



# *avast32*

*kompletní antivirový program pro  
Windows 95  
Windows NT*

Grafická úprava a sazba Jan Pařízek, ALWIL Software  
Editor Roman Švihálek, ALWIL Software  
Dokumentace byla zpracována programy Adobe PageMaker 6.5 CZ a Adobe Acrobat 3.0

ALWIL je chráněná obchodní známka firmy ALWIL Trade s.r.o.  
ALWIL Software, AVAST!, AVAST32, jsou obchodní známky firmy ALWIL Software  
Microsoft, MS-DOS, Windows 95, Windows NT, MS Word, MS Excel jsou obchodní známky firmy  
Microsoft Corp.

Software a dokumentace jsou duševním vlastnictvím ALWIL Software a jsou chráněny autorskými právy České republiky a USA, mezinárodními úmluvami a případnými právními předpisy každého státu, ve kterém jsou software a dokumentace používány. Struktura, organizace a kód softwaru je závazné obchodní tajemství a tajná informace firmy ALWIL Software. Jakákoliv kopie software a dokumentace vytvořená v souladu s licenčním ujednáním musí obsahovat stejný copyright a další náležitosti, které se objeví na nebo v software a dokumentaci. Ochranná známka může být použita v souladu s platnými předpisy, včetně identifikace vlastníka ochranné známky. Použití ochranné známky Vám nedává žádná práva k vlastnictví této ochranné známky. Žádosti o bližší informace zasílejte na

ALWIL Software, Lipí 1244,  
193 00 Praha 9 - Horní Počernice, ČR  
tel. (02) 819 216 61, 819 216 62



Copyright © Pavel Baudiš, ALWIL Software, 1988-98  
Copyright © Michal Kovačič, ALWIL Software, 1992-98  
AVAST! Logo Copyright © Vladimír Jiránek, 1992  
All Rights Reserved

<h1>Obsah</h1>	
1. Úvod	6
1.1 Jak kontaktovat prodejce	6
1.2 Požadavky na vybavení počítače	7
1.3 Instalace	8
1.3.1 Než začnete instalovat ...	8
1.3.2 Spuštění instalace	9
1.3.3 Instalujeme	10
1.3.4 Problémy s instalací	16
1.3.5 Instalace z jiných médií	17
1.3.6 Administrátorská instalace	17
1.4 Deinstalace programu	18
1.4.1 Příprava deinstalace	18
1.4.2 Spuštění deinstalace	18
1.4.3 Průběh deinstalace	19
1.5 Používejte originální software	19
1.5.1 Jak rozeznám originální software	20
1.6 Služba AVS	20
2. První kroky	21
2.1 Spuštění programu	21
2.2 Co spustit nejdříve	23
2.3 Jsou zde nějaké viry?	25
2.4 Jak se bránit makrovirům	26
2.5 Jak objevit i dosud neznámý virus	27
2.6 Jak zabránit průniku viru do systému	27
2.7 Než začnete pracovat s cizí disketou	28
2.8 Návrhy pro práci s AVAST32	29
3. Základní popis programu	33
3.1 Vlastnosti a výhody AVAST32	33
3.2 Základní funkce programu	34
3.3 Jednoduché versus rozšířené ovládání	36
3.4 Jaké ovládání používat?	37
3.5 Možnosti jednotlivých ovládaní	37
3.6 Úloha jako základní prvek	38
3.7 Dodávané úlohy	39
3.8 Základní způsoby ovládání programu	41
4. Vytváření nových úloh	44
4.1 Privátní nebo sdílená?	44
4.2 S průvodcem nebo bez něj?	45
4.3 Co úloha obsahuje?	47
4.4 Popis stránek konfigurace úlohy	48
4.4.1 Stránka „Jméno“	48
4.4.2 Stránka „Činnost“	49
4.4.3 Stránka „Priorita“	50
4.4.4 Stránka „Typy“	51
4.4.5 Stránka „Oblasti“	53
4.4.6 Stránka „Společné“	55

4.4.7	Stránka „Hledání virů“	56	6.2	Položka „Rezidentní ochrana ...“	97
4.4.8	Stránka „Integrita“	58	6.3	Položka „Znakový scanner ...“	98
4.4.9	Stránka „Pokračuj“	59	6.4	Položka „Licence ...“	99
4.4.10	Stránka „Zpráva“	60	6.5	Položka „Společné ...“	100
4.4.11	Stránka „Sítové varování“	60	6.5.1	Stránka „Základní“	100
4.4.12	Stránka „Hlášení“	63	6.5.2	Stránka „Jazyk“	101
4.4.13	Stránka „Zvuky“	64	6.5.3	Stránka „Testovací server“	102
4.4.14	Stránka „Sledování“	65	6.5.4	Stránka „Databázový server“	102
4.4.15	Stránka „Rezidentní bloky“	67	6.6	Položka „Obnova VPS ...“	103
4.4.16	Stránka „Ignorovat“	68	6.7	Nastavení programu přes „Ovládací panely“	103
4.5	Kontrola vkládaných údajů	69	6.7.1	Stránka „Programy“	104
5	Popis ovládání programu	70	6.7.2	Stránka „Úlohy“	105
5.1	Nabídka hlavního okna	70	6.7.3	Nastavení zvuku	106
5.2	Jednoduché ovládání	72	7	Interpretace výsledků	107
5.3	Rozšířené ovládání	73	7.1	AVAST32 našel viry	107
5.3.1	Stránka „Úlohy“	73	7.2	AVAST32 našel změny v souborech	108
5.3.2	Stránka „Výsledky“	76	7.2.1	Nové soubory	108
5.3.3	Stránka „Viry“	82	7.2.2	Změněné soubory	108
5.3.4	Stránka „Nápověda“	84	7.2.3	Smazané soubory	109
5.4	Hlášení o nalezení viru	86	7.2.4	Speciální případy	109
5.5	Vybrání testovaných oblastí	87	8	Program LGW32	110
6	Nastavení programu	89	9	Program RGW32	113
6.1	Položka „Hlavní konzole ...“	89	9.1	Hlášení nebezpečných operací	114
6.1.1	Stránka „Základní“	89	9.2	Hlášení boot viru a viru ve spuštěném souboru nebo otevíraném dokumentu	115
6.1.2	Stránka „Rozšířené“	91			
6.1.3	Stránka „Soubory“	93			
6.1.4	Stránka „Varování“	95			

9.3 Hlášení přítomnosti diskety před ukončením systému	115	B.2 Je to opravdu virus!!!	129
10.Program QUICK32	117	B.2.1 První akce	129
10.1 Nastavení programu QUICK32	118	B.3 Jaký typ viru infikoval můj počítač?	131
11.Program WARN32	119	B.3.1 Kombinované (multipartitní) viry	132
12.Spořič obrazovky	120	B.3.2 Viry zůstávající instalované v paměti	132
12.1 Nastavení spořiče obrazovky	120	B.3.3 Viry napadající soubory	133
12.1.1 Stránka „Spořič“	122	B.3.4 Viry napadající systémové oblasti disků počítače	134
12.1.2 Stránka „Činnost“	122	B.3.5 Makroviry	135
A.Implementace virových rutin	124	C.Implicitní nastavení nové úlohy	136
A.1 Obecné principy	124	D.Popis aktivačního klíče a licencí	138
A.2 Vlastní knihovny	124	E.Sítové vlastnosti a podpora	139
A.3 Optimalizace použití	125	F.Vlastnosti pro programátory	140
B. Co s nalezeným virem	126	F.1 Posílání zpráv o nalezených virech	140
B.1 Je to falešný poplach?	126	Rejstřík	141
B.1.1 Poplach způsobený použitím dvou scannerů virů najednou	126		
B.1.2 Poplach způsobený imunizací	127		
B.1.3 Poplach způsobený žertovnými programy	128		
B.1.4 Poplach způsobený chybou techniky, programu nebo uživatele	129		
B.1.5 Poplach způsobený principy operačních systémů Windows	129		

# 1. Úvod

Vážený zákazníku, blahopřejeme Vám k zakoupení antivirového balíku AVAST32, jednoho z nejlepších programů ve své třídě. Doufáme, že budete s našim produktem spokojeni a že se Vám s ním bude příjemně pracovat.

