

ФАКТОР - ТС

**ТЕХНОЛОГИЯ**  
**ДИОНИС**

**Система**  
**АНТИВИРУСНОЙ ЗАЩИТЫ**

*Руководство по эксплуатации*

**Москва 2010**

# Содержание

<b>1. Общие положения.....</b>	<b>3</b>
1.1. Порядок настройки Системы АНТИВИРУСНОЙ ЗАЩИТЫ.....	4
1.2. Алгоритм антивирусной проверки.....	5
1.3. Нештатные ситуации.....	7
<b>2. Установка антивирусных пакетов.....</b>	<b>8</b>
2.1. Антивирус Касперского-ДИОНИС.....	8
2.2. DOCTOR WEB для WINDOWS.....	8
<b>3. Программа DiAids.....</b>	<b>11</b>
3.1. Установка программы.....	11
3.2. Работа программы DiAids.....	11
3.3. Настройка программы DiAids.....	13
<b>4. Подсистема АНТИВИРУС.....</b>	<b>18</b>
4.1. Функция: Инициализация.....	18
4.2. Функция: Конфигурация.....	19
4.2.1. Контролируются.....	19
4.2.2. Уведомление.....	22
4.2.3. Сканер.....	22
4.2.4. Адрес АЕР-сервера.....	23
4.2.5. Ограничения и возможные проблемы.....	23
4.2.6. Записать.....	25
4.3. Функция: Отладка.....	25
4.4. Функция: Тест.....	26
4.5. Функция: Спам.....	27
4.6. Протокол процесса антивирусной проверки.....	28

# 1. Общие положения

В технологии **ДИОНИС** реализована Система **АНТИВИРУСНОЙ ЗАЩИТЫ**, обеспечивающая антивирусную безопасность всей поступающей на сервер почтовой корреспонденции.

Система **АНТИВИРУСНОЙ ЗАЩИТЫ** состоит из следующих компонентов.

- Подсистема **АНТИВИРУС**, входящая в состав программного обеспечения **ДИОНИС**.
- Программа **DiAids**, размещаемая на отдельной машине, работающей под управлением ОС **WINDOWS**. Эта программа обеспечивает связь с узлом **ДИОНИС** по IP-протоколу и вызов необходимой антивирусной программы после того, как придет задание на проверку.
- Собственно антивирусная программа, размещаемая на той же **WINDOWS**-станции, что и программа **DiAids**. В настоящее время **DiAids** может работать с одним из трех антивирусных пакетов.
  - Антивирус Касперского для **ДИОНИС** - антивирусный пакет лаборатории Касперского, работающий под управлением **WINDOWS 9x/NT/2000/ME**, разработанный специально для работы в рамках технологии **ДИОНИС**.

Если используется пакет Антивирус Касперского для **ДИОНИС**, то кроме проверки файлов на наличие вирусов выполняются дополнительные проверки на наличие **SPAM'a**, ненормативной лексики и подозрений на **SPAM**.

- Антивирус Касперского - антивирусный пакет лаборатории Касперского, работающий под управлением **WINDOWS NT/2000**.

- **DOCTOR WEB** для **WINDOWS 95/98/Me/NT/2000** - антивирусный пакет производства компании «Доктор Веб», работающий под управлением ОС **WINDOWS 9x/NT/2000/ME**.

*Замечание.* Предыдущая версия Системы **АНТИВИРУСНОЙ ЗАЩИТЫ** несколько отличается от современной. Предыдущая версия описана в руководстве Система **АНТИВИРУСНОЙ ЗАЩИТЫ** выпуска 2004 года.

## 1.1. Порядок настройки Системы АНТИВИРУСНОЙ ЗАЩИТЫ

Система АНТИВИРУСНОЙ ЗАЩИТЫ технологии ДИОНИС представлена на Рис. 1-1.

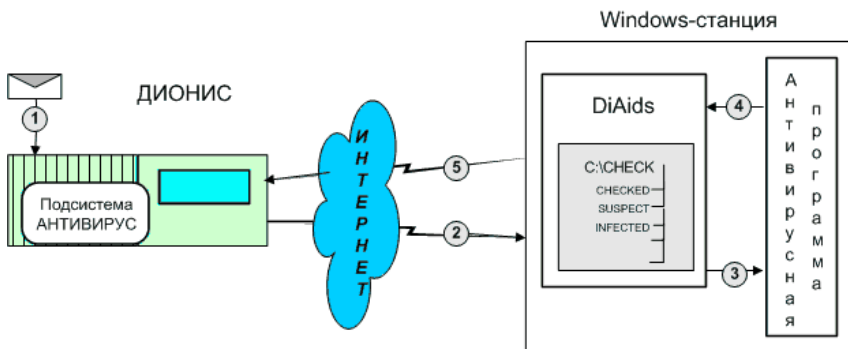


Рис. 1-1

1. На WINDOWS-станции должна быть установлена антивирусная программа.
2. На WINDOWS-станции должна быть установлена программа **DiAids**.

На одном из дисков WINDOWS-станции должна быть выбрана директория для обмена данными между программой **DiAids** и антивирусным пакетом (директория **C:\CHECK** на рисунке). В этой директории автоматически будут созданы поддиректории с системными именами: **CHECKED**, **SUSPECT**, **INFECTED** и др. В эти поддиректории программа **DiAids** будет помещать файлы после проверки, в какую именно - зависит от результата проверки (от кода завершения работы антивирусной программы).

3. На хосте **ДИОНИС** должна быть активизирована и настроена подсистема АНТИВИРУС. При настройке:
  - указывается IP-адрес программы **DiAids** (той машины, на которой установлена программа);
  - определяются те элементы корреспонденции, которые должны проверяться;

**ДИОНИС** может передавать на антивирусную проверку исходящую почту (письма и файлы) локальных абонентов,

---

---

всю почту, приходящую на хост по межхостовому обмену, а также помещаемые в конференцию темы, ответы и «подклеенные» файлы;

- устанавливается размер очередей, действия, которые должны быть выполнены, если **DiAids** недоступна, и т.д.

*Замечание.* Сразу после того, как будет настроена подсистема АНТИВИРУС, первый же появившийся на хосте элемент корреспонденции будет отправлен на проверку. Поэтому необходимо, чтобы сначала был установлен антивирусный пакет, затем настроена программа **DiAids** и после этого настроена подсистема **ДИОНИС АНТИВИРУС**.

## 1.2. Алгоритм антивирусной проверки

1. В программе **DiAids** устанавливаем режим ожидания заданий на проверку (в этом режиме программа ждет входящих TCP-соединений на ее IP-адрес на порт 412).

С точки зрения Internet, **DiAids** представляет собой серверный компонент обычного сервера, который ждет вызова по указанному порту по протоколу TCP.

