ALWIL
SOFTWARE

avast32

The complete antivirus for
Windows 95
Windows NT

Table Of Contents

1.Introduction

Dear customer, we congratulate you for purchasing the antivirus package AVAST32, which is one of the best programs in its category. We hope that you will be satisfied with our product and that you will enjoy the comfort of working with this program.

AVAST32 is a package of applications which aim is to protect your computer from virus infection. Using it correctly and periodically and in coordination with other programs as e.g. data backup utilities, you would be able to reduce radically the risk of your computer being infected by a virus, and thus to avoid losing data.

The aim of this documentation is to make even a less experienced user of computer technology familiar with the control of the AVAST32 program and thus to enable him to make full use of all its functions and properties. However, we do not ignore "highly experienced" users of personal computers either, who will also find the description of operations of individual applications in this documentation.

The documentation has been worked out in a way that the reader will be continually made familiar with the properties and especially the functions of the program as a whole, but also properties and functions of its individual parts. We presuppose good knowledge of basic terms and common skills relating to the environment of operating systems Windows 95 or NT without which some parts of it may seem to be rather incomprehensible. Having known anything about such terms as folder, file, window or not knowing how to activate a window or press a button, we recommend you the studying of the corresponding user's manual or help of the operating system.

In case of any problems or questions relating to the program do not hesitate and contact your dealer or the ALWIL Trade company. Their representatives will be glad and willing to help you.

The staff of the ALWIL Software company wish you pleasant and virus-free work with your computer.

1.1 System requirements

In order to successfully install AVAST32 in your computer and subsequently use without errors, it is necessary that your computer system should meet a few of basic requirements. According to current modern standards they are really minimum:

● processor at least 80386 or fully compatible,

- 8 MB of installed and used **RAM** for operation under the operating system Windows 95 and 16 MB for Windows NT,
- 10 MB of free space on disk for the program itself + 2 MB for installation,
- Windows 95 or Windows NT 3.51 or higher,
- even though AVAST32 may be controlled by keyboard, we recommend to use mouse or any other facility.

It applies generally that the better equipment your computer has, the faster responses from particular applications you would receive.

The work of the AVAST32 program of a computer having less memory than 8 MB has not been tested! The response of the operating system itself on computer like that is so slow that additional load practically makes any other applications impossible. Nevertheless, it is well possible that even on these computers AVAST32 will work, but we recommend it to a really very patient user.

1.2 Installation

AVAST32 is supplied on **CD-ROM** (or on a few diskettes) in compressed form, and hence it cannot be used directly. An installation program creating all works has been developed for its easy installation.

AVAST32 installation is not just copying of all files to your hard drive. The installation makes all necessary changes to your system and sets up automatic launching of resident protection after system reboot ("Resident: full protection" task will be automatically started, see Chapter 2.6)

1.2.1 Before you start installation ...

Work with the installation CD-ROM very carefully and immediately after installation store it in a safe place. If the installation medium is damaged, the program cannot be installed.

If you have the diskette version, then we recommend the creation of a backup copy of the original diskettes as the first step before starting operation. To do so you will need the same number of diskettes of high density (marked as HD). To copy the content of the diskettes we recommend using the DISK-COPY command of the operating system. For further usage use only these newly created diskettes and keep the original diskettes in a safe place.

Before starting the installation be sure that you are really working under the operating systems Microsoft Windows 95 or Microsoft Windows NT. In case you are not working under either of these systems (e.g. you are using Microsoft Windows 3.x featuring Win32s), you would not be able to use neither AVAST32, nor the installation program for its installation. The most probable result of an attempt to start-up will be a "system failure" of your

computer. In this case try to install the AVAST! program.

Furthermore, be sure that there is no preceding version of the AVAST32 program installed in your computer. If there is any, try to uninstall it. The description of uninstallation of a version of AVAST32 is available in its User's Manual or in the Help. Not doing that, the installation program itself will try to uninstall the older version itself. However, we do not recommend this procedure.

To be able to install AVAST32 in the environment of the operating system Windows NT, you must have administrator's rights. If you do not have them, the installation program will advise you of this fact and refuse to install the program! In this case contact the administrator of your network.

If you would like to use AVAST32 help, you have to install **Acrobat Reader** program before you start AVAST32 (It is recommend to do this installation before AVAST32 installation, otherwise you would be warned by installation program that Acrobat Reader is not present on your hard drive. Acrobat Reader installation program AR32E30.EXE can be found on distribution CD-ROM in "ACROWIN" folder. Acrobat Reader installation is similar to AVAST32 installation and it is done automatically except target installation folder question.

It is not recommended to install Acrobat Reader to the same folder as AVAST32. Such a installation would cause conflicts between programs and uninstallation would not work as well. It is recommended to install programs into default folders. AVAST32 can locate Acrobat Reader wherever on your hard drive.

If you met all requirements you could install the product.

1.2.2 Start-up of installation
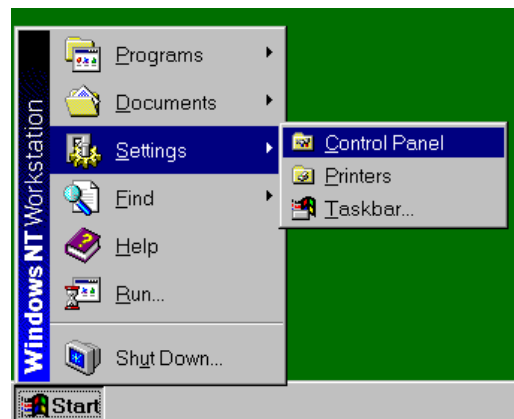
Fig. 1

You can start AVAST32 installation in several ways. The easiest one is to use a tool in your operating system created for this purpose. Firstly, remove all your floppy diskettes and CD-ROMs and insert

installation AVAST32 CD (or first diskette if you have diskette version). Click with left mouse button on Start button, choose Setting and then "Control Panel" (Fig. 1)

Fig. 2

After this a window containing several items would appear. Double click with left mouse button on "Add/Remove Programs" item (Fig. 2).

In the window which opens on the screen of your computer click on the button "Install...". Having done that, click on the button "Next >". The computer will automatically find the installation program, and the only thing to do now is to start-up - click the button "Finish". The installation process itself is described in detail in the next chapter.

More experienced users can also run directly the "Setup.exe" program on the installation CD-ROM or on the first diskette (if you are installing from diskettes). The way of how to run the program is described in detail in the manual or help to the operating system. For normal users we recommend using the first way of the start-up of installation which is described above.

All the ways of the start-up of installation are fully identical and their result will be the same.

1.2.3 Installing

The installation of the AVAST32 program runs in the form of a dialog between the user and installation program. In the following text we will thoroughly describe particular windows which are displayed during the installation.

The installation can be canceled at any time - the way of how to do it is described at the corresponding installation windows. Before the cancelling of installation the user will be asked whether he is serious. After the confirmation of the cancelling of

installation everything which has been installed till that time shall be removed and the system shall be placed in its initial status.

Fig. 3

When you start AVAST32 installation you can choose the language, which you would like to communicate with in the program (Fig. 3). Choosing a specific language from a list, which appears after a click on the arrow to the right form current language, can do the selection.

You will be asked to be patient while the installation is preparing after the language selection.

Once the preparation of the installation is finished, you will see the display of the installation program itself (Fig. 4). The Wizard's window is situated in the center and it will help you with the whole installation process. Its lower part contains three buttons enabling you to communicating with Wizard instructions.
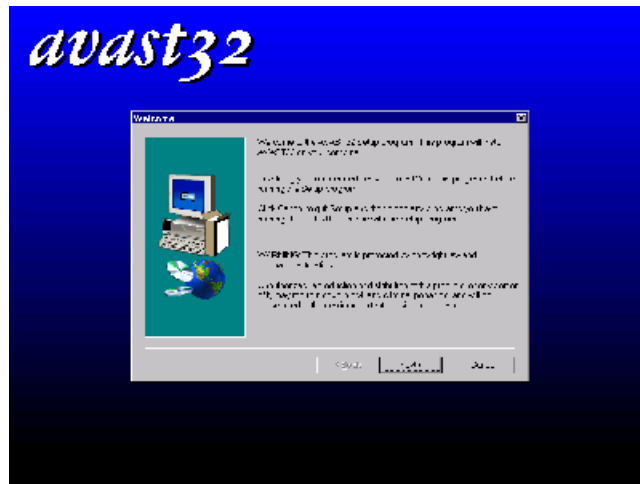
Fig. 4

Button "< Back" takes you to the preceding window of the Wizard. If it cannot be used (e.g. if you are at the first installation step, as in Fig. 4), then the button is gray. Button "Next >" takes you to the next step of the Wizard. Before using it, however, we recommend you reading thoroughly the contents of the Wizard's window. Hitting the "Cancel" button you can interrupt the installation process at any time.

The first window of the Wizard provides the user copyright ownership and warns him from unauthorized usage of the program or its parts. Having read it you would move to the next window of the Wizard by clicking on the "Next >" button.
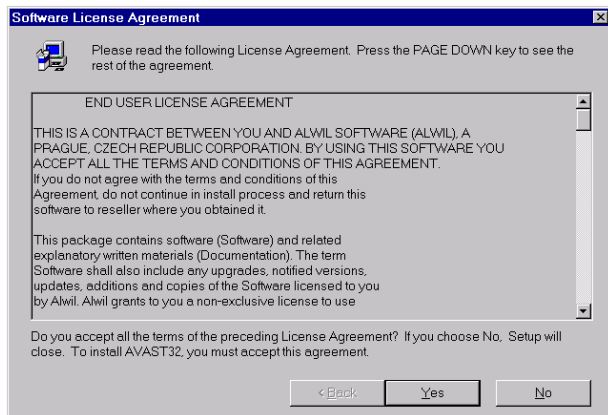
Fig. 5

The next installation program window contains the License Agreement between you and the ALWIL Software company (Fig. 5). This License Agreement includes conditions that you, being a user of AVAST32, must agree with, and the rights which you have as a user of the program. If you agree with the License Agreement and to all of its parts, click on the "Yes" button. Then the Wizard will lead you to the next installation step. If you do not agree with the License Agreement, by clicking on the "No" button you will cancel the installation program and AVAST32 would not be installed then.

As the License Agreement is greater than the Wizard's window, it cannot be displayed as a whole. On the right side of the window you will find a slider enabling move in the License Agreement. Its indicator at the same time shows the current position. To display the remaining parts of the License Agreement it is also possible to use the keys designed for the cursor movement upwards and downwards, or the keys marked as "PgUp" and "PgDn" for the movement to previous or next page of the License Agreement.

The window that follows after the License Agreement window displays the README.TXT file. This file contains important information which we have not managed to insert into this documentation because of time limitations. The information may concern the program itself but also e.g. installation, and it may also contain procedure instructions in case of problems. In any case you should thoroughly read the README.TXT file - thus you will avoid possible complications in the future.

Within the displayed text it is possible to move in the same way as in case of the License Agreement in the previous Wizard's window. Also the window control is similar. If you have read the READ-

ME.TXT file, by clicking on the "Yes" button you will come to the next Wizard's button. The "< Back" button will return you to previous window with the License Agreement and using the "No" button you will cancel the installation of AVAST32.
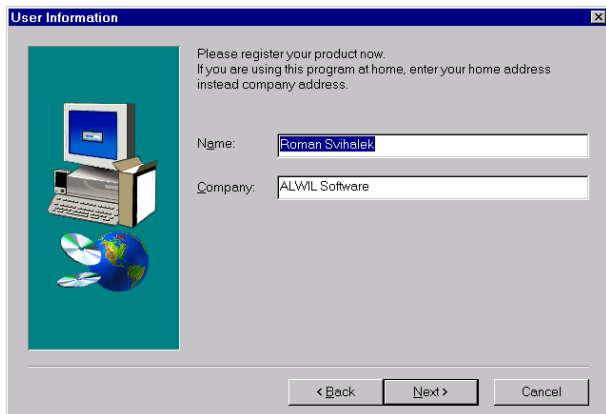
Fig. 6

In the following window (**Fig. 6**) you are required by the Wizard to enter your name and your company's name (possibly also your address if the installation is designated for home use). The Wizard will try to find out required information by itself, so that most of the customers will be able to confirm preset data. If the data does not correspond to reality, it is of course possible to correct it. If you click

with the left button of your mouse to the area of the text box with the data item in question, you will be able to edit it. On the place where you have pressed the mouse button you will see the cursor and using the keyboard you will be able to enter the correct data.

If the data displayed corresponds to the real situation, confirm it by clicking on the "Next >" button and get to the following window of the Wizard. The "< Back" button is used to return to the window with the **README.TXT** file and by using the "Cancel" button it is possible to interrupt the installation.
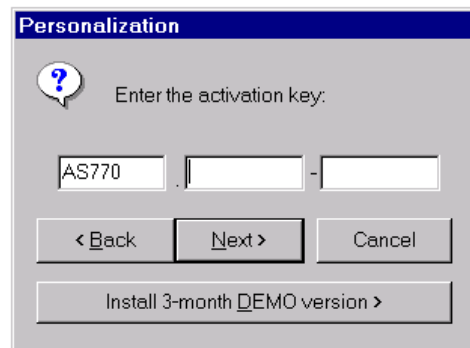
Fig. 7

Fig. 7 shows the Wizard's window into which it is necessary to enter the activation key of your pro-

gram copy. The activation key has this form: **AABBB.CDDDDDD-EEEEEE.** The first part of the serial number (**AABBB**) is already preset by the Wizard, which means that the remaining ones should be entered. The part marked as **CDDDDDD** should be entered into the central text box, and the part marked as **EEEEEE** subsequently into the remaining text box. To enter or change data in a particular text box will be possible for you by clicking the left mouse button on the corresponding box. It is also possible to move to the text box in question by repeating pressing the "Tab" key.

Be careful when typing the activation key. The program can not be installed without a valid key! You can install three month demo version if do not know the key. Just click on "Install 3-months DEMO version >".

Confirm the activation key by pressing "Next >" button, if the key is valid and correctly entered the Wizard let you proceed further. Otherwise you will get error message and you would have to check the activation key. By pressing "< Back" button you can go back to the registration window, where you can change name or company. "Cancel" button quits the installation program.
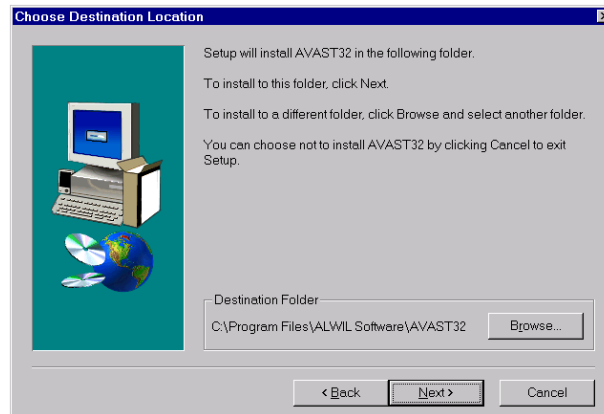
Fig. 8

If the key was entered correctly a window offering change of AVAST32 installation folder would appear (Fig. 8). The folder is in the "Destination Folder" frame. "ALWIL Software\AVAST32" is default folder which would be created on your system disk in "Program files" folder. This is recommended for most users. Others can choose target folder by clicking on the "Browse" button (Fig. 9). Default installation target folder is really recommended for less experienced users. They can avoid possible problems this way.
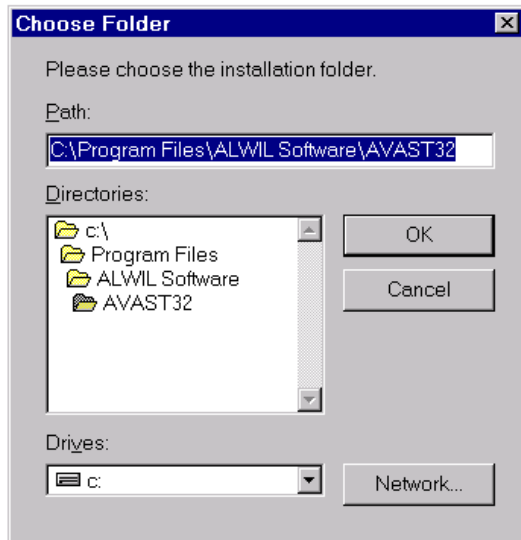
Fig. 9

Fig. 10

The window shown in Fig. 10 appears after window with target installation folder selection. The component list is situated in top part of the window. There you can choose components you would like to install together with AVAST32 e.g. German language support. So you will be able select the language when using AVAST32.
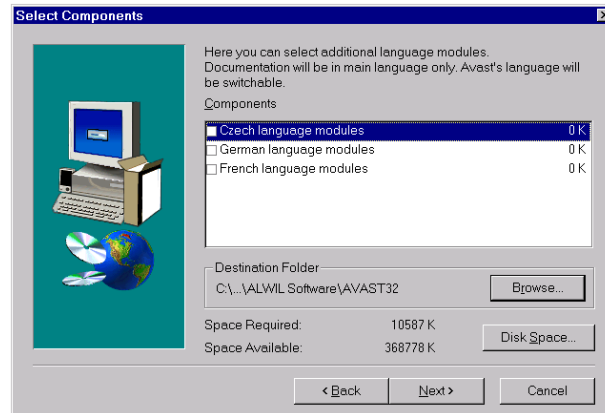
A target installation folder can be changed from this window by clicking on "Browse" button (Fig. 9). The user can see a free space on hard drives as well. You confirm selected components and target installation folder by clicking on "Next >" button.

The following window displays all the information you have entered into the Wizard. It means that it contains the user's name, company's name or the address of the user, activation key of the program copy and destination folder, into which AVAST32 is supposed to be installed. We ask you to check the above listed data and if it is not suitable for you or if these data does not correspond to the real situation, you can return to the previous win-

dows of the Wizard clicking the "< Back" button and correct it as appropriate. If everything is according to your requirements, by clicking on the "Next >" button you can start to install the files of the AVAST32 program onto your hard disk. By means of the "Cancel" button you can interrupt the installation.

An indicator in installation window informs you about amount of copied files. You can break the file installation by clicking on right-bottom button or pressing "F3" key. Once all files are installed installation wizard automatically goes to the next window.

The last window of the Wizard is shown in Fig. 11. It contains the radio buttons by means of which you can specify whether the computer is to be restarted or whether the installation program is to be completed without restarting your computer. We recommend you to keep the default radio button. By clicking on the "End" button you will finish the installation program and depending on the radio button selected your computer will (or will not) be restarted.
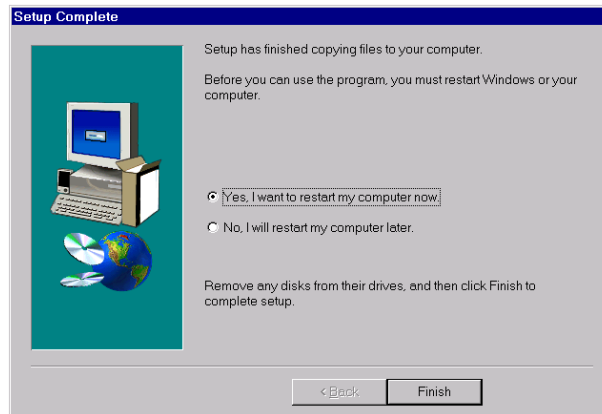
Fig. 11

After the installation of the AVAST32 program and before its first start-up it is necessary to restart your computer. If you did not do so with the help of the Wizard in its last window, you would have to do it later by yourself. In the menu of the "Start" button select the "Shut Down ..." command. Then select the "Restart the computer?" radio button in the window displayed, and by pressing the "Yes" button you will restart your computer.

1.2.4 Problems with installation

The most frequent problems connected with the installation of the AVAST32 program:

- It is not possible to install due to a activation key error. You have entered an incorrect activation key. The activation key is in the format:

    AABBB.CDDDDDD-EEEEEE (described in Annex D). Make sure that it has really been entered correctly. If you are completely sure that it has and that you have not entered the letter "O" instead of zero (and vice versa) and also that you have not entered into any text box a separation period or hyphen (between the text boxes), contact **ALWIL Trade Ltd.** (the adress is on the cover of supplied CD-ROM) and require a check of the activation key.

- AVAST32 cannot be installed because there is not enough space on your hard disk. The only advice applying to this case is: cancel the installation program, empty the necessary space on your hard disk, i.e. empty the recycle bin, delete useless programs, old documents, etc. (we recommend you to make a backup copy of all the things to be deleted, and only then to delete them). For the purpose of a successful installation of the AVAST32 program you will need approximately 10 + 2 MB of free space on the hard disk onto which you want to install the program. Then, when finished, start the installation program again and repeat the installation process.

- program cannot be installed for user without rights (only in Windows NT). It is essential to have administrators rights under Windows NT for AVAST32 installation. Log out and then log in as administrator or contact your network administrator.

If any other installation errors appear it is necessary to make sure whether they are not caused by your own errors or by errors of your system. If you have fully excluded any problem on your side, do not hesitate and contact the technical support. Note, however, all error messages.

1.2.5 Installation from other media

The AVAST32 program can be installed also from any media other than CD-ROM or diskettes. This procedure can be used with an advantage in terms of the speed of installation (which may be rapidly reduced, depending on the type of the medium used) or in the case of installation into the network stations. In this case it is necessary to copy the folders DISK1, DISK2, etc. from the installation CD-ROM onto the medium from which you will perform the installation (should you use diskettes, at first you must create the folders and then copy the distribution diskettes or their copies into them, and when doing so, remember that the first installation diskette is supposed to be copied into the DISK1 folder, etc.), and start the installation from this medium by using the procedure described in the Chapter 1.2.2.

1.2.6 Administrator's installation

The installation program for AVAST32 supports to the limited extent also the "Administrator's installation", which is based on the preparation of the actual client's installation into the shared folder on the file server. The client's installation itself can be done in a fully automatic way without any user's intervention. This way of installation can be used with advantage especially by the administrators of a large number of computers.

The Administrator's installation is created in such a way that the Administrator creates copies of the installation diskettes into the folders DISK1 .. DISKn onto the file server in a similar way as in case of the installations from other media. Then he modifies the values contained in the ADMIN.INI file in the folder DISK1, which has been created, and copies the AVAST32.CNF with the pre-prepared tasks in it. It is necessary to realize that it is not appropriate to use absolute paths to the files (e.g. audible) in the tasks.

If you want to know more information on the Administrator's installation, read the text file **ADMIN.TXT** which is situated on the first installation diskette and contains more detailed information on this type of installation.

1.3 Uninstallation of the program

AVAST32 can be uninstalled from the system at any time. This operation (of course, with the exception of repeated installation) deletes AVAST32 from computer hard disk in an unrecoverable way and places the system to its original status. The uninstallation solves also such problems as the uninstallation of shared libraries and the renewal of internal information in the registers of the operating system.

Individual uninstallation steps are described in following chapters.

1.3.1 Preparation of uninstallation

Before the uninstallation of the AVAST32 program make sure that none of the programs has been run. In other case the uninstallation will not be completed as supposed to be and some rests of AVAST32 will remain on your hard disk, or the uninstallation will not start at all; nor will it be possible to restore the internal data of the system at the end. This may be (and most probably really is) a cause of **SERIOUS** problems in the installation of other versions from the antivirus program AVAST32.

Have a look at the lower part of the screen on task bar. Seeing any of the programs of the AVAST32 system there, cancel it. Press the right button of

your mouse and select the "Close" command for the programs run from AVAST32.

1.3.2 Start-up of uninstalllation

For the start-up of uninstallation we recommend the use of the standard tools implemented into the operating system. You find it in the **"Control panel"** folder called **"Add/Remove Programs"** (it is described in Chapter 1.2.2 how to find and start this tool).

The window of this tool contains in its lower part the list of the installed programs (**Fig. 12**) that support automatic uninstallation (featuring **AVAST32**, of course). If you want to uninstall a program, in our case the AVAST32 program, double-click the left mouse button the name of the appropriate program. Thus you will start the uninstallation process of the AVAST32 program.
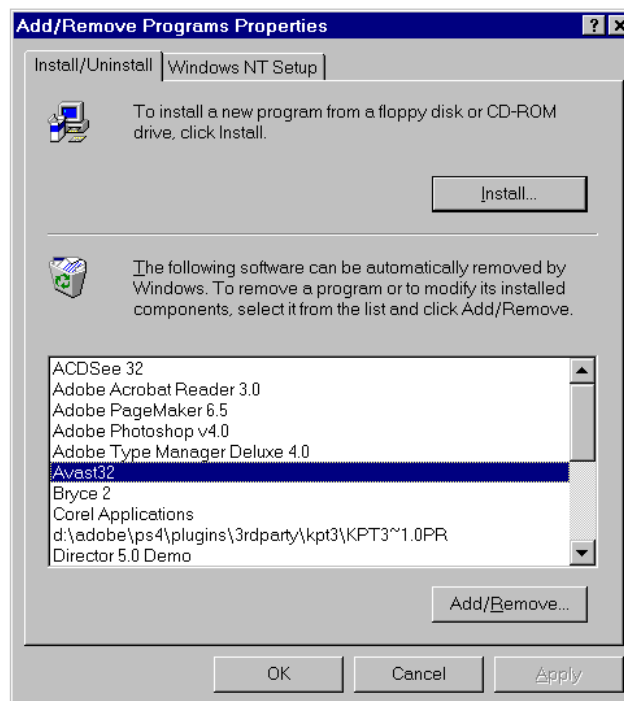
Fig. 12

1.3.3 Uninstallation progress

The uninstallation run itself is fully automatic, except for the primary inquiry, also whether you are serious with the uninstallation. If you answer

"**Yes**", AVAST32 will be uninstalled and the system will be placed in its original status. In case that the uninstallation program is unable to fully uninstall all the parts of the AVAST32 program, this fact will be announced just before the final completion. This situation appears quite frequently, because AVAST32 creates new files during its operation and writes information to the system variables (known as "**register**").

1.4 Use original software

If the protection from viruses is supposed to be effective, it is essential to follow a few principles. Except regular use of the antivirus program, it is necessary to use some of the backup programs, and to keep copies of, at least, the most important data. Data is very often lost even without any contribution from viruses.

Another important principle is to use only original software where is the risk of infection at a minimum. A piracy software package could collect a number of viruses during the time of its travel from the "producer" to your facility and the costs invested into the removal of the consequences caused by the viruses might well exceed several times the price of the original software. Furthermore, using a pirate program you breach the law and expose yourself to possible prosecution.

A paradise for virus is often hidden in various public archives of shareware and freeware you never know who has been handling with. If you decide to use program like that despite this danger, you should at least scan it by antivirus program.

1.4.1 How to recognize original software

No general instructions of how to recognize original software from a pirate copy actually exist, therefore we are only able to give you a few advices. Buy software only at credible sellers, and always have a recept. The proof of software, i.e. license agreement etc. is supposed to be a part of packaging.

Having received anything else, contact reseller. Applies to installation diskettes' labels or CD-ROM covers.

The AVAST32 program is supplied on a **silver CD-ROM** disc where is the logo of AVAST32 printed, and on the data side you will find a hologram with the title "ALWIL". As a special option it is also possible to buy the AVAST32 program on several diskettes. In this case the diskette labels contain the logo of the ALWIL Software company and the name of the program.

Having any doubts according to the legality of your copy contact directly and immediately the ALWIL Trade Ltd. company.

1.5 AVS Service

The field of computer viruses is currently the most dynamic branch in the world of computers, therefore it is necessary to use the latest released versions of antivirus products. This fact means that they must often and by themselves, care for the update of their antivirus program.

In order to make this activity as easy as possible for our customers we have been providing for a long time the antivirus service AVS. Within this service we automatically provide for the period of one year not only the newest databases of viruses, but also all new releases of the program, as well as technical and consultation services.

AVAST32 is updated each month within the AVS service, the internal programs themselves once or twice a year. Additional information may be obtained at your request at ALWIL Trade Ltd. Current releases of the VPS file can are available through our web site.

2.Getting started

2.1 Start of program

You can immediately start using AVAST32 if the installation of the program is succesfully completed. The installation program has created for you an item called "Avast32" in the menu of the "Start" button. By selecting it you can start the program. This item is situated in the menu of the "Start" button (it shall be displayed after clicking on this button by the left button of your mouse), in the folder "Programs". The form of the menu of the "Start" button depends on the presetting of environment of the operating system and on the programs installed so far - one of the possible forms is illustrated in Fig. 13.

If you are working in the environment of operating system Windows NT 3.51, then the installation program has created for you the "AVAST32 antivirus" group, which contains a shortcut to AVAST32. The start-up of the program through this shortcut is fully equivalent to any other way of starting-up the program.
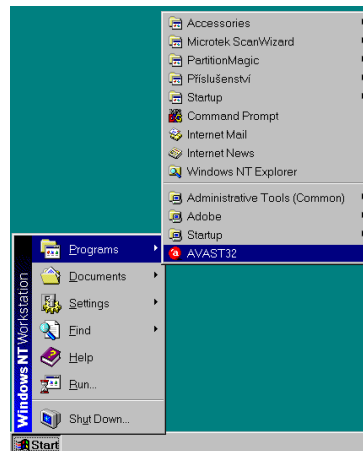
Fig. 13

We recommend you creating a shortcut of the AVAST32 on the desktop of your computer. Doing it you would not have to always pass through the complicated structure of the "Start" button, when you want to start the AVAST32 program. If you want to create this shortcut, start up the "Explorer" - for example by clicking with the right mouse button on the "Start" button, and selecting the "Explore" command from the menu that appears (Fig. 14).
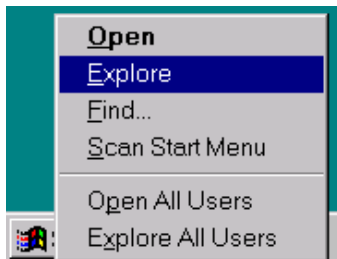
Fig. 14

Select the folder at the "Explorer" where you have installed **AVAST32** (Fig. 15). If you did not change the presetting of the destination folder during the installation, this folder will be

"**Program files\ALWIL Software\Avast32**" on your system disk. Then press the left button of your mouse on the file name "Avast32.exe" and keep it pressed. Now move the mouse pointer over the desktop, i. e. over the area which does not belong to any window, and then release the mouse button.
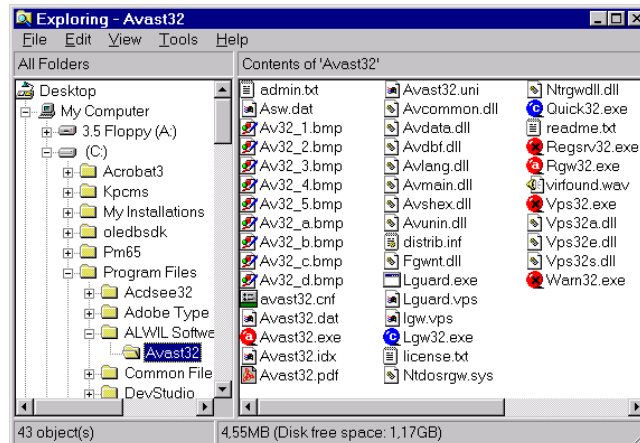
Fig. 15

Having done this operation the shortcut to the **AVAST32** program will be created in the place where you have released the mouse button (Fig. 16). If you press the left button of the mouse on this shortcut twice in a short sequence (double click), the **AVAST32** program will begin.
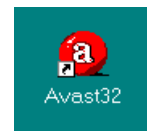
Fig. 16

The AVAST32 program can be started in several ways, all of them being equal to each other. It does not matter at all, whether you have selected the Avast32 item in the menu of the "Start" button, double-clicked on the recently created shortcut on your desktop or double-clicked on the Avast32 item in the "Explorer" program. There are also other possible ways of how to start-up the program, but they will not be object of our interest at the moment.