AVAST32 je soubor aplikací, které mají za úkol ochránit Váš počítač před virovou nákazou. Při jeho správném a pravidelném používání a v součinnosti s dalšími programy, např. pro zálohování dat, tak můžete velmi podstatným způsobem snížit riziko napadení Vašeho počítače virem a zamezit tak ztrátě dat.

Cílem této dokumentace je seznámit i méně zkušeného uživatele výpočetní techniky s ovládnutím programu AVAST32 a umožnit mu tak plně využít všech jeho funkcí a vlastností. Nezapomene však ani na „ostřílené“ uživatele osobních počítačů, kteří v této dokumentaci najdou i popis základních principů činnosti jednotlivých aplikací nebo popis činnosti u nás nejrozšířenějších počítačových virů.

Dokumentace je psaná tak, aby čtenář byl postupně obeznámen s vlastnostmi a hlavně funkcemi programu jako celku, ale i jeho jednotlivých součástí. Předpokládá znalost základních pojmů

a dovedností z prostředí operačních systémů Windows 95 nebo NT, bez nichž mohou být některé její pasáže nesrozumitelné. Pokud Vám tedy nic neříkají pojmy jako složka, soubor, okno nebo nevíte jak aktivovat okno či stisknout tlačítko, doporučujeme Vám prostudovat si manuál nebo návodů operačního systému.

V případě jakýchkoli problémů s programem či nejasností kontaktujte svého prodejce nebo firmu ALWIL Trade. Jejich pracovníci Vám rádi a ochotně poradí.

Příjemnou a viry nerušenou práci na Vašem počítači Vám přejí pracovníci firmy ALWIL Software.

## 1.1 Jak kontaktovat prodejce

V případě jakýchkoli obchodních problémů, jako je například neúplnost Vaší dodávky, nebo nečitelnosti instalačního média, se obraťte na svého dodavatele. Pokud u něj neuspějete nebo jej neznáte, obraťte se přímo na firmu [ALWIL Trade s.r.o.](#) nebo na Slovensku na firmu [Micronic s.r.o.](#)

ALWIL Trade s.r.o.  
Průběžná 76

100 00 Praha 10  
tel.: (02) 782 25 47 - 48  
fax: (02) 781 05 48  
<http://www.alwil.com>  
<http://www.anet.cz/alwil/>

SR: MICRONIC, s.r.o.  
Dunajská 12

040 01 Košice  
tel.: (095) 76 37 41  
fax: (095) 72 99 001

Firmu ALWIL Trade můžete kontaktovat také pomocí elektronické pošty a to na adresách:  
obchodní ředitel  
[rtrnka@alwil.cz](mailto:rtrnka@alwil.cz)

objednávky a jejich zpracování  
[objednavky@alwil.cz](mailto:objednavky@alwil.cz)

prodej programů, AVS  
[jberankova@alwil.cz](mailto:jberankova@alwil.cz)

fakturace  
[pourednikova@alwil.cz](mailto:pourednikova@alwil.cz)

## 1.2 Požadavky na vybavení počítače

K tomu, aby mohl být AVAST32 úspěšně nainstalován na Váš počítač a poté i bezchybně pracovat, je nutné, aby Váš počítačový systém splňoval několik základních požadavků. Vzhledem k dnešnímu standardu jsou to však požadavky opravdu minimální:

- procesor minimálně 80386 nebo plně kompatibilní,
- 8 MB instalované a využívané paměti RAM pro provoz pod operačním systémem Windows 95 a 16 MB pro Windows NT,
- 10 MB volného místa na disku pro vlastní program + 2 MB volného místa na disku pro instalaci,
- běžící operační systém Windows 95 nebo Windows NT 3.51 nebo novější,
- ačkoliv lze celý program AVAST32 ovládat klávesnicí, doporučujeme při jeho ovládání používat myš nebo jiné ukazovací zařízení.

Obecně platí, že čím lepší je vybavení Vašeho počítače, tím budou i rychlejší odezvy jednotlivých aplikací.

Běh programu AVAST32 na počítači s méně než 8 MB paměti nebyl testován! Odezva samotného operačního systému na takovém počítači je ale tak

pomalá, že další zátěž prakticky znemožňuje jakoukoli činnost. Nicméně je možné, že i na těchto počítačích bude program AVAST32 pracovat. To ovšem doporučujeme pouze opravdu trpělivému uživateli.

### 1.3 Instalace

AVAST32 je dodáván na CD-ROM (popř. na několika disketách) v komprimovaném stavu a tudíž není možné jej přímo použít. Pro jeho snadnou instalaci byl vyvinut instalační program, který provede všechny činnosti potřebné k provozování produktu na Vašem systému.

Instalace programu AVAST32 nespočívá pouze ve zkopírování vlastních souborů na Váš pevný disk. Instalace mimo jiné provede veškerá potřebná nastavení systému a zajistí, aby po dalším spuštění systému byla automaticky spuštěna rezidentní ochrana Vašeho systému (bude se automaticky spouštět úloha „Rezidentní: plná ochrana“, viz [kapitola 2.6](#)).

#### 1.3.1 Než začnete instalovat ...

S instalačním diskem CD-ROM pracujte s největší opatrností a po instalaci jej ihned uschovejte na bezpečném místě. Bude-li instalační médium poškozené, nebude možné program nainstalovat!

Máte-li disketovou verzi, pak jako vůbec první operaci před započítím instalace Vám doporu-

čujeme vytvořit si záložní kopie originálních disket. K tomu budete potřebovat stejný počet disket s vysokou hustotou záznamu (diskety jsou označeny písmeny HD). Pro překopírování obsahu disket doporučujeme použít příkaz DISKCOPY operačního systému. Při další práci používejte jenom tyto nově vytvořené diskety a originály uschovejte na bezpečném místě.

Před započítím instalace se ujistěte, zda opravdu pracujete pod operačním systémem Microsoft Windows 95 nebo Microsoft Windows NT. V případě, že pod žádným z těchto systémů nepracujete (používáte například Microsoft Windows 3.x s nadstavbou Win32s), nebudete moci použít AVAST32 ani instalační program pro jeho instalaci. Nejpravděpodobnější výsledek pokusu o spuštění bude „spadnutí“ počítače. V takovém případě se pokuste instalovat program AVAST!

Dále se ujistěte, že již nemáte nainstalovanou předchozí verzi programu AVAST32. V případě, že tomu tak je, pokuste se jí deinstalovat. Popis deinstalace příslušné verze programu AVAST32 naleznete v jejím manuálu, popř. v nápovědě. Pokud tak neučiníte, instalační program se starší verzi pokusí deinstalovat sám. Tento postup však nedoporučujeme.

