іншої графічної інформації – проблема на сьогоднішній день до кінця не вирішена. Разом з тим розпізнавання графічної інформації, в якій міститься динамічна інформація про процес і особливості написання символу (прискорення, сила натиску), відкриває нові можливості для достовірнішого розпізнавання рукописних текстів.

Пристрої вводу, що функціонують за приведеною схемою були б компактнішими та простішими у користуванні і при певних вдосконаленнях змогли б замінити традиційні клавіатури, "мишки", друкарські машинки чи пензлики для письменників. Конструкторів.

Список літератури

1. www.analog.com

2. Стадник Б.І., Василик Ю.М. Інтелектуальні давачі.// Вісник Державного Університету "Львівська політехніка" №292, Автоматика, вимірювання та керування.-Львів, 1995.-с20-29.

3. Дудикевич В.Б., Паламар М.І. Методи спряження датчиків з персональним комп`ютером в системах автоматичного вимірювання і керування // Вимірювальна техніка та метрологія.-1998.-№53.-с.135-142.

Надійшла 15.11.2001

УДК 681.3

Безмалый В.Ф.

АНТИВИРУСНАЯ ЗАЩИТА КОМПЬЮТЕРНЫХ СЕТЕЙ

ВВЕДЕНИЕ

Целью данной статьи является ознакомление с достоинствами и недостатками типовых решений проблемы антивирусной защиты компьютерных сетей, а также рекомендации по созданию такой защиты.

Проблема антивирусной защиты компьютерных сетей далеко не нова и разработчики программного обеспечения предлагают различные варианты решения этой проблемы.

Актуальность проблемы не нуждается в дополнительном описании. Особенно теперь, в связи с появлением вирусных программ типа «троянский конь», остро встает проблема защиты парольного доступа к информации.

Существуют несколько типовых решений. Давайте подробнее рассмотрим некоторые из них.

Антивирусные программы для проверки компьютерных сетей.

В данном случае возможны два варианта решения проблемы

1. Сервер поддерживает создание скриптов для пользователей. В этом случае антивирусное программное обеспечение (например, программа DrWeb) устанавливается на сервере и при подключении клиента к сети автоматически, один раз в день, загружает все антивирусные базы и саму антивирусную программу во временную директорию на машину - клиент, производит проверку локальных дисков и отсылает файлы сообщений (логов) на сервер. К достоинствам данного метода следует отнести простоту использования, легкость в настройке (программа настраивается один раз на сервере и при дальнейшем увеличении числа клиентов в сети не требует перенастройки). К недостаткам относится необходимость входа пользователя в сеть, проверка осуществляется во время входа пользователя в сеть, что существенно замедляет процесс подключения и вызывает нарекания пользователя на машине-клиенте, необходимость физической передачи антивирусной программы каждый раз на машину - клиент, что увеличивает трафик, хотя это увеличение несущественно по объему.

2. Размещение антивирусной программы непосредственно на сервере (в данном случае рассматриваются сетевые операционные системы Novell NetWare и сеть под управлением Windows NT Server).

Рассмотрим подробнее установку антивирусного программного обеспечения AVP for Novell NetWare.

УСТАНОВКА АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ AVP FOR NOVELL NETWARE

Требования к системе

Для работы AVPN требуется:

- Наличие сервера с установленной на нем системой Novell NetWare версий 4.11, 5x.
- Около 10 Мб доступной (свободной) системной памяти сервера.
- Около 3,5 Мб свободного дискового пространства на томах сервера.
- Наличие следующих системных модулей Novell NetWare:
- для всех версий Novell NetWare — модули CLIB.NLM, DSAPI.NLM, CALNLM32.NLM, CLXNLM32.NLM;
- для Novell 5.x — модуль DSEVENT.NLM;
- для работы AVPN 4.1x необходимы последние обновления ОС и системной библиотеки (CLIB) фирмы Novell (http://www.support.novell.com/misc/patlst.htm).
- Наличие рабочей станции, работающей в среде Windows 95 или Windows 98, с установленной системой NetWare Client32 версии 3.0 и выше.

По умолчанию установка модуля конфигурации ядра AVPN производится в каталог PUBLIC\WIN32\SNAPINS, в котором расположен модуль NWAdmin32.

