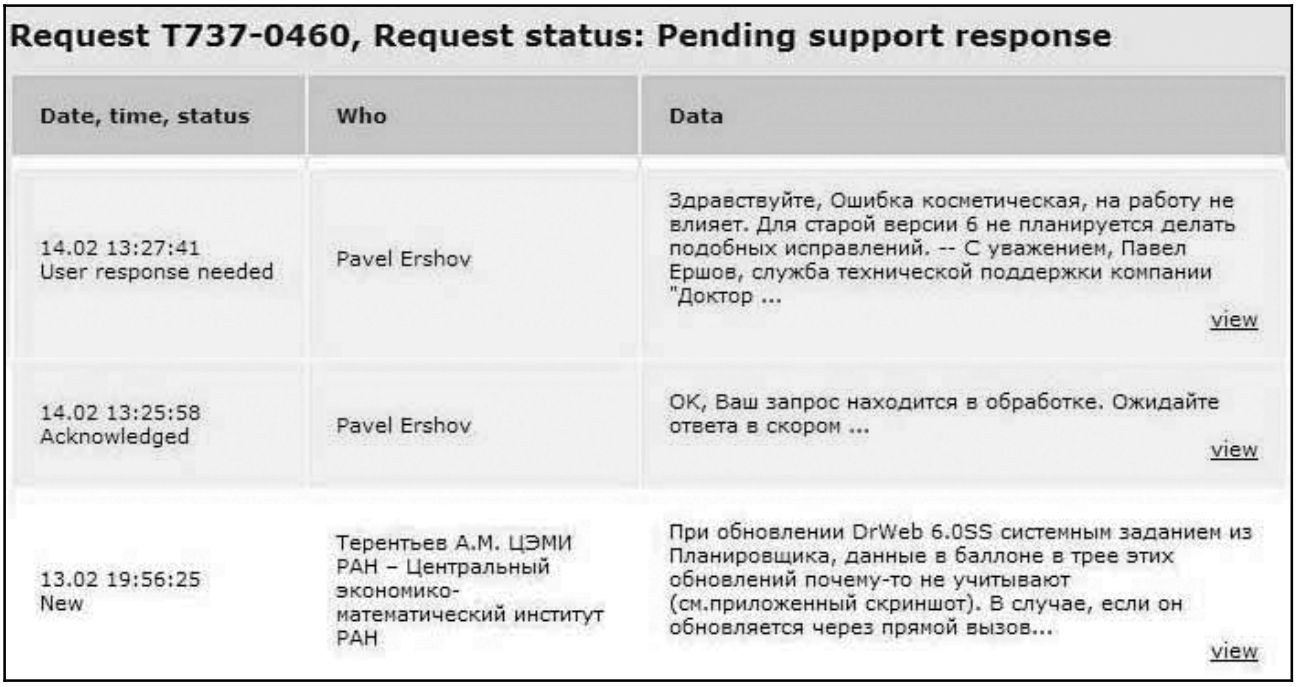
В результате при попытке установки из стандартного дистрибутива вендора порой возникает ситуация, когда пользователь уже ответил на ряд вопросов, но начавшийся процесс установки неожиданно прерывается с выдачей маловразумительного сообщения (на английском языке или русском профессиональном жаргоне программистов), а порой и без такового. Характерным примером может служить сообщение ***«Диск X: не определен»*** с прерыванием установки из стандартного дистрибутива, причем 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 причиной появления сообщения являлось отсутствие в момент установки подключения сетевого диска с указанной буквой, ссылки на который хранились в некоторых частях системного реестра. Зачем и почему стандартный дистрибутив пакета DrWeb это проверяет, остается 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 пакетам DrWeb. Естественно, в такой ситуации пользователь не осознает степени 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, а 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 «программ без ошибок не бывает» в последние несколько десятилетий, к сожалению, приобрело силу аксиомы и тем самым дает фактически индульгенцию на некачественную работу, порождая бесконечные изменения в уже распространенных антивирусных базах, а порой и полное обновление состава исполняющих модулей, а также 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» операциями техподдержки DrWeb (см. рисунок)[5].

[4] Адресное пространство сети, поддерживаемое Узлом ЦЭМИ РАН, состоит из трех сетей класса «С» с различной топологией и нескольких фрагментов сети, выделенных в самостоятельные сегменты.