Abyste mohli AVAST32 nainstalovat v prostředí operačního systému Windows NT, musíte mít administrátorská práva. Nemáte-li je, instalační prog-



ram Vás na tuto skutečnost upozorní a odmítne program instalovat! V takovém případě se obraťte na administrátora Vaší sítě.

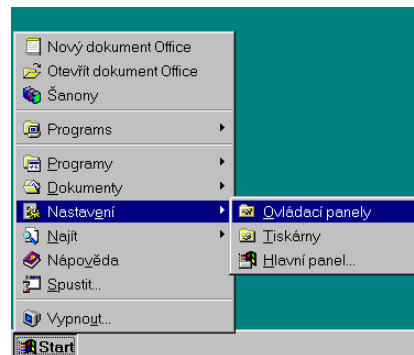
Budete-li chtít používat nápovědu programu AVAST32, musíte před jeho spuštěním nainstalovat také program Acrobat Reader (doporučujeme Vám tento krok provést ještě před vlastní instalací programu AVAST32 - v opačném případě můžete být instalačním programem upozorněni na nepřítomnost Acrobat Reader-u). Instalační program se jmenuje „Ar32e30.exe“ a naleznete jej na dodávaném CD-ROM ve složce „Acrowin“. Instalace programu Acrobat Reader probíhá v podobném prostředí jako instalace programu AVAST32 a kromě dotazu na cílovou složku je zcela automatická.

Není vhodné, aby cílová složka, do které se bude program Acrobat Reader instalovat, byla shodná se složkou programu AVAST32. Taková instalace by zřejmě vedla ke konfliktů mezi programy a správně by nepracovala ani jejich deinstalace. Doporučujeme Vám proto programy instalovat do přednastavených složek. AVAST32 si program Acrobat Reader najde, ať je instalován kdekoli na Vašem počítači.

Pokud jste splnili všechny uvedené podmínky, můžete přistoupit k instalaci produktu.

### 1.3.2 Spuštění instalace

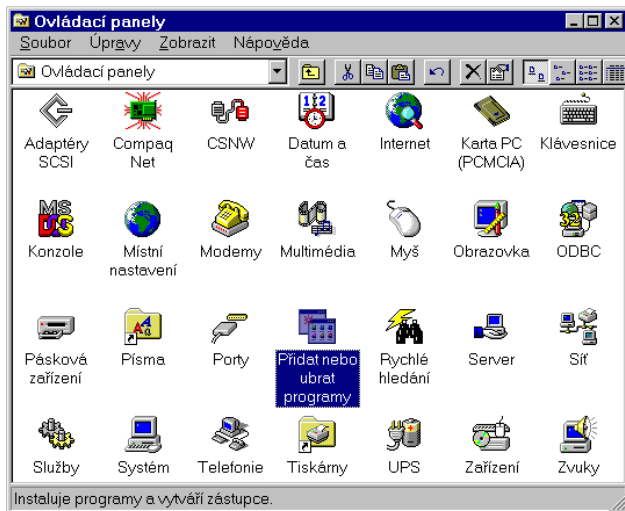
Pro odstartování instalace programu AVAST32 můžete použít několik způsobů. Nejjednodušším z nich je použití k tomu vyvinutého prostředku operačního systému. Nejprve však vyjměte všechny disky a disky CD-ROM z mechanik Vašeho počítače a vložte instalační CD-ROM programu AVAST32 (nebo, máte-li disketovou verzi, první instalační disketu). Klepněte levým tlačítkem myši na tlačítko „Start“ na hlavním panelu a v nabídce, která se objeví, klepněte ve složce „Nastavení“ na položku „Ovládací panely“ (obr. 1).



obr. 1

Po provedení této operace se objeví okno, které obsahuje několik položek. Stiskněte dvakrát krát-

ce po sobě levé tlačítko myši (tomuto úkonu říkáme poklepání) na položce „Přidat nebo ubrat programy“ (obr. 2).



obr. 2

V okně, které se otevře na obrazovce Vašeho počítače, klepněte na tlačítko „Nainstalovat“. Potom klepněte na tlačítko „Další >“. Počítač automaticky najde instalační program, a nyní už jen zbývá jej spustit - klepněte tedy na tlačítko „Dokončit“. Vlastní proces instalace je podrobně popsán v následující kapitole.

Zkušenější uživatelé také mohou přímo spustit program „Setup.exe“ na instalačním CD-ROM, nebo na první disketě (instalujete-li z disket). Způsob, jak spustit program je podrobně popsán v manuálu nebo nápovědě operačního systému. Běžným uživatelům doporučujeme použít první, výše popsaný způsob spuštění instalace.

Všechny způsoby odstartování instalace jsou zcela totožné a jejich výsledek bude naprosto stejný.

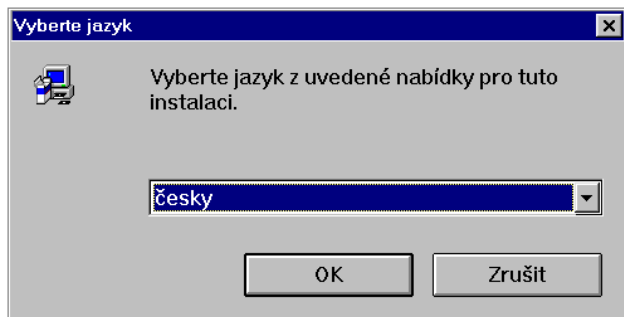
### 1.3.3 Instalujeme

Instalace programu AVAST32 probíhá formou dialogu mezi uživatelem a instalačním programem. V následujícím textu si podrobně popíšeme jednotlivá okna, která budou v průběhu instalace zobrazena.

Instalaci je možné kdykoli přerušit - u jednotlivých oken instalace je popsáno jakým způsobem to lze provést. Před vlastním ukončením bude uživatel dotázán, zda to s ukončením instalace myslí opravdu vážně. Po potvrzení přerušování instalace bude vše, co bylo doposud nainstalováno, odstraněno a systém bude uveden do původního stavu.

Po spuštění instalačního programu budete vyzváni, aby jste zvolili jazyk, kterým chcete s programem komunikovat (obr. 3). Volbu provedete výběrem příslušného jazyka ze seznamu, jenž

se objeví po klepnutí na šipku vpravo od aktuálního jazyka.



obr. 3

Po zvolení jazyka budete požádáni o chvíli strpení, zatímco bude program pracovat na přípravě instalace.

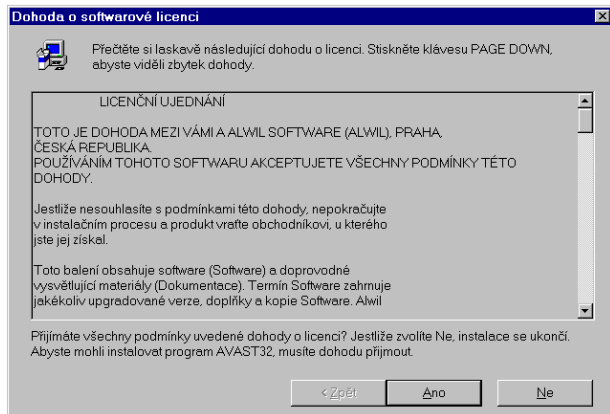
Jakmile je příprava instalace dokončena, objeví se obrazovka vlastního instalačního programu (obr. 4). Uprostřed je okno tzv. průvodce, který Vám pomůže s celým procesem instalace. V jeho spodní části se nachází tři tlačítka, sloužící ke sdělení Vašich pokynů průvodci.



obr. 4

Tlačítko „< Zpět“ slouží k návratu k předchozímu oknu průvodce. Pokud jej není možné použít (např. pokud jste u prvního kroku instalace, jako na obr. 4), pak je tlačítko zšedlé. Tlačítko „Další >“ slouží naopak k přechodu na následující krok průvodce. Dříve než jej však použijete, doporučujeme Vám si důkladně přečíst obsah okna průvodce. Tlačítkem „Storno“ můžete proces instalace kdykoli přerušit.