В процессе установки схема NDS изменяется следующим образом: создается класс "AVP", на основе которого создается объект "AVPN (<имя_сервера>)", где <имя_сервера> — имя сервера, на который устанавливается AVPN. Созданный объект имеет права на просмотр и чтение NDS, а также права чтения и записи своих свойств.

Загрузка AVPN

Загрузка AVPN производится с рабочей станции, работающей в среде Windows 95 или Windows 98.

Чтобы загрузить AVPN на сервер,

Запустите утилиту удаленного администрирования Netware Administrator.

1. Выберите в NDS объект AVPN.

2. Дважды щелкните мышью или щелкните правой кнопкой мыши и выберите из контекстного меню пункт **"Details"**. После этого откроется окно с параметрами объекта AVPN.

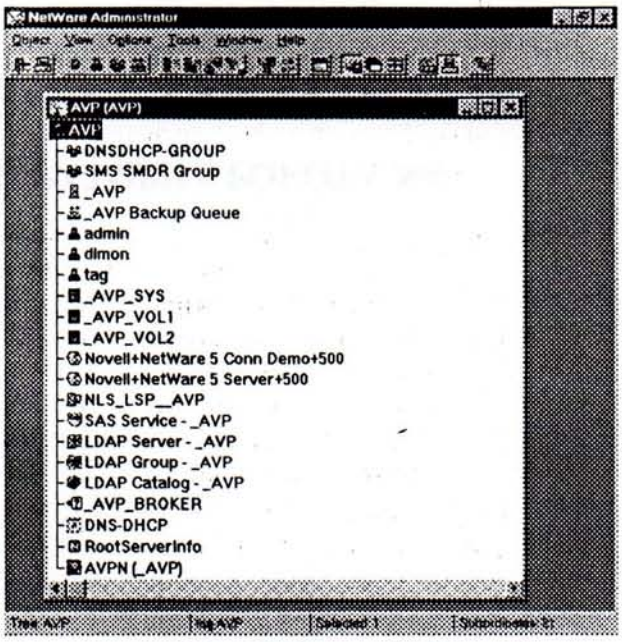

Рис. 0 Запуск AVPN

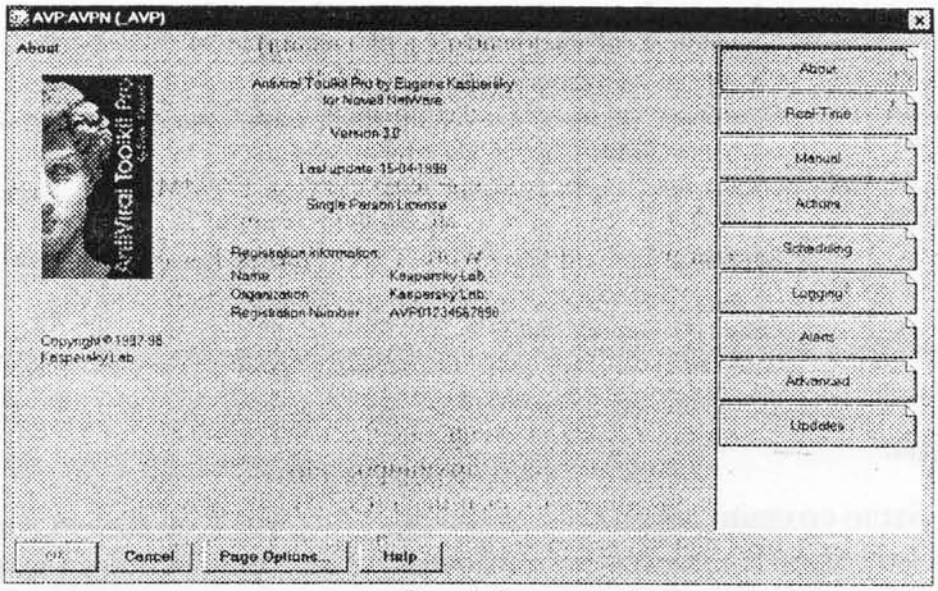

Рис. 1 Окно AVPN

3. Выберите страницу **"Manual"**.
4. Нажмите на кнопку **"Load NLM"** на закладке **"Scan"**.