[5] Справедливости ради следует отметить, что в описанном на рис. 1 случае автору все 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

Один из характерных запросов в DrWeb об устранении ошибок

Указание недостатков, проведенное выше и сделанное ранее [6–7], разумеется, существенно не влияет на заслуженно высокий статус пакетов DrWeb, одного из лидеров отечественного рынка АВ-средств и их разработчиков. Подчеркнем, что именно вследствие неоспоримых достоинств DrWeb и был выбран в 1999 г. и остается 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.

Заключительный анализ. Все 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 объема ручных операций и проверки целого ряда условий, а в целом отнимают заметное время (от 40 мин 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, причем на современных операционных системах (Windows'2008) с дорогостоящими процессорами Xeon, ОЗУ 8Гб и дорогим аппаратным Raid-массивом в целях повышения скорости чтения;
- установки, настройки и ввода в эксплуатацию SQL-сервера, также оснащенного аппаратным Raid-массивом, уже для распределения серьезной нагрузки по записи протоколов на жесткие 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 вышеуказанные условия представляются автору данной работы явно чрезмерными. Однако в варианте Enterprise Suite есть и другие недостатки. К примеру, число пользователей ЦЭМИ РАН – порядка 180, в такой ситуации 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. Однако Enterprise Suite не поддерживает одновременно нескольких 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 оснащенности, выяснения и исследования недокументированной информации, разработки специальных программ и повышенных затрат IT-специалистов.

Из изложенного ясно, что «разрыв» между совокупностью независимых индивидуальных комплектов и жестко 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 жесткого контроля за состоянием зараженности ПК пользователя, и тем более без навязывания ему конкретного времени и частоты проверок сканером.

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». После рассмотрения авторской концепции корпоративного дистрибутива можно определить необходимые условия к выбираемому базовому АВ-средству и его исходному, стандартному дистрибутиву, для возможности построения корпоративной среды.

Во-первых, 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 включен в состав пакета. Файл защищен контрольной суммой и изготавливается службой технической поддержки ООО «Доктор Веб» специально по заказу эксплуатирующей организации. В ЦЭМИ РАН в разное время использовалось до 7 различных файлов, определяющих доступ к 7 различным областям обновления.

Во-вторых, 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.

В-третьих, должен существовать способ включения группы рекомендованных для корпоративного варианта пользовательских настроек в развернутый пакет установленного АВ-средства.

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

В-четвертых, 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 приема файлов [5], что позволило для выдачи обновлений использовать тот же аппарат Apache 1.3.23, что и для HTML-файлов web-сайта. Особенно приятно отметить, что утилита обновления формирует правильное Modification Time для принимаемых файлов.

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

Все современные пакеты DrWeb имеют серию опциональных ключей, которые при их использовании подавляют все выдаваемые сообщения поль-

зователю. 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.

В-шестых, 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 своем составе файл, содержащий в себе имена и признаки актуальности всех необходимых файлов. 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.

В-седьмых, 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.

Конкретная технология предложенного автором корпоративного варианта эксплуатации пакетов DrWeb будет освещена в следующей статье.

Список литературы

1. Интернет-ресурс «DrWeb – инновационные технологии антивирусной безопасности». URL: http://www. drweb. com/?lng=ru.

2. *Терентьев А. М.* Противовирусная защита ПК в Windows 95/98/NT / Препринт #WP/99/078. М.: ЦЭМИ РАН, 1999.

3. *Терентьев А. М.* Антивирусная защита ПК в Windows 95/98/NT / Справочное пособие по антивирусным средствам ЗАО «ДиалогНаука». 2-е изд. М.: ОАО «Перспектива», 2000.

4. *Терентьев А. М.* Выбор адекватных средств информационной защиты персонального компьютера в России // Национальные интересы: приоритеты и безопасность. 2012. № 33. С. 37–42.

5. *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.

6. *Терентьев А. М.* Антивирусное обеззараживание персональных компьютеров с помощью подключения сторонних операционных систем // Национальные интересы: приоритеты и безопасность. 2012. № 37. С. 45–51.

7. *Терентьев А. М.* Ложные срабатывания антивирусных средств // Национальные интересы: приоритеты и безопасность. 2013. № 4. С. 41–46.