První okno průvodce informuje uživatele o majiteli autorských práv a varuje před neoprávněnou manipulací s programem nebo jeho částí. Po jeho přečtení klepnutím na tlačítko „Další >“ přejdete k následujícímu oknu průvodce.



obr. 5

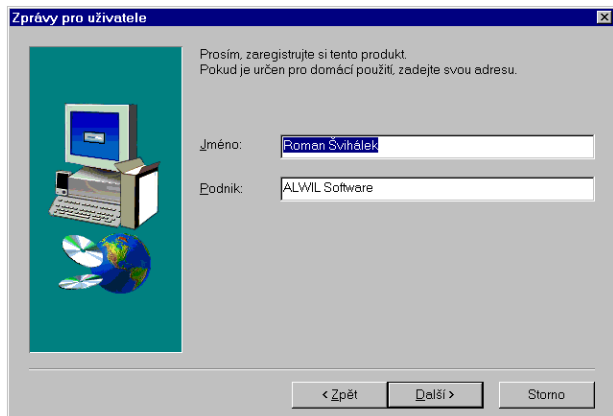
Další okno instalačního programu obsahuje licenční ujednání mezi Vámi a firmou ALWIL Software (obr. 5). Licenční ujednání obsahuje podmínky, které musíte jako uživatel AVAST32 dodržet, a práva, která jako uživatel programu máte. Jestliže s licenčním ujednáním a se všemi jeho částmi souhlasíte, pak klepněte na tlačítko „Ano“. Průvodce Vás poté pustí k dalšímu kroku instalace. Pokud s licenčním ujednáním nesouhlasíte, klepnutím na tlačítko „Ne“ ukončíte instalační program. AVAST32 pak nebude nainstalován.

Protože je licenční ujednání větší než okno průvodce, nelze jej zobrazit celé. Po pravé straně okna se nachází posuvná lišta, pomocí níž je

možné se v licenčním ujednání pohybovat. Její jezdec zároveň zobrazuje pozici, ve které se právě nacházíte. Pro zobrazení zbývajících částí licenčního ujednání je možné též použít kláves pro posun kurzoru nahoru a dolů, popř. kláves označených „PgUp“ a „PgDn“ pro přesun na předcházející nebo následující stránku licenčního ujednání.

Okno, následující za oknem s licenčním ujednáním, zobrazuje soubor README.TXT. Ten obsahuje důležité informace, které jsme již nestihli zařadit do této dokumentace. Informace se mohou týkat vlastního programu, ale také např. instalace a může obsahovat i návody jak postupovat, nastanou-li nějaké problémy. Rozhodně byste si měli soubor README.TXT důkladně přečíst - ušetříte si tak možné komplikace.

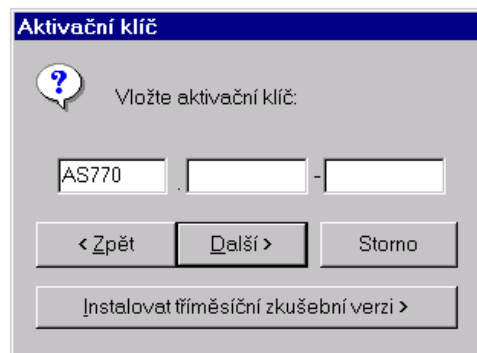
V zobrazeném textu je možné se pohybovat stejným způsobem jako v případě licenčního ujednání v předchozím okně průvodce. I ovládní okna je velmi podobné. Máte-li soubor README.TXT přečtený, klepnutím na tlačítko „Ano“ přejdete na další okno průvodce. Tlačítko „< Zpět“ Vás vrátí na předchozí okno s licenčním ujednáním a tlačítkem „Ne“ instalaci programu AVAST32 ukončíte.



obr. 6

V následujícím okně (obr. 6) po Vás průvodce požaduje, aby jste zadali Vaše jméno a jméno Vaší firmy (popř. Vaši adresu, jestliže je instalace určena pro použití v domácnosti). Průvodce se pokusí zjistit potřebné informace sám, a tak většina uživatelů bude moci přednastavené údaje potvrdit. Jestliže údaje neodpovídají skutečnosti, je pochopitelně možné je opravit. Klepnete-li levým tlačítkem myši do prostoru textového pole s údajem, který chcete upravit, bude Vám umožněna jeho editace. Na místě, kde jste tlačítko myši stiskli, se objeví kurzor a klávesnicí pak provedete vlastní změnu.

Odpovídají-li uvedené údaje skutečnosti, klepnutím na tlačítko „Další >“ je potvrdíte a dostanete se k dalšímu oknu průvodce. Tlačítko „< Zpět“ slouží k návratu k oknu se souborem REA-DME.TXT a tlačítkem „Storno“ je možné instalaci přerušit.



obr. 7

Na obr. 7 je vidět okno průvodce, do kterého je třeba zapsat aktivační klíč Vaší kopie programu. Aktivační klíč má tvar

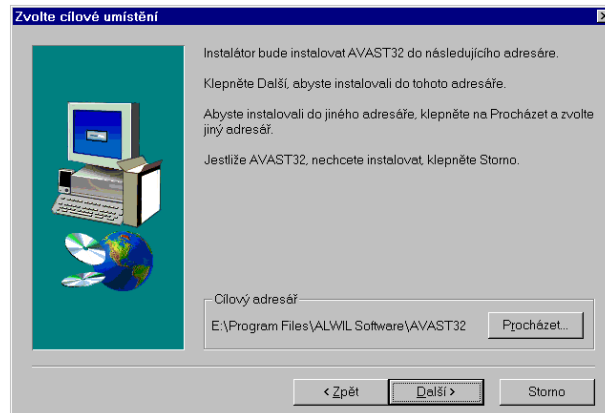
**AABBB.CDDDDDD-EEEEEE.**

První část aktivačního klíče (AABBB) je již průvodcem přednastavena, je tedy zapotřebí zapsat zbývající dvě. Část CDDDDDD se zapisuje do prostředního textového pole a část EEEEEEE pak do zbývajících textového pole. Zapsat nebo

změnit údaje v jednotlivých textových polích Vám bude umožněno po klepnutí levým tlačítkem myši na příslušné pole. Přesunout se na dané textové pole je také možné opakovaným stiskem klávesy „Tab“.