После этого в память сервера будет загружено ядро программы (модуль AVKernel.NLM), антивирусные базы и появится информационное окно.

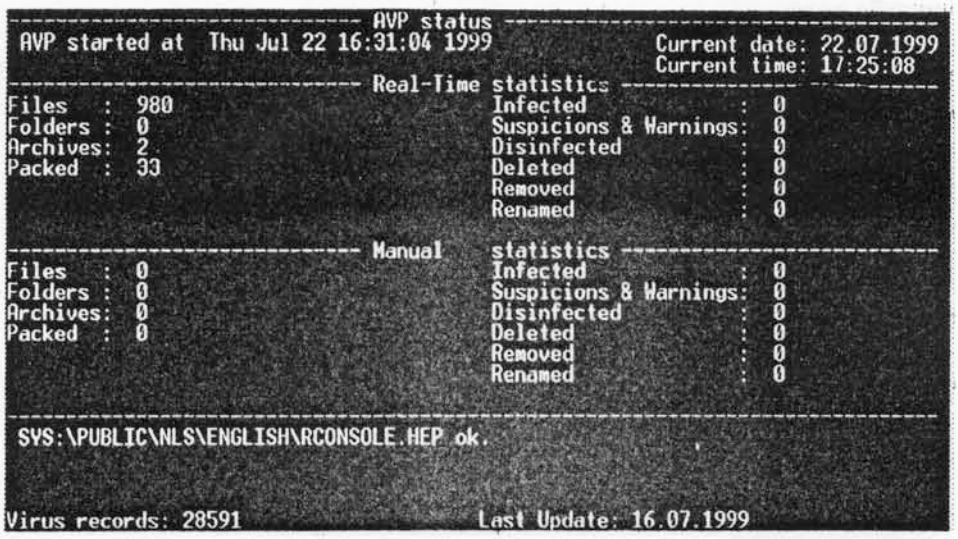

Рис. 2 Информационное окно.

Файлы антивирусных баз и список таких файлов

Файл с расширением .SET содержит список имен файлов антивирусных баз, участвующих в поиске и удалении компьютерных вирусов.

Антивирусные базы вместе с SET-файлом должны находиться в одном каталоге с ядром AVPN.

Приведем пример SET-файла:

SET-файл	Пояснения (не включаются в SET-файл)
KERNEL.AVC	Основная системная база (ядро AVP).
AVPYYMM.AVC	Основная (кумулятивная) антивирусная база (где YYMM — дата создания базы: YY — год, MM — месяц).
UPYYMMDD.AVC	Новая база (update, еженедельная) (где YYMMDD — дата создания базы: YY — год, MM — месяц, DD — день).
MACRO.AVC	База на макро-вирусы (Word, Excel, Access, PowerPoint).
BACKDOOR.AVC	База утилит скрытого удаленного администрирования.
TROJAN.AVC	База "троянских коней".
MALWARE.AVC	База прочих "вредных" программ: конструкторов вирусов, "злых шуток", "взломщиков" и т.д.
UNPACK.AVC	База для механизма распаковки.
EXTRACT.AVC	База для механизма разархивирования.
CA.AVC	База эвристического сканнера (Code Analyzer).
MAIL.AVC	База для проверки локальных почтовых ящиков пользователей.

Файл AVP.SET следует заменять новым каждый раз при обновлении антивирусных баз AVPN. Обычно новый файл AVP.SET поставляется вместе с новыми базами.

Каждая строка SET-файла должна содержать только одно имя файла антивирусных баз. Чтобы добавить новую базу, необходимо вставить в SET-файл дополнительную строку с именем файла антивирусной базы. Чтобы исключить базу из процедуры сканирования/лечения, необходимо либо удалить соответствующую строку, либо сделать ее комментарием, поставив в начале строки символ ";".

База KERNEL.AVC обязательно должна присутствовать в первой строке — в противном случае при запуске программы-сканера остальные антивирусные базы не будут загружены.

Название основной антивирусной базы должно находиться во второй строке SET-файла. Название основной базы имеет следующий вид: AVPyymm.AVC, где YYMM — дата создания базы: YY — год, MM — месяц; например, AVP9811.AVC.