2.2 How to begin

After the start-up of the AVAST32 program you will see its main window (Fig. 17) which contains a list of items. These items represent the tasks which are accessible at that given moment. After the installation of the AVAST32 program we recommend checking the hard disks of your computer whether they contain a virus. In order to see the changes that were made in particular files, and therefore to discover any new virus, which was unknown until that time, it is necessary to create a database of the files. Both of these two activities will be performed by the task called "Scan+Check: all local disks".
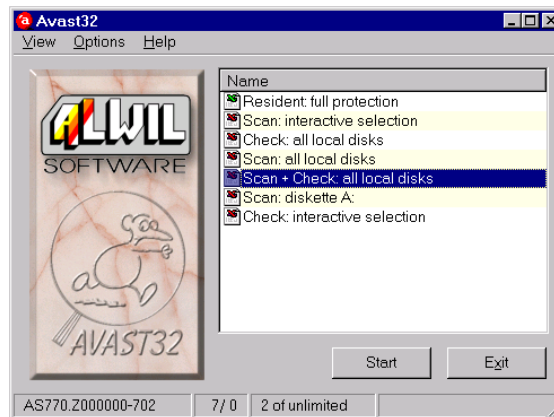
Fig. 17

This task will be started by clicking twice with a short interval on the left button of the mouse (this action is called the "double-click") on its name. If the task has really been started, you would recognize according to the icon situated next to the task name, which should change to the icon illustrated in Fig. 18. If the icon remains unchanged, you probably have not pressed the left button of the mouse fast enough in the sequence.

Fig. 18

The started task "Scan+Check: all local disks" will explore all the folders on your hard disks, and scan all the files found in them for viruses. At the same time it remembers each file which it has located and stores the status in which it is situated on the hard disk. The task will not forget either to check the operating memory of your computer.

If the task does find a virus in a file or in the memory, it will display the warning message (Fig. 19). What to do in this case is described in Annex B. In any case, do not panic, and if you are not sure of your computer skills, it is better for you to leave the removal of the virus found up to someone with more experience. If the task has not found any virus, it will not display any message during the time of its operation.
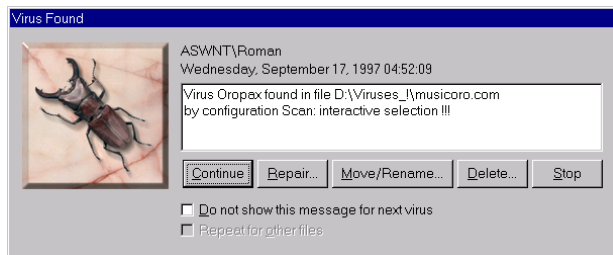
Fig. 19

The duration of the task operation depends on the number and type of the files situated on your

hard disks, and, of course, on the capacity of your computer. It can vary in the range of a few dozen seconds up to a few minutes. Its performance will surely pay in the end, because having enacted it you will find out whether your computer is infected by a virus, and if so, you will also have at your disposal the database of files, with the help of which you can go on to restore the files provided that a virus has entered in your system.
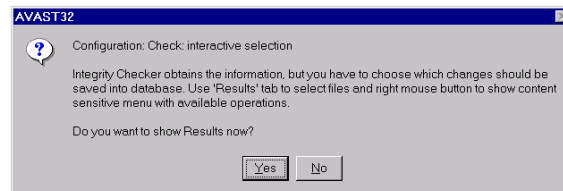
Fig. 20

When task is finished dialog shown in Fig. 20 will appear and the icon would have the previous look (see icons next to the task name in Fig. 17). Press "Yes" button in dialog box and file structure of your hard drive will appear. Now is necessary to fill the file database. So right click on My computer item. A shortcut menu will appear. Select "Accept" command in "File processing" folder (Fig. 21). So you have communicated to the program that it should write the information about all files on the hard drives into the file database.

Fig. 21

Fig. 22
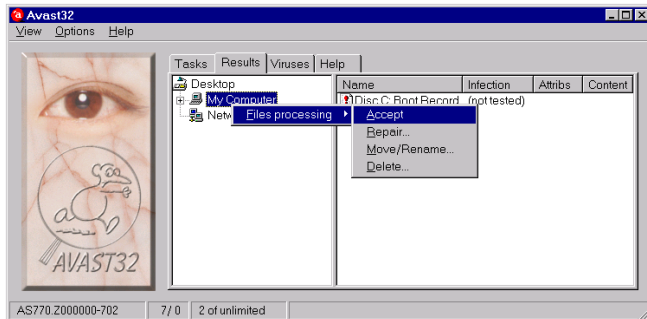
If the window, which remained on the screen after performing the above described actions, is too complicated (that means you are in the "Enhanced user interface" - see Chapters 3.3 and 5) you can switch to the original simple user interface. If you would like to do so select "Simple user interface" from "View" menu (Fig. 22). Thus you will switch back to simple user interface, which is shown in Fig. 17.
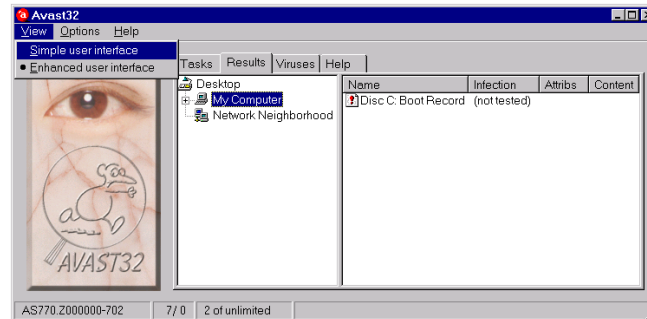
2.3 Are there any viruses?

If you only want to find out whether there are any viruses in your computer, double-click with the left mouse button on the "Scan: all local disks". Thus you will start the task which checks all the files on your hard disks and in the operating memory of your computer. Whether the task is really running or not, you will discover according to the icon situated next to the task name, which should have the appearance as in accordance with Fig. 18.

If AVAST32 finds a virus in a file, each discovery of this type will be announced to the user (Fig. 19, a more detailed description is provided for in Chapter 5.4). If any virus is found, the task ends in the normal way, and the icon situated next to the task

name will again look like the icons in the task names in Fig. 17.
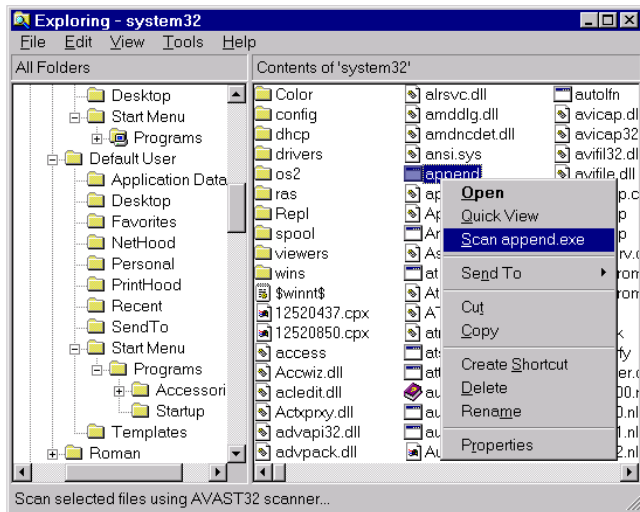
Fig. 23

If you need to find out whether a file is infected, it is not necessary to start the entire AVAST32 program for this purpose. It would be enough for you, in the "Explorer" program, (its start-up is described in Chapter 2.1) move to the folder containing the file in question and press the right button of the mouse on its name. Then select the "Scan <program name> ..." (Fig. 23) in the popup menu which

appears. The file in question will be scaned for viruses. If it contains a virus you will receive a warning message which is shown in Fig. 24 (The message is described in Chapter 10).
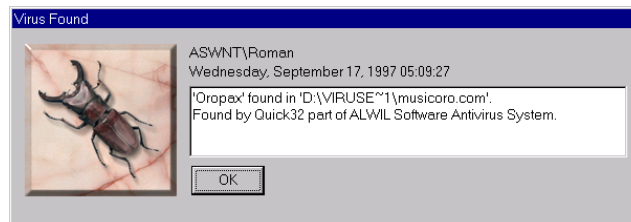
Fig. 24

In the same way it is possible to even scan the entire folders, without having to start-up the whole AVAST32 program. Press again the right button of the mouse on the name of corresponding folder and select the "Scan <folder name>" command from the local menu. If the scaned folder contains some subfolders, then also the files in such subfolders will be scaned.

2.4 How to protect against macroviruses

A serious problems we have been facing recently are "macroviruses". These are viruses that are spreading in form of macros in application docu-

ments, as for example MS Word, MS Excel, etc. Before even opening the document which was even only opened in an unknown computer it is necessary to scan it for the presence of macroviruses.

If you receive a document on a diskette, it is advantageous to start-up the task "Scan: diskette A:", which scans all the documents and files on the diskette, and whether or not they contain a virus. If a virus is found in a document or file, the program will display a warning message (Fig. 19). What to do in this case is described in Annex B.

If you want to check for the presence of viruses only in a certain document, do it using the procedure described above, in Chapter 2.3.

If you need to download the documents, for example from some place in the network and you are not sure whether these documents are "clean" (such an assurance you will practically never have), it is necessary to check these documents as well. Double-click with the left button of the mouse on the name of the task "Scan: interactive selection". After the start-up of the task, which is indicated by a change of the icon situated next to the task name you will see the dialog, in which it is necessary to specify the folder with the files to be scaned (see Chapter 5.5). The dialog as well as its control, is very similar to the standard system dialog for the opening of the files.

2.5 How to detect even an unknown virus

Since the overwhelming majority of viruses somehow change the data situated on the hard disk, it is advisable to check the changes on your disks from time to time. Thus, if you need to find out whether a file situated on your hard disk was changed or not (integrity checking), start the task called "Check: all local disks" (double-click with the left button of the mouse on the task name). After its start-up the task will explore all hard disks and remember each file which it finds, together with the status in which the file in question is situated on the disk.

If a file has been changed, after the completion of the task the program will display a message with the inquiry whether you want to display the results of the task (Fig. 18). After pressing the "Yes" button you will see the structure of your computer with all the files that have been changed since the last check. A more detailed description of the results is provided for in Chapter 5.3.2; the interpretation of the results is dealt with in Chapter 7.

In order that the program can determine which files have been changed and which not, it is to create file's database. How to create the database is described in Chapter 2.2.

Regular data integrity checks of your hard disks is very important, even more important than scanning for viruses. It will protect you from a number of problems, and that is why we recommend you to pay due attention to them.

2.6 How to prevent viruses in the system

In order to protect your computer as much as possible it is better to start the task called "Resident: full protection" (you will again start it by double-clicking with the left mouse button on the task name) even before you start the work to be performed. The task will monitor almost all the activities performed inside your computer. In the case of an attempt to perform a suspicious operation, or if the program finds a virus in the program being run, or in the system area of the inserted diskette, it will display a warning message (it may look like the warning message illustrated in Fig. 25 and Fig. 26). The task, however, will only prevent the virus from its infiltration into the system provided that it is running (the icon illustrated in Fig. 18 is situated next to its name). At the end of its completion, however, the system is no longer protected.

Fig. 25
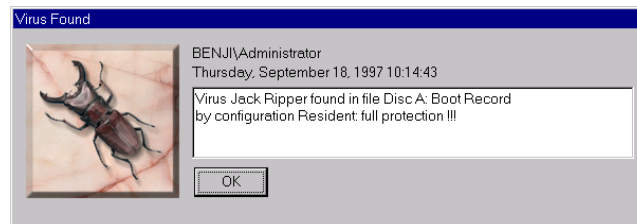
Fig. 26

The task: "Resident: full protection" after AVAST32 installation is automatically started after each system restart, so you do not have to run this task manually. How to disable this option is described in Chapter 2.8 (but it is recommended for most users to have this function enabled!!!).

2.7 Before you start working with an unknown diskette

If the protection of your computer is supposed to be efficient, it is necessary (except regular running of the tasks scaning for viruses, regular updates of the database of the files and regular backup of important data items) to acquire certain habits when working with your computer. One of them is that before you copy into your computer anything from a diskette you cannot be sure about, whether it could have come into contact with a virus or not (it applies to all diskettes which were in any other computer for any length of time), you must test such a diskette for the presence of a virus.

The above described work is provided by the "Scan: diskette A:" task, which will be started in the same way as any other task, i.e. by double-clicking with the left button of the mouse on the task name. The "Scan: diskette A:" will first check the system area of the diskette (called the boot sector), whether there is a virus in it, and then it will scan all the folders of the diskette and scan the files and documents which it will find there. If it contains a virus (and it does not matter whether it is a macrovirus or a virus attacking the programs), the AVAST32 program will display a warning message (Fig. 19), otherwise the task will normally finish its operation.

Another important principle is not to leave the diskette in the drive for a longer time than is necessary. By this you will avoid the accidental booting of the system from any virus-infected diskette and consequently infecting your computer. Most of today's computers provide for the disabling of the possibility to boot the system from any diskette in their SETUPs. Having known nothing about SETUP, contact the Administrator of your network.

2.8 Suggestions for the work with AVAST32

This chapter contains helpful hints about using of AVAST32 program and its components.

Creating shortcut on the desktop
If you periodically run one and the same task, it is possible to create a shortcut to it on the desktop. After double-clicking with the left mouse button on the shortcut the AVAST32 program will start automatically with the appropriate task. It means that it will not be essential to start AVAST32 first and then to start the task in question. The task shortcut on the desktop will be created by clicking the right button of the mouse on the name of corresponding task, and select the "Create Desktop Shortcut" command from the popup menu (Fig. 27).
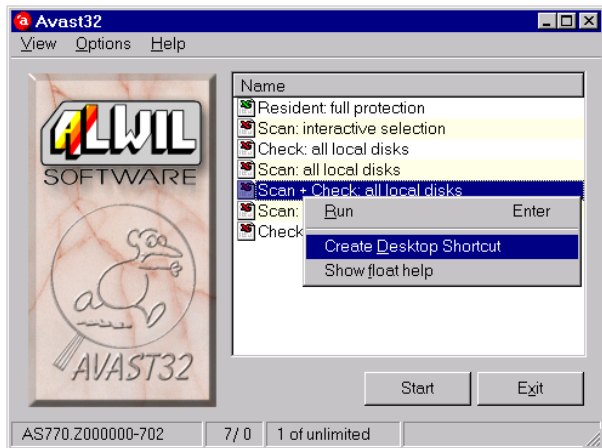
Fig. 27

The shortcut bearing the same name as the task on which you have pressed the right button of the mouse will be created on the desktop. Fig. 29 shows the shortcut to the task "Scan+Check: all local disks".
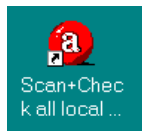
Fig 28

Thanks to the new structure of the AVAST32 you do not have to wait for the start-up of a new task until the running task has been completed. The program is able to process a number of tasks at the same time. The speed of the processed tasks, however, depends on the equipment of your computer.

Screen saver using

Virus scanning is quite demanding on both time and computer equipment, however it is necessary to perform it regularly. So AVAST32 program contains also screen saver, which is capable of scanning viruses on the background of your favorite screen saver. The user is informed about virus scanning progress and of course about virus detection. Detailed information about screen saver can be found in Chapter 12.

If you would like to use it, click on "Start button" in main window. From folder "Settings" choose "Control panel" item and then click on "Display" icon in window which will appear. Dialog box of display setting will be shown. Click on " Screen saver" sheet there (Fig. 29).

If you use Windows 95 choose "AvastSS" item from "Screen saver" list box (Fig.29). Under Windows NT choose "Anti-virus Avast32" from the list.

Fig. 29

To "Wait:" text box write the time in minutes after which screen saver should be activated if there is no user activity (key press, move with mouse and so on).

After pressing "Settings..." button it is possible to set the parameters of screen saver (see Chap-

ter 12.1). If you would like to see how the screen saver will be working click on "Preview" button.

If you are satisfied with screen saver setting, confirm it with "OK" button and next time the screen saver will be started virus scanning will be running too.

Starting the task with operating system

You can let tasks you use immediately after log in start with operating system automatically (like task: "Resident: full protection" in Chapter 2.6). Choose "Enhanced user interface" from "View" menu. Switch to "Tasks" sheet by clicking on its title.

At first make sure that appropriate task is not running or paused. If the task is paused (there is a red ball next to the task name) you have to start it again - click on it with right mouse button and from the menu choose "Continue" item. If the task is running (there is a green ball next to the task name – Fig. 18) it is necessary to stop it - click on it with right mouse button and from the menu choose "Stop" item.

If the program displays a message shown on Fig. 20 when all above described steps are accomplished click on "No" button there.

Fig. 30

simple one again choose Simple user interface from View menu (Fig. 22).
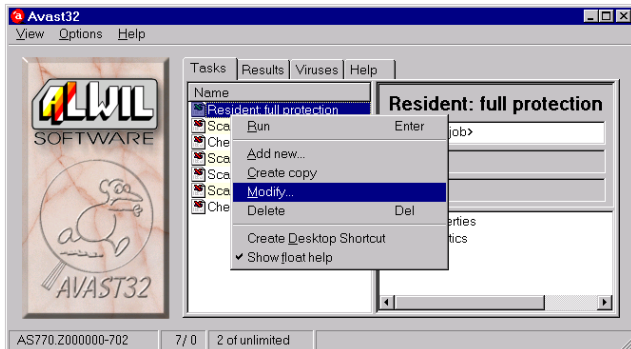
Right click on name of task you would like to have automatically started with operating system and from shortcut menu choose "Modify..." (Fig. 30). A wizard window will appear. It contains Next button, after several clicks on this button you will get to the page with title "Common flags are working for all task variants" (Fig. 45). Check the box "Start the task with Operation system" here and press OK button (further details in Chapter 4.4.6). When you next log in to the system this task will be automatically started.

If you would like to disable this automatic task start, follow the same steps but uncheck that check box.

However the user interface is switched to enhanced interface so if you would like to use the

3.Basic description of program

AVAST32 offers complete antivirus protection of personal computers operated under the operating system Windows 95 or Windows NT. The program allows you to perform tests covering practically all aspects of antivirus protection.

Except today's allready classical program for scanning known viruses, AVAST32 also contains the tools that enable you to find macroviruses and polyform viruses as well, it can even discover the presence of viruses which have been unknown so far.

Thanks to resident tests it is possible to check whether the system did not perform any operations that could be caused by the activity of a virus. The AVAST32 also makes it possible to follow all and any operations that are active within the system, in case of a suspicion, it will block an operation and send a message to the user. It can even scan the files that are being run, and thus prevent the system from virus infection.

The user interface of the AVAST32 program is fully compatible with the environment of the operating systems Windows 95 and NT and it completely follows common standards. That is why the user working in this environment will not have any problems getting familiar with the program.

In order that the users can operate this program comfortably, it contains a wide possibilities of settings, and two user interfaces. The description of the user interfaces is provided for in Chapters 3.3, 3.4, 3.5 and 5.

3.1 Properties and advantages of AVAST32

AVAST32 is an antivirus program designed for the operating systems Microsoft Windows 95 and Microsoft Windows NT. The differences between them under these operating systems are very small and they only result from the different structure of the operating systems, so that the user working with the AVAST32 program under either of these systems will not have any problems with operating this program under the other system.

The main advantage of the AVAST32 program is the quick, and especially, thorough, scanning of your system and all of its parts. The algorithms used, as confirmed by independent tests, are so effective that a virus is recognized in up to one hundred cases out of one hundred! Not only can you test the presence of a virus, but also whether there have

been any changes made in your computer since the last testing. Thus you can discover even a virus which is still unknown! This test is called integrity checking.

It is possible to scan viruses in time when computer is not fully engaged, so when nobody is working on it. Screen saver can do this, which on the background of user selected screen saver scans viruses. AVAST32 screen saver can be fully configured to meet wishes and needs of user similarly to other parts of program. Details about screen saver can be found in Chapter 12.

If a file is infected or damaged and if you maintain the database of the files, you can try to restore using AVAST32. The rate of success when restoring a file is up to ninety-five per cent and the AVAST32 program is able to find out the correctness of the renewal up to one hundred per cent in terms of exactness!

The AVAST32 program is able to make use of the tools of network communication. If a virus has been found, all of the authorized users of the network would be advised in time.This property enables you to reduce the risk of a loss of data very efficiently and so prevent the virus infection from its spreading.

AVAST32 makes use of all the advantages of modern operating systems, as for example long names of files(up to 256 characters), new controls or the possibility to perform several program operations at the same time. The user is not restricted any longer and he can make full use of the time spent at the computer and of its capacities.

User interface of the program can be fully adapted to the needs and skills of the user. Beginners are sure to appreciate the possibility of operating the program without having to learn the details concerning its operation while experts will welcome the possibility of detailed settings of the program activities and its responses to certain events.

To display its help AVAST32 uses the Acrobat Reader program, which is a very good and user-friendly. Nevertheless, the Acrobat Reader program is used in such a way that it seems to be a part of the AVAST32 program. It will enable you to pass through the help system in a very simple way, and thus to move quickly to the part of it, which is the main subject of your interest at that time.

3.2 Basic functions of program

A classical part of the majority of antivirus programs, including AVAST32, is the searching for known viruses (called as virus scanning). The program is to check the tested file for the presence of a certain sequence of bytes, which is then identified as particular viruses.

This way AVAST32 can discover a large number of viruses, but as new viruses appear rapidly and

regularly, it is essential to update the database of known viruses periodically (see Chapter 1.5). AVAST32 is also able to recognize viruses called "polyform viruses" which are able to change their own structure during their activity and thus they are very difficult to recognize. Our product is able to recognize also the macroviruses, which are the viruses spreading out in the form of macros in the OLE documents (e.g. a document of the MS Word application or MS Excel).

A less known way of discovering viruses is represented by integrity checking. This is based on the presumption that at the time when the computer is turned off the virus must be stored in a resident memory. At present the hard disk of the computer is the most frequently used form of such a memory. It implies that if we observe the changes in the files, we will be able to discover even a virus that has been unknown until that time, with the same success as in the case of well-known viruses.

If, for example, a text file (a file with the TXT extension) has been changed, it is possible to say with the probability of ninety-nine per cent that it has not been caused by a virus. However, if a program or even a system file have been changed, the probability of the virus infection is very high.

In order to make possible for the exploration of particular files, it is necessary to maintain information on their status, in which they were for a certain period of time. By comparing the current status of the file with the ones stored in the database it is possible to decide in a reliable way, whether the file has been changed or not. Hence if you perform the integrity checking e.g. every week, the user will be advised of all the changes that have been made in his files during the previous week before the test.

The information on the files, which is stored in the database of the files, can be used by the AVAST32 program, for besides the integrity checking, also for the rerairing of the original status of the files. If you maintain the database of the files periodically, you can attempt to repair your files in case of a virus infection. On basis of the database of the files it is possible to determine with maximum precision whether a file has been repaired successfully or not.

The AVAST32 program also offers the possibility of testing all suspicious operations on the files and system areas of the disks in the system, and to inform the user before they are performed. Then the user will have two options, either to authorize such an operation or to prevent it from being performed. This resident protection is called "Behaviour blocker", and it is based on the fact that the overwhelming majority of viruses perform certain operations with files during their activity, no matter whether or not they infect the files or damage them in a certain way.

It can even happen that a virus is present in the computer, but it may not be infected. For a virus to become active, it is necessary to start it. It implies that the majority of viruses attack the executable files, i.e. especially programs. AVAST32 offers you a resident activity called "Executable and OLE document protector", which performs a test of all programs run in your computer. Thus, if you want to start a program, AVAST32 will first check it, and whether or not it contains any virus. If everything is O.K., the program will normally be started. However, if a virus has been found in the program, you will receive a warning message, and the program will not be started without your authorization.

Another relatively frequent group of viruses is represented by viruses spreading out in the system areas of disks, i.e. in regular in the boot sector of diskettes. To state the truth, a computer cannot be infected if an infected diskette has only been inserted into the drive, but it can happen that the system is accidentally booted from a diskette forgotten in the drive, and thus the computer is likely to be infected. AVAST32 contains a resident activity called "Boot sector Protector", which at the first access to any diskette, first checks its boot sector, whether it does not contain any virus. If a virus is found, the program informs the user about the findings through a warning message. If no virus has been found, it is possible to work normally with the diskette.

3.3 Simple versus enhanced user interface

The AVAST32 program can be controlled in two basic ways that differ from each other essentially by the quantity of their controls, and thus also in the complexity of the control itself. This results in two target groups of users, for which the user interfaces are designed.

The first possible form of the AVAST32 program user interface is illustrated in Fig. 31. This user interface is called "simple", because it contains only the most important controls of the program, and thus it protects users from a large number of the controls with which they usually do not work.

It is possible to perform only the most basic works and operations with the tasks under the Easy user interface.

Fig. 31

The user interface of the AVAST32 program can also take the form illustrated in Fig. 32. The enhanced user interface, as it is called, contains all the controls of the program. Thus, the user can access all the functions and settings which are offered by the AVAST32 program.

In terms of its contents, the enhanced user interface is divided into a few sheets, that contain their own functions and parameters. It is possible to move between sheets by pressing the left button of the mouse on the name of appropriate sheet.
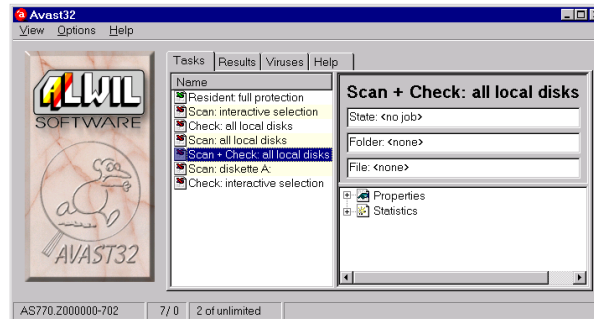
Fig. 32

The used user interface depends on the current program setting, the simple user interface is preset by default. A detailed description of the two user interfaces of the AVAST32 program and the switching between them are provided for in Chapter 5.

3.4 Which user interface should be used?

The division of the AVAST32 program user interface into two groups is inspired by the fact that users working with the program can be divided according to the activities which they perform with the computer. There are experts on the one hand (as for example Network Administrators responsible for the correct setting and operation of a computer network), and normal users on the other side.

A typical normal user basically does not need a large number of parameters - his main requirement is quite often the simplest user interface as possible without having to learn how to set and control another program. For these users we recommend the use of the Simple user interface of the program, because its concept fully complies with those requirements.

On the other hand, Network Administrators and more experienced users will need to preset the activity and behaviour of the program exactly. The Enhanced user interface of the AVAST32 program is designed for them because it makes all functions and controls accessible, and thus it enables the users to adapt the program to their own requirements.

Every user can select the user interface which is most suitable for him, and work in it. The user interface used is "remembered" by the program for each user separately.

3.5 Possibilities of particular user interfaces

Everything that can be done under particular user interfaces is connected with their fields of use.

Simple user interface is designed for a normal user who needs to perform a task (i.e. to test a certain part of the system) without having to deal with the details of the activity and program settings. It is

respected, and thus the simple user interface makes it possible to perform very simply basic operations with the tasks.

Under the Simple user interface it is possible for the user to start the tasks or, alternatively, to interrupt or stop their operations. In case a task has found a virus, the user is advised about it. However, the Simple user interface does not make possible to display details of the results of the tasks, which means that it does not enable the user to find out either, which of the files tested has been infected or changed.

Furthermore, the Simple user interface makes it possible to perform basic functions, such as to close the program, call the program help or to create a shortcut on the desktop. The Simple user interface of course also enables you to turn to the Enhanced one as well.

The purpose of the Enhanced user interface is to make accessible everything what is offered by the AVAST32. Besides basic operations with the tasks, as they were previously mentioned in the case of the Simple user interface, the user can change the parameters of regular tasks or even to delete them. It is of course possible to create new tasks as well.

Users have at their disposal the complete results of all the tasks that have been performed up to that time, and the tools which will enable him to respond to those confirations results. Thus it is pos-

sible to accept the task results or to try to correct the files changed. It is also possible to delete the suspicious or infected files, or to simply rename them and move to any other appropriate folders.

The Enhanced user interface also provides the possibility of setting the environment of regular parts of the program as well as for the AVAST32 program as a whole. Controls that give every user the possibility to adapt the program properties to his own requirements are available. The setting of the program environment also contains the possibility of switching the program user interface to its "simple" mode.

Brief characteristics of viruses are also a part from the current VPS file. The information of its release, as well as on the program version, and information on the owner of the license. This information is important, especially at the moment when it is necessary to contact the technical support.

3.6 Task as a basic element

The basic element with which the AVAST32 program works is the "task". This term means a detailed description of all tests, that will be performed after the start-up of a task. In case of individual tests it is possible to also set afterwards a sequence of parameters which will define the task behaviour with more precision.

Each task must have its name and must contain some tests. The test can be represented, for example, by the scan of files on the hard disk for the presence of viruses, or system monitoring which is performed from time to time. A task can perform even several tests at the same time; e.g. it is possible to test for the presence of a virus and to perform the integrity checking at the same time.

Tasks can be private, shared or read only. Shared tasks can be accessed by all users working on certain computer, in contrast to private ones, which are available only to its owner, to the user who created them. User determines during task creation whether the task will be private or shared. Read only tasks are special type of tasks – they are available to all users, but they can not be modified (these tasks usually comes with the program).

All the tasks that are accessible at a given time, are listed in the task list, which is included in both the Simple and Enhanced user interfaces.

The creation of new tasks is described in detail in Chapter 4.

3.7 Supplied tasks

A part of the installation of the AVAST32 program is also formed by several tasks that have already been created, and that enable the user to use the program immediately after its installation. Par-

ticular tasks will be described in following paragraphs.

All supplied tasks, if there is not said otherwise, are read only, so they can not be modified or deleted.

Task "Scan: all local disks"

The task will scan all the executable files and the OLE documents on all of the local hard disks of the computer in question. In the case that the AVAST32 finds a virus, it will announce this through a warning message and an audible alarm (if the sound card is installed in the computer). The task will announce every virus found. Also the compressed files and operating memory of the computer are to be tested. The system area of each of the disks will be checked as well.

Task "Scan: interactive selection"

The task will completely run the same tests for the presence of viruses as the previous task, but before the test itself the user will have the possibility to select which areas are to be tested. It is of course possible to select several areas at the same time (see Chapter 5.5).

At the selected folders it is possible to determine whether you also wish to scan the subfolders.