2. Запускаем хост **ДИОНИС**, активизируем и настраиваем подсистему АНТИВИРУС. Между хостом и **DiAids** устанавливается IP-соединение по специальному серверному протоколу АЕР (Antivirus Exchange Protocol).

Для этого соединения **ДИОНИС** занимает отдельный порт (в линейке портов на консоли он окрашивается в черный цвет).

3. Если на хост приходит (или на хосте создается) корреспонденция, которая должна пройти антивирусную проверку, то она обрабатывается стандартным образом и размещается в **ДИОНИС**, но доступ к ней блокируется до окончания проверки.
4. Как только на хосте появляется объект для проверки, **ДИОНИС** передает объект **DiAids** и переходит в режим ожидания результатов проверки.
5. После того, как подлежащее проверке сообщение будет принято *полностью*, **DiAids** запускает антивирусную программу, передает ей файл на проверку и ждет результата.

положения

6. Антивирусная программа проверяет файл и возвращает **DiAids** код, соответствующий результату проверки.
7. В соответствии с полученным кодом **DiAids** перемещает проверенный файл в одну из поддиректорий:
  - в поддиректорию **CHECKED**, если файл «чистый»;
  - в поддиректорию **INFECTED**, если обнаружен известный программе вирус;
  - в поддиректорию **SUSPECT**, если есть подозрение на наличие неизвестного программе вируса.
  - в поддиректорию **SPAM**, если обнаружен SPAM;
  - в поддиректорию **SPAMFOUL**, если обнаружена ненормативная лексика;
  - в поддиректорию **SPAMSUSP**, если есть подозрение на наличие SPAM'а.
8. Как только в одной из поддиректорий появляется файл, **DiAids** посылает на **ДИОНИС** по протоколу AEP сообщение, содержащее код, соответствующий результату проверки. Сам проверенный файл остается на **WINDOWS**-станции и удаляется сразу после того, как **ДИОНИС** подтвердит получение сообщения.
9. Получив результат проверки, **ДИОНИС** выполняет следующие действия:
  - если файл «чистый», то с него снимается блокировка, и он становится доступным адресату;
  - если в файле обнаружен вирус, то он остается заблокированным, а действия **ДИОНИС** зависят от настройки подсистемы **АНТИВИРУС** (см. раздел 4.2.2, стр. 22): корреспонденция возвращается автору и/или абоненту с именем **aidsmaster** (или администратору, если такой абонент на хосте не создан), автору посылается уведомление и т.д.;
  - файлы с подозрением на наличие неизвестного вируса **ДИОНИС** в зависимости от настройки подсистемы значением параметра **Подозрение на вирус** (раздел 4.2.5, стр. 25) считает или «чистыми» или «инфицированными» и поступает с ними соответствующим образом;
  - если в файле обнаружен SPAM, ненормативная лексика или есть подозрение на наличие SPAM'а, то **ДИОНИС** поступает

---

---

так, как задано при настройке подсистемы АНТИВИРУС (раздел 4.5 стр. 27): блокирует файл или передает адресату, а также может послать копию файла администратору хоста.

### 1.3. Нештатные ситуации

Предполагается, что все необходимые настройки выполнены и подсистема АНТИВИРУС на хосте ДИОНИС настроена на работу с **DiAids**. Если после этого:

- по каким-либо причинам не удается организовать IP-канал между ДИОНИС и **DiAids**
- или происходит обрыв канала в процессе работы, то возникает ситуация «*Отсутствует путь проверки*».

В отсутствие связи с программой антивирусной проверки ДИОНИС работать не сможет и будет выполнять те действия, которые заданы при настройке подсистемы АНТИВИРУС значением параметра **Отсутств .** (раздел 4.2.5, стр. 25): отменит проверку, перезагрузится или «заблокирует источники».

## 2. Установка антивирусных пакетов

Настоящее руководство содержит описание процедуры установки на WINDOWS-станцию антивирусных пакетов Касперского для ДИОНИС и Dr.WEB для Windows только с дистрибутивных дисков, специально подготовленных фирмами-разработчиками для поставки в составе Системы АНТИВИРУСНОЙ ЗАЩИТЫ технологии ДИОНИС.

Возможна установка этих пакетов с любого другого диска, но в этом случае необходимо пользоваться рекомендациями документации, поставляемой вместе с антивирусными программами.

Перед установкой любого из пакетов необходимо удалить с компьютера другие антивирусные программы и закрыть все работающие приложения.

### 2.1. Антивирус Касперского-ДИОНИС

Антивирус Касперского для ДИОНИС поставляется в виде самораспаковывающегося архива **Dionis2005\_install.exe** и не имеет каких-либо параметров настройки в процессе инсталляции.

После окончания инсталляции необходимо в директорию **Program Files/Kaspersky Lab/Dionis2005/Bin** поместить лицензионные ключи, поставляемые вместе с инсталляционным пакетом.

После установки ключей Антивирус готов к работе.

Подробнее см. документ **АНТИВИРУС КАСПЕРСКОГО для ДИОНИС**. Руководство администратора.

### 2.2. DOCTOR WEB для WINDOWS

Настоящее руководство содержит описание процедуры установки антивирусного пакета DOCTOR WEB для WINDOWS только с дистрибутивного диска, специально подготовленного компанией «Доктор Веб» для поставки в составе системы антивирусной защиты технологии ДИОНИС.

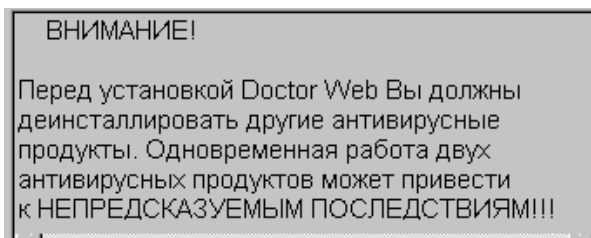
Возможна установка пакета DOCTOR WEB для WINDOWS или пакета Антивирус Касперского с любого другого диска, но в этом случае необходимо пользоваться рекомендациями документации, поставляемой вместе с этими пакетами.

*Внимание!* Коммерческие пользователи, приобретающие пакет DOCTOR WEB у законных поставщиков продукта, получают лицензионный ключевой файл. Без него все компоненты установленного на компьютер пакета блокируются.

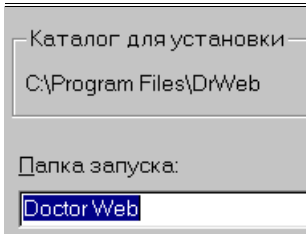
Перед тем, как вставить диск в компьютер, необходимо закрыть все приложения. После установки диска на экран будет выведено первое окно, в котором надо активизировать альтернативу **Установка**.