Далее должны следовать файлы обновления основной базы (если они есть). Названия файлов обновления имеют вид **UPyymmdd.AVC**. Затем должны следовать все остальные базы (если они есть).

Пример обновленного SET-файла:

SET-файл	Пояснения (не включаются в SET-файл)
KERNEL.AVC	Антивирусная база Kernel.
AVP9808.AVC	Основная антивирусная база.
UP980904.AVC	Новая база (update) — от 4.09.98.
UP980912.AVC	Новая база (update) — от 12.09.98.
MACRO.AVC	База на макро-вирусы.
...	...

Порядок работы с AVPN

AVP для Novell NetWare ищет и удаляет вирусы на файл-сервере (серверах), работающих в сети под управлением Novell NetWare версий 4.x, 5.x.

AVPN работает в трех режимах:

- *Режим фильтра.* В режиме фильтра AVPN постоянно контролирует файлы, хранящиеся на сервере, осуществляя т.н. проверку файлов "на лету": в момент считывания, запуска и создания файлов на сервере.
- *Режим планового сканирования.* В режиме планового сканирования AVPN ищет и удаляет вирусы в файлах файл-сервера. Поиск вирусов запускается в определенные дни (часы, минуты) по расписанию, заданному администратором.
- *Режим ручного сканирования.* В режиме ручного сканирования поиск вирусов запускается по требованию администратора — с помощью модуля удаленного администрирования.

В режимах планового и ручного сканирования программа AVPN позволяет искать вирусы не только на файл-сервере, где она установлена, но и на других серверах локальной сети. Для этого администратор должен присвоить объекту AVPN соответствующие права доступа на файловую систему удаленных серверов.

Необходимо настроить параметры двух режимов работы AVPN: режима фильтра и режима планового сканирования.

После загрузки работа AVPN в режимах фильтра и планового сканирования не требует вмешательства администратора. Если администратору понадобится изменить настройки этих режимов, он может это сделать в любой момент, используя модуль удаленного администрирования.

Что такое "сканирование в режиме фильтра"

Сканирование в режиме фильтра представляет собой автоматическую проверку (проверку "на лету") файлов сервера, к которым происходит обращение с рабочей станции и других серверов сети. AVPN проверяет все файлы, удовлетворяющие заданным критериям. Режим фильтра является основным режимом работы AVPN и вводится в действие сразу после загрузки модуля AVPN на сервере.

AVPN проверяет все файлы перед их запуском или открытием, что позволяет находить и обезвреживать вирусы до дальнейшего заражения сервера. При создании новых файлов AVPN проверяет их перед закрытием, тем самым, обеспечивая запись на сервер только незараженных файлов.

Хотя AVPN позволяет управлять степенью использования центрального процессора сервера, сканирование в режиме реального времени несколько замедляет работу сервера. Поэтому для режима фильтра не рекомендуется включать механизм распаковки архивов, если проверяемые архивы имеют слишком большой размер.

При обнаружении инфицированных или "подозрительных" на вирус (обнаруженных с помощью эвристического анализатора) файлов, программой будут предприняты действия, указанные администратором.

Отчет о проверке в режиме фильтра можно просматривать в журнале результатов.

Что такое "ручное сканирование"

В *режиме ручного сканирования* AVPN выполняет функции стандартного антивирусного сканера — проход дерева подкаталогов и поиск зараженных файлов. Механизм поиска вирусов запускается вручную администратором сети из окна объекта AVPN. Затем AVPN проходит дерево подкаталогов указанных томов сервера и проверяет файлы, указанные в настройках, на наличие вирусов. При обнаружении инфицированных

или "подозрительных" на вирус (обнаруженных с помощью эвристического анализатора) файлов, программой будут предприняты действия, указанные администратором.

После окончания сканирования Вы можете просмотреть журнал результатов проверки.

Программа AVPN может проверять файлы не только сервера, где она установлена, но и других серверов, находящихся с ним в одном дереве NDS. Для этого администратор должен с помощью модуля удаленного администрирования присвоить объекту AVPN соответствующие права доступа на файловую систему удаленных серверов.

Для запуска ручного сканирования на сервере должен быть загружен модуль AVKernel.NLM.