Task "Scan: diskette A:"

This task performs the same test as the two previous tasks, but they are done on the diskette in the drive A:. We recommend running this task for all potentially infected diskettes. In particular it concerns the diskettes which were used in other computers or by other users. Also the system area, i.e. the boot sector, will be scaned on a diskette.

If you get used to scanning every diskette which is not your own before its use, you will intensivelly reduce the risk of your computer being infected.

Task "Check: all local disks"

The task will check whether some executable files and OLE documents situated on all local hard disks have been changed since the time of the last check. The contents of the files will only be checked if a parameter has been changed since the last check, e.g. such as attributes, size of the file, etc. The results will be recorded in a well-arranged tree control (see Chapter 5.3.2). The task will also check whether a change in the system areas of the disks checked appeared since the last check.

According to text above, the changes in the files can only be checked between two integrity checking. The result of the first run of the task will be the message that all the files on the disk check "have been added". Therefore it is necessary to record the status of the files onto an internal database, so that

in the case of the next integrity check it will be possible to compare the current status of the files with the previous ones. It is described in Chapter 2.2 how to create the database of the files.

Task "Check: interactive selection"

The task will perform the same test as the previous one, but it will ask the user for the areas to be checked. The areas to be tested are selected through the dialog described in Chapter 5.5. Also in the case of this test it applies that if the results are to be usable, it is necessary to fill the database of the files first.

Task "Resident: full protection"

The protection performed by this task is based on two facts. If a virus is about to infect the computer, it must be run first (i.e. the control must be passed to it), and therefore it is advantageous to scan all the executable files and all the boot sectors of the diskettes inserted. The other presumption is that the virus is performing an activity in the computer: it writes into a file to be run, into the boot sector of diskettes or it even tries to re-format a certain part of the disk.

All of the above described activities are checked by this task, and in the case of an attempt to perform a potentially dangerous operation it first inquires of the user, whether such an operation can be performed. Without his authorization it will not be possible to perform that operation.

We recommend you to start this task always after the start-up of the operating system or, which is even better, to preset its automatic start jointly with the start-up of the operating system, or to place its shortcut in the "Programs\Startup" folder. If this task and its protections are to be effective, you must let it run!

"Resident: full protection" task is shared.

Task "Scan+Check: all local disks"

This task is a combination of the tasks "Scan: all local disks" and "Check: all local disks". If you need to run both of the tasks, it is faster (also from the operational point of view) to start the task "Scan+Check: all local disks". What has been written about the two tasks mentioned above applies also to this one.

Special tasks

They are tasks of special meaning in AVAST32 program. There are tasks: "Quick32" (see Chapter 10.1) and "Screen saver" (see Chapter 12.1).

All special tasks are private and accessible only via "Control panels" (see Chapter 6.7).

3.8 Basic description of program control

The user interface of AVAST32 has been designed in accordance with generally used standards in this area as much as possible. That is why only the standard controls of the system are used.

In principle, the program can be controlled in two ways; by a keyboard or a mouse. For the purpose of faster work with the program we recommend the use of mouse for its control, and the use of a keyboard only for entering texts. A detailed description of the use of mouse and keyboard is provided for in the manual or in the Help of the operating system.

In the following text the term "active item" will identify the item which is highlighted in a certain way. In Fig. 31, for example, the "Start" button is active, whilst in Fig. 32 the task "Scan+Check: all local disks" is active. The color of the highlighting of an item depends on the current setting of the environment in your operating system (folder "Control panel", item "Display").

The program is controlled through the control elements. One of the most important elements is represented by the property sheet, which is illustrated in Fig. 33. It always contains several sheets with various contents and function, when at any given moment only one sheet is visible. Any sheet can be made visible by clicking with the left button of the mouse on the name of the sheet in question.

Fig. 33

With help of the keyboard you may move along regular sheets by the activation of the property sheet and by using the right and left cursor keys. This way you activate the sheet on the left or on the right.

Another very important control element is called the tree control. It represents a hierarchically composed structure which can have arbitrary content. It can concern, for example, a tree structure of the folders stored on a disk (the tree is used by the "Explorer" program in this way), or the information on current status (Fig. 32).

The tree control contains items. If you want to "unpack" an item, click with the left button of the mouse on the icon displayed before the name of the item in question. If you are using a keyboard, you must activate the item first, and then use the left cursor key (to "pack" the item) and right cursor key (to "unpack" the item).

Another element in which the AVAST32 program works as well, is a list. Fig. 31 shows the list of the tasks available, it is, however, obvious that the list is

used also in other places. It can contain several columns, the meaning of which is always described on the first line. The width of the regular columns of the list can be changed arbitrarily. It can be done by pressing the left button of the mouse on the right edge of the column name. Keep the mouse button pressed and by move of the mouse pointer set the required width of the column. Then release the button of the mouse.

One item of the list is highlighted - we say that it is active. For an item to become active, it is necessary to click on it with the left button of the mouse, or to highlight it with the help of keys designed for the cursor movement upwards and downwards. If the list contains too many items, it is possible to move along it also "by pages" with using the "PgUp" and "PgDn" keys.
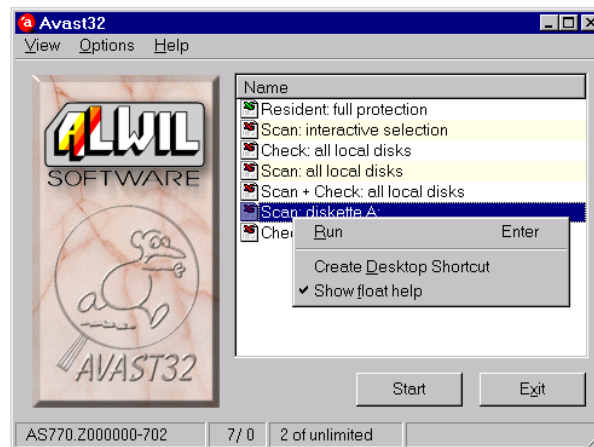
Fig. 34

The right button of the mouse is used in the Microsoft Windows operating systems to call up the popup menu (Fig. 34). The same applies also with the AVAST32 program. The commands of the popup menu are always connected with an item, onto which the right button of the mouse was pressed (in Fig. 34 it is the task "Scan: all local disks") and it contains operations which can be performed with the given element. The command, which you want to start, will be selected by pressing the left button over its name. The popup menu can contain not only the commands, but also their folders, in

which the commands or other subfolders, etc. can be stored again.

The popup menu is used very often to control AVAST32, and therefore, in regular in the case of beginners, we recommend getting used to working with the right button of the mouse, because some parts of the program can be controlled only through the popup menu or with the use of a keyboard.

4.Creation of new tasks

A part of the installation of AVAST32 features also several pre-created tasks (Chapter 3.7), which enable you to use the program immediately after its installation and to make use of the majority of its functions. After a certain period of time, however, most users will require the creation of their own tasks which will simply comply with their own requirements and needs.

Fig. 35

New task can be created via Enhanced user interface only or from "Control Panel" (see Chapter 6.7). If you use Simple interface choose "Enhanced user interface" from "View" menu. Switch to "Tasks" page and right click on tasks list here. Choose "Add new..." from shortcut menu (Fig. 35).

If you would like to change or create new task and you are not running AVAST32 you can do this via "Control Panel". For details see Chapter 6.7.

A detailed description of the procedure for the creation of new tasks you will find only in this Chapter. Not only we will list the description of regular controls, but we will also mention the recommendations that should be observed especially by less experienced users of personal computers.

4.1 Private or shared?

Before creating the proper task, the user should think over the purpose to which the new task is to be used and who will use it. Some tasks should be available for all users of a regular computer system; e.g. the testing of a diskette in the drive A:, or the test of the system as a whole. On the other hand, some tasks can be available for one user only. As for an example it is possible to mention the testing of private documents and applications.

Such a division of tasks is very convenient, because it leads to avoiding the re-creation of entirely

identical tasks individually for each user, and at the same time it is possible for the user to create his own tasks according to his requirements.

The tasks available for all the users of the system are called "shared tasks". These are the tasks that appear in the list of all users' tasks. Their services can be utilized by all the users. The shared tasks are marked with an icon in the task list. This icon is illustrated in Fig. 36.

Fig. 36

One user should create shared tasks if there are more people using one computer. In most cases network administrator does it. A possibility of password protection is related to this. The users without a valid password can just run, stop or make a private copy of such a task. For modifying a valid password will be required (see Chapter 6.1.2).

As "private" we identify those tasks which are available only for the user who created them. Such tasks will not appear in the list of other users either, which means that none of the other users are allowed to perform any operations with those tasks. The private tasks have their icons, see Fig. 37, which is situated next to their name in the task list.

Fig. 37

Whether a new task is to be shared or private, it will be determined by the user at the time of its creating (see Chapter 4.4.1). Later it is possible to modify this presetting at any time (of course, in case of shared tasks and active protection knowledge of the password is essential).

4.2 With or without the Wizard?

The user interface of AVAST32 has been designed with respect to all the users who will work with it. As we have already mentioned, it is possible to work with the program in its simple or enhanced user interface. The main purpose of the division of the user interface is to help normal users with the control of the programs and not to bother them with excessive details and, on the other hand to make the complete control and its presetting possible for experts.

The same also applies to the creating of a new task, when it is possible to use the Wizard or classical property sheet. The main difference between the two control systems for the creation of a new task is based in particular on different approaches by the user. While in the case of your using the

Wizard's services the program itself operates in fact as an assistant for you, the bookmark list is only a tool for the creation of a new task. Nevertheless, the controls are identical in both of the control systems.

When creating a new task, the Wizard can be activated through the check box "Use Wizard to create new task definiton" on the "Basic" sheet in "Options/Main console ..." menu (see Chapter 6.1.1).

If the user uses the Wizard (Fig. 38), he is led by the program when creating a new task. He gradually passes through the entire process of the task creation, sheet by sheet, and he is setting the controls on regular sheets. The user can move to the next sheet at any time when he is satisfied with the settings. He can also move to the following sheet or return to the previous sheet by using the "Next >>" and "<< Back" buttons. It is also possible to cancel the creation of the new task at any time using the "Cancel" button or the "Esc" key. The task can also be created only on the basis of the preset parameters by the "OK" button. In this case the default values will be used for the parameters which are not preset.

We recommend the use of the Wizard especially for the users who are only learning to work with the AVAST32. Its usage is easy, and it practically excludes any failure in respect to some important parameter. In this way the user can learn particular options of settings as well as their layout on individual sheets.
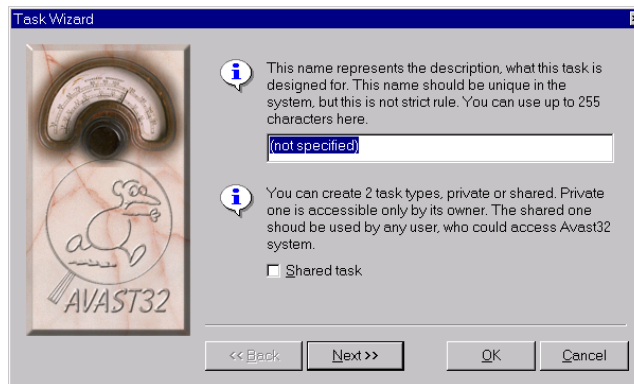
Fig. 38

If the use of the Wizard is turned off, all of the sheets available would be situated in the classical property sheet (Fig. 39), which use is described in Chapter 3.8. This enables the user to move directly to the sheet containing the necessary controls without having to go through all the previous sheets. In the same way as in the case of using the Wizard, it is possible to cancel the creation of a task by using the "Cancel" button or, alternatively, to ask for the creation of a task by using the values preset using

the "OK" button when the parameters which have not been entered will be defined by default.

The property sheet is likely to be used by more experienced users, because of its faster service. The user will only set what he needs, and then he can directly go on to creating a new task (this way of work is not, however, recommended for less-experienced users). The property sheet is convenient in particular for the modification of the parameters of a task which already exists.
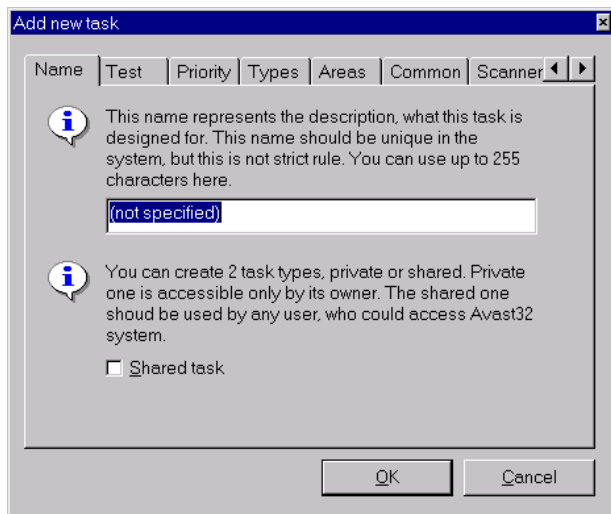
Fig. 39

Using Wizard for creating or modifying tasks is set by default.

The modification of the parameters of existing tasks is made in the same environment as the creation of new tasks. It implies that all what has been written about the creation of new tasks applies to their changes as well. The only difference is that, if you press the "Cancel" button when modifying the task parameters, the values of all parameters will be left unchanged, and of course, the task itself continues to exist as well.

A Wizard for task modification can be enabled by checking "Use wizard to edit existing task definition" check box on "Basic" sheet in "Options/Main console ..." menu (see Chapter 6.1.1).

4.3 What does the task contain?

A task is the basic element with which the AVAST32 works. Every task has its name and contains a detailed description of all its tests and their properties, which would be performed at its start-up. It also contains information on its priority, respectively.

The tests which can be performed by a task, are basically three: virus scanning, integrity checking and various resident tests. The above listed basic tests can generally be divided into subgroups, but in principle it is not essential. Each of the tests listed can be preset exactly according to the user's needs.

Furthermore, it is possible to combine the above tests almost arbitrarily, what eventually means the accelerating of the overall testing processes. If you for example preset the virus scanning, and at the same time integrity checking, the tests will be performed on particular files at the same time, so that it will not be essential to read the files from the disk more times than necessary, etc.

A part of the task is the information about its start-up time. It is possible to preset that the task should be started automatically after the start-up of the operating system, and will thus protect your computer for practically all the time of its activity. This is very practical in case of resident tests, when it is necessary that the computer be "under control" for as long as possible. It is also possible to preset the starting of the tasks with the start-up of the AVAST32 or to leave the starting of the tasks exclusively up to the user.

The task also contains the manner showing how the user will be advised of possible viruses. The AVAST32 enables you to enter the text of an error message, and thus it is also possible to select the type of audible alarm following the message.

4.4 Description of task sheets

The following text deals with the description of individual sheets with controls. Always the description of all the controls situated on the sheet and their defaults are provided for herein. The figures accompanying the use of individual sheets show the same as when the Wizard is being used. When the property sheet is used, the appearance of the window is different, nevertheless the controls and their meanings are the same (see the difference between Fig. 38 and Fig. 39).

It is necessary to mention that the number of currently available sheets depends on the selected activities of the task, and it can often change at the time of its creation. There is a generally valid rule stating that no sheet with the task presettings will be displayed for an test which is not used in the task in question. This rule protects the user from going through excessive sheets that have no influence on the operation of the task.

4.4.1 Sheet "Name"

On the "Name" sheet the program requires that the name of the task being created be entered (Fig. 38 and Fig. 39). It should be as appropriate as possible and, to avoid possible confusion, it should not be identical to any name of the already existing tasks, even if the program is capable to work also with tasks having the same names. If you fail to enter a name, no new task will be created. The text field contains "(not specified)" as a default.

Through the check box called "Shared task" it is possible to preset whether the task is to be shared

or private. The shared tasks can be used by all the users of the computer, unlike the private tasks, which can be used only by their creators. If the box remains to be non-checked, the newly created task will be private, which is also the presetting by default.

The "Name" sheet is present in every version of the created task.

4.4.2 Sheet "Test"
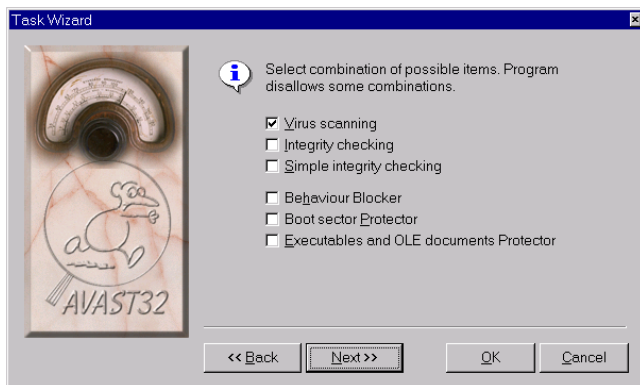
Fig. 40

The "Test" sheet contains the controls through which the proper test of the task is to be defined (Fig. 40). It is possible to preset that the task will perform even more tests at the same time. The pre-setting of the controls on this sheet results in the crucial importance with regard to the number of subsequently available sheets. Having not selected even a single test, you will not be allowed to create any new task.

The "Virus scanning" check box activates the scanning for the presence of known viruses. It means, anyway, that all known viruses will gradually be searched for in each of the selected files and their possible presence will be announced to the user. The search for viruses is activated by default.

The "Integrity checking" check box is used for the activation of data integrity tests. The test will check anyway for each of the selected files and whether it has been changed or not, then in case of its change the test will try to determine the way in which the changes have been made. The box is checked off by default.

The "Simple integrity checking" check box, similarly to the previous box, activates the data integrity test. Unlike the previous one, however, only the simplified checksums of the file contents will be calculated, no file attributes will be tested. It means that the check of the changes in the file will be faster. Simple integrity checking is not activated by default.

The above described tests are called non-resident tests. The following ones belong to the resident tests. Depending on the type of the tests performed we

use the terms resident and non-resident tasks. If there is any non-resident test allowed the task will be non-resident and all resident settings will be ignored. If it is not checked any non-resident test the task will be resident.

The "Integrity checking" box cannot be checked off at the same time with the "Simple integrity checking" box (eventually, it does not make a sense either). If you should check off both the boxes, the AVAST32 will leave checked off only the box which was the last to be checked off. In other words, the AVAST32 will change the checking off so that it can be acceptable.

By checking off the "Behaviour blocker" box the user will activate the resident blocking of suspicious operations for the task in question. It is based on monitoring the system and subsequent the blocking of potentially dangerous operations. It concerns some of the file operations and the operation of the formatting of disks. If the behavour blocker is permitted, the user is advised of each action of this type and asked whether the operation in question should really be performed. This box is checked off by default.

The "Boot sector Protector" check box makes it possible to include among the activities performed by the task also the scanning of the boot sector of the inserted diskette, from which the operating system of the computer is booted. It is called the boot sector. This box is checked off by default.

The "Executables and OLE document Protector" check box activates the check of the programs and documents to be started for the task in question. Every program, which is to be started, will be checked first whether it does not contain any one of the known viruses. If a virus is found, the program will not be started and the user will be advised by means of a warning message. Otherwise the program is started in the normal way. The monitoring of the programs is activated by default.

The "Test" sheet is present at every version of the created task.

4.4.3 Sheet "Priority"

Every non-resident task makes it possible to preset its operation priority. It means that the user will announce to the operating system, how important the task is for him. The higher priority the task has, the more time of the processor it will get, and thus also the faster it will run. It is necessary to realize that the speed of the task operation depends not only on its priority, but also on the current status of the operating system and on the priorities of all the other programs that are currently running. The default value of the task priority is smaller than the priority of the AVAST32 program itself.
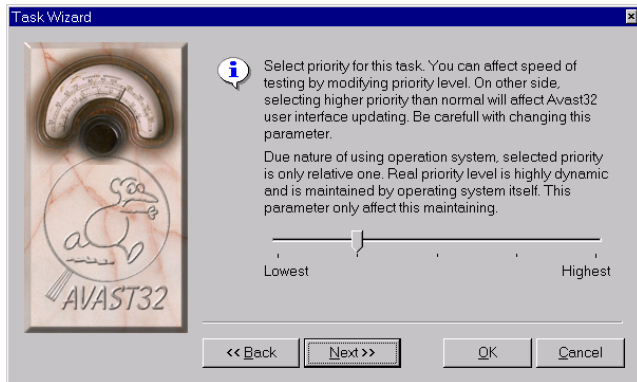
Fig. 41

Only this sheet is used to preset the task priority (Fig. 41). It contains only a slider, through the setting of which it is possible to change the priority of the task. The more to the left the slider indicator is, the lower priority the task has, and vice versa. As it concerns intervention into the operating system task planning, we do recommend the change of the position of the slider indicator only for those users who knows what they are doing. The preset priority will be suitable in the overwhelming majority of cases for the normal user. If the preset priority of a task is too high, it may mean that the restoring of the user's environment of the program will be slowed down. It is not a fault of the program, but only a consequence of the fact that the task has a higher priority than the user interface of the AVAST32.

The "Priority" sheet is present only when the virus scanning or integrity checking, whether normal or simplified, are permitted, i.e. when the task contains non-resident tests.

4.4.4 Sheet "Types"
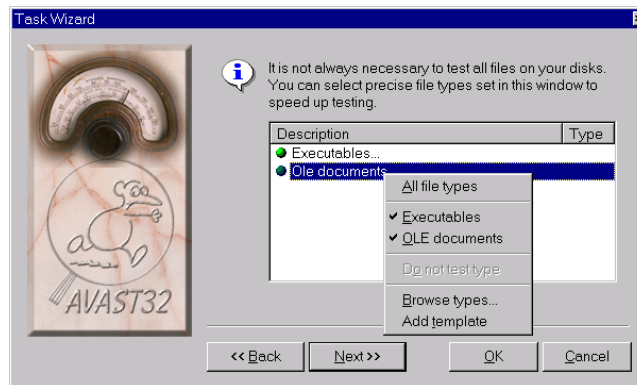
Fig. 42

The "Types" sheet is designed for the determination of the types of files which are to be tested in the areas selected (Fig. 42). In most of cases it is not necessary to test all the files, because viruses attack only some of them. It is for example useless to test the text files (files with the TXT extension), because

even if there was a virus in them, the operating system will not allow it to start the text files, and thus the virus will never become active. By reducing the number of files to be tested you will make the progress of the task faster.

All the types of files to be tested can be seen in the list on this sheet. The list contains a brief description of the type of the files, and possibly also its extension. The file extension can also contain the wildcards, as "*" (asterisk) and "?" (question mark), the meaning of which is the same as in the case of the use in any other place in the operating system.

The adding of another type to the list of the tested types is possible through the popup menu (Fig. 42). It will be displayed after pressing the right button of the mouse on the list of the types. The first three items of the popup menu are the preset types, by the checking off of which the type in question will be placed also to the list of the types. It concerns the following items: "All files types" - the test of all the types selected will be activated, "Executables" - only the executable files will be tested (including the libraries), and the list item "OLE documents" activates the test of the documents created by using OLE technology. If their checking off has been canceled, they are also automatically removed from the list of the types tested.
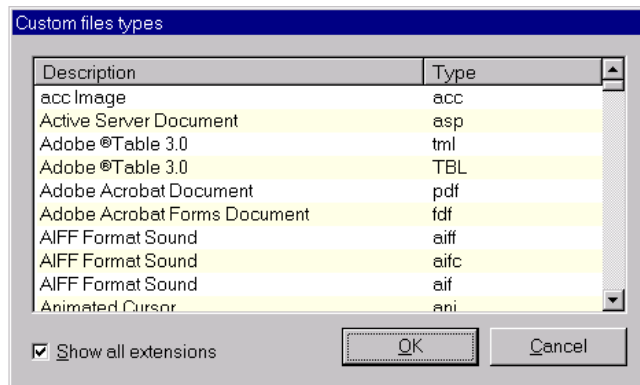
Fig. 43

It is also possible to add the types from the database of known types to the list of the types. This can be done by using the "Browse types ..." command in the popup menu. If it is selected, the dialog containing the database of the known types of files will be displayed (Fig. 43). It can contain either the most important types of the files or, after checking off the "Show all extensions" box, it will contain all the known types of the files. If you want to include a type into the list of the checked types, first make it active, and then press the "OK" button. After pressing the "Cancel" button the dialog will be closed and the list will remain unchanged.

The "Add template" command is used to enter the type of the files selected directly. After selecting

it the user is enabled to write the type extension. After writing it and pressing the "Enter" key the new type is added to the list.

Types entered by user can be changed at any time – after click with left mouse button on appropriate type you will be able to edit it. If you are running Windows NT 3.51 than click with left mouse button on type name.

The icon illustrating how to work with the type is situated next to the name of the checked type of the file:

- files of this type will be tested. This way all the newly added types, including the preselected ones are marked by default,
- files of the type marked this way will not be tested. Thus it is possible to announce to the program that it e.g. should test "All files" **except** for the files of the TXT type, etc. The marking of the type can be performed by checking off the item "Do not test type" in the popup menu. However, it is not possible to exclude the preset types from the tests.

If some of the types are marked as not to be checked in the list, it can result in a slight slowing down of the task. The program will have to check not only whether a file of this type is to be testd, but also whether it should be excluded from the test. On the other hand, by excluding a file type from the test you can also accelerate the task operation considerably. Each particular situation depends on the sample of the files to be tested, nevertheless it is possible to sum up that because of e.g. a test of one file performed uselessly it will not pay to exclude its type from the list of the types to be tested. A file type can be excluded from the list by its selection and pressing the "Del" key or, if it is a preset type (see above), it is possible to cancel its checking off in the popup menu.

Firstly the file type of selected file is tested when the task is running. If the file is listed in the list on this page and is marked with green ball all operations will be performed with it. Otherwise the file will be skipped. The program (executable) files and OLE documents are tested by default.

If the task is to perform the behaviour blocker, only the tests with those files, the type of which is provided for on this sheet, will be checked. The "All files types", "OLE documents" items and the types which are to be excluded from the checks (i.e. types marked with a red ball) will be ignored, which means that their presence in the list has no influence on the behaviour blocker.

The "Types" sheet is present only when the task contains at least one of the following activities: virus scanning, integrity checking (normal or simplified) or behaviour blocker.

4.4.5 Sheet "Areas"

The "Areas" sheet enables the user to preset which disks or folders are to be tested by the newly created task (Fig. 44). Thus it is possible to determine exactly just those areas that are to be checked and accelerate the task operation by excluding the areas, the testing of which is useless.
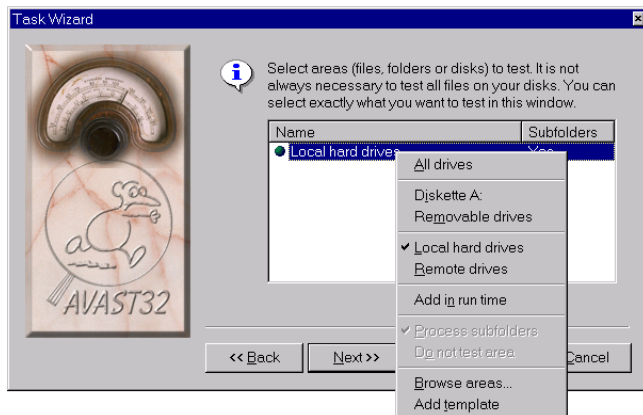
Fig. 44

All the tested areas are displayed in the list on this sheet. It is possible to add an area through the popup menu. It contains the preselected areas "All drives", "Diskette A:", "Removeable drives", "Local hard drives", "Remote drives" and "Add in run time".

The last item means that before the start-up of the task the user will be asked about other areas to be tested together with those specified in the list. By checking off the area in the popup menu it will appear also in the list of the areas to be checked.

By means of the "Proccess subfolders" checking item of the popup menu you can specify whether in a selected area also all the inserted folders are to be tested. If the folder is not checked off, only the files situated in the folder or disk selected will be checked - the folders which are possibly inserted will not be tested. The item can be preset for each of the tested area separately. The testing of the subfolders is enabled by default.

The icon illustrating how to work with the area is situated next to the name of the tested areas:

● the area will be tested. This way all the newly added areas, including the preselected ones are marked by default.

● areas marked this way will not be tested. Thus it is possible to announce to the program that it e.g. should test "Local hard drives" **except** for the folder "C:\Known_viruses", etc. The marking of the type can be made by checking off the item "Do not test area" in the popup menu. However, it is not possible to exclude the preset areas from the tests.

The "Browse areas ..." command of the popup menu enables you to select directly those areas which are to supposed to be tested. Having selected it you will see the standard dialog which enables you to select even more areas at the same time. The areas selected in this dialog will be put into the list.

The "Add template" command is use for entering the area directly from a keyboard. After its entering, the "Edit this file/folder name template in this box..." item will be added to the list of the tested areas, and its editing will be possible. Once you have entered the area, press the "Enter" key. It is also possible to use the wildcards "*" (asterisk) and "?" (question mark) and to specify more folders at the same time.

Areas entered by user can be changed at any time – after click with left mouse button on appropriate area you will be able to edit it. If you are running Windows NT 3.51 than click with left mouse button on area name.

If you want to remove an area from the list, select it with the left button of the mouse first, and then press the "Del" key. Preselected areas can also be removed from the list by canceling their being checked off in the popup menu.

The "Types" sheet is present only when the virus scanning or integrity checking are permitted, whether normal or simplified ones.

4.4.6 Sheet "Common"

The "Common" sheet contains the controls of the parameters which cannot be put on any other sheet because of their nature (Fig. 45).
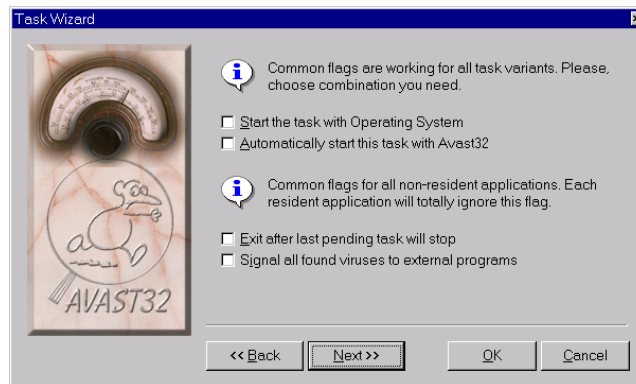

Fig. 45

By checking off the box "Start task with Operating system" the user tells the program that the task being created is going to be started immediately after the user's logging on. This box is not checked off by default. If the task is shared, and the box is checked off, this task will be run for every user of the computer immediately after his logging into the system.

The check box "Automatically start this task with AVAST32" starts the run of the task automatically after the start-up of the AVAST32 program. If the task is shared, it will automatically be run for all the users, otherwise it will be run only for the user who has created the task. The running of the task with the AVAST32 is disabled by default.

The following two check boxes will influence only the non-resident tasks, i.e. the tasks containing the virus scanning or the integrity checking (normal or simplified ones). Their presetting will be ignored by the resident tasks.

The check box "Exit after last pending task will stop" activates the automatic closing of the AVAST32 after the end of the last task running. This possibility can be used especially in the case of the tasks which are started otherwise than directly from the AVAST32, e.g. with help of a shortcut on the desktop. The box is not checked off by default.