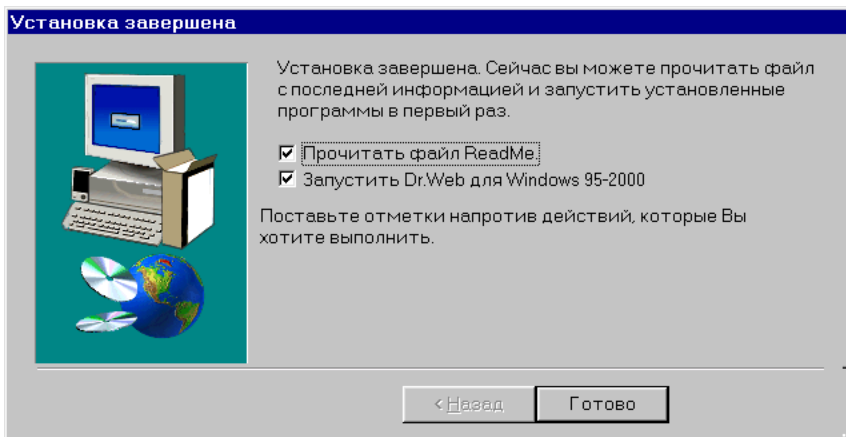
Установка начнется с предупреждения, на которое необходимо обратить внимание:



Далее необходимо следовать инструкциям, сохраняя везде предлагаемые программой умалчиваемые значения:



Заканчивается установка последним запросом:



*Внимание!* Если Вы решите для проверки запустить программу (оставите соответствующий флажок), то потом обязательно ее закройте (это необходимо для нормального запуска Системы АНТИВИРУСНОЙ ЗАЩИТЫ **ДИОНИС**).

После окончания процесса инсталляции в заданной папке запуска (**Doctor Web**) появится иконка: .

Подробнее см. документ **АНТИВИРУС Dr.WEB для WINDOWS**. Краткое руководство пользователя, Версия 4.33.

## 3. Программа DiAids

### 3.1. Установка программы

Программа **DiAids** должна быть установлена на отдельной машине, работающей под управлением ОС WINDOWS. Дистрибутивный пакет **DiAids** поставляется на отдельной дискете. Инсталляция выполняется запуском программы **SETUP**. Начинается установка с сообщения:

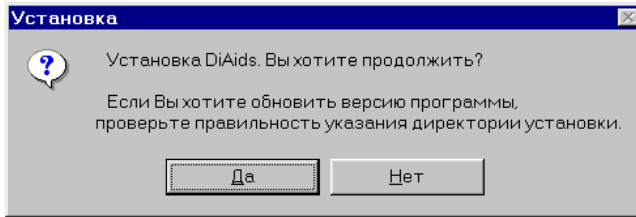



Рис. 3-2

Необходимо нажать кнопку **Да** и далее следовать инструкциям, сохраняя везде предлагаемые программой умалчиваемые значения.

После окончания процесса инсталляции иконка программы  будет помещена в группу программ **Автозагрузка**.

### 3.2. Работа программы DiAids

После вызова программы на экран выводится окно, вид которого представлен на Рис. 3-3.

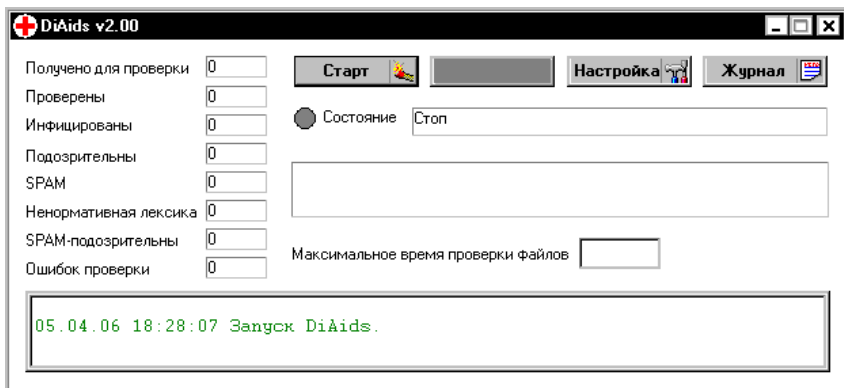


Рис. 3-3

Для всех параметров (настроек) установлены умалчиваемые значения, и программа готова к работе.

При необходимости умалчиваемые значения можно изменить. Как это сделать, рассмотрено ниже в разделе 3.3, стр. 13.

Чтобы перевести программу в рабочее состояние, надо в окне (Рис. 3-3) нажать кнопку **Старт**.

В рабочем состоянии в этом окне (Рис. 3-5):

- активна кнопка **Стоп**, которая служит для остановки программы;

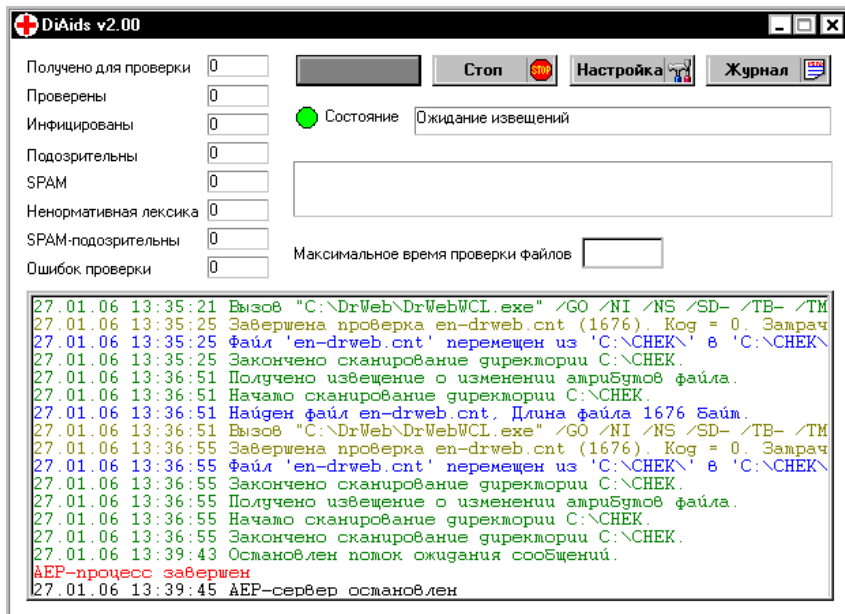


Рис. 3-4

- горит зеленым цветом индикатор слева от параметра **Состояние**, и в окошке справа от параметра выводится текст, отражающий выполняемые программой действия («**Ожидание извещений**», «**Сканируем директорию**», и т.д.);
- в окошке, расположенном ниже, – расширенная информация о выполняющейся или завершенной операции;
- **Максимальное время проверки файлов** – максимальное время в секундах, затраченное на проверку поступивших на проверку файлов в течение сеанса работы **DiAids**;

- в полях в левой части окна выводятся цифры, показывающие, сколько файлов поступило на проверку (**Найдено файлов**), сколько проверено (**Проверено**), в скольких из них обнаружены известные вирусы (**Инфицировано**), сколько из них заведомо содержат SPAM (**SPAM**), в скольких есть подозрение на наличие неизвестного вируса (**Подозрительных**) или на наличие SPAM'a (**SPAM-подозрительны**);
- в нижнюю часть рабочего окна выводится протокол работы системы; этот же протокол заносится в журнал

Чтобы просмотреть журнал, надо в окне (Рис. 3-4) нажать кнопку **Журнал**. Журнал – это обычный текстовый файл, для его просмотра используется программа **Блокнот (NotePad)** (подробнее о журнале см. раздел 3.3, стр. 15).