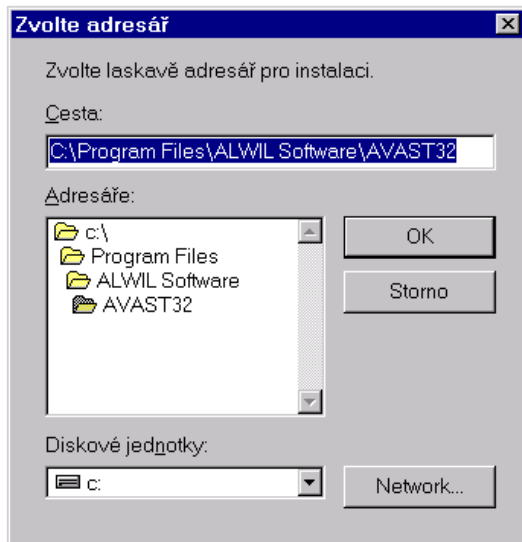
Po zapsání aktivačního klíče jej pro jistotu ještě jednou zkontrolujte. Bez jeho správného zadání nebude program nainstalován! Neznáte-li aktivační klíč, můžete si nainstalovat tříměsíční demoverzi programu - klepněte na tlačítko „Instalovat tříměsíční zkušební verzi >“.

Tlačítkem „Další >“ potvrdíte zadané aktivační klíč a jestliže bylo zadáno správně, pak Vás průvodce pustí k dalšímu oknu. V opačném případě obdržíte chybové hlášení a aktivační klíč budete muset opravit. Tlačítkem „< Zpět“ se vrátíte k oknu se jménem uživatele a firmy. Tlačítko „Storno“ ukončí instalační program.



obr. 8

Jestliže zadaný aktivační klíč byl správný, objeví se okno, ve kterém průvodce požaduje určit cílovou složku, do které má být AVAST32 nainstalován (obr. 8). Tato složka je uvedena v rámečku „Cílový adresář“. Přednastavena je složka „ALWIL Software\AVAST32“, která bude vytvořena na Vašem systémovém disku ve složce „Program Files“. Většině uživatelů bude přednastavená složka vyhovovat, ti ostatní mohou klepnout na tlačítko „Procházet ...“ a pomocí dialogu na obr. 9 vybrat cílovou složku. Méně zkušeným uživatelům doporučujeme použít přednastavenou složku; vyhnou se tak možným problémům.

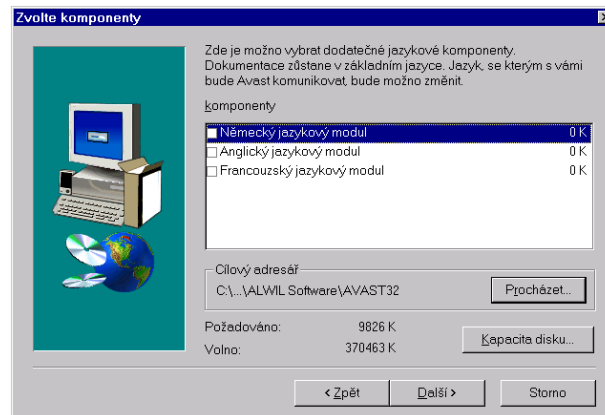


obr. 9

Jste-li s výběrem cílové složky spokojeni, tlačítkem „Další >“ přejdete na následující okno. Klepnutím na tlačítko „< Zpět“ se vrátíte k oknu s aktivačním klíčem a tlačítkem „Storno“ můžete přerušit instalaci.

Okno na obr. 10 následuje po okně s volbou cílové složky pro instalaci programu. V jeho vrchní části je umístěn seznam komponent, které můžete si můžete nechat nainstalovat spolu s vlastním programem AVAST32. Můžete si tak

např. nainstalovat podporu anglického jazyka. Při práci s programem si pak každý uživatel může vybrat, jaký jazyk chce používat.



obr. 10

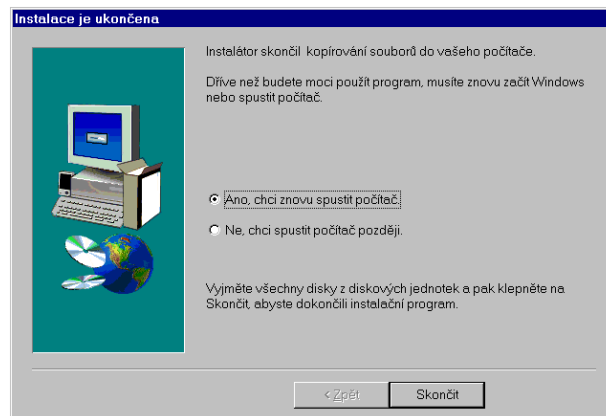
Okno umožňuje také pozměnit cílový adresář pro instalaci programu AVAST32 a to po klepnutí na tlačítko „Procházet ...“ (obr. 9). Uživatel si může též nechat zobrazit informace o volné kapacitě na jednotlivých discích počítače. Klepnutím na tlačítko „Další >“ potvrdíte vybrané komponenty a cílovou složku.

Následující okno zobrazuje všechny informace, které jste průvodci zadali. Obsahuje tedy jméno uživatele, jeho firmy nebo jeho adresu, aktivační

klíč programu a cílovou složku, do které má být AVAST32 nainstalován. Prosíme, zkontrolujte uvedené údaje a pokud Vám nevyhovují nebo neodpovídají skutečnosti, můžete se pomocí tlačítka „< Zpět“ vrátit k předchozím oknům průvodce a příslušné údaje v nich opravit. Jestliže je vše podle Vašich představ, můžete klepnutím na tlačítko „Další >“ přikročit k vlastní instalaci souborů programu AVAST32 na Váš pevný disk. Tlačítkem „Storno“ můžete instalaci přerušit.

O množství zkopírovaných souborů Vás informuje indikátor na obrazovce instalačního programu. Instalaci souborů můžete přerušit klepnutím na tlačítko v pravé dolní části obrazovky, nebo stiskem klávesy „F3“. Jakmile budou nainstalovány všechny soubory, průvodce automaticky přejde na následující okno.

Poslední okno průvodce ukazuje obr. 11. Obsahuje přepínače, pomocí kterých můžete určit, jestli má být počítač znovu spuštěn nebo jestli má být instalační program ukončen bez spuštění počítače. Doporučujeme Vám nechat zvolený přednastavený přepínač. Klepnutím na tlačítko „Skončit“ ukončíte instalační program a v závislosti na zvoleném přepínači bude znovu spuštěn i Váš počítač.



obr. 11

Po instalaci programu AVAST32 a před jeho prvním spuštěním je zapotřebí počítač znovu spustit. Pokud jste tak neučinili za pomoci průvodce na jeho posledním okně, musíte to provést později sami. V nabídce tlačítka Start zvolíte položku „Vypnout“. V zobrazeném okně potom zaškrtnete položku „Restartovat počítač“ a stiskem tlačítka „Ano“ provedete nové spuštění počítače.

### 1.3.4 Problémy s instalací

Nejnámější problémy s instalací programu AVAST32 jsou popsány zde:

- nelze nainstalovat kvůli chybě aktivačního klíče. Zadáli jste špatně aktivační klíč. Aktivační klíč



je ve formátu: AABBB.CDDDDDD-EEEEEE (jeho význam je popsán v příloze D). Ujistěte se, zda jste jej skutečně opsali správně. Pokud jste si stoprocentně jisti, že ano, písmeno „O“ si nepletete s nulou a nezapsali jste do nějakého textového pole oddělovací tečku nebo pomlčku (jsou uvedeny mezi textovými poli), je nejvyšší čas kontaktovat firmu **ALWIL Trade s.r.o.** a požadovat kontrolu aktivačního klíče.