The check box "Signal all found the viruses to external programs" provides the user with the possibility to preset, whether the external programs (i.e. programs that are not a part of the AVAST32) should be informed only about the first virus found during the run of a task (the box is not checked off) or about all the viruses found (the box is checked off). By default the box is not checked off. More detailed information on the system of informating the external programs is provided for in Annex F.1.

The sheet "Common" is present at each variant of the task being created.

4.4.7 Sheet "Scanner"

One of the main tests of the AVAST32 program is virus scanning. The "Scanner" sheet (Fig. 46) is used to preset the part of the AVAST32 program, which is only responsible for searching for the viruses.
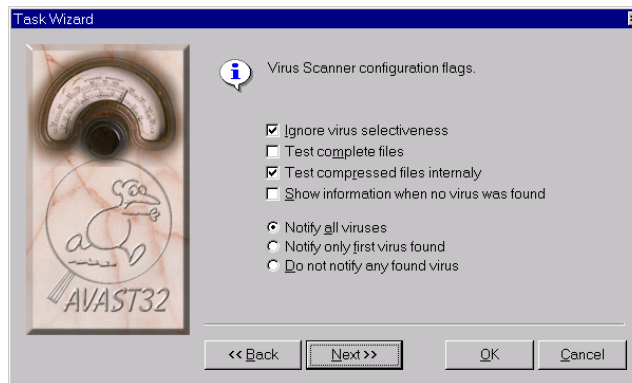

Fig. 46

Through the checking off the box "Test operating memory" the user has a possibility to preset whether the operation memory of the computer is also to be checked at the time of searching for viruses. Thus it is possible to find a virus which has

already infecteded the computer. This test will be done by default.

Under the operating system Windows NT, with respect to its structure the test of the operation memory makes no sense, and therefore if you are working under the system Windows NT, you will not be offered this possibility. Thus the "Scanner" sheet does not contain the check box "Test operating memory" in the operating system Windows NT.

The check box "Ignore virus selectivness" is used to activate the scan of the files for the presence of all viruses in the database. If the box is not checked off, the files are only tested for the presence of viruses that are attacking the file type in question. It means that if the file is of the COM type, it will not be tested for the presence of viruses attacking only the files of the EXE type, etc. By checking off this box you will ensure that the files are tested for the presence of all the viruses, regardless to the type being infected. This box is checked off by default.

The check box "Test complete files" determines, whether the entire files are to be scaned for the presence of viruses. If the box is not checked off, the AVAST32 will scan only some of the file areas. It is convenient in particular from the point of view of the task. The program is based on the fact that the overwhelming majority of viruses infected files adding to the end of the files or rewriting of their beginnings, and thus it is usually useless to test the entire file. This box is checked off by default.

With help of the check box "Test compressed files" it is possible to activate the scan of the compressed files. In fact, compressed files can be attacked in two ways: before the compression and after it. If the file is infected only after the compression, AVAST32 will discover the virus without having to decompress it. In order to make possible even the discovering of a virus which already infected the file before the compression, it is necessary to decompress the file first, and only then to scan it.

After checking off the box AVAST32 will first scan the files that were compressed, and then it will internally decompress the files (the files on the disk will remain compressed), "the resulting" files will be scaned again.

At present the AVAST32 program supports the Diet, Lzexe, Pklite and Ice compression programs. The testing of the compressed files is enabled by default.
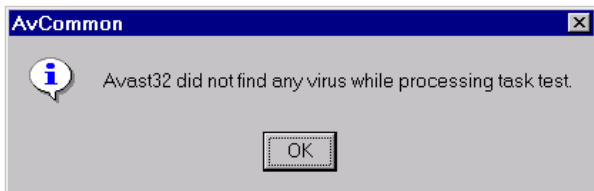
Fig. 47

By checking "Show information when no virus was found" check box AVAST32 will display message when the scan task is done, even if no virus was found (Fig. 47). This is disabled by default.

Furthermore you can decide when you want to be notyfied on viruses found. The choice can be made by selecting one of the following radio buttons:

● the selection of the "Notify all viruses" radio button will cause that the AVAST32 program displays a warning message (see Chapter 5.4) for every virus found, and will wait for the user's response,

● the "Notify only first virus found" radio button will activate the display of the warning message in a similar way as the previous radio button, but only for the first virus found. If the user only needs information on whether his computer is infected or not, he will select this radio button. If it is necessary to find out all the files infected, after the completion of this test, it is sufficient to go through the "Results" sheet of the enhanced user interface,

● the "Do not notify any found virus" is used to suppress the displaying of warning message on the viruses found. If the radio button is selected, the user will not be informed about any of the viruses found. Since there is a danger of over-looking the finding of a virus within the system, we recommend the use of this option only in con-nection with e.g. the report on the finding of a virus after the user logging on (Chapter 6.5.1, check box "Show virus warning message after user logon").

The default setting is to report all the viruses found.

The "Scanner" sheet is only available if the task in question is to virus scanning, it means this test is selected on the "Test" sheet (see Chapter 4.4.2).

4.4.8 Sheet "Checker"

The "Checker" sheet (see Fig. 48) is used for the setting of the parameters of the integrity checking on your disks. Under the term "integrity checking" it is possible to imagine the monitoring of the changes which have been performed on individual files since the last check. Thus the user is enabled to discover the activity of viruses, including the vi-ruses which are still unknown.
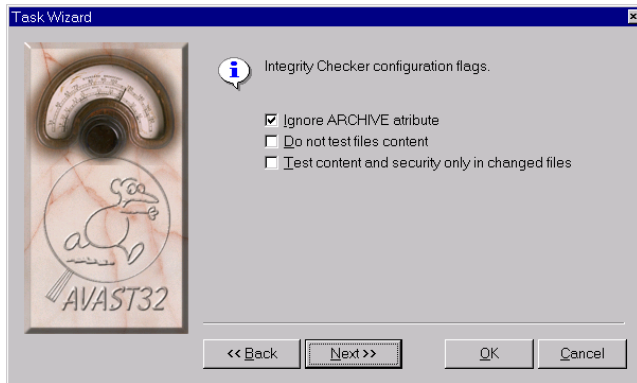
Fig. 48

By checking off the box "Ignore ARCHIVE atribute" you will inform the program that it is about to ignore the change in the ARCHIVE attribute at the checked files. The attribute is used especially by the backup programs to recognize the files which are to be archived. The operating system will set this attribute on any record made into the file.

If the box is checked off, the integrity checker will not report any change of this attribute, which means that the file, in which the ARCHIVE attribute was the only one which has changed since the last check, will not be put on the list of changed files. This box is not checked off by default.

Using the check box "Do not test file contents" it is possible to disable the checking of the change in the file content. The files will be checked only according to their parameters as to the date of the last change, size, attributes, etc., but no checksums of their contents will be created. By checking off this box you will make the task run faster, but for the reason of higher safety of your system we recommend to leave the file content tests enabled. The contents of the files will be tested by default.

Through the check box "Test content and security only in changed files" the user has the possibility to preset that the contents of the files should only be checked if a change in basic properties of the file (attributes, date of the last change, etc.) has appeared. This possibility is based on the presumption that if the file content was changed, also the parameters of the same were changed. By checking off this box it is possible to make the task run faster. This box is not checked off by default.

The "Integrity" sheet is present only in the case that one of the tests to be performed is also in the integrity checking, whether normal or simplified (see Chapter 4.4.2).

4.4.9 Sheet "Continue"

The user can choose a task that will start when the current task is finished in the "Continue" sheet (Fig. 49).
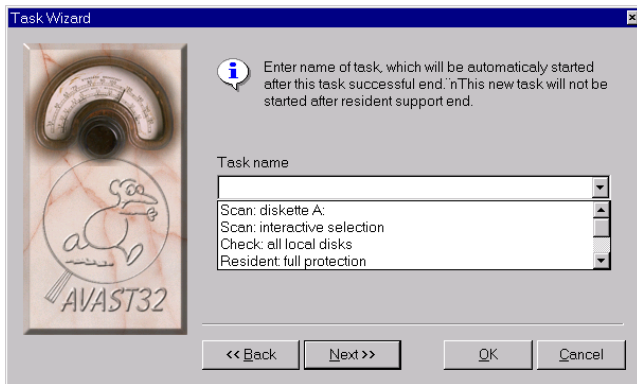
Fig. 49

The name of such a task can be type in the task name box or can be chosen from already created tasks list. If you click on the arrow next to the text box tasks list will appear. Text box contains no text by default.

The sheet "Continue" is available for non-resident tasks only it means that at least one non-resident test must be selected on "Test" sheet.

4.4.10 Sheet "Report"

During the task progress the AVAST32 program can create a file containing a detailed message on its activity and results. The permission to create such a report and the setting of its name is just the object of the "Report" sheet (Fig. 50). The message on the task operation is stored in the form of a pure ASCII text to the selected file (See below). It contains the information on the files that were tested, on the viruses found and other important information, including statistics of tests.
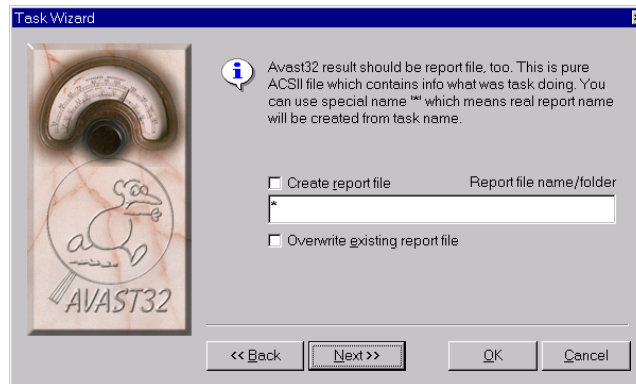
Fig. 50

The check box "Create report file" enables the creating of the file with a report on the task activity. The file with the report will be created by default.

The text box into which it is possible to write the folder and name of the file, to which the report will be recorded, is situated under the previous control element. If the user enters the "*" (asterisk) instead of the name, the file with the report will have the same name as the task, only the file extension will

be RPT. If no extension is specified at the file name, the above mentioned **RPT** extension will be used automatically. The text box contains "*" by default.

The check box "Overwrite existing report file" advises the program that if a file with a report of the given name already exists, it is to be overwritten. If the overwriting is not enabled, and a file with the report already exists, then the report on the activity of this task will be added to the already existing file. The box is not checked off by default.

The "Report" sheet is available only in case that the task contains at least one non-resident activity, i.e. at least the virus scanning or integrity checking.

4.4.11 Sheet "Net alert"

The "Net alert" sheet (Fig. 51) contains the controls designed for the presetting of the parameters of sending warning messages in the network. In case of finding a virus the **AVAST32** provides sending warning message about the possible danger to the computers accessible for the local network in question, and thus prevent from wide spread of the virus.

The check box "Send alert over the network" will activate the sending of a warning message throughout the network. The sending of such messages through the network is not permitted by default.
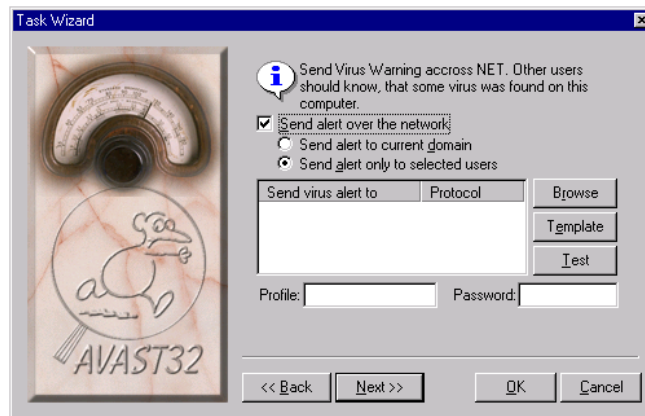
Fig. 51

If you have enabled the sending of a warning message through the network, you must also decide, to which computers the message reporting possible appearence of a virus should be sent. It can be done with help of one of the following radio buttons:
- through the radio button "Send alert to current domain" you will preset the sending of a warning message reporting that a virus has been found to all the computers which will be connected at that given moment to the current domain,
- the radio button "Send alert only to selected users" will result in the fact that the message will be

sent only to the computers which are specified in the list on this sheet.

The sending of a warning message only to the selected computers is preset by default.

If the sending of a message through the network is permitted and if the sending to the selected computers only has been chosen, it is necessary to determine which computers. The list of the computers selected is situated under the above controls.

The name of computer which virus warning should be send to can entered to the list of selected computers. Press "Template" button for protocols shortcut menu:

- "Internet" item determines that computer to which warning message will be send is specified by standard URL address. The SMTP (Internet Mail) protocol will be used for message delivery,
- by "Microsoft" item you tell the program that appropriate computer is available via Microsoft Mail,
- "Internal" item assign that computer for sending virus alert will be available via local network.

After selecting appropriate protocol an item "Edit for valid address or name..." will be added to the list. Right click on the item for edit. When finished press "Enter" key.

Computer names entered by user can be changed at any time – after click with left mouse button on appropriate name you will be able to edit it. If you are running Windows NT 3.51 than click with left mouse button on computer name.

After pressing "Browse" button a shortcut menu with protocols will appear again (in this version "Internal" only). You can choose a computer available via local network from a dialog box shown on Fig. 52. Click on appropriate computer and press "OK" button for adding to the list or press "Cancel" for no changes.
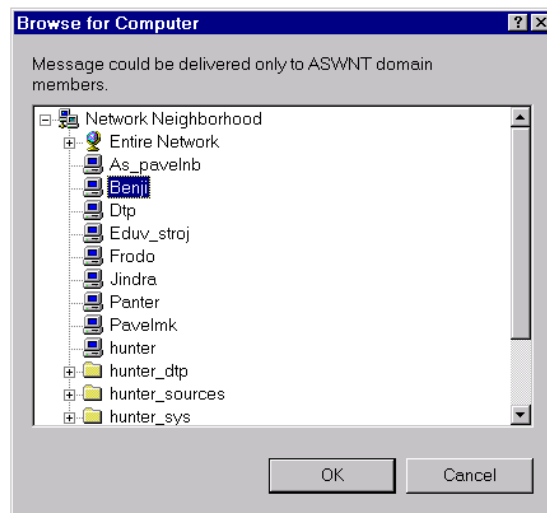

Fig. 52

For deleting the computer from a list press on it and press "Del" key.

You can change parameters of listed computers here. Click on "Protocol" column for protocol change. From shortcut menu choose new protocol. You can change name/address in the similar way, after left click on the name an edit will be allowed.

If you are not sure about the delivery of a warning message, you can test the "connection" by using the "Test" button. A testing message will be send to each of the selected computers.

If you would like to send message via Microsoft Mail or Internet it is necessary to write profile name and its password if necessary into appropriate text box. If you leave "Profile" text box blank (or entered name is invalid) and program will try to send warning message you will be asked to enter valid profile name.

For sending or reading network messages under Windows NT "Alerter" and "Messenger" services must be enabled ("Control panel", "Services" item). I you do not have the required permission contact your system administrator. You need "WinPopup" program enabled for Windows 95 messaging.

A warning message can come to a selected computer several times. It is not a fault of the program, but a matter of the system. The number of the message copies sent depends on the number of the network protocols installed.

The "Net alert" sheet is present at each variant of the task being created.

4.4.12 Sheet "Message"

This sheet is used for editing the text of the message which will be displayed at the finding of a virus (see Fig. 53). If the sending of message through the network is enabled, this message will be sent also to all of the computers selected (see Chapter 4.4.11).
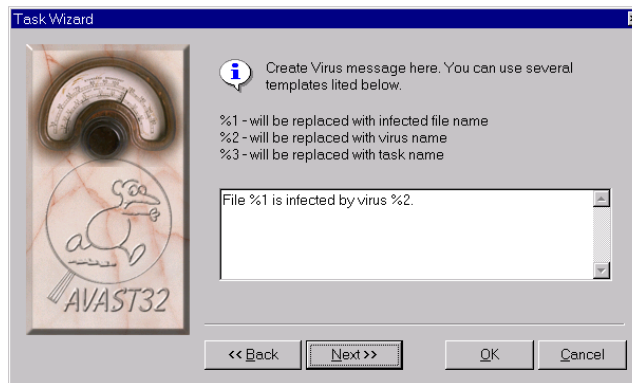

Fig. 53

There is a text box available, which enables the user to enter the proper text of the report. With help of the formatting marks it is possible to enter even variable parameters into it, as the file name, task name, etc. The appropriate formatting mark

will then be replaced with a regular name. The meaning of the formatting marks is as follows:

%1 - infected file name,

%2 - name of the virus which infected the file,

%3 - name of the task which the virus appeared.

If for example the task "Proper" has found the virus "OneHalf" in the "D:\PRG.EXE" file, and the text to be inserted will have the form "Warning! Virus %2 has been found in the file %1. Used task %3.", the resulting message will read: "Warning! Virus OneHalf has been found in the file D:\PRG.EXE. Used task Proper.".

By default the text box contains the message in the form:

File %1 is infected by virus %2.

Sheet "Message" is available if at least one of the following activities is selected: virus scanning, boot sector protector and executables and OLE protector.

4.4.13 Sheet "Sound"

When virus is found AVAST32 can also play a sound file. If you would like to use this feature press "Setup" button on "Sound" sheet (Fig. 54) and choose the sound file in this dialog box (for details see below).
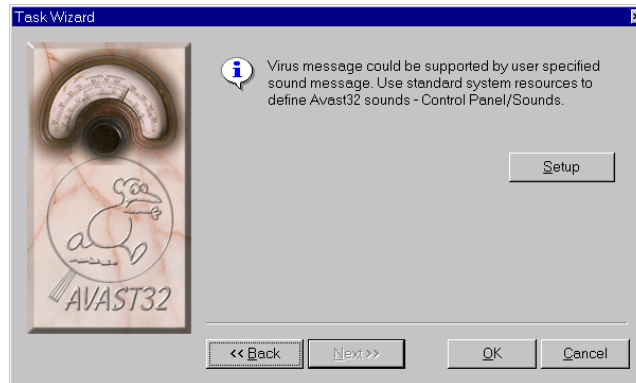
Fig. 54

AVAST32 uses for virus alert sound setup a system Control Panel "Sounds" (Fig. 55).
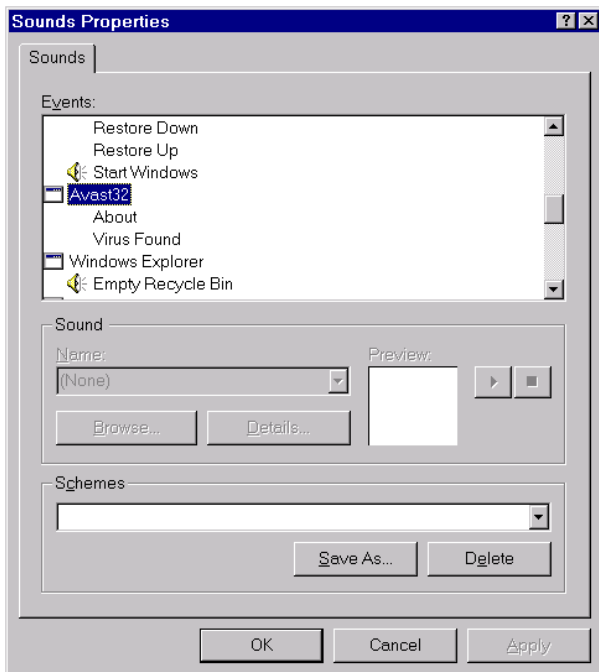
Fig. 55

Firstly find "Avast32" item and then "Virus Found" subitem in "Events" list.

You can enter the folder and filename with sound into the text box or browse it via standard dialog box for file opening. This box will appear after pressing "Browse" button. More detailed informa-tion about this dialog box can be found in operating system help or manual.

Appropriate sound file can be also chosen from a list which appear after clicking on arrow next to "Name:" text box.

It is possible to set up AVAST32 sound events via "Sounds" in control panel even if AVAST32 is not running - see Chapter 6.7.3.

Your computer must be equipped with sound card and its drivers for playing sound files. And everything must be correctly installed and set up. If your operating system plays sounds (e.g. during system start, if the sounds are enabled) AVAST32 program will play sound files as well.

"Sound" sheet is available if at least one of the following tests are selected: virus scanning, boot sector protector, behavior blocker.

4.4.14 Sheet "Online scan"

The "Online scan" sheet contains the controls used for the more detailed specification of the files to be scanned before running (Fig. 56). The newer type of viruses that has recently appeared, which does not attack neither executable files, nor boot sectors of disks, but the new data files, namely the OLE documents. These viruses are called macro-viruses. AVAST32 therefore contains a possibility to also check from time to time the OLE documents to be opened. By reducing the number of scaned

files it is possible to accelerate the start-up of programs and the opening of the OLE documents.

Fig. 56

At each attempt of running a program or opening a document AVAST32 will scan them first and whether or not they are infected with a known virus. If not, the file will be run, in the other case the user will be announced. However, the files containing the OLE documents will be scaned only in the case when they are opened with help of the OLE functions. With the standard operations with the files, as to their copying, etc. the document will not be scaned.

The executable files and the are scaned at the moment when their run or their opening with help

of the OLE functions are required. It implies that the speed of the task run can only be slightly reduced at the start-up of the scaned application or at the opening of an OLE document - but not during the proper work with the started application or with the opened document.

It is possible to check the OLE documents, 16-bit applications for Windows 3.1x, MS-DOS applications and, of course, 32-bit programs. Whether the appropriate type of the file is to be scaned or not you will specify by checking off the appropriate box. The 32-bit applications (i.e. the applications designed for the operating systems Windows 95 and NT) will always be scaned. It is possible to mark an arbitrary combination of the programs monitored. All the items are checked off by default.

Furthermore, the user can determine, whether at the start-up of a program all of its files will be scaned or not, i.e. including all libraries, or all the files except for the system libraries or all files except for the libraries. The selection will be made by selecting one of the given radio buttons.

The selected presetting will have a large impact on the speed of the starting-up of the applications, especially when always the same libraries are used. If you periodically scan your system, it is convenient, from the point of view of the speed, to disable at least the checks of the system libraries. Alternatively, if you intend to install a program, the origin

of which is unknown, we recommend that the check of all the executable files, including its libraries should be enabled.

All launched executable files and DLLs except system ones will be tested by default.

The "Online scan" sheet is present only in the case that also the executables and OLE documents protector belongs among the tests performed by the task (see Chapter 4.4.2).

4.4.15 Sheet "Online block"

Fig. 57

The "Online block" sheet contains the controls for the presetting of another possible activity of the task, which is the blocking of potentially danger-ous operations (Fig. 57). At any attempt to perform such an operation the user will be advised, and the operation will be performed only with his approval.

At this approach, however, the user can often be disturbed by useless inquiries, and therefore AVAST32 offers a possibility to select only the op-erations that are to be monitored.

The checking off of the box "DOS file operations" will mean that AVAST32 will check potentially dan-gerous operations with the files, which attempt to perform the applications designed for the operat-ing system MS-DOS. The box is checked off by de-fault.

The check box "Windows file operations" is used to activate the checks of potentially dangerous op-erations with the files, the carrying out of which will be attempted by the application designed for the operating systems Microsoft Windows. The box is checked off by default.

If you work under the operating system Win-dows 95, the "Online block" sheet contains also the check box "Formatting". We recommend you keep-ing this box checked off, because the viruses using this system service are especially dangerous - in a lesser case you can lose a certain part of your hard disk, in a severer case its entire content. The box is checked off by default.

In the environment of the operating system Win-dows NT the sheet contains only the check boxes

"MS-DOS file operations" and "Windows file operations".

The "Resident locks" sheet is accessible only in the case that one of the task tests is also behaviour blocker (see Chapter 4.4.2).
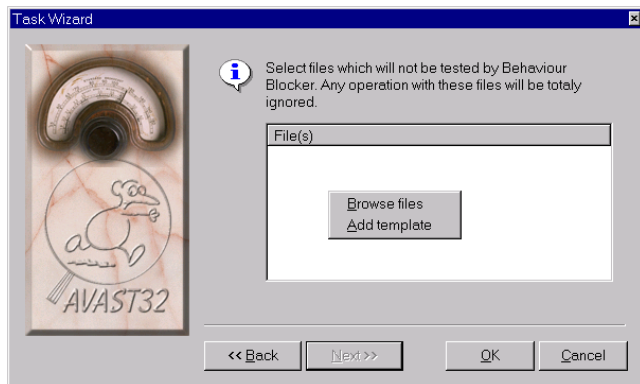
4.4.16 Sheet "Ignore"

Fig. 58

This sheet will enable the user to specify the files with which all the operations (both **MS-DOS** and Windows operations) are fully ignored by **AVAST32** by the activated behaviour blocker (see **Fig. 58**). This possibility was implemented into the program especially due to the fact that there is a large number of programs about which it is known that they store into themselves various information during their activities. The reporting of such program activity might be uncomfortable and time-consuming.

This sheet contains the list of the files, at which no operations will be done. If the task contains also other tests than behaviour blocker, then these tests will be performed also with the files specified on this list. The file list is empty by default. If you want to add a file onto the list, use the popup menu:

- the "Add template" command will add into the list the item bearing the name "Edit this file name template in this box..." and will enable the user to edit it. After you have entered the file name, press the "Enter" key,
- command "Browse files..." will open the standard dialog for the opening of the files (Fig. 88) and will enable the user to select the file required. Then the file selected will be moved onto the file list.

Files entered by user can be changed at any time – after click with left mouse button on appropriate file you will be able to edit it. If you are running Windows NT 3.51 than click with left mouse button on file name.

The file name must not include any wildcards "*" (asterisk) and "?" (question mark). The file can be deleted from the list in a usual way, i.e. first it is necessary to select it and then to use the "Del" key.

The "Ignore" sheet is accessible only in the case that one of the task activities is also the behaviour blocker (see Chapter 4.4.2).

4.5 Checking the entered data

When creating a new task, the AVAST32 program requires setting of some data and, of course, it checks its correctness and completeness. If the set data is incorrect, the user will be advised accordingly. If the use of the Wizard for the given operation with the task is enabled, the user will not even be allowed to move to the next sheet without setting the correct data.

The task name should be as true to its nature as possible and for the reason of easy comprehension it should not be used for more tasks. Nevertheless, the program will not prevent you from creating more tasks bearing the same names. If the task name has not been entered, AVAST32 will not allow for its creating.

Any new task must contain an activity so that its creation will make sense. Regular tests, which will be performed by the task, are to be set on the "Test" sheet (Chapter 4.4.2). If you failed to enter any task activity, the creation of such a task will not be permitted.

AVAST32 also does not enable you to create a new task if the task contains the virus scanning or integrity checking, and if no type of the files to be

testeded has been specified (Chapter 4.4.4), or no areas to be testeded have been defined (Chapter 4.4.5). In other words, if the lists on the "Types" and "Areas" sheets are empty.

AVAST32, however, does not check, whether the entered files (e.g. the file with sound or the files to be ignored) really exist. Of their non-existence the user is only advised in the case of their need. The accessibility of the computers provided for on the "Net alert" sheet (Chapter 4.4.11) is not checked either - it can be tested by using the "Test" button on that sheet.

5.User interface

AVAST32 can be controlled in two ways. The first user interface is the "Simple" one which is, with regard to its nature, suitable for the users who need to perform ordinary functions without having to know details of the program's work and its functions.

The other user interface, the "Enhanced", contains the extension for all and any functions and possibilities offered by AVAST32. It will be used especially by more experienced users, because it makes possible to adapt the program to their own requirements and makes use of all its functions and advantages.

Common feature of these two user interfaces besides the logo of the ALWIL Software company and Window menu (for detail see next Chapter), it is the status bar which is situated at the lower edge of the window. It contains four columns. The first column provides the exact number of the AVAST32 program version, including the number of its compilation. If you contact the staff of our firm in the case of any problems, you will need these numbers.

The second column contains the number of the tasks available and the number of the currently running tasks. The number of the licenses used,

and the one of the licenses bought is provided in the sequence in the third column. The last column is not used at present.

At the first start-up of the program the Simple user interface of the AVAST32 program appears.

5.1 Main window menu

Next common feature for simple and enhanced interface is Window menu (Fig. 59). It is situated under the main window menu bar and it is available any time when program is running.
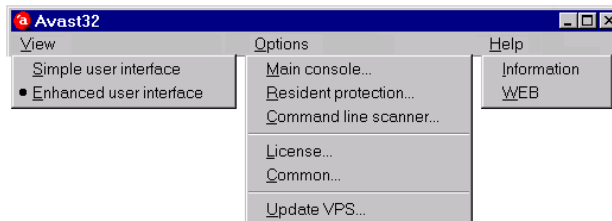

Fig. 59

"View" menu

It offers switching between "Simple User Interface" and "Enhanced User Interface". Current user

interface is marked with ball (Fig. 59 shows Enhanced user interface usage)

"Options" menu

Use this menu to customize AVAST32 program and its components behavior. It contains e.g. Wizard option for creating or modifying task. "Options" includes also virus database file updating (VPS file update). Because of complexity and importance of these items a whole chapter is dedicated to it. So all detailed program settings information can be found in Chapter 6.

"Help" menu

By choosing "WEB" item a Web browser would start (if it is installed of course) and if you are connected to the Internet the ALWIL Software web page would appear.

"Information" item from this menu is intended for displaying information about the program (Fig. 60).
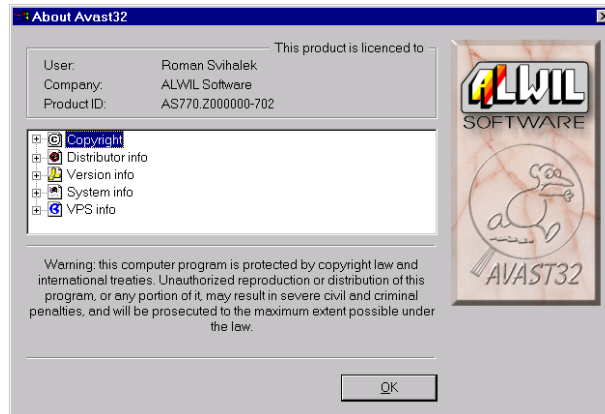
Fig. 60

You should pay attention to these information, because you may need some of them when you call our technical support for help.

The stuff can refuse your questions if you do not provide these information!

You can find these information here:

● copyright information,
● license owner and the number of licenses available across the network,
● AVAST32 and its components version information, including detailed build number,
● operating system information and available physical memory,
● VPS file version and its build information,

• AVAST32 version and the build number can be found also in the first column of status bar in main program window.

5.2 Simple user interface

Simple user interface is shown in Fig. 61. It contains the list of available tasks and several control buttons.