Во время своей работы программа **DiAids** выполняет следующие действия:

- ожидает поступления на проверку файла от **ДИОНИС** в **Директорию сканирования**;
- при поступлении файла вызывает антивирусную программу для проверки этого файла;
- анализирует код завершения работы антивирусной программы и перемещает файл из **Директории сканирования** в одну из поддиректорий в зависимости от значения кода;
- посылает на **ДИОНИС** по протоколу АЕР сообщение, содержащее код, соответствующий результату проверки;
- ждет от **ДИОНИС** подтверждения о получении сообщения и удаляет проверенный файл с компьютера;
- переходит в режим ожидания следующего поступления на проверку.

Для завершения работы программы надо нажать кнопку **Стоп** (становится активной кнопка **Старт**).

### 3.3. Настройка программы DiAids

Для того, чтобы просмотреть (изменить) значения параметров и настроек служит кнопка **Настройка** (Рис. 3-3 и Рис. 3-5).

Окно, выводимое на экран после нажатия кнопки **Настройка** представлено на Рис. 3-5.

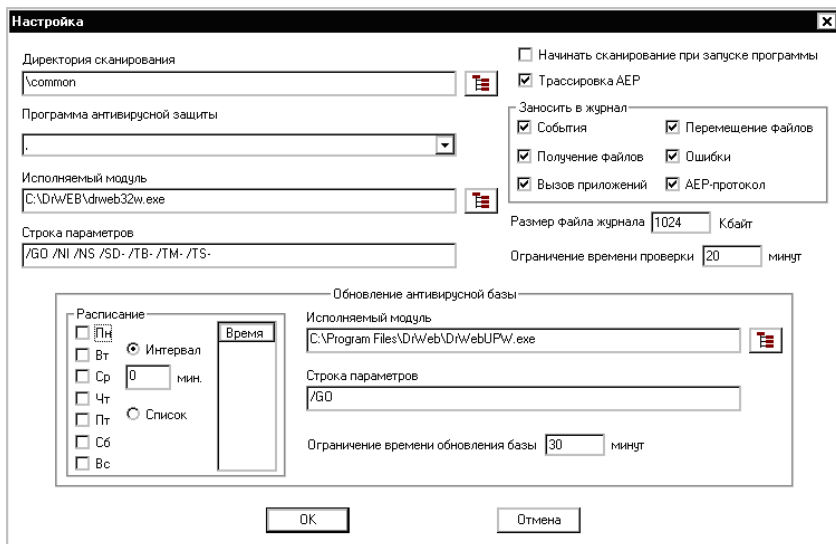



Рис. 3-5

При первом запуске программы для всех настраиваемых параметров устанавливаются стандартные значения, которые администратор имеет возможность изменить по своему усмотрению. *Мы не рекомендуем* менять установленные значения, так как они согласованы с настройкой других компонентов Системы АНТИВИРУСНОЙ ЗАЩИТЫ.

**Директория сканирования** – поле содержит имя директории, предназначенной для обмена данными между программой **DiAids** и антивирусной программой.


Значение поля можно изменить вручную, введя имя директории с клавиатуры, а можно нажать кнопку  справа от поля и выбрать директорию сканирования с помощью выведенного на экран окна.

**Программа антивирусной защиты** - значение поля определяет, какой антивирусный пакет будет использоваться для проверки.

Возможные значения:

- *Доктор Веб* (DOCTOR WEB для WINDOWS)

- 
- *Лаборатория Касперского* (Антивирус Касперского)
  - *Лаборатория Касперского-Дионис* (Антивирус Касперского для ДИОНИС).

**Исполняемый модуль** - поле содержит название файла с исполняемым модулем антивирусной программы (умалчиваемое значение *C:\Program Files\DrWeb\DrWebWCL.exe*). Значение параметра можно изменить вручную, введя имя файла с клавиатуры, или нажать кнопку  справа от значения параметра и выбрать файл с помощью выведенного на экран окна.

**Строка параметров** - поле содержит набор параметров, который используется при запуске антивирусной программы.

**Начинать сканирование при запуске программы** - флажок определяет, в каком состоянии программа **DiAids** начнет работу: если флажок установлен, то после вызова программа будет готова принимать информацию от ДИОНИС и передавать ее на проверку антивирусной программой. Если флажок сброшен, то для перевода программы в рабочее состояние надо нажать кнопку **Старт** (по умолчанию флажок не установлен).

**Трассировка АЕР** – если флажок установлен, то на **DiAids** будет выполняться трассировка прохождения файлов.

**Заносить в журнал.**

Флажки под этим заголовком (**События, Получение файлов для проверки, Вызов приложений, Перемещение файлов, Ошибки, АЕР-протокол**) определяют ту информацию, которая должна быть отражена в журнале. Эта информация дает представление о работе программы, некоторые записи являются служебными и предназначены для разработчиков системы (по умолчанию все флажки установлены).

**Размер файла журнала.** Журнал - это текстовый файл с системным именем **di aids.log** в поддиректории **DI AID S\DI CHECK\LOG**. В журнал заносится информация о работе программы (какая именно, определяется установкой флажков под заголовком **Заносить в журнал**). После того, как файл превысит заданный размер (умалчиваемое значение **1024 Кбайт**), он переименовывается в **di aids1.log**, файл **di aids.log** начинает заполняться снова. Затем **di aids1.log** переименовывается в **di aids2.log**, новый

---

**diaids.log** - в **diaids1.log**. Т.о., текущий журнал хранится в файле **diaids.log**, а в файлах **diaids1.log** и **diaids2.log** - последняя и предпоследняя копии.

**Ограничение времени проверки** – после того, как время проверки файла превысит заданное параметром значение, **DiAids** прервет работу антивирусной программы и отправит на **ДИОНИС** соответствующее сообщение.