Что такое "плановое сканирование"

В *режиме планового сканирования* AVPN выполняет ту же процедуру, что и в режиме ручного — проход дерева каталогов и поиск зараженных файлов. Поиск вирусов инициируется автоматически через определенные интервалы времени, указываемые в настройках. Там же указываются файлы, которые будут проверяться. При обнаружении инфицированных или "подозрительных" на вирус (обнаруженных с помощью эвристического анализатора) файлов, программой предпринимаются действия, указанные администратором.

Результаты планового сканирования заносятся в журнал результатов проверки.

Режим планового сканирования начинает действовать сразу после загрузки модуля AVKernel на сервере.

При необходимости режим планового сканирования может быть отключен.

ЗАЩИТА СЕРВЕРА, РАБОТАЮЩЕГО ПОД УПРАВЛЕНИЕМ ОС WINDOWS NT/2000

Для защиты сервера, работающего под управлением ОС Windows NT/2000 Server, необходимо установить на него программное обеспечение AVP for Windows NT Server. Я считаю, что нет необходимости в описании установки данного программного обеспечения ввиду его огромной популярности и простоты установки. Поэтому сразу же перейдем к запуску программы.

1. Запуск AVP и дополнительные ключи

Запуск программы может быть произведен любым стандартным способом, принятым в Windows NT Server

Выполняемый файл, который надо запустить, называется «AVP32.EXE».

AVP позволяет использовать *дополнительные ключи*. Их нужно указывать в командной строке. Рекомендуется использовать ключи при запуске AVP с помощью ярлыка.

При использовании ключей командная строка может выглядеть так:

AVP32.EXE [/P=имя_профайла] [/S] [/W] [/N] [/Q] [/D] [/@[!]=имя_файла] [имя_файла] [имя_директории]

где:

- ключ **/P=имя_профайла** - означает, что AVP запустится с теми настройками, которые были записаны в профайле с именем «имя_профайла»;
- ключ **/S** - означает, что сразу после запуска AVP начнет сканирование.

• ключ **/W** - включает флажок «Файл отчета» во вкладке «Настройки», т.е. обязательно будет создан файл отчета, даже если в профайле указано, что не следует создавать его;

• ключ **/N** - означает, что при запуске программы главное окно AVP будет свернуто в иконку.

• ключ **/Q** - означает, что сразу после окончания сканирования главное окно AVP будет закрыто и программа будет выгружена из памяти;

• ключ **/@[!]=имя_файла** - означает, что сканироваться будут только те файлы, которые указаны в файле с именем «имя_файла». Где файл «имя_файла» - это обычный текстовый файл (ASCII), содержащий список имен файлов, предназначенных для сканирования. Каждая строка в нем должна содержать только одно имя файла (с указанием полного пути). Если в ключе указан знак «!» (т.е. **/@!=имя_файла**) то файл «имя_файла» будет удален после окончания сканирования. Если «!» не указан (т.е. **/@=имя_файла**) то данный файл удаляться не будет.

• ключ **/D** - означает, что AVP не будет запускаться, если в течение данного дня уже было произведено сканирование, и оно завершилось успешно (то есть оно не было прервано и не было найдено ни одного вируса).

• если подстрока в командной строке начинается не со знака «/», то она распознается как имя файла или директории (**имя_файла, имя_директории**) (использование в именах универсальных символов, таких как «*» или «?», не допускается). В этом случае AVP сразу после загрузки начнет сканирование этих файлов или директорий. При этом все настройки (кроме настроек из вкладки «Область») будут браться из prf-файла (либо Default.prf, либо указанного в соответствующем ключе). Пример: "C:\AVP\Avp32.exe" C:\CONFIG.SYS D:\EXCHANGE.

ЗАМЕЧАНИЕ: Если в имени файла/директории присутствуют длинные имена, содержащие пробелы, то данное имя файла/директории следует указывать в кавычках. Например:

"C:\Program Files\AVP\Avp32.exe" /S "C:\My documents"

Запускать AVP на выполнение с указанными ключами можно следующим способом. Нажмите кнопку «Start» и выберите пункт «Run...»; в появившемся окне «Run» в строке ввода укажите полный путь и имя файла AVP32.EXE с необходимыми Вам ключами.