Fig. 61

List of available tasks contains tasks, which can be used by user in current time. There is an icon next to the file name of each task showing its current state. If the task is not running, icon shows
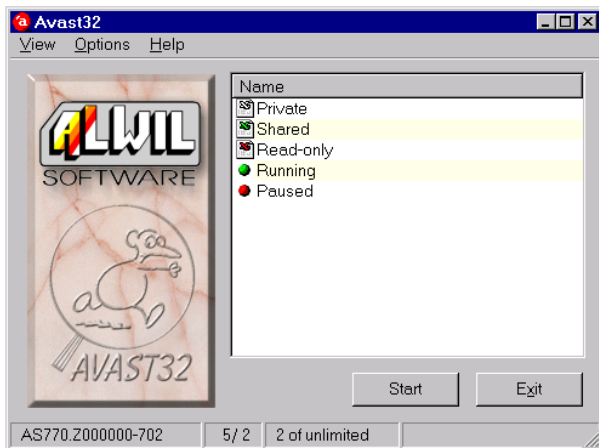
type of the task (tasks: "Shared", "Private" and "Read only" in Fig. 61). If the task is running, there is a green ball (task "Running" in Fig. 61) next to the task name. If the task is paused the ball is red (task:"Paused" in Fig. 61).

The left button is used for the starting or stopping of the task run. Its meaning will always change depending on the active task, i.e. the task which is highlighted on the list of the tasks available. If the active task is not running, the button bears the name "Start" and is used to start-up the task. If, on the other hand, the task is running, the button bears the name "Stop" and is used to stop the task.

The task can also be started or paused (but not stopped) by your activating it first, and then pressing the "Enter" key, or by double-clicking with the left button of the mouse on its name.

By using the "Exit" button you will end the activity of the AVAST32 program. At the same time also, all of the non-resident tasks will be stopped.
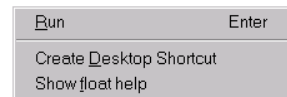

Fig. 62

The popup menu called up by pressing the right button of the mouse on the task name is illustrated in Fig. 62. Its regular contents, however, depends

on the current state of the task. The function selected will be performed with the task on the name of which the mouse button has been pressed.

The popup menu can contain the commands as follows:

● the "Run" command will start-up the task. It is only available for the tasks that are not running at the moment,

● the "Stop" command will stop the task. It is only available for the tasks that are running or paused at the moment,

● the "Pause" command will pause the task run. It is only available for the tasks that are running at the moment,

● the "Create Desktop Shortcut" command will create a shortcut to the task on the desktop. Such a shortcut can then be used for the direct start-up of the task, without having to start AVAST32 first. This command is always available in the popup menu,

● the "Show Float Help" command opens the Help of AVAST32. To open the Help it is also possible to use the "F1" key. This command is always available in the popup menu.

5.3 Enhanced user interface

The enhanced user interface contains the user-friendly interface for the access to all functions and settings which are offered by AVAST32. Since the number of such functions and settings is too high for one sheet, the enhanced user interface is structured on several sheets. The following chapters deal with individual sheets in detail.

5.3.1 Sheet "Tasks"

The sheet is divided into two parts (Fig. 63). The left part contains the list of the tasks available, as it was described in the case of the Simpe user interface. Its utilization and characteristics, except for the popup menu, are fully identical.
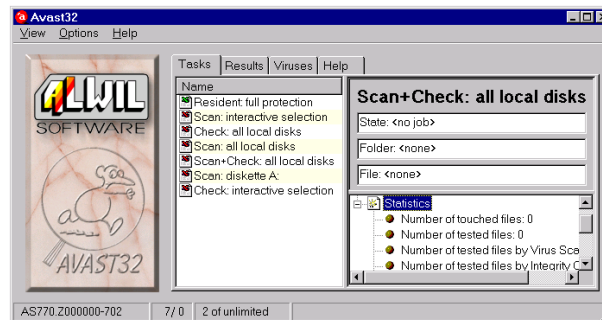

Fig. 63

The right part of the sheet contains the information on the status of an active task, its characteristics and progress.

The information on the status of an active task is situated in the text box in the upper part. The first

text box is the "State:" indicating the current state of the task. Three states are possible: the task has not been started ("<no job>"), the task has been started ("RUNNING") or the task has been started, but at the time being its run has been paused ("<paused>"). The complete path to the folder which is currently tested is indicated by the second (in sequence) text box - "Folder:", while the last text box contains the name of the file which is being tested. If the active task is resident (see Chapter 4.4.2), only the information on the task state is displayed.

The characteristics and statistical data relating to the progress of the task are arranged in the tree control, which is situated under the text boxes mentioned.Unpacking the appropriate item you will gain access to regular data. It can be done by double-clicking on the sign before the item name using the left button of the mouse.

The information relating to the task owner, tests performed during the task run, date of creation and date of the last utilization of the task will be found in the "Properties" item. In this item you will also find the information on the total number of task start-ups since its creation.

The last item is "Statistics" (it is unpacked in Fig. 63) which informs the user on the number of the files found, files tested, files tested for the presence of viruses, files in which their integrity was checked, the files which were not tested, files in-

fected and on the number of the viruses found. All the items are related to the active task. If the active task checks, for example, the data integrity, the item relating to the number of viruses found will always be equal to zero!

If the active task (i.e. the task which is selected on the task list) is currently running, the information is updated in real time, and thus the user is kept informed on its progress.

Popup menu
Similarly to the Simple user interface, also the Enahnced user inteface contains the popup menu which will be displayed after pressing the right button of the mouse on the name of appropriate task (Fig. 64). Besides the commands for starting-up, stopping and cancelling the task it contains the commands described below.

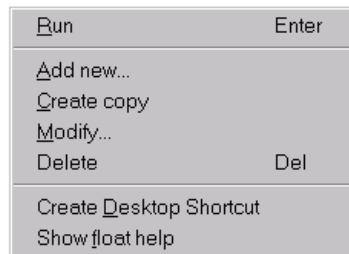*Fig. 64*

● the "Add new ..." command is used for the creation of new tasks. Its detailed description is provided for in Chapter 4,

● using the "Create copy" command it is possible to create an exact copy of the task in question. The new task will contain a fully identical setting of all parameters, as the task selected. However, the name of the new task will have the form "Copy <selected task name>". However, the copy can be created only from a task which is available for the user, i.e. from a private task, or in case that the shared tasks are not protected with a password or if the user knows such a password, then the copy can be made also from the shared task.

If the user would like to create a copy of shared task and if shared tasks are password protected by to this user unknown password the new task will be private. All other setting will remain untouched.

● the "Modify ..." command enables the user to modify the setting of the task parameters. The modification of the task is done in the entirely same environment as the task creation. Therefore, everything what has been written in Chapter 4 on the creation of new tasks, holds well also for their modifications. If you press the "OK" button in the window of the modification of task controls, and if the changes made comply with the conditions provided for in Chapter 4.5, the modification in the task will be made. If you, however, press the "Cancel" button, no change in the task will be made, and the settings of all its parameters will remain unchanged,

● the "Delete" command is used to delete the appropriate task from the list of tasks and at the same time also from the hard disk. After selecting it the user will be asked, whether he is serious about the deletion of the task (Fig. 65). After the pressing of the "Yes" button the task will be irrevocably deleted from the list of available tasks and from the hard disk of the computer,
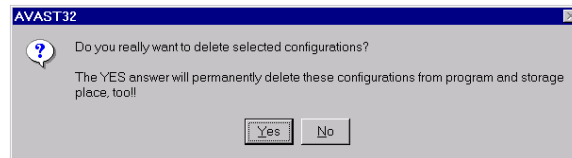

Fig. 65

● the "Create Desktop Shortcut" command will create, in the same way as in case of the Simple user interface, a shortcut to the task on the desktop of the computer. This shortcut can later be used to start the task directly without having to start the AVAST32 program first,

● the "Show float help" function will display the Help of the AVAST32 program. The Help can also

be displayed by using the "F1" key.

5.3.2 Sheet "Results"

The "Results" sheet contains the results of all the tasks which contain virus scanning or integrity checking (Fig. 66). The control of this sheet is very similar to the control of the "Explorer" program. This chapter describes only the control and the meaning of regular facts, which are contained on the "Results" sheet. The interpretation of these facts is described in .
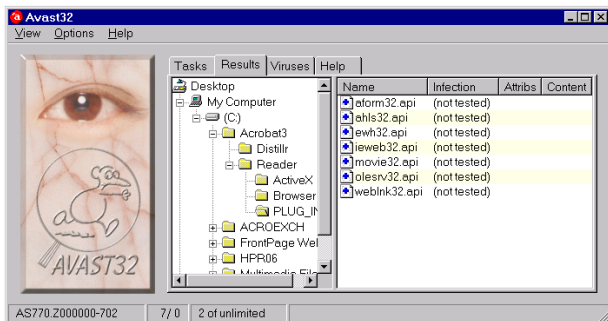

Fig. 66

The task results are summed up to the unique tree of the folders, thanks to which the user is well informed as to the results of all the tasks, which have been performed since the start-up of the program. However, only the files that indicates the vi-rus infection or that have been changed somehow since the last check, will be inserted into the tree by AVAST32. In other words, here you will find all suspicious files.

Also the new files will be inserted on the tree control, more exactly said, it concerns those files which have not been found by AVAST32 in its internal database of the files, you will also find here the names of the files which have been deleted or moved. The boot sectors of the disks and the memory are dealt with in the same way as files, which means that in case of their changes they will be inserted to the tree control as well. They will be inserted directly to the folder "My computer".

The suspicious files are inserted to the tree control according to their real path. It means that if the tree contains a folder, this folder (or an inserted folder of its) is sure to contain the suspicious file. If you want to learn the contents of some of the folder, activate it, and in the right part of the sheet you will see the suspicious files (if there are any). The icon illustrating the action which has been performed with the file in question will be situated before the name of each file.

Fig. 67

If the blue sign plus (Fig. 67) is here, it means that the file is new, i.e. it has been created since the last check. If you have started the integrity checking for the first time, all the files found will be marked as new, because the internal database of files is still empty, and it must be filled first.

Fig. 68

The green sign minus (Fig. 68) signals, on the contrary, that the file bearing a given name is missing here (the file was deleted). It is good to realize what you have been doing with the computer. If you, for example, have emptied the recycle bin since the last check, it is obvious that the program will report the files missing on the disk in question in the folder "RECYCLED", in the same way you are likely to be informed on the disappearing of temporary files, etc.

Fig. 69

Another character which could appear next to the file name is red exclamation mark (Fig. 69).

AVAST32 uses this for telling the user that file is infected or during the file testing an error appeared.

If the file is infected there will be name of the virus in "Infection" column displayed. If the column is blank an error during the file testing appeared. This may happened due to many reasons, most often however it is file sharing error, it means that the file is used by other application.

Fig. 70

If you have performed a repairing of the OLE document (see below), a yellow question mark can appear next to the name of the corrected file (Fig. 70). Thus AVAST32 indicates that the file state is unknown after the performing of the repair or after the removal of a macrovirus from the file. If you need to find out, whether the state of the file marked this way differs from the one which is stored in the database, check integrity of the file again.

The green ball (Fig. 18) may appear, similarly to question mark, next to the recovered files. In contrast to question mark it appears only next to the files, which are not OLE documents and has been successfully recovered. So files marked this way are in the state, in which has been stored in file database.

Fig. 71

If there is icon as shown in Fig. 71 next to the file, such a file has been changed somehow. Detailed information about the change are listed in columns next to the file name. For detailed information see below.

- the "Infection" column contains the name of the virus with which the file is likely to have been infected. The column, however, is appropriate only on the condition that the file in question has really been scaned for the presence of viruses. If it has, and the column is empty, it means that none of the viruses known has been found in the file in question. However, if the column contains a virus name, the file is very likely to be infected! If the file has not been tested, the column contains the text "(not tested)",

- "Attrib" column informs user about attribute change and change of the last time of writing into file. There will be also information about the change of security setting of file under Windows NT. If the file has been tested for integrity and column is blank, it means that parameters of appropriate file have not been changed since last test. In other case column would contain "!!!"(three exclamation marks),

- "Content" column informs user about content change or file size. If the file has been tested for integrity and column is blank, it means that file content has not been changed since last test. In other case column would contain "!!!" (three exclamation marks).

We again give warning that if the "Infection" column is empty, it does not have to mean that the file is not infected. If the file in question has been scanning for the presence of viruses, and the column is empty, it means that at the given setting of the program no known virus has been discovered in the file!

Popup menu

The popup menu (Fig. 72) always relates to those files that have been marked. The same popup menu is used also for the folders situated in the left part of the sheet. The function selected for the folder in question will be performed with all the files that it contains, as well as with the files situated in all subfolders.
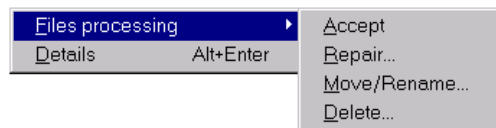

Fig. 72

The "Details" command is used to display the dialog with more exact information on the type of the file change (Fig. 73). It provides information about the file selected, as to its state, attributes, date of creation and the last modification and, of course, the length of the file, and possibly also the name of the virus which infecteded the file. All this information is displayed on the original state of the file (it is stored in the internal database) as well as for the current state of the file, in which it is situated on the disk.

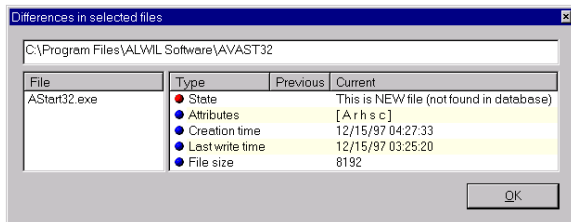Also the hot key "Alt + Enter" can be used to display the dialog.

Fig. 73

The popup menu contains the folder "File processing", which contains the commands for the work with suspicious files:

Accepting files

The "Accept" command will announce to AVAST32, that you know about the changes in the files, and that it should not report them any more. The files treated this way will disappear from the list of suspicious files, and so should the folder, in which they were situated, remained empty, also the folder would disappear. In fact, this command will record the current state of the files into the internal database, which means that it will act as the starting state at the next check.

Repairing files

The "Repair ..." command will try to return the marked files to their original state. When you select it, you will see the dialog illustrated in Fig. 74. If the file being corrected is an OLE document, the user is enabled to preset some parameters. If this is not the case, their presetting makes no sense, and they will be ignored.
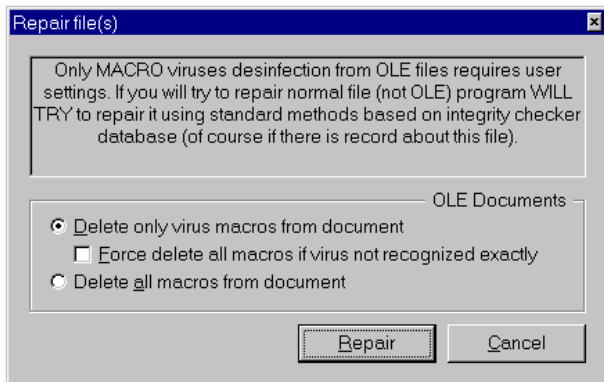
Fig. 74

Through the radio button "Delete only virus macros from the document" it is possible to preset that only the macros, in which a virus has been found, should be removed from the document. The other macros will remain untouched.

The radio button "Delete all macros from document" will cause that all the macros will be removed from the OLE document, whether they contain a virus or not.

The default setting is to remove only those macros that contain a virus.

Checking the box "Force delete all macros if virus not recognized exactly" you will set to the program that if the virus has not been recognized with full exactness (in the case of some macroviruses the detection is very difficult), all the macros are to be removed from the document.

If a file which does not contain an OLE document is to be corrected, AVAST32 will try to correct the file by using the method based on the integrity checking. The truth is that AVAST32 maintains its internal database of files, into which it records important information on the status of individual files, and with the help of checksums, also on their contents. With using this information AVAST32 will try to repair the file selected. It is possible to repair up to ninety-five per cent of the files infected. AVAST32 is able to determine at one hundred per cent precision, whether the file has been repaired or not.

It follows from the previous text that if you want to repair the files successfully, you will need a periodically updated database of the files on your disks. This database must be maintained, in other words, it is necessary to perform integrity checking from time to time, and to record authorized changes in the files into the internal database of the "Accept" command.

The algorithms used for the repairing of the files in AVAST32 are exclusively able for the repairing of the files infected by a virus. Thus they cannot be used for the renewal of rewritten or edited files. The presetting of the controls of the dialog is ignored for the files that do not contain any OLE documents.

By pressing the "Repair" button the file repairing process itself will be started-up. Using the "Cancel" button you will close the dialog, and the marked files will not be manipulated.
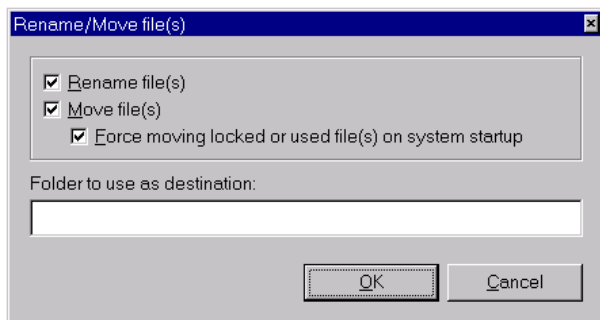
Renaming and moving files

Fig. 75

The "Move/Rename ..." command enables you to move the suspicious files to another folder or to rename them. The command will display the dialog, which is illustrated in Fig. 75. This dialog contains three controls:

The check box "Rename file(s)" enables you to change the extension at the marked files. The files renamed this way will be distinguished from the others and in case of the executable files you will also prevent their accidental running. It would lead,

in case that the file in question contains a virus, to the infecting of the computer (if it has not happened yet). The existing extension will be replaced with the preset one at the given file (see Chapter 6.1.3). The proper name of the file will remain unchanged.

If the program finds an unknown type of the file during the renaming, it will inquire the user about how the extension of the file found is to be changed. The program will remember the extension entered, and when it finds a file of the same type next time, it will automatically use such a extension.

By checking off the box "Move file(s)" you will activate the moving of the files marked to the folder selected. The name of the folder, into which the files marked are to be moved, and the path to it, will be written to the text box "Folder to use as destination:".

If the moving of the files is activated, it is possible to determine, by checking off the box "Force moving locked or used file(s) on next OS startup", that if it is not possible to manipulate the file at the given moment (e.g. it is used by another application), it is possible to postpone its moving till the next start of the operating system. Thus it cannot happen that you would forget to move the file - the program takes care of everything by itself.

The default is that both the renaming of the files and their moving including the possibility of post-

poning it till the next start-up of the operating system is activated.
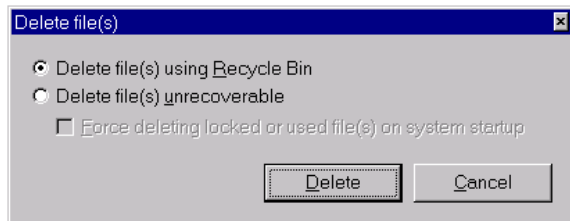
Deleting files

Fig. 76

The last command in the "File proccessing" folder is the "Delete ..." command. When selecting it, you will see the dialog in which the user can select the ways of deleting files (Fig. 76).

By selecting the "Delete file(s) using Recycle bin" radio button you will determine that the marked files will be deleted by being moved to the recycle bin. Thus it is possible to restore the files deleted at any time, and for this reason we recommend this way especially for less experienced users of personal computers.

If you use the operating system Windows NT version 3.51, then this radio button will be inaccessible for you and you will have to use the following procedure.

The "Delete file(s) unrecoverable" radio button will start the direct deleting from the disk of the files, without any possibility of restoring them.

If the radio button is selected, by using the check box "Force deleting lock or used file(s) on next system startup" you may determine that if it is not possible to manipulate the file at the moment (e.g. it is used by another application), it is possible to postpone its being deleted till the next start-up of the operating system. This box is not checked off by default.

The "Delete file(s) using Recycle bin" radio button is selected by default.

After pressing the "Delete" button all the marked files will be deleted in the way selected. The "Cancel" button will close the dialog.

5.3.3 Sheet "Viruses"

If you are interested in more detailed information about all viruses, that AVAST32 currently recognizes, click on the name of "Viruses" sheet. This sheet contains a complete, alphanumerically sorted list of all the basic types of viruses (Fig. 77).
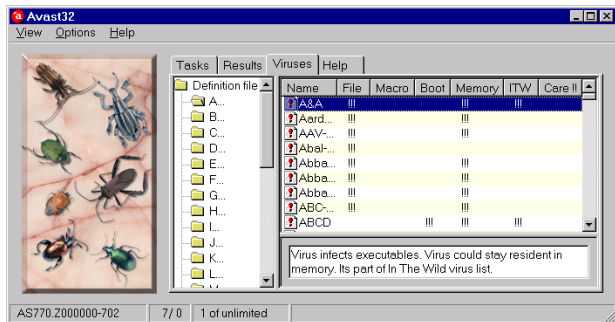
Fig. 77

Similarly to all other sheets, this one is also divided into two parts. On the left the user has the possibility to select the first letter or digit of the virus name, about which he would like to learn more detailed information. The viruses, the names of which start with the character selected, will appear together with their characteristics in the right part of the sheet.

Viruses can spread out basically in the following ways: as a part of an executable file, as a macro of a certain document ("macroviruses"), or by rewriting the boot sector (the sector which is read when initializing a system) of a disk.

The first three columns provided for after the virus name correspond to all the above listed ways. Thus, if a column at the virus in question contains "!!!" (three exclamation marks), it means that this virus infects the computer system using that given way.

The "Memory" column says whether the virus may be present in the operation memory of the infected computer on a long-term basis (it is called resident). The next column contains the information on whether the virus is situated on the ITW list, which is the list of the most frequent viruses. The last column marked "Care !!" (three exclamation marks) informs you about the dangerous nature of the virus. If you should find the marking "!!!" (three exclamation marks) at a virus, you had better not alter with it. The viruses marked this way are very difficult to remove from computers, or they may seriously damage your data. The removal of such viruses should be done by somebody who is really experienced!

If you mark a virus on the list situated in the right part of the "Viruses" sheet, its brief characteristic will appear in the text box in the lower part. It actually concerns a understandable listing of the contents of particular columns as they are described.

The left part of the "Viruses" sheet contains, besides alphanumeric and other characters also two special items. By using the "ITW" item it is possible to display in the right part of the sheet a list of all viruses from the current VPS file, which are found on the ITW list. In a similar way also the "Care !!" item is working providing that the most dangerous

viruses will appear on the list in the right part of the sheet. In both these cases the viruses will be sorted alphanumerically.

Since it is necessary to explore the entire VPS file in order to find the viruses from the two above named items, their displaying can take some time.

No more detailed description of the all known viruses, their activities and special features is available. It is neither achievable, nor useful to find out all and every detail with regard to each virus especially due to their huge amount. The individuals who are interested in more detailed information on a certain virus are asked to contact the staff of our company who will be glad to provide them with the information required.

5.3.4 Sheet "Help"

Sheet "Help" contains AVAST32 help (Fig. 78). The users can found all needed information here.

In case of any problems with the program we ask you to look into the Help of the AVAST32 program first, and only when you do not find there what you are looking for, contact our technical support.

If the Acrobat Reader program is not installed in your computer, it will not be possible to display the Help of the AVAST32 program. In such a case you must exit AVAST32, install the Acrobat Reader program (see Chapter 1.2.1) and then start AVAST32 again.
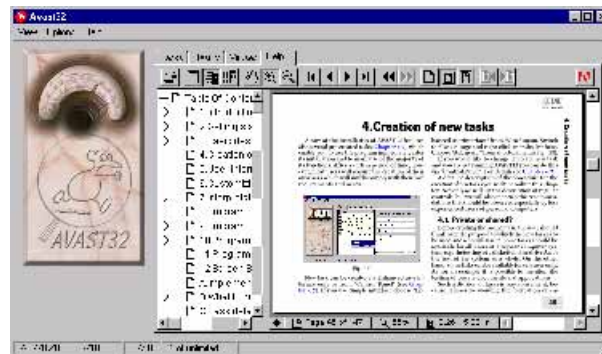

Fig. 78

The Help of AVAST32 can be either a part of the "Help" sheet as it is illustrated in Fig. 78, or "floating". The term floating Help identifies the window with the Help, which is freely movable about the desktop (Fig. 79). It means that the Help is not tied to the "Help" sheet, but it can be placed at any place and thus available all the time.
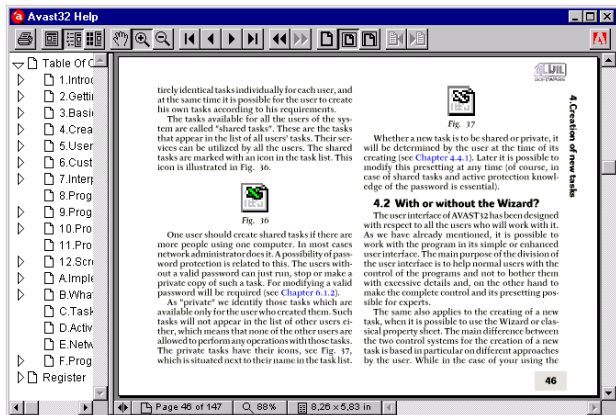
Fig. 79

The floating Help can be called up at any time during the operation of the AVAST32 program, it can be done either from the popup menu, or by using the way common in the environment of the operating systems Windows 95 and NT, i.e. by pressing the F1 key. It will be closed by using the "Esc" key.

If the floating Help is displayed, the "Help" sheet does not contain the Help any more. In other words, it is possible to have only one Help displayed.

Whether the Help is situated on the above mentioned sheet, or it is floating, its control is always the same, because the favorite program Acrobat Reader is used to display the Help in both of these cases. It is, however, used in such a way that it appears to be an integral part of AVAST32.

The following paragraphs deal with the Help control.

The button is used to print the Help or a part of its. When pressing it, you will see the dialog which enables you to preset the parameters, quality and extent of the print.

The following three buttons determine the options of passing through the Help:

If this button is pressed, the window with the Help will contain only the part displaying the Help itself. The part facilitating the movement within the Help will not be displayed.

If this button is pressed, the window with the Help will contain, besides the part displaying the Help, also the part in which the content of the Help will be displayed (Fig. 79). By pressing the left button of the mouse on the content item it is possible to move to the appropriate part of the Help.

The button activates the displaying of individual numbered sheets next to the Help itself. By pressing the left button of the mouse on the appropriate sheet it is possible to move to the sheet with the appropriate number.

The following three buttons determine the way of work with the Help (the mouse pointer will take the appearance shown by the button selected):

If this button is selected, then after the clicking with the left button of the mouse over the Help it is possible to move the page of the Help, which is just displayed, in an arbitrary direction, and to display the part of it, which the user wishes to see.

If this button is pressed, the part of the Help in question will be magnified twice its size after the pressing of the left button of the mouse over the Help.

If this button is pressed, then, after the pressing of the left button of the mouse over the Help, the document will reduce twice its size, which means that the larger part of its will be seen, but with smaller details.

The following four buttons serve for the movement in the Help (the other parameters, as e.g. zoom will remain unchanged):

This button is designed for the movement to the first page of the Help.

By pressing this button it is possible to move to the previous page of the Help.

By using this button you will move to the next page of the Help.

After your pressing this button the last page of the Help will be displayed.

The following two buttons enable you to pass through the steps which have been performed so far:

This button will cancel the command which was the last to be performed, i.e. it will return the window with the Help to the state, where it had been before the command was performed. This way it is e.g. possible to return to all the pages of the Help, which have been listed so far.

If you have returned one step back, using the previous button you may, alternatively, go forward by one step. In other words, you will run the same operation, which you canceled with the previous button. The button can be used if no operation was performed after the pressing of the previous button.

The following three buttons serve as a quick zoom presetting according to the page displayed:

The button will preset the displaying of the page in its real size, i.e. it presets the zoom value to one hundred per cent. It is possible that the page displayed will be greater or, on the other hand, smaller than the part of the window dedicated to the displaying of the page in question.

After pressing this button the zoom parameter will be preset to such a value that always the complete Help page can be seen. In the case of a change in the window dimensions also the page size will change.

Using this button you will preset the magnifier parameter to such a value that the page width can correspond to the width of the Help window, regardless to the height of the page. If the width of the window changes, the width of the displaying of the page will change as well.
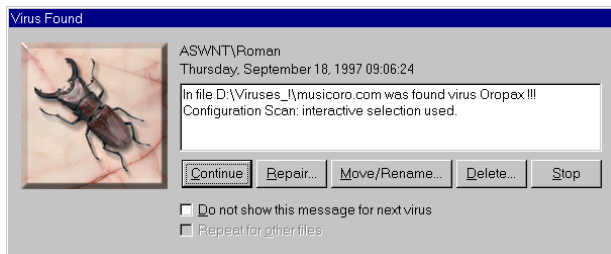
5.4 Finding virus message

Fig. 80

If a virus has been found during the operation of a task, AVAST32 will display a warning message (Fig. 80). The text provided in this message depends on the setting of the task which found the virus in question (see Chapter 4.4.12).

By using the "Continue" button you will inform to the program that it should continue running the task in question. The file infected can be treated later on the sheet "Results" (Chapter 5.3.2).

The "Repair ..." button serves for immediate repair of the file infected. Completely the same dialog will be called as in case of the "Repair ..." command situated in the popup menu on the "Results" sheet of the Enhanced user interface. The detailed description of the dialog is provided for in Chapter 5.3.2. After reapiring the file you may continue performing the task.

The "Move/Rename ..." button enables the user to move the infected file to another folder and/or to change its extension. The detailed description is provided for at the command bearing the same name as in Chapter 5.3.2. After the file has been moved and/or renamed, the task will continue running.

The "Delete ..." button is used to delete the infected file from the disk. A detailed description of the dialog, which appears, is provided for at the "Delete ..." command in Chapter 5.3.2. After the dialog has been closed, the task that found the virus will continue to run.

By means of the "Stop" button you will end the run of the task that found the virus.

The virus warning message still contains two another controls.

By checking off the box "Do not show this message for next virus" you will inform to the program that if it finds another virus during the run of the current task, it should not display the appropriate warning message anymore. This box is not checked off by default.

By checking off the box "Repeat for other files" you announce to the program that if it finds another file infected by a virus during the run of the current task, it should perform with it in entirely the same way which has been performed with this file. The box is only available if the box "Do not show this message for next virus" is checked off. This option is not checked off by default.

5.5 Selecting tested areas

AVAST32 requires, in a few places, the specification of which areas, i.e. files, folders, possibly if the entire disks are to be tested. Therefore it contains the dialog which facilitates this activity (Fig. 81). It enables the users to select also more folders or disks at the same time, whereby it makes the work with the program much easier.