**Обновление антивирусной базы.** Выполняется обновление путем обращения на серверы разработчиков антивирусных пакетов.

Поле под заголовком **Расписание** задает расписание, по которому будет выполняться обновление антивирусной базы.

В левой части поля перечислены дни недели, «галочка» в соответствующем окошке указывает те дни, в которые будет выполняться обновление. Время обновления базы в указанные дни можно задать одним из двух способов.


1. Определить временной интервал, через который в течение суток будет выполняться обновление - для этого надо установить значение переключателя **Интервал** и в открывшееся окошко занести значение интервала в минутах - целое число от 0 до 1440 (число минут в сутках).

*Примечание.* Заданный интервал времени начинает отсчитываться от момента нажатия кнопки **ОК** (Рис. 3-5).

2. Составить список значений конкретного времени в течение суток, когда будет выполняться обновление - для этого надо установить значение переключателя **Список**, в открывшемся справа окошке (под заголовком **Время**) перевести курсор на одну из строчек и дважды щелкнуть левой клавишей мыши, после этого занести число в формате **hh:mm** (час:минута). Список может содержать от одного до 8 значений. Заполненные строки не обязательно должны идти подряд, допускается удаление любой промежуточной строки.

*Замечание.* По умолчанию расписание отсутствует. Чтобы выполнялось обновление базы, в окне (Рис. 3-5) должен быть указан хотя бы один день и интервал или хотя бы один день и хотя бы одно значение в поле  
В р е м я .

---

**Исполняемый модуль** - поле содержит название файла, содержащего тот исполняемый модуль, который будет выполнять обновление антивирусной базы. Такие модули входят в комплект поставки соответствующих антивирусных пакетов. Значение параметра можно изменить вручную, введя имя файла с клавиатуры, или нажать кнопку  справа от значения параметра и выбрать файл с помощью выведенного на экран окна.

**Строка параметров** - поле содержит набор параметров, который используется при запуске программного модуля, выполняющего обновление антивирусной базы.

**Ограничение времени обновления базы** – если время обновления базы превысит заданное параметром значение, то обновление будет прервано.

*Внимание!* Для того чтобы сделанные настройки вступили в силу, надо выйти из окна Рис. 3-5 нажатием кнопки **ОК**.

## 4. Подсистема АНТИВИРУС

Подсистема АНТИВИРУС является одним из компонентов программного обеспечения хоста ДИОНИС.

Полное описание программного обеспечения ДИОНИС дано в документе **Телекоммуникационный сервер «DioNIS TS»**

Для вызова подсистемы АНТИВИРУС администратор должен активизировать альтернативу основного меню **Подсистемы** и в меню следующего уровня альтернативу **Антивирус** (Рис. 4-6).

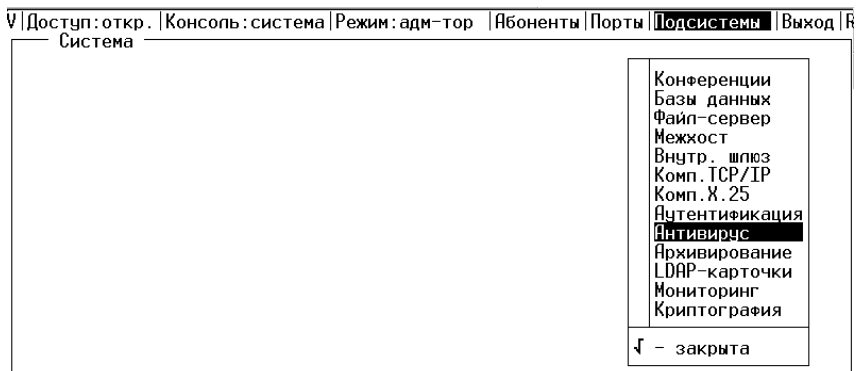


Рис. 4-6

В верхнюю строку экрана будет выведено основное меню подсистемы, содержащее шесть функций:



Рис. 4-7

### 4.1. Функция: Инициализация

Инициализацию необходимо произвести при первом вызове подсистемы. Инициализация заключается в выборе директории, используемой для обмена данными между хостом ДИОНИС и программой **DiAids**.

После активизации функции **Инициализация** включается просмотр файловой системы (Рис. 4-8). Большими буквами представлены директории, маленькими - файлы. Движение по директориям выполняется с помощью клавиш управляющих стрелок и клавиш

<PgUp>, <PgDn>, <Home>, <End>; вход в директорию, на которой установлен курсор, - с помощью клавиши <Enter>; выход из директории - нажатием клавиши <Enter> в момент, когда курсор установлен на строке с двумя точками.

Нажатие клавиш <Alt+F1> обеспечивает переход на другой доступный логический диск. Клавиша <F7> позволяет создать пустую директорию (не выходя из системы в MS-DOS). Нажатие клавиш <Ctrl+L> позволяет посмотреть полный размер текущего диска и размер свободного пространства на нем.

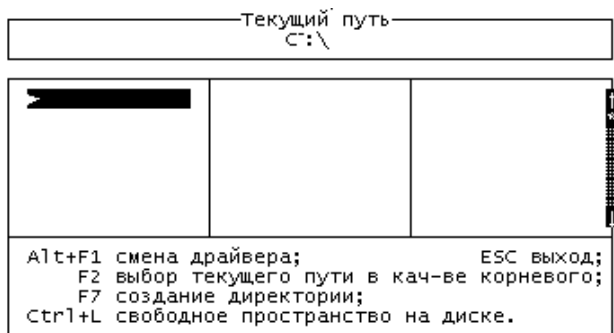


Рис. 4-8

Текущее значение директории отражается в верхней строке меню. Когда в этой строке будет получен искомый корневой путь, надо нажать клавишу <F2>, чтобы зафиксировать найденное значение.

## 4.2. Функция: Конфигурация

При активизации функции **Конфигурация** (Рис. 4-7) на экран выводится меню, представленное на Рис. 4-9.

### 4.2.1. Контролируются

Альтернативы меню под заголовком **Контролируются** позволяют указать элементы, которые будут проверяться антивирусной системой.

**Конференции.** При значении параметра *ДА* будут проверяться помещаемые в конференцию темы, ответы и «подклеенные» файлы, при значении параметра *НЕТ* элементы конференций проверяться не будут.