Например:

"C:\Program Files\AntiViral Toolkit Pro\Avp32.exe" /P= My_Settings.prf /S /N /Q

Очень удобно использование дополнительных ключей при запуске с помощью ярлыка. Можно изменить командную строку в уже созданном для AVP ярлыке. Для этого, щелкнув по ярлыку правой кнопкой мыши, выберите в появившемся меню пункт «Properties». Появится диалоговая панель «Properties AVP32». В ней откройте вкладку «Shortcut», а затем в поле ввода «Target» допишите в конце строки нужные ключи.

Например:

"C:\Program Files\AntiViral Toolkit Pro\Avp32.exe" /P= My_Settings.prf /S

В этом случае при запуске AVP с помощью ярлыка, будут загружены настройки из файла с именем «My_Settings.prf», и программа сразу запустится на сканирование.

Поместив ярлык AVP в группу «Autorun» Вы сможете запускать AVP автоматически сразу после загрузки Windows.

2. Коды возврата AVP

При использовании AVP в командном файле, после завершения его работы, можно получить следующие коды возврата (errorlevel):

0 - вирусов не обнаружено;

1 - сканирование не закончено;
2 - найдены объекты, содержащие измененный или поврежденный вирус;
3 - найдены объекты, подозрительные на вирус;
4 - обнаружен известный вирус;
5 - все обнаруженные вирусы удалены;
7 - файл AVP32.EXE поврежден;
10 - внутренняя ошибка программы AVP.

Для постоянной проверки файлов на сервере используется программа AVP Monitor

AVP Monitor™ представляет собой резидентную антивирусную программу, которая постоянно находится в оперативной памяти и контролирует операции обращения к файлам и секторам. Прежде чем разрешить доступ к объекту, **AVP Monitor**™ проверяет его на наличие вируса и, если вирус обнаружен, предлагает вылечить зараженный объект (либо удалить, либо заблокировать доступ к объекту - в зависимости от выбранных Вами опций). Таким образом, **AVP Monitor**™ позволяет обнаружить и удалить вирус до момента реального заражения системы.

3. АНТИВИРУСНАЯ СЕТЬ НА БАЗЕ AVP NETWORK CONTROL CENTER

Но все предложенные выше подходы обладают одним существенным недостатком. Они защищают сервер, но либо не обеспечивают защиту пользователей сети, либо защищают их ценой некоторых усилий (**DrWeb**), но лишь в том случае, если пользователь присоединен к сети. Существует иной подход к решению данной проблемы. Он заключается в создании сети на базе сетевого антивирусного программного обеспечения **AVP Network Control Center** (сетевой центр управления). В данном случае формируется антивирусная сеть на базе станций, работающих под управлением Windows 95/98/NT/2000. Недостатком данного способа является жесткая привязка клиентских машин к вышеуказанным операционным системам, а также необходимость установки на каждую клиентскую машину антивирусного программного обеспечения. Однако тем самым решается сразу **глобальная задача защиты**, как пользовательских машин, так и серверов сетей. При этом возможно как создание не только локальных, но и глобальных антивирусных сетей, так как необходимым является лишь наличие у каждой машины-клиента сети AVP IP-адреса, а не физического членства в данной локальной сети.

С целью проверки данного предположения на базе Крымской региональной таможни производилось тестирование удаленной машины (сервер антивирусной сети находился в г. Симферополе, а клиентская машина в г. Керчи, то есть расстояние составило более 200 км). Трафик по сети составил 3 килобайта (это письмо с подтверждением о состоянии проверяемой машины). Для усложнения эксперимента сервер в заранее заданное время был отключен (время запуска антивирусного сканирования на машине-клиенте было задано заранее с машины-сервера), но благодаря встроенному в AVP Планировщику задач программа на клиенте была запущена и письмо-сообщение отправлено на сервер, где и получено с помощью почтовой программы The Bat.

Таким образом, можно сделать следующий вывод:

При комплексной защите компьютерной сети, имеющей удаленные подразделения (компьютеры) и работающей с применением протокола TCP/IP рекомендуемый способ защиты – создание антивирусной сети на базе AVP Network Control Center с одновременной защитой сервера с помощью серверных приложений AVP.

Поступила 10.10.2001