The upper part of the dialog is practically the same as in the case of the standard dialog designed for the opening of the files, which forms a part of the operating system. Here, in the common way,

the user selects the required file, folder, or possibly the entire disk, which he wants to select, and by pressing the "Add" button he will add the selected item into the list in the lower part of the dialog. This way the user will proceed until the list contains all the areas which need testing.
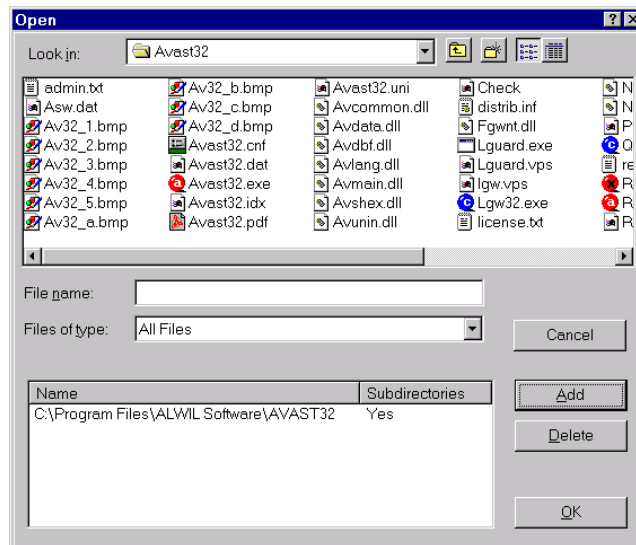

Fig. 81

If you made a mistake during your selection, or if you simply do not want to test any of the selected areas, simply remove it from the list. It can be re-

moved by your first selecting it, and then by pressing the "Remove" button you would remove it from the list of the selected areas. The appropriate operation will not be performed with any area removed from the list.

Next to the name of the area is written if its subfolders should be tested too. If you would like to change this setting, click on name of the area with left mouse button. Test of subfolders is enabled by default in newly added areas.

If you have selected all of the areas required, by pressing the "OK" button you will start-up the performing of the operation in question. If you press the "Cancel" button (or if you close the dialog in any other way), the performing of the operation selected will be canceled, and the files selected will be ignored.

6.Customizing AVAST32

Use "Options" menu (Fig. 82) to customize AVAST32 program behavior.

Main console...
Resident protection...
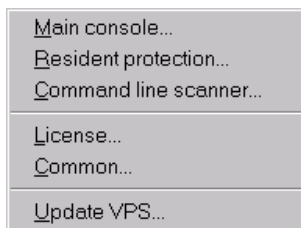Command line scanner...

License...
Common...

Update VPS...

Fig. 82

After selecting whatever item a dialog box will appear where you can set up appropriate things. All dialog boxes are divided into several sheets similar to AVAST32 main window between which you can switch.

The pages are marked with balls of different colors. If the ball is blue, control items on such a page are intended for all users – its settings do not affect functionality of the program. If the ball is red, control items on such a page should be changed by experienced users only who know what this change can cause. So the pages marked with red ball are available only to users with administrator's rights – these pages will not appear to other users.

Detailed information on particular items from "Options" main window menu are described below.

6.1 Item "Main console ..."

After selecting this item dialog box divided into several sheets with AVAST32 settings will appear.

6.1.1 Sheet "Basic"

Sheet "Basic" lets user to customize program behavior (Fig. 83). All controls here are saved for each user separately so AVAST32 retains individual access to each user. These changes will not take effect until you restart the program.
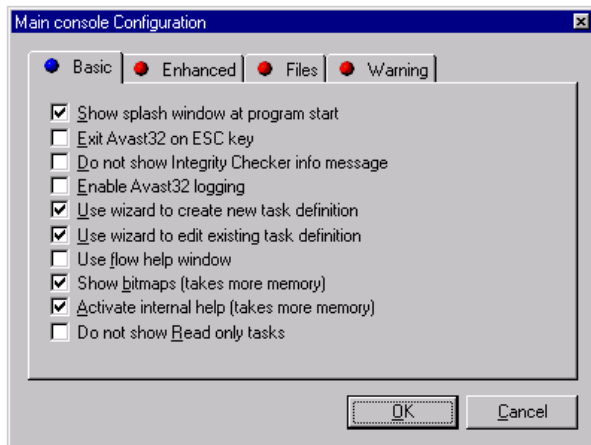
Fig. 83

By checking "Show splash window at program start" box you enable showing splash window during AVAST32 start-up. If this window upsets you or you would like to slightly speed up program start do not check this box. This check box is checked by default.

"Exit Avast32 on Esc key" check box defines if it would be possible to close AVAST32 program by pressing ESC key. This is suitable for experienced users who prefer shortcut keys. Not checking this box prevents inexperienced users from involuntary program exit. It is not enabled by default.

"Do not show Integrity Info message" check box disables displaying integrity checking message (Fig. 20). No matter if it is normal or simple integrity checking.

The message will not appear until at least one of tested file has been changed. It contains also prompt to display task results. After pressing "Yes" button the "Results" sheet from enhanced user interface is activated. This message displaying is allowed by default.

"Enable Avast32 logging" check box enables logging. It means in Windows 95 that all activities performed with AVAST32 will be written into the "AVAST32.log" text file which will be created in AVAST32 program folder. Information on found viruses and users working with this program will be logged as well.

The size of the log file is given by the value recorded in the text field "Logging file size" on "Files" sheet (Chapter 6.1.3). The logging is disabled by default.

Under the Windows NT the program will try to write logging information into the system log file. You can view this file via "Event Viewer" program which can be started from "Programs/Administrative tools" folder. If the program is unable to write to this mentioned file it will write logging information in the same way like in Windows 95.

The use of logging is suitable especially in the network environment where it is possible to check the activity of individual users.

"Use Wizard to create new task definition" check box will activate the Wizard, which will guide you through the creation of a new task (see Chapter 4). We recommend checking this box especially for beginning users. This box is checked by default.

The check box "Use Wizard to edit existing task definition" will activate, similar to the preceding box of the Wizard, this time, however, for the use at a change in the existing task (see Chapter 4). The use of the Wizard is preset by default.

By means of the check box "Use floate Help window" it is possible to preset that the Help of the AVAST32 program should have arbitrary position on the screen, and thus it should not be tied with the "Help" sheet (Chapter 5.3.4). This box is not checked by default.

"Show bitmaps" check box will activate the displaying of the pictures in the main window of AVAST32. The pictures illustrate the activities performed and make work with the program more pleasant. Their use, however, requires more operating memory of the computer, and therefore, if you do not have enough operating memory, or if you simply do not care for the pictures, do not check the box. The use of the pictures is enabled by default.

The check box can influence only AVAST32 program - the pictures originating from the dialogs of the WARN32 and QUICK32 programs will not be removed.

"Active internal help" check box serves for the automatic lunch of the Help file of AVAST32 after its start, and thus it will not be necessary to load it from the disk at every calling of the Help again. If the box is not checked the Help file will only be loaded at the user's request, i.e., after the selection of the appropriate item of the menu, or after pressing the "F1" key. The box is not checked by default.

If you have enough operating memory and if you often look into the Help, we recommend checking the box. It will make the displaying of the Help faster.

6.1.2 Sheet "Enhanced"

Controls from "Enhanced" sheet shows Fig. 84. Their change will influence all the users working with the program, because the setting of these controls is stored for AVAST32 as a whole. The change will take effect after program restart.
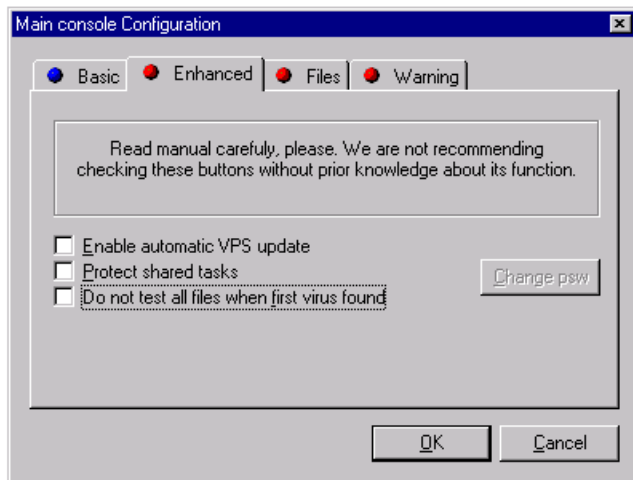
Main console Configuration

● Basic ● Enhanced ● Files ● Warning

Read manual carefully, please. We are not recommending checking these buttons without prior knowledge about its function.

☐ Enable automatic VPS update
☐ Protect shared tasks
☐ Do not test all files when first virus found

Change psw

OK   Cancel

Fig. 84

"Enable Automatic VPS update" check box is used for the enabling of the automatic VPS file update, which contains the database of the known viruses. If the box is checked the AVAST32 program will automatically search the preset folder (Chapter 6.6, the text box "Source filename") after its start-up. If it finds a newer file than the existing one, the existing VPS file will be automatically replaced with the newer one. Otherwise nothing will happen with the existing VPS file.
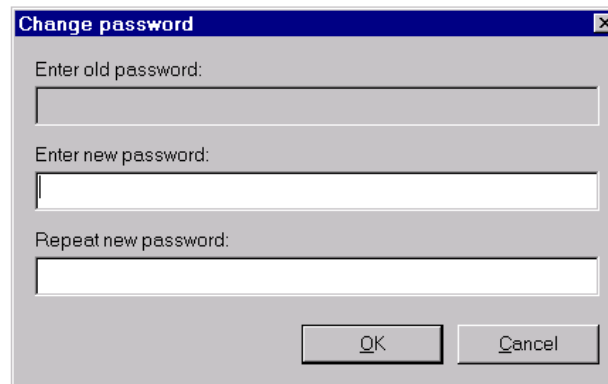
The automatic VPS update is not enabled by default.

Change password

Enter old password:

Enter new password:

Repeat new password:

OK   Cancel

Fig. 85

"Protect shared tasks" check box enables you to protect the shared tasks from a change by a password. After its checking you will see the dialog enabling you to enter the password (Fig. 85). The password needs to be written twice, at first into the "Enter new password" text box and for check purposes also to the text field "Repeat new password". If the password has been written identically to both of the boxes, it will be used, otherwise you will be warned and given a possibility to write the password again. The checking of the box can be disabled only if you know the currently valid password.

If shared tasks are password-protected users without a valid password can just run, stop, make pri-

94

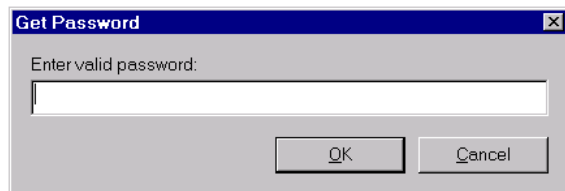vate copy of such a task or create a desktop shortcut but all other actions will not be permitted.

Dialog for entering the password is shown on Fig. 86. If the password is correct the user will be allowed to perform the desired operation with the task. The user is required to enter the password only once - the program remembers the correct password and its new entering will be required only after the new start-up of the AVAST32 program, or after its change.

To change the existing password use the "Change psw" button. After pressing it you will see the same dialog as in the case when the protection of the shared tasks was enabled. Before setting a new password it is necessary to enter the existing one into the "Enter valid password" text box even in the case that the user has already entered the password during the operation of the program. Without setting it correctly you will not be able to carry out the change of the password!

By checking "Do not test all files when first virus found" box you disallow to AVAST32 program to test all files for all viruses when the first virus is found. By default it is set, that once first virus is found program starts to test all following files (it does not care about file type) for all viruses (no matter if the virus infects that type of file). It is not recommended for inexperienced users to check this box. The check box is not checked by default.

6.1.3 Sheet "Files"

Sheet "Files" provides the user with the possibility to specify the files with which AVAST32 works (Fig. 87).

The controls preset on this sheet are kept for the program as a whole, and thus their change will influence all the users. The changes will take effect after the program restart.
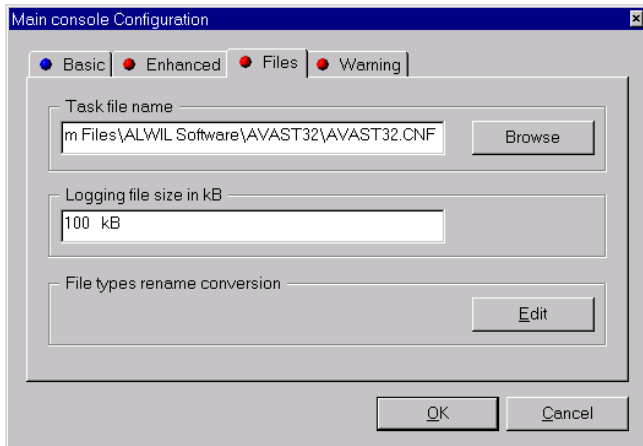
Fig. 87

Fig. 88

Through the "Task file name" text box the user has a possibility to enter the name of the configuration file (*.CNF) of AVAST32, including the path to it. The configuration file specified in the above described way will be used instead of the existing ones.

The "Browse" button serves for determining the configuration file via standard system dialog for opening the files (Fig. 88). The name of the selected file will be automatically placed into the above specified text box. The CNF file situated in AVAST32 folder is used by default.
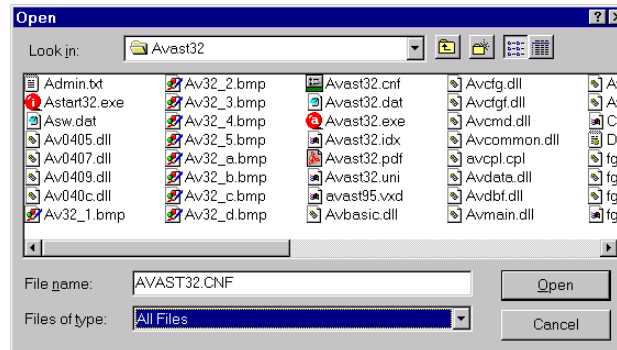
Within the "Logging file size in KB" text box it is possible to set the maximum size of the logging file. The size of the file is stated in KB (in kilobytes). If the log file reaches the specified size approximately the first third of this file will be deleted. Thus the oldest data will be deleted from the file and the space for new data will be created. The default maximum size of the logging file is 64 KB. The value in the text box makes sense only in Windows 95 and if the logging is enabled (for details see Chapter 6.1.1, "Enable Avast32 logging" check box).
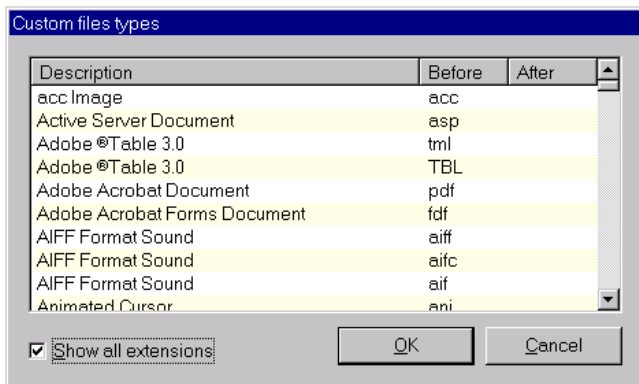
Fig. 89

The "Edit" button serves to open the dialog in which it is possible to set a new extension for a given type of files (Fig. 89).

The dialog contains the list of the known file types and their extensions (the "Before"column). The "After" column contains the extensions which will replace the existing ones at the renaming of the given type of files. The dialog can contain only the most important extensions, or all the extensions known – these options can be selected by checking the "Show all extensions" box.

The extensions listed in this dialog will be used at the renaming of the file on the "Results" sheet (Chapter 5.3.2). The files provided in the tree struc-ture on this sheet have been changed somehow or the program have found a virus in some of them.

If this is the case, it is suitable (especially for the executable files) to rename them so that their start-up even accidental can be avoided.

If you would like to change the extension of a type of the files first select it and then click on it using the left button of the mouse. Thus you will be enabled to edit it. The new extension will be confirmed by pressing the "Enter" key.

If you are satisfied with the changes you have made with the file extensions, press the "OK" button. If you prefer to use the extensions which have been used so far, use the "Cancel" button.

6.1.4 Sheet "Warning"

Sheet "Warning" serves for the selection of the computers (Fig. 90) to which the warning message will be sent in case a virus has been found. The users of these computers will be informed together with those whose computers were selected during the task creation (Chapter 4.4.11) which has found the virus.
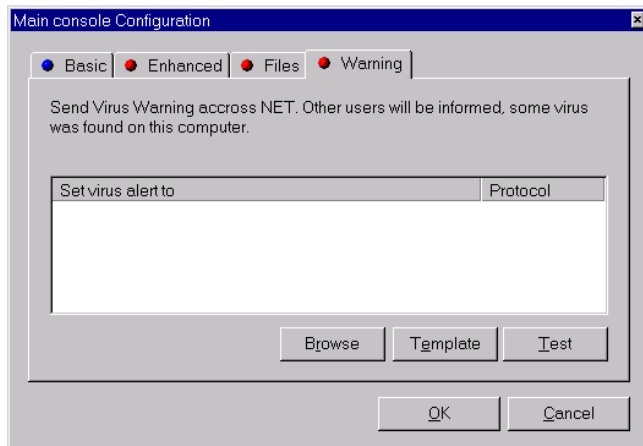
Fig. 90

The list of selected computers is stored for AVAST32 as a whole, which means that its change will influence all users. The changes will take effect after the program restart.

The computer to which the message should be sent will be determined by writing its name on the list of selected computers. By pressing "Template" button shortcut menu with protocols will appear:

● "Internet" item determines that computer to which warning message will be send is specified by standard URL address. The SMTP (Internet Mail) protocol will be used for message delivery,

● by "Microsoft" item you tell the program that appropriate computer is available via Microsoft Mail,

● "Internal" item assign that computer for sending virus alert will be available via local network.

After selecting appropriate protocol an item "Edit for valid address or name..." will be added to the list. Right click on the item for edit. When finished press "Enter" key.

After pressing "Browse" button a shortcut menu with protocols will appear again (in this version "Internal" only). You can choose a computer available via local network from a dialog box shown on .

For deleting the computer from a list click on it and press "Del" key.

You can change parameters of listed computers here. Click on "Protocol" column for protocol change. From shortcut menu choose new protocol. You can change name/address in the similar way, after left click on the name an edit will be allowed.

If you are not sure about message delivery you can try the connection by pressing "Test" button. A test message will be send to all selected computers. The list of selected computers for alert message is blank by default.

6.2 Item "Resident protection ..."

By choosing this item dialog as shown in Fig. 91 will appear. It contains controls for resident protection part settings (it is RGW32 program, see Chapter 9).

The changes will take effects after the program restart.
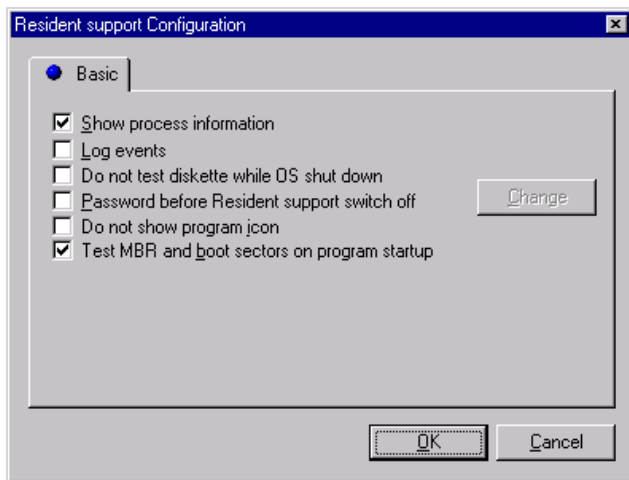

Fig. 91

"Show process information" check box determines if user will be informed about running resident activities. If the box is checked there will be short information about running resident activities on the right bottom of the desktop. If the box is not checked no information will appear and this is also default setting.

By checking "Log events" box user can enable logging of resident activities to the log file (for detailed information see Chapter 6.1.1, "Enable Avast32 logging" check box).

You can prevent diskette drive testing during operating system shutdown when resident part of AVAST32 is running by checking "Do not test diskette while OS shut down" check box.

If inserted diskette is infected and left in drive operating system would be infected during next system start (If a boot from drive A: is allowed in BIOS setup). If diskette is found in drive and the check box is not checked a warning message will be displayed as described in Chapter 9.3. The check box is not checked by default.

"Password before resident support switch off" check box allows to prevent closing of resident program and hereby protect i.e. less experienced users against virus infection. On each attempt to close RGW32 program a dialog box, as shown in Fig. 86, will appear and without entering a valid password will not be possible to exit the program.

A dialog box shown in Fig. 85 will appear after checking the check box. It is not possible to uncheck

the check box without knowledge of valid password. The check box is not checked by default.

By "Change" button you can change the password of RGW32 program – if you know the current password. The change of password is done via dialog box in Fig. 85.

By checking "Do not show program icon" check box you can cause that RGW32 program will not display its icon on task bar when the program is active (Fig.103). It is not recommended for inexperienced users to check this box. This check box is not checked by default.

"Test MBR and boot sectors on program startup" check box allows to RGW32 program to check system parts of local hard drives on its start up. This check box is checked by default.

If you are running Windows 95 the dialog will also contain "Test memory on program startup" item, by its checking you cause that RGW32 program will test operating memory on its start up.

6.3 Item "Command line scanner..."

After choosing "Command line scanner..." item a dialog as shown on Fig. 92 will appear. It contains controls for basic setting of command line scanner – program for virus scanning – which is started from command line (it is LGW32 program, see Chapter 8).
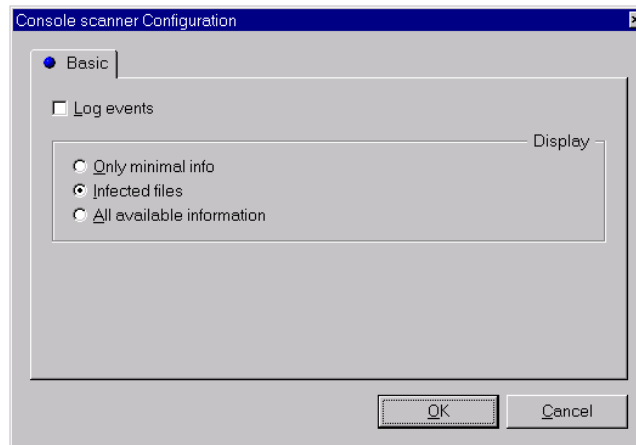

Fig. 92

Dialog also contains switches for amount of information displayed on standard output (usually a command line window):
- "Only minimal info" radio button causes that command line scanner will write only its header,
- When "Infected files" radio button is selected the information about command line scanner header, infected files and the name of viruses will be displayed. The table containing the whole test will be also displayed,

- After selecting "Available information" switch all information about scanner activities and results will be displayed.

Amount of displayed command line scanner information can be also set via command line parameter (see Chapter 8, /V parameter). In such a case the settings on this page will not be respected.
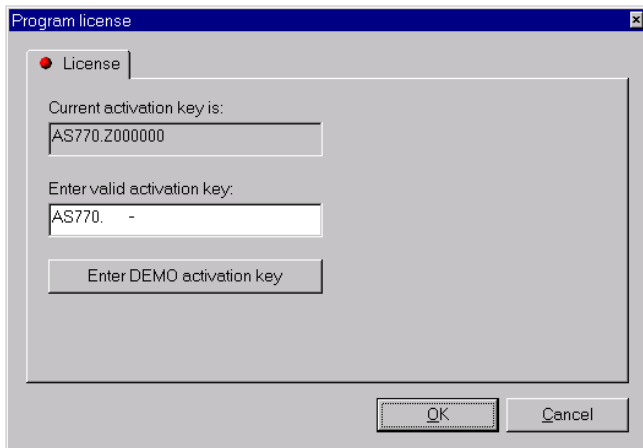
6.4 Item "License ..."

Fig. 93

From "License" item dialog the user can change the activation key of the program (Fig. 93). Among others it contains also the information on the num-ber of bought licenses and therefore if you decide to buy other licenses you will not have to repeat the installation of AVAST32. You will only change the activation key on this sheet and everything will be ready.

The page contains current activation key. There is a text field under it, where new activation key can be entered. By pressing "OK" button the change itself is performed. If entered activation key is not valid, an error message will appear and activation key will not be changed.

Activation key will be changed to demo version number by pressing "Enter DEMO activation key" button. The program will be fully functional for three months only with this activation key (of course, if the valid activation key would not be set up).

The meaning of particular parts of the activation key is provided for in Appendix D.

6.5 Item "Common ..."

Dialog shown after selecting this item provides sheets with common controls for all parts of AVAST32 program.

6.5.1 Sheet "Basic"

This page contains controls for basic setting of all AVAST32 parts (Fig. 94). Control settings on this page are stored for the program as a whole so the changes here will affect all users.

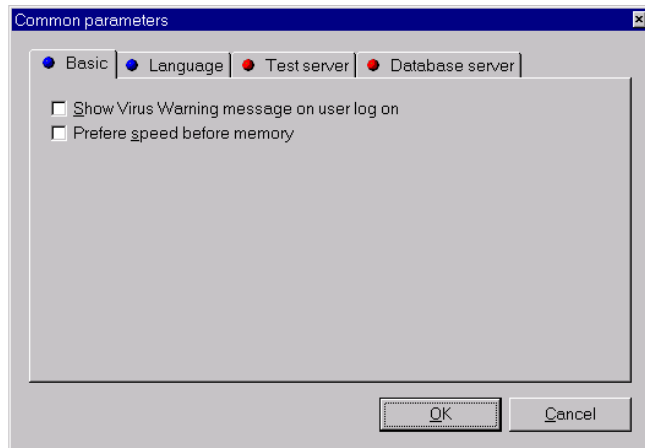The changes will take effect after the AVAST32 restart.

Fig. 94

The "Show Virus Warning message after user log on" check box is designed for enabling the warning message to be displayed after the user's log on into the system. The warning message will only be displayed if a virus has been found during the last start-up of the computer. Thus the user is kept informed that he is working with an infected computer. The box is not checked by default.

The WARN32 program is used to display the warning message and it is described in details in

The "Prefere speed before memory" check box determines the conditions how the testing server ("VPS32.DLL" file, see Appendix A) will be present in memory.

If the box is checked the testing server will be present in the memory from its first utilization, and it will not be removed from it even at the termination of its last activity. If the box is checked the testing server will be removed from the operating memory of the computer immediately when it is not needed anymore i.e. after the termination of the last running task. After the start-up of the next task the testing server will be loaded from the disk again.

If you have enough operating memory, we recommend not checking the box. Thus you will make the run of AVAST32 faster. In case you have a lack of the operating memory it will be better if you check the box - but you will have to be prepared for slower responses of the program. The box is not checked by default.

6.5.2 Sheet "Language"

"Language" sheet allows switching among the languages supported by AVAST32 program (Fig. 95). The languages are named in the list in first column on the sheet. The currently using lan-

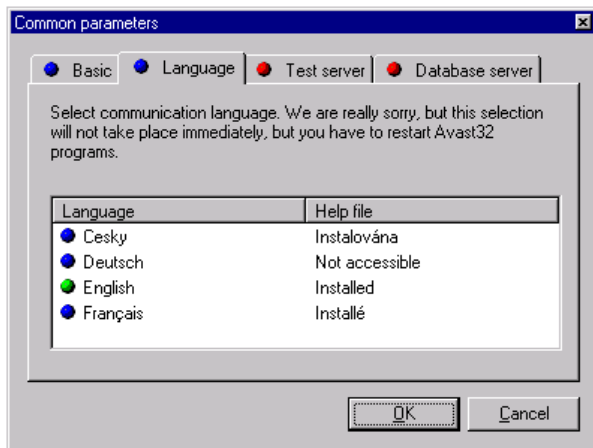guage is marked with green ball, the others with blue one.

Fig. 95

The second column of a list informs user about availability of documentation in appropriate language, i.e. if the documentation has been installed or not.

For language change in AVAST32 program double-click on the appropriate language with the left mouse button. This change will take effect after the next program start. AVAST32 stores this language setting for each user separately so this change will affect the current user only.

By default the language chosen during the installation process is preset (Fig. 3).

6.5.3 Sheet "Test server"

"Test server" sheet allows the user to set basic parameters of the testing server (Fig. 96). It is used by all parts of AVAST32 program so all changes here will have an influence on all the users on current computer (for details see Appendix A).
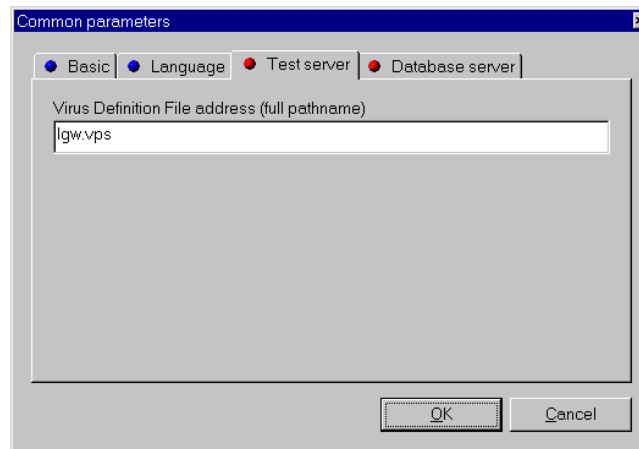

Fig. 96

"Virus Definition File address" text box contains the name of the VPS file, i.e. of the file containing the database of the known viruses including the

complete path to it. As it is a very important file users should realize that by setting an incorrect VPS file they expose themselves to the danger of failing to recognize viruses, or alternatively, to the danger of false positives. The default value is the name of the "lgw.vps" file from the folder of AVAST32.

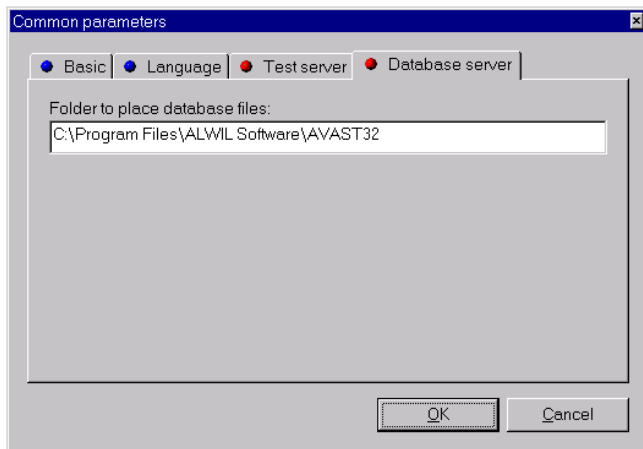### 6.5.4 Sheet "Database server"

Fig. 97

You can set via "Folder to place database files" text field (Fig. 97) to which folder AVAST32 will be storing its database files. It is mainly database of

files stored on your hard drives, which is used during data integrity test.

6.6 Item "Update VPS..."

AVAST32 program provides easy update of known virus database file. It is only necessary to replace the current LGW.VPS file with the newer one, so you do not have to reinstall whole program again.

You can copy LGW.VPS file manually (not recommended) or use this item. After its selecting dialog as shown in Fig. 98 will appear.
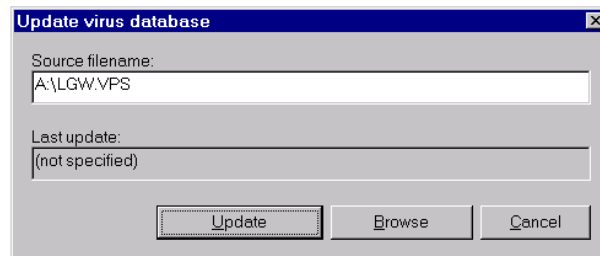

Fig. 98

"Source file name" text box contains the path to the folder in which a newer VPS file will be searched for. The VPS file update can be also performed automatically (Chapter 6.1.2, "Enable automatic VPS update" check box). If you have installed the AVAST32 program from the CD-ROM disc, the text

box will contain the default path "<cd>:\AVS\LGW.VPS" where the identification of your CD-ROM unit is written instead of <cd>. In the case of the diskette installation the path is "A:\LGW.VPS".

