УДК 004.492

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

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». Описана оригинальная, разработанная и реализованная автором технология эксплуатации этих пакетов в условиях научного учреждения. Статья является второй частью серии статей, посвященных оригинальной разработке корпоративного варианта антивирусных пакетов «Доктор Веб».

***Ключевые слова**: информационная безопасность, антивирусные средства, Доктор Веб, корпоративный вариант антивирусных пакетов, научное учреждение.*

В предыдущей статье [2] было показано, что простое реплицирование одиночных экземпляров пакетов серии «Доктор Веб» по количеству пользователей для учреждений (организаций) неэффективно. Однако, как было показано, для таких организаций, как научные институты, столь же неэффективно использование этих пакетов в стандартном варианте Enterprise Suite.

В данной статье, продолжающей вышеупомянутую, приводится описание предложенного автором корпоративного варианта реализации антивирусных пакетов ООО «Доктор Веб» (далее – DrWeb) [1].

Корпоративная среда как предложенное решение. Альтернативой стандартному решению Enterprise Suite, впервые предложенному автором данной работы в 2003 г., является создание корпоративной среды установки и поддержки антивирусных пакетов DrWeb, включающей:

- многоцелевой антивирусный сервер, хранящий как области обновлений указанные антивирусные пакеты (в момент написания данной работы – до 5 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 ООО «Доктор Веб»;
- 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 паке-

тов DrWeb, установке и использованию этих пакетов.

Действия пользователя при установке. Действия пользователя описываются для варианта DrWeb 6.0 для рабочих станций. Зайдя на Антивирусный сайт, в соответствующей области пользователь щелчком по ярлыку запускает на своем 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. Подробнее об авторизации на сайте см. ниже.

После старта корпоративного дистрибутива исполняется его развертка во временную папку, которая впоследствии будет удалена, а затем автоматически стартует командный файл. При запуске первым срабатывает программный модуль поддержки, 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 удаленных деинсталлятором прежней версии. Разумеется, проверяется наличие альтернативных антивирусных программ (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 самозащиты в версии 6.0 модули сопровождения заносятся в отдельно создаваемую папку общего доступа TAMDrWeb в корне системного тома.

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 выдается соответствующая ошибка доступа, работа 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 введенной 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[1], 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 еще 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 учета лицензий. Выводится завершающее информационное сообщение пользователю с рекомендацией его последующих действий.

Далее, собственно, запускается показ рабочего стола Windows, и сразу же исполняется вариант стандартного задания пакета DrWeb на обновление. После исполнения обновления программный модуль поддержки запускается еще 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 развернутое четкое сообщение на русском языке о создавшейся ситуации с ее описанием и возможных последующих действиях. Такое сообщение либо выдается программой поддержки, либо предусмотрено в BAT-файле как текстовое сообщение, выдаваемое стандартной программой «Блокнот» (notepad. exe). Варианты таких аварийных сообщений включают широкий спектр воз-

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

можных 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 всем 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 тех ПК, которые находятся вне формальной корпоративной вычислительной сети ЦЭМИ РАН и составляют менее 4% от числа всех пользователей.

Схематически работа корпоративного дистрибутива (с некоторыми упрощениями) изображена на рис. 1. Упрощения включают отсутствие детализации многочисленных проверок при каждом запуске программы поддержки и сведение множества форм и текстов ошибок к двум-трем. 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, каким он получается после развертки.