- AVAST32 nelze nainstalovat, protože na Vašem pevném disku není dostatek místa. V tom případě existuje jediná rada a tou je instalační program ukončit, uvolnit potřebné místo na Vašem pevném disku, tzn. vysypat koš, smazat nepoužívané programy, staré dokumenty apod. (doporučujeme Vám si všechny mazané věci nejprve zazálohovat a potom teprve smazat). Pro úspěšnou instalaci programu AVAST32 budete potřebovat zhruba 5,5 MB volného místa na pevném disku, na který budete program instalovat. Nakonec instalační program znovu spusťte a proces instalace zopakujte.
- program nelze nainstalovat pro nedostatečná práva (pouze ve Windows NT). Pod operačním systémem Windows NT je pro instalaci AVAST32 potřeba mít práva administrátora. Odhlašte se, a přihlašte se jako administrátor nebo kontaktujte administrátora Vaší sítě.

Pokud dojde k nějaké jiné chybě instalace, je zapotřebí přesvědčit se, zda se nejedná o Vaši chybu či chybu Vašeho systému. Pokud zcela vyloučíte problémy na Vaší straně, kontaktujte technickou podporu. Opište si však doslovně veškerá chybová hlášení.

### 1.3.5 Instalace z jiných médií

Program AVAST32 je možné instalovat i z jiného média než z CD-ROM či disket. Tento postup je možné s výhodou použít pro urychlení instalace (až o několik řádů, dle typu použitého média) nebo v případě instalace na síťové stanice. V tomto případě je nutné zkopírovat složky DISK1, DISK2, atd. z instalačního CD-ROM na médium, ze kterého budete instalaci provádět (používáte-li diskety, pak složky musíte nejprve vytvořit a potom do nich nakopírovat distribuční diskety nebo jejich kopie, přičemž první instalační disketu nakopírujete do složky DISK1, atd.) a spustit instalaci z tohoto média způsobem uvedeným v kapitole 1.3.2.

### 1.3.6 Administrátorská instalace

Instalační program pro AVAST32 omezeně podporuje tzv. „administrátorskou instalaci“, která spočívá v připravení vlastní klientské instalace do sdílené složky na souborovém serveru. Vlastní klientská instalace pak může probíhat bez jaké-

hokoli zásahu uživatele zcela automaticky. Tento způsob instalace s výhodou použijí zejména správci většího množství počítačů.

Administrátorská instalace se vytváří tak, že si administrátor vytvoří kopie instalačních disket do složek DISK1 ... DISKn na souborový server, podobně jako při instalaci z jiných médií. Pak zmodifikuje hodnoty v souboru ADMIN.INI ve vytvořené složce DISK1 a nakopíruje na ni soubor AVAST32.CNF s předpřipravenými úlohami. Je třeba si uvědomit, že není vhodné používat v úlohách absolutní cesty k souborům (např. zvukovým).

Pokud chcete vědět o administrátorské instalaci něco bližšího, na první instalační disketě se nachází soubor ADMIN.TXT, který obsahuje podrobnější informace o tomto typu instalace.

## 1.4 Deinstalace programu

AVAST32 je možné kdykoli ze systému deinstalovat. Tato operace nenávratně (samozřejmě s výjimkou opakované instalace) odstraní AVAST32 z pevného disku počítače a uvede systém do původního stavu. Deinstalace řeší i takové problémy, jako je odinstalování sdílených knihoven a obnovení interních informací v registrech operačního systému.

V následujících kapitolách si popíšeme jednotlivé kroky deinstalace.

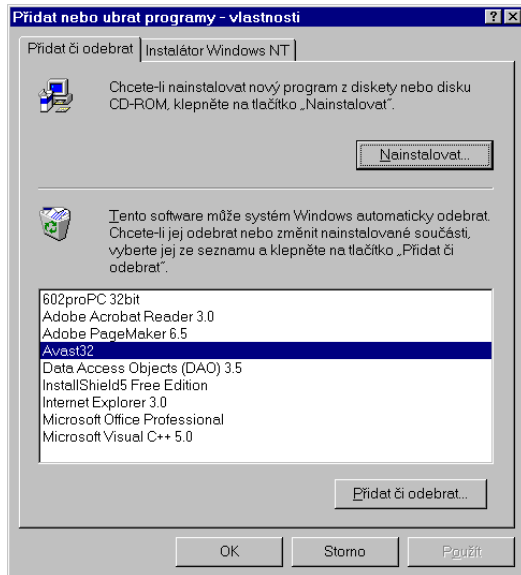
### 1.4.1 Příprava deinstalace

Před deinstalací programu AVAST32 se přesvědčte, že žádný z programů není spuštěn. V opačném případě deinstalace neproběhne v pořádku a na pevném disku zůstanou zbytky AVAST32, popř. se deinstalace odmítne spustit. Také obnova interních dat systému nebude moci být provedena do konce. To může být (a většinou bývá) příčinou **VÁŽNÝCH** problémů při instalaci dalších verzí antivirového programu AVAST32.

Podívejte se na spodní okraj obrazovky na hlavní panel. Pokud na něm uvidíte některý z programů systému AVAST32, ukončete jej. Stiskněte pravé tlačítko myši a zvolte příkaz „Konec“ pro spuštěné programy z AVAST32.

### 1.4.2 Spuštění deinstalace

Pro odstartování deinstalace důrazně doporučujeme použít standardní prostředek implementovaný do operačního systému. Ten naleznete ve složce „Ovládací panely“ se jménem „Přidat nebo ubrat programy“ (nalezení a spuštění tohoto prostředku je popsáno v [kapitole 1.3.2](#)).



obr. 12

V okně tohoto prostředí se ve spodní části nachází seznam instalovaných programů (obr. 12), které podporují automatickou deinstalaci (AVAST32 mezi ně samozřejmě patří). Jestliže chcete deinstalovat nějaký program, v našem případě tedy AVAST32, potom poklepejte levým tlačítkem myši na jméno příslušného programu. Tímto způsobem spustíte proces deinstalace programu AVAST32.

### 1.4.3 Průběh deinstalace

Vlastní průběh deinstalace je plně automatický, kromě prvotního dotazu, zda odinstalování opravdu myslíte vážně. Pokud odpovíte „Ano“, bude AVAST32 deinstalován a systém bude uveden do původního stavu. V případě, že deinstalační program nebude schopen plně odinstalovat všechny součásti AVAST32, oznámí tuto skutečnost těsně před vlastním ukončením. Tato situace nastane poměrně často, protože při práci si AVAST32 vytváří nové soubory a zapisuje si informace do systémových proměnných (tzv. „registr“).

### 1.5 Používejte originální software

Pokud má být ochrana před viry účinná, je potřeba řídit se několika zásadami. Kromě pravidelného používání antivirového programu je potřeba používat některý z programů pro zálohování a uchovávat kopie alespoň nejdůležitějších dat. O data totiž většinou přijdete i bez přičinění některého viru.

Dalším důležitým návykem je používání pouze originálního software, u kterého je riziko napadení virem naprosto minimální. Pirátský získaný software mohl po dobu, po kterou putoval od výrobce až k Vám, nashromáždit nejen virus a prostředky na odstranění následků nákazy virem mohou několikanásobně přesáhnout cenu

originálního software. Navíc, používáním takto získaného programu porušujete zákon a vystavujete se tak možnosti trestního stíhání.