You can also specify appropriate folder via standard file opening box which will appear after the pressing "Browse" button.

"Last update" text box contains date and time of the last VPS file update (if there was any).

By pressing "Update" button you start the update of LGW.VPS file. Update will be performed only if the specified LGW.VPS file is newer than the current one.

6.7 Program customizing via Control Panel

It is possible to set up all AVAST32 parts without starting the main program. Just press "Start" button and choose the "Control Panel" item from "Settings" folder (Fig. 99).

Double-click on the "Avast32 configuration" item in the window just shown. A window with several sheets will appear. Description of the sheets will follow.
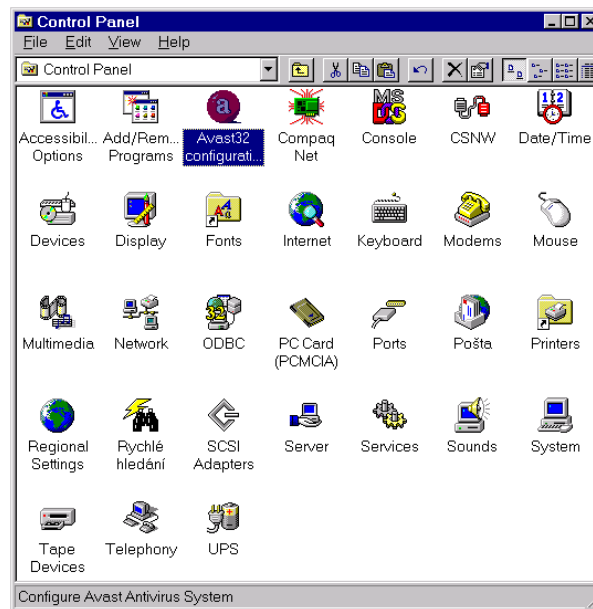

Fig. 99

6.7.1 Sheet "Programs"

"Programs" sheet provides a selection of the program part you would like to set up (Fig. 100). After clicking on the appropriate item a dialog will appear in which you can change program setting via controls.
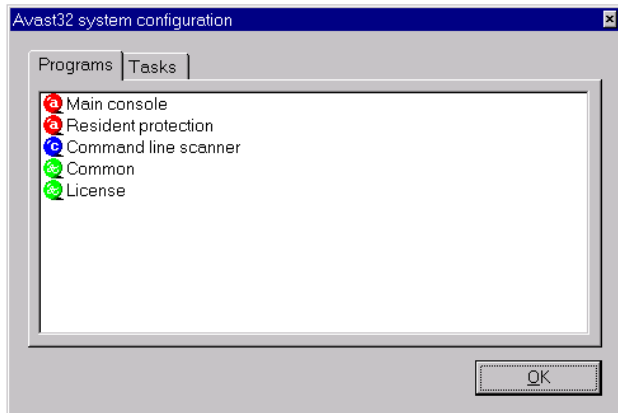
105

Fig. 100

This sheet contains the following list of items:
- "Main console" item shows dialog for setting of AVAST32 program itself. Shown dialog is described in Chapter 6.1,
- "Resident protection" item allows change of resident part of AVAST32 program (RGW32 program, see Chapter 9). Description of displayed dialog can be found in Chapter 6.2,
- "Command line scanner" item serves for basic setting of known virus scanning program which is designed for command line (LGW32 program, see Chapter 8). This dialog box is described in Chapter 6.3,

- You can set various parameters, which are common for AVAST32 program via "Common" item. For detailed information about the displayed dialog see Chapter 6.5,
- The last "License" item provides a possibility to change the serial number of your program copy. This way you can change the number of available licenses without new program installation, see Chapter 6.4.
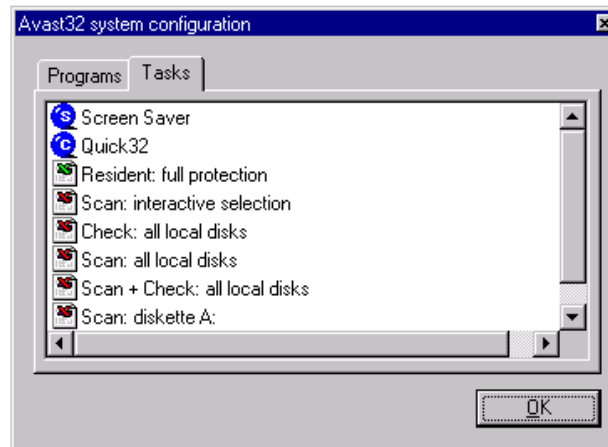
6.7.2 Sheet "Tasks"

Fig.101

From this sheet you can call dialogs for modification of each AVAST32 task (Fig. 101). The tasks list here is similar to the task list in simple or enhanced user interface. If you click on the task name you would like to change a dialog box described in Chapter 4 will appear (description of each sheet from this page can be found in Chapter 4.4.1 to Chapter 4.4.16).

Task list besides usual tasks contains two special tasks, which has special meaning. "Screen saver" task is described in Chapter 12.1 and "Quick32" task in Chapter 10.1.

Shortcut menu

The shortcut menu displayed after the click of right mouse button on the task list on "Tasks" sheet shows Fig. 102.

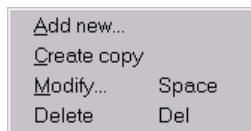*Fig. 102*

- "Add new..." item serves for creating new AVAST32 task without necessity to start the program (see Chapter 4),
- Through "Create copy" item user can create a copy of the task. New task copy will have the same parameter setting as original task. Only if it is shared task and user do not know the valid password copy will be created as a private task,
- "Modify" item as well as clicking on the task name will call the dialog box where task setting can be modified (see above),
- By choosing "Delete..." item it is possible to delete appropriate task from a task list. At first it is necessary to confirm deletion by pressing "Yes" button from a dialog box which will appear after the selection of this item (Fig. 65).

If you perform any change with tasks via "Control panel" and AVAST32 program is running the changes will take effect after the AVAST32 program restart!

6.7.3 Sound setting

AVAST32 has the option to set the sounds for its events which will be played when the chosen event takes place.

Sounds can be chosen from "Sounds" in "Control panel" which is shown on Fig. 55. Since for sound setting is used standard system tool it is not necessary to have AVAST32 program running.

In "Events" list find "Avast32" item and choose the item for which you would like to modify the sound file.

The way to set sound file for certain program events is described in Chapter 4.4.13.

7.Interpretation of results

We recommend reading this chapter thoroughly, and to think over its content. It is possible that we will only repeat old known facts here, but one is never careful enough. Especially the less experienced users of personal computers should pay attention to this chapter and should not ignore it.

The basic fact which you must observe is that there is a direct proportion between the work, knowledge, experience and safety of your computer. You may be surprised to hear that no matter how good an antivirus program is, it will not help you till you pay continual attention to what you are doing especially from the point of view of a possible virus infection. At the same time, if you are not interested in computers, being a physician, economist or lawyer and not having enough time to care for "secondary things" such as the computer and your data safety, we must disappoint you. You are really wrong. And if you do not even want to respect our advice and do not want to learn even the basic principles, then our recommendation for you is to return your program to the seller, who will give you back your money. Thus you will avoid a lot of your as well as our company's worries. In order to carry out your work well, you need to know orthography and grammar. The same applies to the work with computers, because they also require some basic knowledge without it you can rarely be successful.

It is possible to write a program for editing texts, databases or a table processor, which is fully user-friendly and does not practically require any special knowledge, or which could teach you the necessary things. The issues of the safety and anti-virus protection, however, is really something else. We do beg you that you do devote the necessary time and attention to them.

7.1 AVAST32 has found viruses

This part is quite simple, even though not fully trivial. If the AVAST32 program reports that it has found a virus, it does not mean yet that there is really a virus. And even if there is a virus, it does not mean yet that your computer is infected by viruses. Also this text has been written by using a computer that contains a large amount of various viruses, and yet the author is calm, because these viruses are not **active.**

A detailed description of what to do with a piece of information on the virus found is provided for in

Annex B, the thorough study of which we recommend you.

7.2 AVAST32 has found changes in files

This situation is a bit more complicated, but not unsolvable. Nevertheless, only the experience with periodic work with the AVAST32 program and data integrity tests can bring you the expected results.

The interpretation of results is not easy. The reason is not that the program would provide complicated information or codes, but that each of you will get at each start-up of the integrity tests different information, and its processing may differ on a case-by-case basis. For this reason it is not possible to write there a "cookery book" with a general field of application, which could satisfy all the users. We may only provide for a few pieces of general advice, suggestions and procedures, the application of which we recommend you. Nevertheless, the details and particular implications you must derive by yourselves.

7.2.1 New files

If AVAST32 reports that it has found new files, it may concern several cases. The most easy of them is that it really relates to a new file originating from a legal source. The solution is simple, just accept it,

and thus it will be stored in the database of files. What is the legal source, however, it is a more difficult question. For example, a really legal source is represented by the installation media of the program, which you have recently installed. The program mentioned could also have been installed by your colleague or the Network Administrator. If you have good relationships in your firm, then they were sure to have informed you about this matter, and you may decide whether the file is O.K. or not.

It may also concern a temporary file which was created by a program for its need, and such a program is currently using it or it "has forgotten" to delete it. It is probably also O.K., but a file of this type could also create a virus. The decision may be very difficult and it is fully up to you.

Also the use of the "Recycle bin" for the deleting of files will cause that the new files in the appropriate folder will be detected.

Do not be confused by the fact that a new file has arisen in a folder of a well-known name, e.g. in the operating system folder. The authors of viruses know these directories too, and use them with success.

7.2.2 Changed files

There may really be a large number of reasons for a change in a file. Also the operating system itself lives "its own life" and uses the files very intensively. Each start-up of a program or editing of a

document results in a track which will be detected and annouced by AVAST32. Here it is your turn to decide, which change is valid and which is not. For example, a change in text files will be caused by you ninety-nine per cent of the time, while a change in the **COMMAND.COM** file will be caused ninety-nine per cent of the time by a virus. Please, notice that nothing is one hundred per cent sure, which applies to the whole area of virus problems. The other types of files are situated between the two above specified extreme examples. For example, it is really difficult to say about the documents of the Microsoft Word program (*.doc) why they have changed. The cause may have been you, by simple reading the content, or the "macrovirus" which attacked the document in question.

Nevertheless, it generally applies that if an executable program (extensions exe, sys, dll, bin, vxd, scr,...) is infected, the change is much more suspicious than in the case when a document or data file have been changed. But be careful, even here you may face some exceptions.

7.2.3 Deleted files

There are not many things to help you. The repairing of such a file is only possible by using special tools of the operating system or backup copies. By the way, when was the last time you made backup copies of your data? Do you really want to rely just on good luck?

7.2.4 Special cases

There are several special cases when you will not manage to work with the files. In such a case you will find out that AVAST32 is signaling an error during the work with a file (Chapter 5.3.2).

In the majority of cases you will not be able to check the file which is currently using another program. This file is locked, and the operating system will not allow you to access it. It applies to both the operating system, that uses the files on behalf of itself, and the working programs. The latter need not be seen on the screen of your computer every time. However, if they are working and using the files, Avast32 will not be able to check these files.

If you are working with the operating system which supports safety aspects on the level of files, and if you are using the system of files which also supports this characteristic (Windows NT with NTFS), you must have sufficient rights to be able to check individual files. If your rights are not sufficient, the file will remain unchecked.

8.Program LGW32

The program is used to search for known viruses, including polyform viruses and macroviruses. It is an equivalent to the task in which we would only scan for the presence of the known viruses in the AVAST32 program, and thus it has also very similar setting options.

Since both the AVAST32 and LGW32 programs are using services of the VPS32 testing server, their results are fully identical. The only difference between them is that the LGW32 program uses for its activity only the possibilities of a command line, unlike the very user-friendly environment of the AVAST32 program

The command line of the LGW32 program reads as follows:

```
LGW32 [@<task name> | [+ | -] <area
name>[-][<parameter>, ...]]
```

If you want to run a task created by the AVAST32 program write the character "@" (the at sign) and then its name. If the task name contains spaces it must be inserted between quotation marks. If not, the program will not perform the task! If there is no task name the LGW32 program will check the set areas. The way in which the check is to be per-formed you will specify with parameters as in the case of operating system commands.

It is possible to set several parameters in LGW32 program. Detailed description of these parameters can be found in Chapter 6.3.

But if there is a switch written on command line the parameter will be set after this switch.

[+ | -]
- the signs before an area name mean that also the subfolders are to be tested. The plus sign will enable the test of the subfolders, while the minus sign will disable it.

[-]
- the minus sign after an area name will cause that area is not subject to test. In this way it is possible to inform to the LGW32 program that, for example, the entire disk "D:" except for the folder "D:\Viruses" should be scaned. It has the same effect as the red ball at the name of the area checked in the AVAST32 program (see Chapter 4.4.5).

The **LGW32** program supports the following parameters:

/?, /H, /HELP
- program will display short help. The help contains several pages between which it is possible to switch by using numerical keys, which always identify the number of the page to be displayed. After pressing any key you will return to the command line.

/A
- it will actuate the file scan for the presence of all viruses including those that do not attack the given type of the file. As a result, for example, the file with the **COM** extension will be checked also for the presence of viruses which attack only the **EXE** files.

/C[+]
- it actuates the scan of the complete files (see Chapter 4.4.7). The program will switch to this mode automatically by itself after finding a virus. The "+" (plus) character will also cause that the compressed files will be scaned, internally decompressed and scanned again.

/E[A|E|O|<types>]
- it informs the program of what types of files are to be checked (see Chapter 4.4.4). The letter "A" means that all the files will be checked, the letter "E" identifies the executable files, and finally, the letter "O" identifies the **OLE** documents. You may also directly specify the types of the files to be checked. Their number is not limited and they must be separated by commas. If the parameter is not specified, only the executable files and the **OLE** documents will be scaned.

/X[types]
- the specified types of files will not be checked. This way it is possible to arrange that e.g. all the files except for the text ones (the **TXT** extension) should be checked. The parameter has the same effect as the red ball at the name of the type on the list of the types to be checked in the **AVAST32** program (see Chapter 4.4.4).

/L[-]
- for the operation enables logging. Detailed information about this logging is described in Chapter 6.1.1, at "Enable Avast32 logging" check box.

/M

- it will start the operating memory test. However, nothing else than the operation memory is to be tested.

/R[<name>]

- when carrying out the check, a file containing the report of the progress will be created (see Chapter 4.4.10). If the file name is not specified, the protocol will be written into the "LGW32.RPT" file in a currently valid folder.

/V[N|I|A]

- it specifies about what files the information is to be displayed on the screen. The letter "N" will disable the listing, the letter "I" will enable only the listing of the infected files and "A" will actuate the listing of all the files found.

/U<name>[,<name>]

- it specifies the name of the computer or domain, to which the message of finding a virus is to be sent. At least one name must be written after the parameter.

/Z[+|V]

- it will actuate the automatic removal of the macroviruses found in the OLE documents. The sign "+" will cause that if the virus has not been recognized with full precision in an OLE document, all the macros in the document will be deleted. The letter "V" will ensure the automatic removal of all macros from the document infected. If no character is provided after the switch, only the macro containing a virus will be removed from the OLE document.

When the LGW32 program ends, it returns code to the operating system. This code can later be tested either by the program which launched it, or on the command line by means of the **IF ERRORRLEVEL** command. The return code of the LGW32 program can have only the following values:

0	- program has finished normally, no virus found,
1	- program has found a virus,
10	- time, for which program demonstration version could be used, has expired,
11	- program cannot be run, probably wrong installation,
255	- serious error at the program run.

9.Program RGW32

The program takes care of all the resident tests. It means for example that if you start-up a resident task in the AVAST32 program, just the RGW32 program will be run. Its presence in the memory is indicated by an icon in the right part of the task bar (Fig. 103). By double-clicking with the left button of the mouse on this icon the program window will be displayed.

It is possible to turn off displaying of RWG32 program icon – see Chapter 6.2, "Do not show program icon" check box. For most users it is recommended to let the icon visible.

Fig. 103

You can close RGW32 program and stop running task via this window (Fig. 104). The window contains tree control with two main groups: "Resident Guard" and "Behavior Blocker". By expanding of these items you can see details about activities which are currently performed by the program.

It is possible to set several parameters in RGW32 program. Detailed description of these parameters can be found in Chapter 6.2.
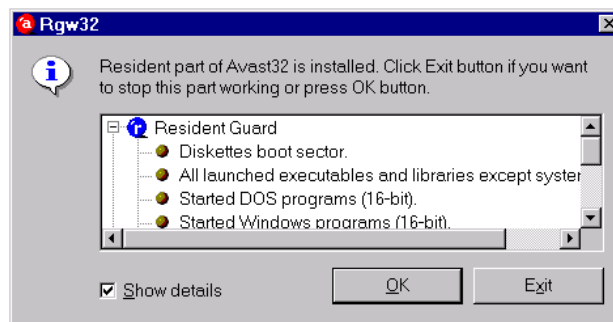

Fig. 104

The command line of the RGW32 program reads as follows:

```
RGW32 <name> | /E
```

The <name> parameter specifies the resident task which is to be run. If the parameter is not specified, or if no task with this parameter exists, the program will display an error message. Only one resident task may be run on one and the same computer. If

114

any other resident task is started, the first task will be canceled.

If the command line contains "/E" parameter instead of task name the current resident task will be terminated. This parameter is suitable especially for terminating of RGW32 program within batch files.

If the task contains also some non-resident activities these activities and their setting will be ignored – always the resident tests will be performed only.

The RGW32 program does not send any return codes.

RGW32 can display several other dialogs during its operation. These dialogs announce to the user a dangerous operation within a file, the finding of a virus in the boot sector of the diskette inserted, or a virus in the program being run or in an OLE document opened using an OLE function. Their description is provided for in the following chapters.

9.1 Reporting dangerous operations

As we have already mentioned, the RGW32 program cares for all the resident tests, which can be performed by the tasks. Also the behaviour blocker belongs among these tests. If a task which contains in itself the activity of behaviour blocker is started-up, then all the operations of the operating system selected are monitored (Chapter 4.4.15).

Fig. 105

At an attempt of performing any suspicious operation the RGW32 program will display a warning (Fig. 105) and will delay the performing of the operation in question until the user informs to it what to do. The warning contains a text box with the name of the file, with which the suspicious operation was to be performed. Furthermore, it contains three buttons:

● if you click on the "OK" button, the operation will be performed with the file. Other possible suspicious operations with the file will be announced as well,

● the "OK & Ignore" button will permit the operation in question, and the RGW32 program will not advise the user of any operations with the file in question till its termination and restart,

- the "Cancel" button will inform the program that it should restrain the performing of the operation in question. After your pressing it the program will not enable the performing of the operation and, of course, it will also inform the user every next attempt of performing the dangerous operation with the file in question.

9.2 Reporting a bootvirus and virus on file starting or document opening

The RGW32 program can also scan the programs being run, OLE documents opened with the help of the OLE functions and boot sectors of the diskettes inserted. The above listed tests will be performed by the RGW32 program, if they were checked off on the "Test" sheet (Chapter 4.4.2).
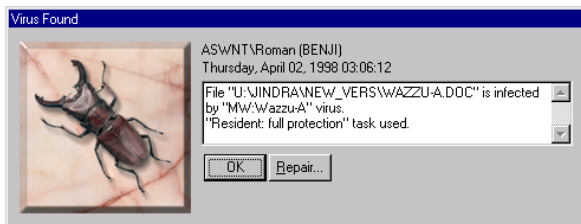

Fig. 106

If you insert a diskette into the drive, then at the first access to it the program will check the boot sector, whether or not it contains a virus. If it finds a virus, it will display a warning message (Fig. 106). You can continue to work with the diskette, because for a virus to become active it has to be started-up first, which occurs in case of a boot virus only at the booting of the system. The purpose of the warning message is to advise you of threatening danger.

The warning message illustrated in Fig. 106 will also be displayed, if a known virus has been discovered in an executable program, or if the user attempted to open an OLE document containing a virus. In order that the RGW32 program can display the message, a task containing the test executable and OLE documents protector must, of course, be started-up, and the check of appropriate files must be selected.

If macrovirus has been found in some document, the warning message contains "Repair" button (like in Fig. 106). By clicking on this button a dialog shown on Fig. 74 will appear, via which you can remove detected macrovirus from document.

If you click on the "OK" button, you can continue your work.

9.3 Warning about diskette presence in drive before system shutdown

When RGW32 program is running it will check if there is not diskette forgotten in drive before system shutdown. The computer is usually infected this way. If there is diskette inserted in drive the program will display an error message and system shutdown will be terminated. In other case the system shutdown is performed as usual.
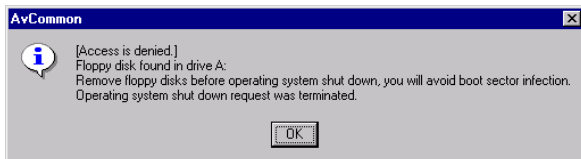

Fig. 107

The check of diskette presence in drive before system shutdown can be disabled – see , "Do not test diskette while OS shut down" check box.

10.Program QUICK32

QUICK32 program is used similarly to AVAST32 and LGW32 for file testing on presence of some known virus.

It is mainly used for file scan called by popup menu (Fig. 23) i.e. in "Explorer" program. In other cases is more useful to use AVAST32 or LGW32 program.

QUICK32 program is set up by default to test all files for virus presence. Compressed files will be at first scanned in its compressed form, then internally decompressed and scanned again.

The command line of the QUICK32 program reads as follows:

```
QUICK32 <name>
```

<name> parameter determines name of folder or file, which will be scanned, including its path. In case that as a parameter was entered folder, all its subfolders will be also scanned.
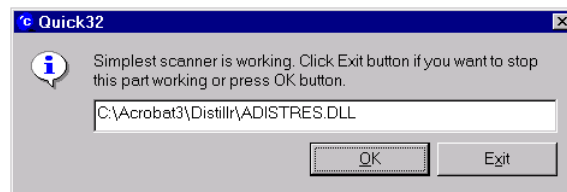

Fig. 108

Fig. 109

The program informs the user on its progress through a small icon situated in the right part of the task bar (Fig. 108). Double-clicking the left button of the mouse on this icon you will see the window with the name of the file being currently scanned (Fig. 109). If you want to close the program erlier, press the "Exit" button. The window will be closed by using the "OK" button.

If the QUICK32 program has found a virus, it will inform the user by means of a warning message (Fig. 24). However, the program will finish after the finding and announcing of the first virus, and that is why the user will only be advised of the first virus in case that the tested folder contains more infected files.

The QUICK32 program does not send any return codes.

10.1 QUICK32 program setting

It is possible to set parameters of QUICK32 program via "Avast32 configuration" item in "Control panel" (see Chapter 6.7).
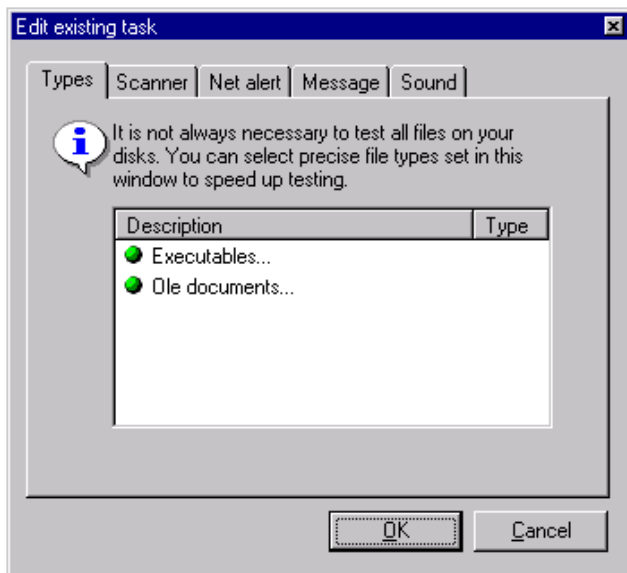

Fig. 110

List on "Tasks" sheet contains "Quick32" item then. By clicking with left mouse button on this item (or by selecting "Change..." item from short-cut menu) it is possible to make appropriate settings.

The window, where changes of QUICK32 program are made (Fig. 110), contains property sheet with sheets of controls:

- "Types" sheet allows to set types of files, which will be scanned, and on the contrary which will be ignored (see Chapter 4.4.4),
- "Scanner" sheet contains controls for setting of virus scanning parameters. Items which setting has no effect on QUICK32 are gray and can not be set up. This sheet is described in details in Chapter 4.4.7,
- On "Net alert" sheet is possible to set, that in case of virus detection, message will be sent to other computers (see Chapter 4.4.11),
- "Message" sheet contains message text, which will be displayed when virus is found (see Chapter 4.4.12),
- "Sound" sheet determines which sound will be played on certain events of Avast32 program (i.e. when virus is found). It is described in details in Chapter 4.4.13.

11.Program WARN32

The purpose of the WARN32 program is to advise the user of the fact that a virus has been discovered in the given computer. It is automatically run after the start-up of the operating system, if the displaying of the warning message is enabled (see Chapter 6.5.1, check box "Show virus warning message after user log on").

The command line of the program reads as follows:
```
WARN32
```
As you can see, the program does not need any parameters to be started-up, and because of the nature of its activity (see below) it does not send any return code either.
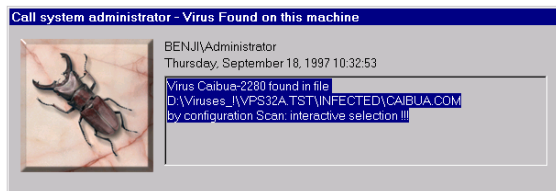

Fig. 111

At its start-up the program looks into the operating system register, whether a virus has been discovered in the computer in question (this information for WARN32 into the register is provided by the AVAST32, LGW32 and QUICK32 programs). If a virus has been found, the program will display a warning message (Fig. 111) which will move along the desktop. The warning message informs the user of the last infected file which was found, on the name of the virus which ifected the file and on the name of the task which discovered the virus.

If no virus has been found, the program will be ended without sending any message about its operation. The user may even not notice that it was started.

If the program has displayed a warning message, its ending is not simple. For this reason a normal user should not start the WARN32 program (by the way, there is no reason to do that).

If a warning message appears after the user's logon into the system, it should be immediately annouced to the Network Administrator or any other authorized person.

The removal of the WARN32 program message from the desktop itself is not sufficient, it is also necessary to arrange for the program message not

to be displayed at the next start-up of the operating system again!

12.Screen Saver

AVAST32 program contains also screen saver, which allows you to scan viruses in time when computer is not engaged, when you are not working on it. Virus scanning works on the background of screen saver chosen by user, so the look of screen saver is fully controlled by user.
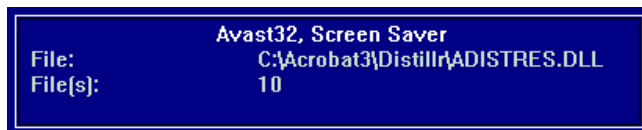

Fig. 112

About test progress is user informed via window moving on the screen (Fig. 112). It contains information about just tested file and the number of already tested files. In case the virus is found the test is stopped and message about virus detection is displayed in the window.

The window can be in several colors. If color depth of display is set to low number of colors (less then 65536) the background is white and the text is black, if virus is found background will be black and the text white. If color depth is set to high colors the text will be white and background blue or red (if virus is found).

Screen saver can be interrupted by key press or mouse move. Only in case the virus has been found the window showing message like in Fig. 106 will be displayed after screen saver interruption. If you would like to use AVAST32 screen saver and you do not know how to tell this to operating system see Chapter 2.8.

12.1 Screen saver setting

It is possible to set parameters of the screen saver via "Avast32 configuration" item in "Control panels" (see Chapter 6.7). List on "Tasks" sheet contains "Screen saver" item then. By clicking with left mouse button on this item (or by selecting "Change..." item from shortcut menu) it is possible to make appropriate settings. You can get to screen saver properties if you click on "Display" icon in "Control panels". In displayed dialog switch to "Screen saver" sheet (Fig. 29) and click on "Settings" button.
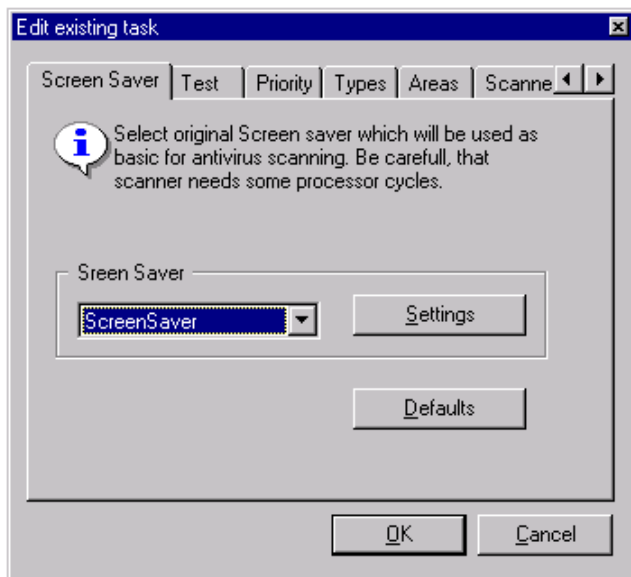
Fig. 113

The window, where changes of screen saver (Fig. 113) are made, contains property sheet with sheets of controls:

- "Screen saver" sheet contains basic controls for screen saver setting – details in Chapter 12.1.1,
- "Test" sheet allows to set what screen saver will be doing (see Chapter 12.1.2).

All the following sheets are available only if "Virus scanning" check box is checked on the "Test"

sheet (see Chapter 12.1.2).

- "Priority" sheet determines priority of testing thread (see Chapter 4.4.3). Higher priority is recommended for screen saver.
- "Types" sheet allows to set types of files, which will be scanned, and on the contrary which will be ignored. (see Chapter 4.4.4),
- "Areas" sheet determines areas where the screen saver will be scanning viruses (see Chapter 4.4.5),
- "Scanner" sheet contains controls for setting of virus scanning parameters. Items which setting has no effect on screen saver are gray and can not be set up. This sheet is described in details in Chapter 4.4.7,
- On "Net alert" sheet is possible to set, that in case of virus detection, message will be sent to other computers (see Chapter 4.4.11),
- "Sound" sheet determines which sound will be played on certain events of Avast32 program (i.e. when virus is found). It is described in details in Chapter 4.4.13.

12.1.1 Sheet "Screen saver"

This screen contains basic controls for screen saver setting (Fig. 113).

The "screen saver" combo box allows choosing screen saver, on which background the viruses will be scanned. The appropriate screen saver can be selected from a list, which will appear after clicking

on arrow on the right part of the box. If no screen saver is chosen or selected one is not available, program will try to find other suitable screen saver.

"Settings…" button allows to set parameter of screen saver selected via above described combo box. Its function depends on chosen screen saver.

By "Defaults" button user can set all controls to its default values.

"Screen saver" sheet is available at whatever setting of screen saver.