**Базы данных.** Функция в данной версии **ДИОНИС** не реализована.

Контролируются		Ограничения и возможные проблемы	
Конференции ДА		Максимальный размер очереди 500	
Базы данных нет	→ Индив.	Превышен: заблокировать источники	
Напр./аб-ты ДА	→ Правила	Время ожидания проверки 10	
Уведомление		Истекло : заблокировать источник	
Автора ФАЙЛ		Путь C:\АЕР	
Администр. письмо		Отсутств.: перезагрузить систему	
По списку нет	Список	Подозрение на вирус <b>ОСТАНОВИТЬ</b>	
Адресатов нет		Адрес АЕР-серв.: 192.168.97.2	
	Сканер АЕР	<input type="button" value="Записать"/>	<input type="button" value="Отменить"/>

Рис. 4-9

**Напр. /аб-ты.** Параметр может иметь 4 значения:

- *ДА* - при таком значении параметра будут проверяться все письма и файлы, отправляемые всеми локальными абонентами хоста и приходящие на хост по всем направлениям межхостового обмена;
- *НЕТ* - проверка выполняться не будет;
- *ИНДИВ.* - проверка писем и файлов будет выполняться выборочно для указанных параметром **Индив.** (см. ниже) абонентов (локальных абонентов и межхостовых направлений);
- *ПРАВИЛА* - будет выполняться проверка только тех писем и файлов, которые удовлетворяют заданным правилам (см. ниже параметр **Правила**).

**Индив.** Альтернатива позволяет создать список абонентов (локальных абонентов и межхостовых направлений), для корреспонденции которых будет выполняться антивирусная проверка. Активизация альтернативы приводит к выводу на экран всех групп абонентов, созданных на хосте (Рис. 4-10).

Можно перевести курсор на имя группы и нажать клавишу <Ins> - группа целиком будет занесена в список на антивирусную проверку. Если нажать клавишу <Enter>, на экран будут выведены имена абонентов группы и предоставлена возможность занести в список на антивирусную проверку отдельных абонентов.

После того, как список будет сформирован, в клеточке справа от параметра **Индив**. (Рис. 4-9) появится «галочка».

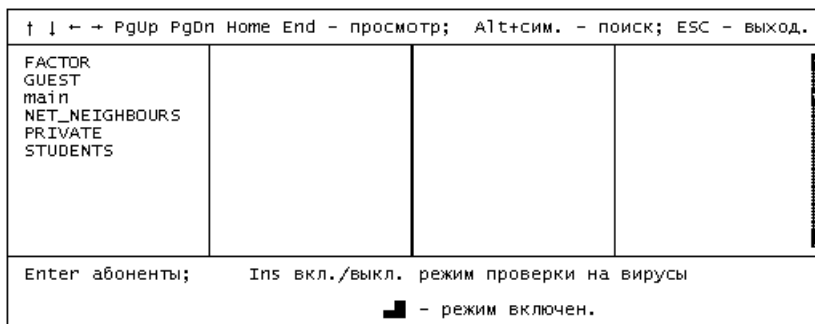


Рис. 4-10

**Правила.** Альтернатива позволяет создать (отредактировать) набор правил (фильтров), по которым будет отбираться корреспонденция для выполнения антивирусной проверки. Активизация альтернативы приводит к выводу на экран набора созданных ранее фильтров, например, такого, как представлено на Рис. 4-11.

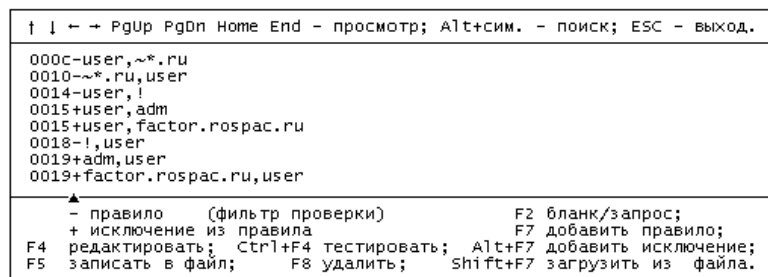


Рис. 4-11

Правила отбора (алгоритм фильтрации) для антивирусной проверки и формат фильтров для антивирусной проверки полностью совпадают с теми, которые применяются в **ДИОНИС** для фильтрации почтовых потоков. Они подробно описаны в документе **Телекоммуникационный сервер «DioNIS TS»**. Руководство администратора, раздел 9.9.3 (издание 2004 г).

## АНТИВИРУС

---

После того, как список фильтров будет сформирован, в клеточке справа от параметра **Правила** (Рис. 4-9) появится «галочка».

### 4.2.2. Уведомление

Альтернативы меню (Рис. 4-9) под заголовком **Уведомление** позволяют указать адресатов, которых **ДИОНИС** будет уведомлять, если антивирусная проверка выявит наличие вирусов в проверенной корреспонденции.

В качестве такого уведомления **ДИОНИС** посылает письмо: в поле заголовка конверта помещаются слова о том, что разосланная информация инфицирована, текстом этого письма служит заголовок конверта «инфицированного» письма. Кроме письма, **ДИОНИС** может отослать сам файл, содержащий вирус, если это задано значением соответствующего параметра (см. ниже).

**Автора** - уведомлять автора «инфицированной» корреспонденции.

**Администратора** - уведомлять абонента с именем **aidsmaster** (или администратора хоста, если такой абонент на хосте не создан).

**По списку** - уведомлять всех абонентов, занесенных в список (см. ниже - параметр **список**).

Эти три параметра могут иметь значения:

- *письмо* - в качестве уведомления посылается письмо;
- *ФАЙЛ* - кроме письма, посылается «инфицированный» файл;
- *нет* - не посылается ничего.

**Адресатов** - уведомлять всех адресатов «инфицированной» корреспонденции. Параметр может иметь значения *Да* - посылается письмо, *Нет* - письмо не посылается.

**Список**. После активизации альтернативы на экран выводится окно, позволяющее ввести адреса абонентов (через пробел), которые будут занесены в список для отсылки уведомлений. После того, как список будет сформирован, в клеточке справа от параметра **Список** (Рис. 4-9) появится «галочка».

### 4.2.3. Сканер

Параметр **Сканер** (Рис. 4-9) может иметь одно из трех значений:

- *АЕР*

- *DrWebNW*
- *DiAids*

В современной версии Системы АНТИВИРУСНОЙ ЗАЩИТЫ параметр **Сканер** должен иметь значение *АЕР*.

Два последних значения используются в предыдущей версии Системы АНТИВИРУСНОЙ ЗАЩИТЫ (см. документ **Система АНТИВИРУСНОЙ ЗАЩИТЫ**, выпуск 2004 г.):

- *DrWebNW* - если **ДИОНИС** работает непосредственно с **DOCTOR WEB** для Novell NetWare;
- *DiAids* – если для передачи файлов на проверку используется сетевой диск.

#### 4.2.4. Адрес АЕР-сервера

В качестве значения параметра **Адрес АЕР-сервера** (Рис. 4-9) должен быть указан IP-адрес программы **DiAids** (той машины, на которой установлена программа).

#### 4.2.5. Ограничения и возможные проблемы

**Максимальный размер очереди.** Параметр позволяет задать максимально возможное число элементов, которые могут находиться в очереди на антивирусную проверку.