Rámec pro viry bývají i různé veřejné archívy shareware a freeware, u kterých nikdy nevíte, kdo s nimi manipuloval. Pokud se přeci jen rozhodnete takovýto program používat, měli byste jej alespoň prohlédnout antivirovým programem.

### 1.5.1 Jak rozeznám originální software

Obecný návod na rozeznání originálního software od pirátsky zkopírovaného neexistuje, a tak Vám můžeme dát pouze několik rad. Software kupujte pouze u důvěryhodných prodejců a vždy si nechte vystavit doklad o zakoupení. Součástí balení by měl být i nějaký doklad o původu software, jako např. licenční smlouva nebo ujednání, certifikát pravosti apod.

Jestliže místo dokumentace dostanete např. několik archů formátu A5 tisknutých na jehličkové tiskárně, je to přinejmenším podezřelé. Podobné je to i se štítky na instalačních disketách či s potiskem CD-ROM.

Program AVAST32 je dodáván na jednom stříbrném disku CD-ROM, na kterém je vytištěno logo programu AVAST32 a na datové straně se nachází hologram s nápisem „ALWIL“. AVAST32 je možné na zvláštní objednávku zakoupit i na ně-

kolika disketách. Štítky disket potom obsahují logo firmy ALWIL Software a jméno programu.

Jestliže máte pochybnosti o legálnosti Vaší dodávky programu AVAST32, kontaktujte ihned přímo firmu [ALWIL Trade s.r.o.](#)

## 1.6 Služba AVS

Oblast počítačových virů je dnes nejdynamičtějším odvětvím ve světě počítačů vůbec, a proto je nutné používat nejnovější verze antivirových produktů. Pro uživatele to však znamená, že se musí často a sami starat o aktualizaci jejich antivirového programu.

Abychom našim zákazníkům tuto činnost co možná nejvíce usnadnili, poskytujeme již delší dobu antivirovou službu AVS. V rámci této služby poskytujeme po dobu jednoho roku automaticky nejen nejnovější verze databáze virů (tzv. malá aktualizace), ale i případné nové verze programu a zajišťujeme technickou a poradenskou službu.

AVAST32 je aktualizován v rámci služby AVS každý měsíc, vlastní programy pak jednou nebo dvakrát ročně. Další informace o službě AVS Vám na požádání rádi poskytnou pracovníci firmy [ALWIL Trade s.r.o.](#) Aktuální verze souboru VPS je možné získat i prostřednictvím našich WWW stránek.

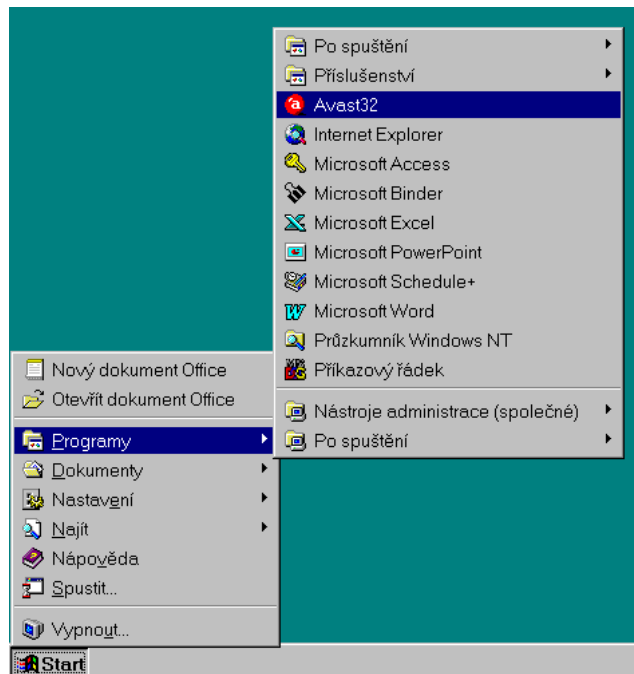
## 2. První kroky

### 2.1 Spuštění programu

Po úspěšně dokončené instalaci můžete ihned program AVAST32 začít používat. Instalační program pro Vás vytvořil položku jménem „Avast32“ v nabídce tlačítka „Start“. Jejím zvolením můžete program spustit. Položka je umístěna v nabídce tlačítka „Start“ (zobrazí se po klepnutí levým tlačítkem myši na toto tlačítko), ve složce „Programy“.

Podoba nabídky tlačítka „Start“ záleží na nastavení prostředí operačního systému a dosud instalovaných programech - jednu z možných podob ukazují obr. 13.

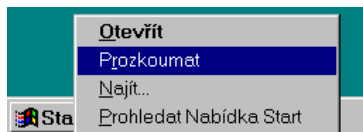
Pracujete-li v prostředí operačního systému Windows NT 3.51, pak pro Vás instalační program vytvořil skupinu „AVAST32 antivirus“, která obsahuje zástupce AVAST32. Spuštění programu tímto zástupcem je naprosto ekvivalentní jakémukoli jinému způsobu spuštění programu.



obr. 13

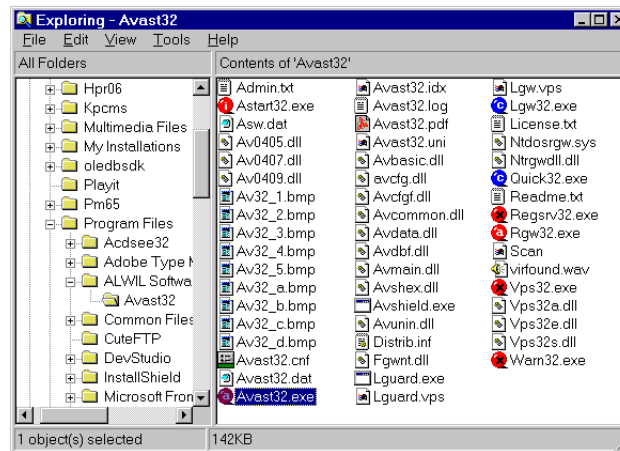
Doporučujeme Vám vytvořit si zástupce programu AVAST32 na pracovní ploše Vašeho počítače.

Nebudete potom muset vždy když budete chtít program AVAST32 spustit procházet složitou strukturou nabídky tlačítka „Start“. Chcete-li si zástupce vytvořit, pak spusťte program „Průzkumník“ - např. tak, že pravým tlačítkem myši klepnete na tlačítko „Start“ a z nabídky, která se objeví, zvolíte položku „Prozkoumat“ (obr. 14).



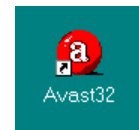
obr. 14

V programu „Průzkumník“ se nastavte na složku, do které jste AVAST32 nainstalovali (obr. 15). Pokud jste neměnili nastavení cílové složky při instalaci, pak je to složka „Program files\ALWIL Software\Avast32“ na Vašem systémovém disku. Potom stiskněte levé tlačítko myši na jménu souboru „Avast32.exe“ a nechte jej stisknuté. Přesuňte ukazovátka myši nad pracovní plochu, tedy nad plochu, která nepřínáleží žádnému oknu, a tlačítko myši uvolněte.



obr. 15

Po provedení této operace se na místě, kde jste tlačítko myši uvolnili, vytvoří zástupce programu AVAST32 (obr. 16). Stisknete-li dvakrát krátce po sobě levé tlačítko myši na tomto zástupci, bude AVAST32 spuštěn.