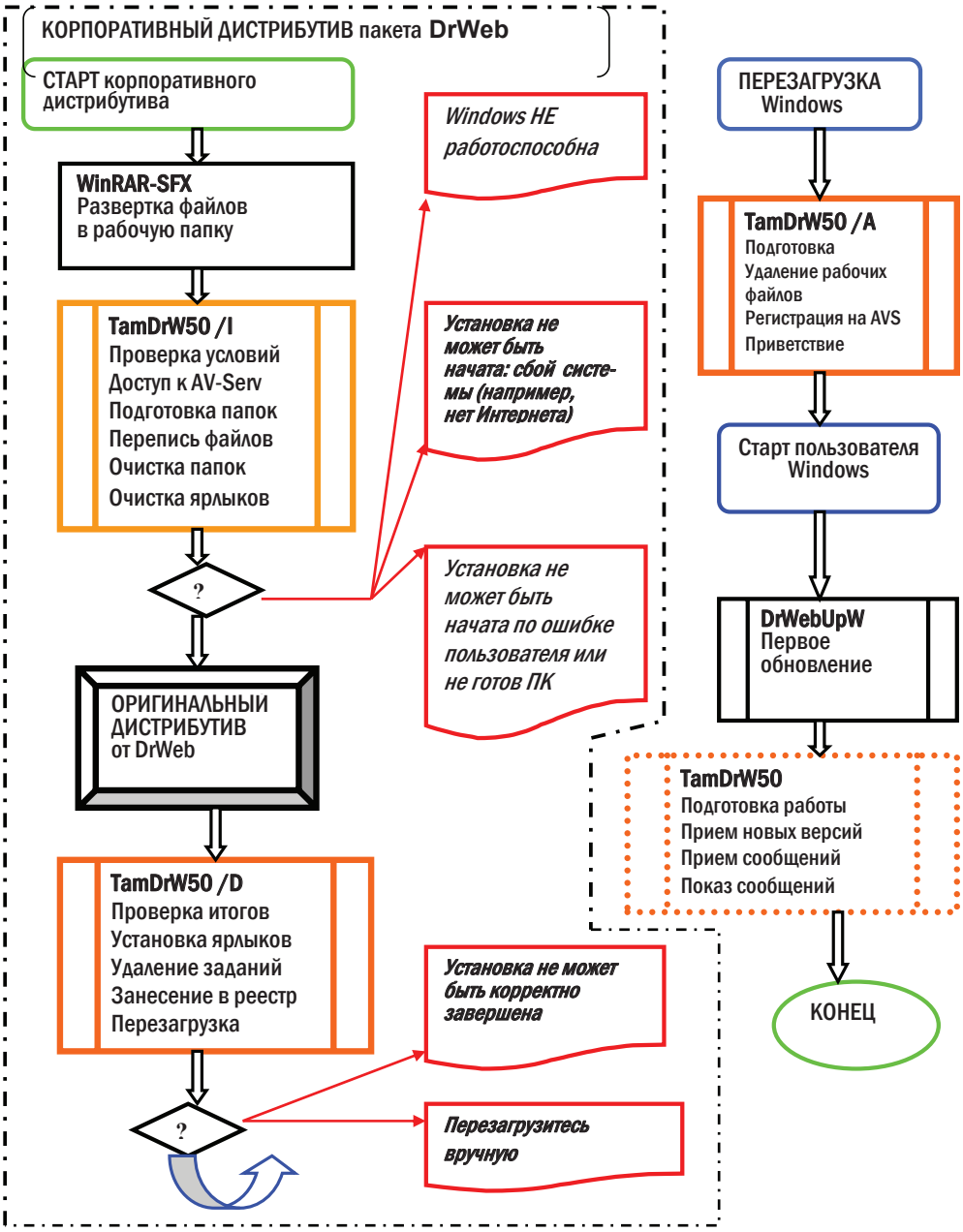

Рис. 1. Упрощенная схема работы корпоративного дистрибутива DrWeb

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.

Как было показано, в процессе установки антивирусного пакета программа поддержки несколько раз в различных целях обращается к Антивирусному серверу ЦЭМИ РАН. Каждое такое обращение оставляет в протоколе работы Антивирусного сервера «след», по которому Антивирусная служба легко определяет, с какого адреса поступил запрос на тот или иной этап установки, была ли завершена установка пакета. Если да, то фиксируется ряд све-

дений 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.

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 семь лет отмечен также случай, когда попытка обновления привела к ошибке вследствие совпадения по времени обновления с процессом реорганизации области на сервере обновления (одна часть файлов обновилась, другая часть – нет). В противоречие с многократными заверениями ООО «Доктор Веб» о том, что у них постоянных ошибок по связи и обновлениям не бывает, в распоряжении автора имеется сравнительно свежий пример, когда одновременно отказали в обновлении все 9 серверов ООО «Доктор Веб» (!). Наконец, при отсутствии Интернета из-за жары в июле 2010 г. сеансы обновлений с антивирусных серверов не проходили, однако это не сбивало работу основной части пользователей. Дело в том, что Антивирусный сервер ЦЭМИ РАН находится во внутренней сети, отсутствие Интернет-связи не влияло на работу пользователя, который получал 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 значительно 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 – 300–700 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, а в ряде случаев – от напоминаний о приближающемся сроке истечения ключевого файла и др. К сожалению, эти процедуры организованы ООО «Доктор Веб» 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 определенного времени не ответит, обновление вообще не исполняется (версия 4.44). Такая политика нежелательна для корпоративных пользователей рабочих станций, представляется недопустимой 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-шестых, в целях полного исключения возможности контрафактного использования ключей вне ЦЭМИ РАН, корпоративный вариант обновления предусматривает работу своих пользователей с особыми, заблокированными у вендора ключевыми файлами. Такая блокировка не мешает работе компонентов антивирусного пакета, однако не позволяет провести обновление с серверов вендора. Антивирусный же сервер ЦЭМИ РАН контролирует IP-адреса пользователей либо связку «логин-пароль», причем «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. Такое

решение весьма существенно для вендора: оно позволяет быть уверенным в нераспространении пакетов, возлагая всю ответственность за организацию работы на Антивирусную службу.

Несколько упрощенная 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 семи. Также не указано, что возможна одновременная обработка нескольких протоколов обновления утилиты DrWeb, накопленных в результате несрабатывания по той или иной причине утилиты поддержки обновлений.

Из представленной схемы на рис. 2 видно, 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, исполняются с предварительной многоэтапной проверкой результата, а реорганизация области пользователей исполняется во время, когда раздача обновлений отключена. Этим достигается полная корректность области обновления, предлагаемой пользователям.