Значением параметра может быть любое целое число, включая 0. При нулевом значении параметра размер очереди не ограничен. Умалчиваемое значение 100.

*Замечание.* Мы не рекомендуем устанавливать нулевое значение параметра, так как не ограниченный размер очереди может привести к нарушению функционирования **ДИОНИС**.

**Превышен.** Параметр определяет, что будет делать система, если число элементов в очереди на проверку превысит разрешенное предыдущим параметром значение.

Возможные значения параметра и действия системы:

- *закрыть систему* - хост будет закрыт для входа новых абонентов до тех пор, пока число элементов в очереди не сократится до разрешенного;
- *очистить очередь* - все данные из очереди будут удалены, все поставленные на проверку элементы будут **разблокированы без проверки (!)**;

**АНТИВИРУС**

---

- *заблокировать источники* - абонентам, чья информация находится в очереди на проверку, будет закрыт доступ в систему до тех пор, пока число элементов в очереди не сократится до разрешенного.

**Время ожидания проверки.** Параметр позволяет задать максимально возможное время (в минутах), в течение которого пришедшая на хост информация может ожидать проверки.

Значением параметра может быть любое целое число, включая 0. При нулевом значении параметра время ожидания не ограничено. Умалчиваемое значение 10 мин.

*Замечание.* Мы не рекомендуем устанавливать нулевое значение параметра, так как не ограниченное время ожидания проверки может привести к нарушению функционирования **ДИОНИС**.

**Истекло.** Параметр определяет, что будет делать система, когда для какого-либо элемента истечет разрешенное предыдущим параметром время ожидания.

Возможные значения параметра и действия системы:

- *закрыть систему* - хост будет закрыт для входа новых абонентов до тех пор, пока не будет проверен этот и все остальные элементы, у которых истекло разрешенное время ожидания;
- *удалить из очереди* - элемент, у которого истекло разрешенное время ожидания, будет удален из очереди на проверку и разблокирован (**без проверки!**);
- *заблокировать источник* - источнику рассматриваемого элемента будет закрыт доступ в систему до тех пор, пока элемент не будет проверен.

**Путь.** Параметр позволяет изменить директорию на хосте **ДИОНИС**, в которую помещаются данные для проверки антивирусной программой (изначально параметр имеет значение, заданное при инициализации подсистемы). После активизации альтернативы **Путь** включается просмотр файловой системы. На экран выводится такое же меню, как и при инициализации подсистемы, и предоставляется возможность выбрать директорию.

**Отсутствие.** Параметр определяет, что будет делать система, если окажется, что отсутствует указанная предыдущим параметром директория или отсутствует IP-канал между ДИОНИС и DiAids.

Возможные значения параметра и действия системы:

- *перезагрузить систему* - ДИОНИС корректно закончит работу системы и выполнит перезагрузку хоста;
- *отменить проверку* - антивирусная проверка выполняться не будет;
- *заблокировать источники* - абонентам, чья информация находится в очереди на проверку, будет закрыт доступ в систему.

**Подозрение на вирус.** Параметр определяет, что делать с корреспонденцией, если антивирусная программа диагностировала возможность наличия неизвестного программе вируса. Значения параметра: *пропустить*, *ОСТАНОВИТЬ*. В первом случае (значение *пропустить*) система считает корреспонденцию свободной от вирусов, снимает с нее блокировку и пропускает к адресату; во втором - считает корреспонденцию «инфицированной» и выполняет все действия, заданные настройкой для «инфицированных» файлов.

#### 4.2.6. Записать

Для того чтобы настроенная конфигурация вступила в силу, надо выйти из меню (Рис. 4-9) по команде **Записать**. Перед тем как выполнить команду, система проведет тестирование (см. раздел 4.4, стр. 26). Если какой-либо из тестов не пройдет, конфигурация записана не будет.

### 4.3. Функция: Отладка

При активизации функции **Отладка** (Рис. 4-7) на экран выводится окно, представленное на Рис. 4-12

Функция предназначена для разработчиков системы ДИОНИС. Если у Вас возникают проблемы с работой подсистемы АНТИВИРУС, то установите «звездочки» в обеих правых клеточках и дайте системе поработать некоторое время. После этого пришлите разработчикам фрагмент системного журнала (файл **log.ema**) с момента включения отладки.



Рис. 4-12

#### 4.4. Функция: Тест

Функция **Тест** (Рис. 4-7) служит для проверки работоспособности всей системы антивирусной защиты. Выполнять тестирование надо после того, как будут установлены и настроены все компоненты системы. При активизации функции на экран выводится окно (Рис. 4-13), в котором отражается выполнение отдельных тестов. Тестов всего 5, выполняются они по очереди.

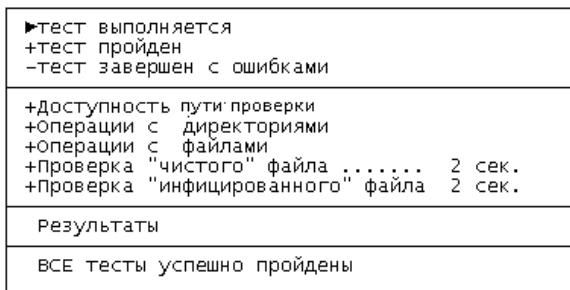


Рис. 4-13

1. **Доступность пути проверки** - проверяется, во-первых, есть ли доступ к директории обмена данными (см. раздел 4.1, стр. 18), и, во-вторых, работоспособность протокола АЕР.
2. **Операции с директориями** - проверяется есть ли у **ДИОНИС** все необходимые права для работы с директориями.
3. **Операции с директориями** - проверяется есть ли у **ДИОНИС** все необходимые права для работы с файлами.
4. **Проверка «чистого» файла** - проверяется, правильно ли Система АНТИВИРУСНОЙ ЗАЩИТЫ выполняет проверку неинфицированного файла.

5. Проверка «чистого» файла - проверяется, правильно ли Система АНТИВИРУСНОЙ ЗАЩИТЫ выполняет проверку файла, имитирующего наличие вируса.

Результат выполнения тестов выводится в нижнее окно. Если какой-либо тест не будет успешно пройден, необходимо проверить настройки и повторить тестирование.

#### 4.5. Функция: Спам

Как было сказано выше, если Система АНТИВИРУСНОЙ ЗАЩИТЫ в качестве антивирусного пакета использует Антивирус Касперского для ДИОНИС, то после проверки почтовой корреспонденции на наличие вирусов система выполнит три дополнительные проверки.

*Обращаем Ваше внимание.* Проверяться будут только те элементы информации, которые назначены к проверке при конфигурации подсистемы АНТИВИРУС (раздел 4.2.1, стр. 19), и только после того как будет выполнена проверка на наличие вирусов и файл окажется «чистым».