12.1.2 Sheet "Test"

"Test" sheet allows to set in details what screen saver will be doing (Fig. 114).

"Virus scanning" check box allows virus scanning by AVAST32 program screen saver. If the check box is not checked, viruses will not be scanned. Virus scanning is enabled by default.

By checking "repeat scanning" box you will cause that after scanning of all selected areas (see Chapter 4.4.5) the scanning operation will be repeated. It is enabled by default.
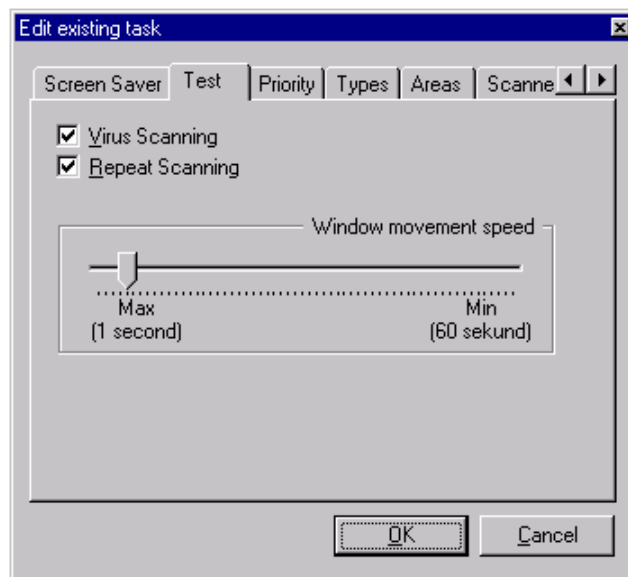

Fig. 114

Scroll bar in "Speed of window moving" box allows to set how fast the window of AVAST32 program screen saver will be moving around the desktop. Default value is 5 seconds.

A.Implementation of virus routines

The information provided for in this Annex are especially designed for the users who want to optimize the work of the system, in which the AVAST32 program is used. This Annex deals with the principles of program work, and it also includes brief descriptions of certain libraries. Normal users probably will not use the information provided for herein.

A.1 General principles

Since the antivirus package AVAST32 contains several programs scanning for viruses, the actual testing is implemented as an independent part which is called out from those programs. Thus the repeating of the code and associated data is avoided, for it would uselessly cause longer running times of the programs and occupation of space in your hard disk and in the memory of your computer. All the programs which need to find out whether there is a virus in your equipment are using the same procedure and libraries, which results in a drastic reduction of operating memory requirements.

Also the use of data is optimized. As it has already been noted, all the data necessary for the searching for viruses is situated in the LGW.VPS file. This file is already large enough, and the bad news from the user's point of view is, that with regard to the continually increasing number of viruses it will continue to grow. If you had a look into it, you could see that its contents are not too meaningful at first sight, nevertheless it is essential for the proper operation of the program. Most of the information contained in it is static. It means that this information can be used by many programs without any danger of rewriting data.

A.2 Used libraries

Several libraries are used for the actual calling up of the antivirus functions. The first of them is the AvMain.DLL library, which is a normal dynamic library, already well-known since the time of the Windows 3.x version. Besides other applications, this library is used for the initialization, "cleaning" and generalization of calling the antivirus services from various types of programs. Generally it is possible to say that it forms an envelope of the actual implementation.

The actual search for viruses takes place in the Vps32s.DLL library. This library is implemented as an "InProc server" working in the "Apartment" work

model. It represents the COM server, which is mapped to the address space of the program, which initializes it. If the above information is all Greek to you, and nothing happens, and you may calmly ignore this chapter.

For its own work this library uses still several auxiliary libraries (Vps32a.DLL, Vps32e.DLL), but these auxiliary libraries perform special works, which are not interesting with regard to the content of this chapter.

The used implementation has one feature which may strike you as interesting, and perhaps you would like to make a use of it. The truth is that the COM servers has an interface which can be observed in a readable and comprehensible form from the external point of view. Many times this fact attracts the users to use them also in any other way than the one in the program which is authorized to do so. We would like to warn you from this temptation! We have two reasons for it. At first, this behaviour is not in accordance with the law, and if we find out about it, we will have to contact our lawyers. The other, much more essential reason is that these functions are not officially documented, and their usage can caused **real damage**. If you rely on the current implementation, you may be really unpleasantly surprised in the future.

A.3 Optimizing of use

The possibility of optimizing the use of the virus routines directly results from the way of their implementation. In fact, each program which uses these functions must have access to all the data which is situated in the LGW.VPS file. This file must be checked, read and analyzed before each use, which lasts a relatively long time. Therefore the above mentioned operations are performed only when the LGW.VPS file is not used any longer.

It means that if a data file is used by other programs, then the start-up of a following program from the AVAST32 package will be faster. For this purpose we also deliver the Vps32.EXE program, the only task of which keeps the data file of viruses in the memory, and thus makes its use faster. This property you will appreciate especially in the case when you are using the check of the files in your computer by means of the local menu of the " Windows Explorer" program, when the initialization of the entire VPS file for each particular file can be frustrating.

The other aspect of this acceleration is less area of the free operation memory in your computer, even at the time when the LGW.VPS is not used by any application.

B.What to do with a virus found

If any program of the AVAST32 package has announced t you presence of a virus it does not have to always mean that the file is really infected. What to do in such a case will be described in the following chapters. Nevertheless, it applies also to this chapter, that the operations described below should be performed by the users who have some experience with the operating systems Windows 95 and NT and know what happens after the performing of the individual operations and what results it can bring about.

B.1 What is a false positive?

Before you start to act under the influence of panic and delete the files detected, send for the antivirus service or ask for a time-unlimited vacation, you must find out whether the file detected is really infected, or whether the pozitive is false. Such a false positive can be caused by a few various reasons, for example:

- alarm caused by using two scanners at the same time (see Chapter B.1.1),
- alarm caused by the immunization of the files (see Chapter B.1.2),
- alarm caused by joking programs (see Chapter B.1.3),
- alarm caused by a failure of computer technology, program equipment or by user's faults (see Chapter B.1.4),
- alarm caused by the operational principles under Windows (see Chapter B.1.5).

AVAST32 is created with a regard to minimizing false positives. The regular tests against them includes about 4 GB (4096 MB) of the files of various origin and content. Nevertheless, despite these thorough tests it may happen that some of the programs from the package returns a false positive message. If this is the case, we ask you to contact us. You will help us to improve our product, and you yourself will have a feeling of higher safety.

If you do not understand the following explanations in this chapter, do not worry about it. Experience in the field of computer work does not belong among the properties which one gets at birth. We just ask you to contact real experts in case of finding a virus.

B.1.1 Alarm caused by using two scanners at the same time

If you are using several different scanners at the same time or immediately after each other, it may happen that some of them will announce to you the presence of a virus in the memory. The reason for doing so is simple. Each of the scanners needs to have, at least for a while, the information of viruses non-coded and accessible in the memory. If at the same moment this memory is tested by another scanner, or if this memory is transferred into the virtual memory, and later used without cleaning, it may happen that this information becomes a cause of the false positive.

The situation is easier, if these scanners are written "improperly", i.e. when they do not clean their memory. In this case it is highly probable that you fill find several (e.g. 5 and more) different types of viruses. In this case the situation is clear, it is the case of a false positive.

The situation is worse in the case when the scanners are written "properly", and they clean their memories after themselves. Also in this case it may happen that you will find a virus in the memory.

How to find out whether it is the case of a false positive? It is easy enough, but maybe quite time-demanding. Terminate your work with all the ap-plications, terminate the operating system and turn off your computer by the power switch. Turn it on again and start-up the operating system. Start the scanner that announced you the presence of a virus in the memory. If it does not announce its presence repeatedly, try to repeat the work (running of pro-grams) which you were doing before starting the scanners, and after some moments start testing against viruses again. If even in this case no virus is found in the memory, it is a false positive.

AVAST32 thoroughly cleans all the used memory and what is more, all the information and virus samples it maintains only in a coded form. Only at the moment of testing it decodes the information on a virus, and having used this information it de-letes it. It means that at any moment there can be not more than one decoded sample of a virus in the memory.

B.1.2 Alarm caused by immunization of files

There are some antivirus means offering and working with the function which we call the "im-munization of files" or with a function which of-fers the adding of the checksum to the file tested. During the next testing the above mentioned utili-ties will simply test the added information compar-ing to the current conditions, and on the basis of

the result they can announced a suspicion of the file being infected by a virus. This process is very fast and quite simple for the implementation.

But this relatively simple and fast process is followed by a few crucial problems. Imagine that there are two products working this way and used for the testing of one file. Through their alternating use they will mutually interfere each other, and both the products will report that the file has been changed.

Another problem is represented by the fact that the testing itself of a file will physically change it. If we do not speak about the copyright problems of the original files, we will face the question, whether you can be sure that the program changed continues working in the same way as its original. Probably it will, but there are programs which check themselves before the start-up, and such programs will not work in case of any change. Furthermore, the above lines only apply in the executable files. Any change in the data files is followed by a high risk of a failure of the program that is using these files.

If you are persuaded that the viruses cannot spread out in the data files you were right until recently. Today we already face a special group of viruses ("**Macroviruses**"), which are spreading out exclusively with help of data files.

AVAST32 does not modify any tested file in any way. For the reasons of higher safety it even opens the tested file only for reading in order that they should not be spoiled even accidentally. If some of the AVAST32 parts save information about files, they do it into an independent file.

Only in a special case, that is at the removal of the viruses found, the writing into the files occurs, but even in this case this process is performed with a file copy and only after the successful completion the file corrected is written with its original name.

B.1.3 Alarm caused by joking programs

If it happens to you, that your computer starts to behave unexpectedly, even suspiciously, it need not be any virus, which is behind it. It may be a joking program, installed in your computer by your colleague, or which was presented to you with false or misleading information on its purpose. An example may be the installation of the presentation of "blue" pictures at the computer start-up. People of weaker characters or less experienced users may have problems with placing into original status, and they may consider a similar "joke" to be caused by the effects of an especially treacherous virus.

Nevertheless, it may not be true. And how to recognize a "joke" from a real virus? It may be difficult as it is not possible to specify the exact borders of these two groups. It is necessary to base

your analysis on the particular situation. For example, viruses cannot afford presentations of some graphical images (especially in colors) because such pictures are too large. The most important difference, which, however, is not easy to recognize, is that unlike "jokes", viruses are reproducing.

B.1.4 Alarm caused by a failure of technology, program equipment or by a user's fault

Problems with technology, programs installed or with other equipment can be easily changed with a virus infection. For example, the frequent problems, which are confused this way, are the problems with printing or with the hard disk. However, there are very few viruses which can cause these problems.

On the other hand, to qualify the message "**Memory parity error**", is really an expert's job because this message can be caused by a defecting memory chip, but also by a virus which writes it on the screen. Only experience may help you here.

B.1.5 Alarm caused by the principles of Windows

Windows uses such a way of memory administration that it will enable you to use more memory than you have in reality. However, it can cause a false positive because the virus "signatures" which are present in the "physical" memory can appear also on the disk in the "virtual" memory. Then it may happen that you will find a virus e.g. in the WIN386.SWP file (in the Windows NT system it is the PAGEFILE.SYS file). It may also happen quite often that the "normal" virus will be found in the .DOC file. Also this is the case of a false positive which you can avoid by opening the file in the Word program, selecting "Save as" and saving it under the same name. Attention! Here you must find out, whether it is not a macrovirus.

B.2 What is really a virus !!!

Probably the first question which comes to your mind may be "**Why just me ?!**". It is not anything strange, a large majority of users have already met a virus, and no danger is threatening only to the "computer recluses". If you have at least a piece of good luck, the infection need not cause any serious harm. **On the other hand, good luck tends to help the more prepared individuals!!**

- The first action (see Chapter B.2.1),
- What type of virus has infected my computer (see Chapter B.3)?
- Combined (multipartity) viruses (see Chapter B.3.1),
- Viruses that remain installed in the memory (see Chapter B.3.2),
- Viruses attacking the files (see Chapter B.3.3),
- Viruses attacking system areas of disks (see Chapter B.3.4),
- Macroviruses (see Chapter B.3.5).

B.2.1 The first action

The most important thing is not to allow panic to govern you. The damage that could be caused by the virus is negligible in comparison with what you may cause by your own hurried action.

Panic is your enemy! If you are the type of character who is easily panicked, leave the computer, if you find a virus, and drink a cup of coffee. Then call your Administrator. You will see that the problem is not so serious.

If you want to do something without any help of others, calmly terminate the work of all the programs running and save your data. It may also happen that you must finish the program which is just running. Nothing happens, you may finish what needs finishing. You have time, only a very small number of viruses may be depending on the time, for which they are active. Only avoid executing other programs (if it is possible). In no case turn off your computer by means the power switch. The consequences would be catastrophic for your data on the hard disk.

The turning off of the computer through the power switch without having finished the work of the operating system ("shut down") is a very bad custom which is sure to have deplorable consequences for you.

If you have managed to end the operating system, turn off the computer by means of the power switch. Have a rest because you will have to think over what to do now.

It is necessary to use this time. Not only do you need to remove the virus, but you also need to discover the exact (or at least highly probable) source of the infection (probably your friend with the latest release of a well-known game). A very important question is how long time you can have the virus in your computer.

You had better be pessimistic, it will pay. The underestimation of this time means beginning the first step to a repeated infection!!!

It is also very important to think about whether you could bring the virus to other places. It does not matter whether you use a company computer and your company has sent thousands of infected diskettes, or you have given only a new release of a

game to your friend. In both cases it is the best thing to inform the others whom the potential infection may concern immediately. **Do it at once!!**

The shame connected with the spreading of a virus infection is much more bearable when you yourself advise of the danger of infection. In case of a company it is the trust of your customers which could be absolutely lost if they found out about the infection and learnt that you knew about it and did not inform them (maybe you can afford it).

One of the most important questions that you must assess is whether you have really saved all important data from the infected computer.

Every removal of a virus brings about the risk of absolute loss of data on your hard disks even in the case that the removal is carried out by a trained and highly experienced expert.

We are sure that you know about the need of saving your data. But be sincere, when did you backup for the last time? And if you do it periodically, did you ever try to restore the saved data in your computer? And even if you comply with both of the conditions, do you have a backup copy of the backup program in any other place than the infected computer? What will you do if the computer will not be accessible anymore?

So, if you do not have any current backup copy, it is high time that you made it. Nothing else can be done, and you must make it bearing in mind that the saved data can contain the virus and that each future start-up of the computer can increase the level of the infection of the system. But you cannot do anything else. A backup copy is really needed, also in the case that the next work could be done by somebody else completely (especially somebody who bears no responsibility for your data).

And now such a small summary of what to do in case of an infection by a computer virus:

- finish your work, do not be in a hurry uselessly, but do not delay with other measures either,
- find out as much information on the virus as possible,
- end the work of the operating system,
- turn off the computer through the power switch,
- think over for how long the computer may have been infected and what is the probable source of the infection,
- inform all to whom you may have sent the data or media infected,
- if necessary, make a backup copy of your data. Do not leave anything up to chance!!

If you have performed the above steps, you may continue your work. Now you must critically assess your own skills and experience with the computer. If you do not understand computers so much, we do not recommend you to remove the virus by your own forces only. However, if you understand the following explanations, you may try it without any

specialized help. How? It is the question that we will try to explain.

Be carefull and avoid the various, so called "would-be experts". If you hear from them e.g. the expression "low level format", run away fast. In fact they may try to destroy you and your data.

Also when you are working in a larger company, contact as the first person your Administrator or the person responsible for computers.

B.3 What type of virus has infected my computer?

It is important to know what type of virus is present in your computer. The next steps directly depend on this fact, and at the same time some of fine aspects of the virus type determination can markedly change the procedure of the virus removal.

If the following explanations seem to be a little unprofessional to somebody, this is caused by our maximum effort of maintaining the readability of this chapter also for users who do not meet viruses very often.

The main types of viruses are the following:
- combined (multipartity viruses),
- viruses that remain installed in the memory,
- viruses attacking the files,
- viruses attacking the system areas of disks,

- macroviruses.

If you meet a virus that appears very rarely and that changes or modifies data files other than the OLE documents, you are likely to have hard luck, because such data is very unreliable or even unusable. At the same time there are no means of how to restore the data files destroyed (perhaps except for the backup of statistical data).

In the following text we will suppose that you are using the operating systems Microsoft Windows 95 or Microsoft Windows NT. The removal of viruses under the MS-DOS system may differ from the procedures described here.

B.3.1 Combined (multipartity) viruses

Combined viruses are simply those viruses that attack some of the file combinations, disk system areas and memory at the same time. Their removal is the combination of the removal of simple types of viruses in an exactly defined order. The following applies to this order:
- it is not possible to remove a virus from the disk if it is present in the memory,
- when removing viruses from the disk it is necessary to remove first the viruses from the disk system areas,
- viruses in particular files are the last to be removed,

B.3.2 Viruses that remain installed in the memory

These viruses are not installed only in the memory, but they are sure to be also present somewhere on the disk.

If some "would-be expert" tells you that a virus can be present in the memory without being present somewhere else (on the hard disk, diskette or any other medium of a similar type), contact somebody else. The safety of your data will be much greater.

A virus may be present in the memory and not active at the same time. Imagine the situation that you are copying the infected file from a diskette to a diskette. Also in this case you use the operation memory of the computer and both source and target files are stored in it. It means that the virus can exist in the memory even after finishing the copying operation, simply because there is no reason for cleaning the memory used in the above described way. However, it does not mean that the virus in this form can cause any kind of harm.

At the same time you cannot remove a virus from your computer at the moment when it is present in the operation memory and it is active. The reason is very simple: the virus immediately attacks each program or disk system area which you try to treat.

You can do nothing about that. It applies generally that you cannot eliminate a virus in the memory at the time when it is present in it. Of course, there can be some exceptions, but you cannot rely on it.

At the same time we must point out that the viruses developed exclusively for the operating systems Windows 95 and NT today practically do not exist, and none of the several very rare examples is capable of remaining residentially in the memory. If the situation changes, we will inform you accordingly.

It follows from the previous paragraph that only the memory can contain the viruses designed for the MS-DOS system, which entered into it at the start-up of the computer or during the work in the DOS window. If it is at the same time a virus which attacks disk system areas, you can directly move to the chapter dedicated to the viruses of this type. As far as the viruses infecting files are concerned, the solution how to remove the virus from the memory is not complicated.

Boot the system from a system diskette. In fact you may use an arbitrary system diskette from MS-DOS 5.0 and higher. Nevertheless, we recommend you to use a system diskette for the system which you have installed in your computer.

Continue the work depending on the type of virus.

Under the operating system Windows NT there are practically no problems with viruses in the memory. The only viruses that can disturb you this way are the viruses attacking disk system areas.

B.3.3 Viruses attacking files

The removal of viruses from the files is simple and rather boring work. The main problem is to decide how to remove the virus.

A one hundred per cent sure renewal will only be ensured by restoring files from their backup copies (of course, if you have any backup copy and if this copy is not infected by the same or another type of viruses). It may be simple and reliable to restore the files from the backup copies. If you devote time to creating backup copies periodically, you will find out why it will pay. It is fast and comfortable work.

If you periodically use the integrity checking program and have the current version of the database at your disposal, you can practically be without any worries. AVAST32 will enable you to restore the files which are infected practically by all the viruses (approximately 95 per cent of different types of viruses). The reliability of the renewal is the same as in the case of the restoring of your files from the backup copies, because AVAST32 is checking, whether it has managed to restore the file to the last bit.

If you cannot use anything from the above paragraphs, the situation starts to be more difficult. Yet you do not have to lose any of your programs. Nevertheless, you must have the original diskettes or their copies at your disposal. It, however, means much more work because you must uninstall and again install the infected programs, which brings about a lot of well-known problems connected with the saving of all the tasks and settings which you have invented with so much effort.

Uninstallation of programs is not limited to their simple deletion from the disk. All the "serious" programs for the operating systems Windows 95 and NT (including AVAST32) are capable to be uninstalled, which means more than just to be deleted from the disk only.

If you cannot use this way either, you are facing a problem. Really a serious problem, because the only thing we can recommend to you is to delete the infected files. To tell the truth, there is still one possible variant, which you can use, but its results may be sad enough. It concerns the possibility of removing the viruses from the files by means of some other antivirus program. Such a removal has a big advantage. You cannot find out whether the file corrected is in the same state in which it was before the infection. It is also the main reason for which AVAST32 does not contain any similar property.

B.3.4 Viruses attacking disk system areas

There are a very large number of viruses which are capable to attack the system area of the hard disks. However, only several of them are the "combined viruses" which are able to infect files and spread with the help of files. Therefore we can say, with a small objection only, that if you have found a virus in the system area of a disk (boot virus), it happened when you were trying to start-up the computer from the diskette. It does not matter whether you managed to do it or not. If there was a virus on the diskette in question, it has infected your computer regardless to the operating system which you currently use.

It is fully useless to think or even persuade somebody that e.g. the virus "J&M" called also "JiMi" entered into your computer by reading data from the diskette only. Simply this is not true, whoever may tell it to you. It is simply nonsense.

An exception is e.g. the virus "OneHalf", which can spread also by means of files, which means that by executing the file infected the computer will be infected. Similar viruses are, however, very, very rare.

Procedure for removal: start up the system from your system diskette and run the following program: **fdisk /MBR** of the appropriate operating system.

It is only important that this diskette should not be infected by a virus. After you have performed these commands successfully, the virus will be removed from the system areas of the disk operating Microsoft Windows 95 and NT.

If you manage to start up the operating system, you have practically won. You can make use of the restoring capabilities of the operating system which are built into it, and they will care for the rest. If you, however, do not manage to start up the operating system at all, it is a disaster.

B.3.5 Macroviruses

They are the viruses which spread through documents. At present these viruses are some of the most frequented viruses in the world. Most often they attack the documents of the Microsoft Word application, but recently they have started to appear also in other office applications.

The removal can be carried out directly from the AVAST32 environment (Chapter 5.3.2). Nevertheless, we recommend that you save the virus-infected documents somewhere, remove the viruses from the originals and then test their readability in your programs. If the documents treated this way are O.K., it is possible to delete their virus-infected backup copies. If not, do not hesitate and contact the staff of our firm.

The algorithms used by the AVAST32 program for searching for macroviruses and their subsequent removal from the OLE documents belong at present to the top products on the world-wide level, which means that your documents will really be cared properly.

C.Task default settings

Sheet "Name"

The text field for the entering task name contains the text "(not specified)". The new task is private by default.

Sheet "Test"

There is selected only "Virus scanning" from non-resident test. "Integrity checking" and "Simple integrity checking" is not selected. There is no resident test checked.

Sheet "Priority"

The priority of the task is preset to a lower value than the priority of the AVAST32 program user interface.

Sheet "Types"

The check of all executable files and OLE document is preset for a new task.

Sheet "Areas"

By default the check of all local hard disks is preset i.e. of all the hard disks which are installed directly in your computer. Also their subfolders will be checked.

Sheet "Common"

None of the boxes on this sheet is checked which means that the new task will be run directly by the user. The AVAST32 program will not be closed at the same time as the last task and only the first virus found by the task will be reported to the external programs.

Sheet "Scanner"

The checked boxes are: "Test memory" (available only under Windows 95), "Ignore virus selectiveness" a "Test compressed files internally".

The task will test the operating memory under the operating system Windows 95. It will ignore the characteristics of viruses. It will test all the files and the compressed files will be scanned both compressed and decompressed. If there is no virus found no message will be displayed.

"Notify all found viruses" check box is selected by default.

Sheet "Checker"

The only "Ignore ARCHIVE attribute" check box is checked. So the integrity checking will ignore the

ARCHIVE attribute of thew files and it will always test the file content.

Sheet "Continue"
The "Task name" text field is blank. After finishing this task no other task will be started.

Sheet "Report"
The check box "Create report file" is not checked. The text box "Report file name/folder" contains the "*" (asterisk) and the box "Overwrite existing report file" is not checked. Thus the new task will not create a report of its activity.

Sheet "Net alert"
The box "Send alert over the network" is not checked so the sending of messages along the network is not permitted and the setting of the other controls on this sheet is ignored. The check box "Send messages only to selected computers" is selected.

The list of the computers on this sheet is empty by default.

Sheet "Message"
Text box for the text of the report contains the following text by default:

File %1 is infected by %2 virus.

Sheet "Sound"
This sheet contains no controls.

Sheet "Online scan"
The "OLE documents", "16-bit Windows applications" and "MS-DOS applications" are checked which means that all the applications running in your computer will be checked. The check box "Scan all except for system libraries" is selected.

Sheet "Online block"
Boxes "DOS file operation" and "Windows file operation" are checked. The "Format" field is not checked under the Windows 95. So all operations except the formatting will be monitored.

Sheet "Ignore"
The file list on this page is empty by default. So suspicious operations with all files on your computer will be monitored.

D.Activation keys and licenses

Activation key is the sequence of characters AABBB.CDDDDDD-EEEEEE. The first part contains the identification of the program, the BBB part defines the number of the program version, and the C item is the character specifying the number of available licenses. If the letter "A" is written here, then only one license has been bought, if "B" is here, then two licenses have been bought, etc. DDDDDD defines the serial number of the program copy and EEEEEE is the code through which the authenticity of the whole activation key is verified.

The AVAST32 program monitors the number of copies running in the network at any given time. If you have purchased fewer licenses than ten, the program will allow you to run always as many licenses as you purchased, plus one. If you have purchased at least ten licenses, you will be allowed to run as many licenses of the AVAST32 program as you purchased, plus two.

The user will be informed by warning message (Fig. 115) about the fact that is running more program copies than bought licenses. By clicking on "Activate" button a dialog box would appear, which allows to change activation key (see Chapter 6.4). You can close the dialog box by "OK" button.
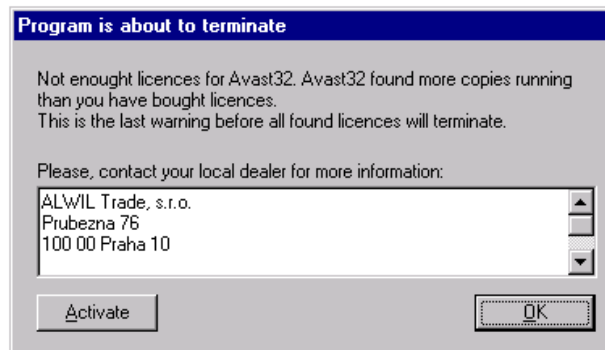
Fig. 115

If the users, despite this message, try to run still other copies of the AVAST32 program, all of its copies that are still running will be terminated.

If you would like to find out on which computers there is AVAST32 program running with your activation key in your network, click with right mouse button on the third item in status bar (this item contains information about available and currently using licenses).

E.Network properties and support

The AVAST32 program of course supports the work in the network, which forms today standard equipment of a number of workplaces.

When a virus is found, the AVAST32 program makes it possible to send a message to anyone of the users connected, the most frequent case is the Network Administrator, or another responsible person. To this purpose the AVAST32 program uses the services which are provided for by the Windows operating systems, which means that no additional task is necessary.

When working in a network, it is necessary to observe the license agreement. The AVAST32 program monitors the number of the program copies which are running so that their number shall not exceed the number of the purchased licenses. More detailed information is available in Annex D.

When working in a network, it may be sometimes a problem to maintain all of the programs used in a release which is up-to-date enough. This applies still more to the antivirus programs. In order that the Network Administrator shall not have to update the databases of viruses in each computer separately, the self-regulation of this activity is built into the AVAST32 program.

All that has to be done is to create the folder, from which all the network users can read. This folder will be entered into the AVAST32 program as a folder which is to be used for the automatic update of the VPS file (Chapter 6.6, text box "Source file name") and, of course, it is also necessary to permit the actual automatic update (Chapter 6.1.2, check box "Enable automatic VPS update").

Then it is enough to copy each of the new VPS file updates (called "small update") to the created folder, and the update will be performed automatically along the entire network. The truth is that the AVAST32 program after its start-up will check whether the selected folder does not contain a newer VPS file. If this is the case, then it will remove the old VPS file and replace it with the newer one.

F.Programer's support

AVAST32 is aimed mainly at the users' public, but it has also a few properties, which can be used especially by programmers. The most important one is described in the following chapter.

If you are entering the path at any place of the AVAST32 program, the name can contain also the name of the system variable which is closed between two "%" (per cent) characters. Hence the root folder of the system can be referred to e.g. this way: "%SystemRoot%". If the system variable of the given name does not exist, then this part of the path will be ignored.

F.1 Sending messages of the viruses found

The AVAST32 program works with the mechanism which makes possible to inform external programs of the viruses found. For this purpose the mailslot bearing the name "\\.\mailslot\AVAST32\VIRUSFOUND" was created. This mailslot contains all the information on the first virus found by a non-resident program, and the information on all the viruses found by the resident programs. It is possible to preset that the information on all the viruses found should be sent into the mailslot (Chapter 4.4.6).

The message of the virus found contains the names of domain, computer, user, infected file and virus which infected the file. The data items are written to the box in the form of a string, they are separated by a zero character from each other.

Index

Microsoft Mail 63, 98
MS-DOS 67, 68, 134

N

network
  alert 62
  drives 55
  properties 141

O

OLE documents 53, 66, 67, 80, 112, 113, 116
  repairing 78

P

password 94
  change 95
Pklite 58
popup menu 43
  Explorer 26, 118
  sheet
    "Areas" 55
    "Ignore" 69
    "Results" 79
    "Tasks" 75
    "Types" 53
  simple user interface 73
programer's support 142
property sheet 42, 46, 47

Q

QUICK32 118
  settings 119

R

README.TXT 11
recycle bin 16, 78, 83
removeable drives 55
reporting
  bootvirus 116
  dangerous operation 115
results 77
  interpretation 108
RGW32 114
  options 99

S

screen saver 30, 34, 41, 122
  settings 122
services
  "Alerter" 64
  "Messenger" 64
sheet
  "Areas" 55
  "Common" 56
  "Continue" 60
  "Checker" 59
  "Ignore" 69

U

uninstallation 8, 17, 18, 135
user interface 36, 42, 46, 71
  enhanced 25, 36, 74
    sheet "Help" 85
    sheet "Results" 77
    sheet "Tasks" 74
    sheet "Viruses" 83
  simple 36, 73
  switching 25, 71

V

virus
  characteristics 112
virus scanning 34, 40, 50, 70
  implementation 125
  presetting 57
  results 77
viruses 83, 130
  attacking files 135
  founded 59, 64, 108, 127
  characteristics 58, 84
  memory resident 134
  multipartity 133
  reporting 57, 59
  system areas *See* boot viruses
  types 133
  warning message 64, 88

VPS file 20
  update 103
    automatic 94

W

WARN32 120
Web 20, 72
wildcards 53, 56, 69
Windows 6, 67, 68, 86, 127, 130, 134
  Windows NT 7, 8, 30, 58, 79, 110, 135
    3.51 21, 54, 56, 63, 69, 83
  Windows 3.1x 67
  Windows 95 7, 30, 64, 68, 92, 96, 138
Wizard 46, 47, 93
Word 27, 35