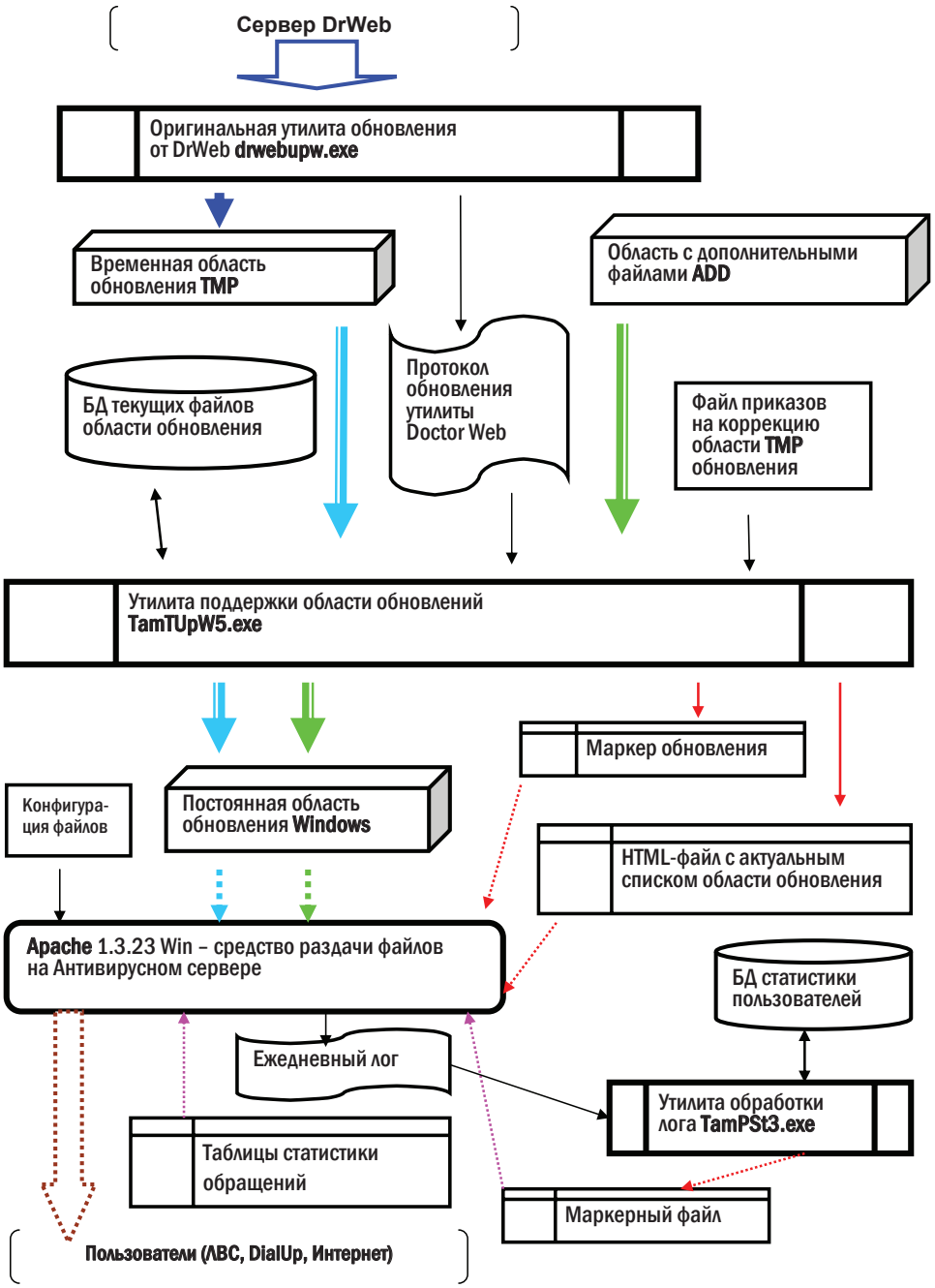

Рис. 2. Схема потоков информации при обновлении DrWeb

Алгоритм формирования конечной области (WINDOWS, имя выбрано вендором) сложен. Он включает анализ корректности ее текущего состава, одного или более протоколов обновлений, принятых от серверов ООО «Доктор Веб», учет управляющих приказов утилиты, фильтрацию приказов на обновление в соответствии с корпоративными правилами[2] и др. По каждой области обновления хранится своя текстовая база данных с рядом характеристик включенных файлов.

[2] 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.

Реализация предложенных решений. В ЦЭМИ РАН автором велась разработка предложенного варианта в течение ряда лет. Внедрен в эксплуатацию антивирусный сервер, хранящий корпоративные области обновления пакетов «Doctor Web для Windows» и «Doctor Web для файловых Windows-серверов» (1999–2003 гг.), инструктивные материалы по эксплуатации этих пакетов (2004–2013 гг.), Антивирусный сайт (2004 г.) с полной поддержкой статистики получения обновлений пользователями (2005–2008 гг.), корпоративный дистрибутив (2006 г.). Создание программы поддержки развертки 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 антивирусными 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 / 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 прежний вариант 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 приведенными 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.

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.

Список литературы

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

2. *Терентьев А. М.* Корпоративный вариант реализации антивирусных пакетов Doctor Web в научных учреждениях: предпосылки // Национальные интересы: приоритеты и безопасность. 2013. № 17.