Функция основного меню подсистемы (Рис. 4-7) под заголовком **Спам** позволяет установить, как поступит ДИОНИС с «грязным» файлом. Окно на экране после активизации функции **Спам** представлено на Рис. 4-14.

Если все клеточки пустые, то при обнаружении в почтовой корреспонденции SPAM'а, ненормативной лексики или подозрений на SPAM «грязный» файл будет снят с доставки без каких-либо уведомлений адресату или администратору.

*Замечание.* Снятие с доставки будет зафиксировано в системном журнале ДИОНИС – файле LOG\_USER.EMA.

Если в какой-либо клеточке под заголовком **Доставка адресату** поставить «звездочку», то соответствующий файл будет доставлен адресату без дополнительных сообщений. Если поставить «звездочку» в клеточке под заголовком **Отсылка копии администратору**, то копия «грязного» файла будет отправлена администратору.

	Доставка адресату	Отсылка копии администратору
СПАМ		
ненормативная лексика	*	*
подозрение на СПАМ	*	

Рис. 4-14

*Замечание.* Посылать копию файла со СПАМ'ом администратору следует только в каких-то исключительных случаях, например, для проверки работы антивирусного пакета.

## 4.6. Протокол процесса антивирусной проверки

Все события и операции, выполняемые программой в процессе антивирусной проверки (кроме факта успешной проверки элемента информации и отсутствия вирусов), фиксируются в системном журнале - LOG-файле с именем **LOG\_USER.EMA**.

Каждая запись для процесса антивирусной проверки в файле **LOG\_USER.EMA** занимает одну строку и имеет следующий формат

```
ai_oo_exit: Who hh:mm:ss dd-mm-yy Add
```

**ai** - значение кода процесса антивирусной проверки (**PP=ai**);

**oo** - код операции (возможные значения - ниже в таблице);

**exit** - код завершения операции; возможные значения: **OK** - при успешном завершении, **ERR** - при аварийном (код завершения может отсутствовать);

**Who** - имя абонента, при работе которого производится запись в log-файл; если выполняются какие-либо общесистемные действия, то используется имя **DIONIS**;

**hh:mm:ss dd-mm-yy** - время и дата записи в log-файл;

**Add** - дополнительная информация (может отсутствовать).

Операции, коды завершения и дополнительная информация для каждой из операций представлены в таблице.

OO (код)	Операция	Exit (код завершения)		Add (дополнительная информация)
in	проверенный элемент инфицирован	OK		
su	проверенный элемент подозрительен	OK		
pe	потеря доступа к директории обмена	OK		Pt: <путь>
pc	замена директории обмена в конфигурации	OK		Pt: <нов. _путь>
l-	запрещен вход	OK		Pt: <сост.> Qe: <сост.> Tq: <сост.>
l+	разрешен вход	OK		Pt: <сост.> Qe: <сост.> Tq: <сост.>
cl	хост закрыт	OK		Pt: <сост.> Qe: <сост.> Tq: <сост.>
op	хост открыт	OK		Pt: <сост.> Qe: <сост.> Tq: <сост.>
rb	перезагрузка хоста	OK		Pt: <сост.> Qe: <сост.> Tq: <сост.>
of	отмена проверки	OK		Pt: <сост.> Qe: <сост.> Tq: <сост.>
on	возобновление проверки	OK		Pt: <сост.> Qe: <сост.> Tq: <сост.>
cu	элемент «вылечен»			

В этой таблице:

- **первая графа (OO)** содержит код операции;
- **вторая графа (Операция)** - название операции;
- **третья графа (exit)** - значение кода завершения операции (OK или ER);

- **четвертая графа (Add)** может содержать информацию такого вида (символ # означает число):

- путь к директории обмена данными **Pt**:<путь>;
- доступность директории обмена **Pt**:<сост.>, где <сост.> может принимать одно из двух значений: **OK** – путь доступен, **LOST** – путь недоступен;
- количество элементов в очереди **Qe**:<сост.>, где <сост.> может принимать одно из двух значений: **OK** – кол-во элементов в очереди на проверку меньше максимального значения, заданного в конфигурации, **FULL** – очередь переполнилась;
- время ожидания проверки **Tq**:<сост.>, где <сост.> будет иметь значение **OK**, если время ожидания проверки меньше максимального значения, заданного в конфигурации; если время превышено, то значение **hh:mm:ss**, показывающее на сколько превышено;
- если запись в журнал любой из операций делается в условиях какого-либо беспорядка в подсистеме антивируса, то в самый конец этой записи заносится конструкция **Fe:#**, где # - код ошибки в шестнадцатеричном формате (возможна сумма кодов):

**#=0001** - нет доступа к директории обмена данными;

**#=0002** - нет места на диске;

**#=0004** – ошибка инициализации очереди;

**#=0008** – ошибка открытия файла с очередью;

**#=0010** - ошибка чтения файла с очередью;

**#=0020** – отсутствие свободных элементов в очереди.

### Переход директории обмена в нерабочее состояние

При переходе директории обмена по той или иной причине в нерабочее состояние в системном журнале делается запись с кодом **pe**.

Эта запись может быть, например, такой (причина перехода в нерабочее состояние - на диске, на котором размещается директория обмена, кончилось место):

**ai\_pe ER: DIONIS 14:52:41 20-04-98 Pt:N:\DIONIS\AIDS  
Fe:0001**

Несколько **примеров** записей в log-файле **LOG\_USER.EMA** с нашими комментариями. Комментарии выделены курсивом.

<i>Путь проверки недоступен</i> <b>ai_pe_ER: DIONIS 14:52:41 20-04-98 Pt:N:\DIONIS\AIDS Fe:0001</b>
<i>Запрещен вход авторам инфицированной информации</i> <b>ai_l-_OK: DIONIS 14:52:41 20-04-98 Pt:OK Qe:FULL Tq:OK</b> <i>Ситуация нормализовалась, вход разрешен</i> <b>ai_l+_OK: DIONIS 14:52:41 20-04-98 Pt:OK Qe:OK Tq:OK</b>
<i>ДИОНИС закрыт для входа</i> <b>ai_cl_OK: DIONIS 14:52:41 20-04-98 Pt:OK Qe:OK Tq:00:00:01</b> <i>Ситуация нормализовалась, ДИОНИС открыт</i> <b>ai_op_OK: DIONIS 14:52:41 20-04-98 Pt:OK Qe:OK Tq:OK</b>
<i>Будет выполнена перезагрузка ДИОНИС</i> <b>ai_rb_OK: DIONIS 14:52:41 20-04-98 Pt:LOST Qe:OK Tq:OK Fe:0001</b>