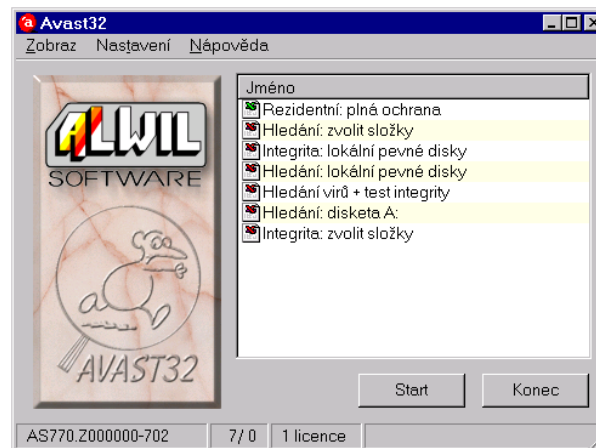


obr. 16

Spustit program AVAST32 je možné mnoha způsoby a všechny jsou si rovny. Je naprosto lhostejné, jestli jste vybrali položku „Avast32“ v nabídce tlačítka „Start“, poklepali na právě vytvořeného zástupce na pracovní ploše anebo jste poklepali na položku „Avast32“ v programu „Průzkumník“ tak, jak ji ukazuje obr. 15. Existují i další možné způsoby spuštění programu, ale těmi se zabývat nebudeme.

## 2.2 Co spustit nejdříve

Po spuštění programu AVAST32 se objeví jeho hlavní okno (obr. 17), které obsahuje seznam položek. Tyto položky představují úlohy, dostupné v danou chvíli. Po instalaci programu AVAST32 Vám doporučujeme zkontrolovat pevné disky Vašeho počítače, zda neobsahují nějaký virus. Aby bylo možné také sledovat změny, které byly provedeny s jednotlivými soubory, a odhalit tak i virus nový a dosud neznámý, je potřeba si vytvořit databázi soborů. Obě dvě tyto činnosti vykoná úloha jménem „Hledání virů + test integrity“.



obr. 17

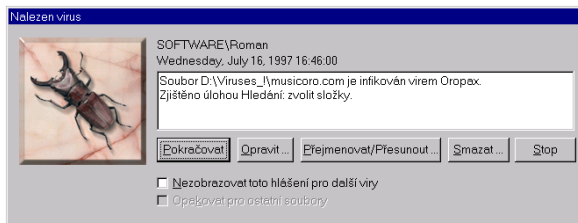
Úlohu spustíte tak, že stisknete dvakrát krátce po sobě levé tlačítko myši (tomuto úkonu říkáme „poklepání“) na jménu úlohy. Že jste úlohu opravdu spustili, poznáte tak, že ikona, která je vedle jména úlohy, se změní na ikonu na obr. 18. Pokud ikona zůstala beze změny, pravděpodobně jste levé tlačítko myši nestiskli dostatečně rychle za sebou.



obr. 18

Spuštěná úloha „Hledání virů + test integrity dat“ prohledá všechny složky na Vašich pevných discích, a soubory, které v nich najde zkontroluje, zda neobsahují nějaký virus. Zároveň si každý nalezený soubor zapamatuje a poznamená si stav, v jakém se nachází na pevném disku. Úloha nezapomene zkontrolovat ani operační paměť počítače.

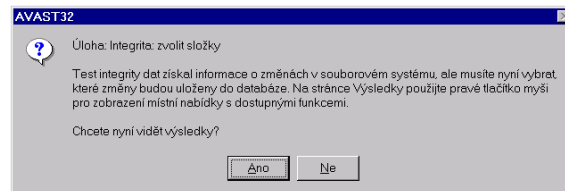
Objeví-li úloha v nějakém ze souborů nebo v paměti virus, zobrazí varovné hlášení (obr. 19). Jak se v takovém případě zachovat, je popsáno v příloze B. V každém případě nepropadejte panice, a pokud si nejste jisti svými počítačovými schopnostmi, odstranění viru raději nechte na někom zkušenějším. Pokud úloha žádný virus nenašla, v průběhu své činnosti nezobrazí žádné hlášení.



obr. 19

Délka provádění úlohy závisí na počtu a typu souborů na Vašich pevných discích a samozřejmě

na rychlosti Vašeho počítače. Může se pohybovat v rozmezí od několika desítek sekund až po několik minut. Její provedení se však rozhodně vyplatí, protože po jejím provedení, můžete zjistit, zda Váš počítač není napaden virem a budete mít k dispozici databázi souborů, pomocí které se můžete v případě proniknutí viru do Vašeho systému pokusit o obnovení souborů.

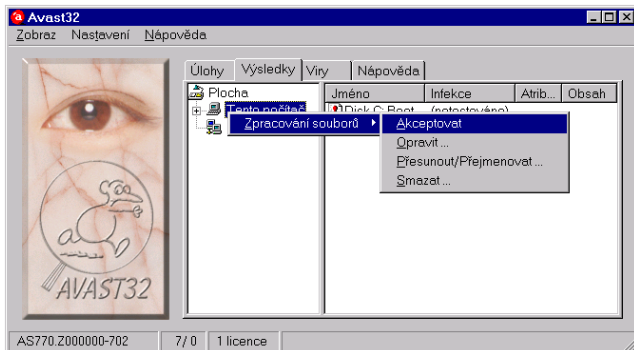


obr. 20

Po skončení úlohy program zobrazí dialog, který ukazuje obr. 20 a ikona vedle jména úlohy bude mít opět svou původní podobu (viz ikony u jmen úloh na obr. 17). Stiskněte tlačítko „Ano“ v dialogu a zobrazí se struktura disků Vašeho počítače se všemi nalezenými složkami a soubory. Nyní je potřeba naplnit databázi souborů. Pravým tlačítkem myši pak klepněte na položku „Tento počítač“. V místní nabídce, která se poté objeví, vyberte ve složce „Zpracování souborů“ funkci „Akceptovat“ (obr. 21). Tím jste sdělili programu,

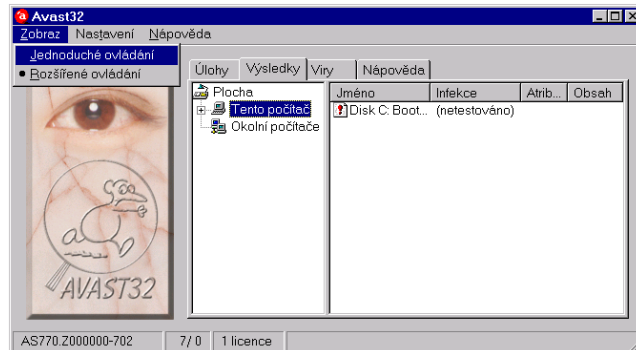


že údaje o všech souborech na pevných discích si má zapsat do databáze souborů.



obr. 21

Pokud je okno, které po provedení předchozích úkonů zůstalo před Vámi na obrazovce, příliš složitě (jste totiž v tzv. rozšířeném ovládání - viz kapitoly 3.3 a 5), můžete se vrátit k původnímu jednoduchému ovládání. Jestliže tak chcete učinit, vyberte z nabídky „Zobraz“ položku „Jednoduché ovládání“ (obr. 22). Přepnete se tak zpět do jednoduchého ovládání, které ukazuje obr. 17.

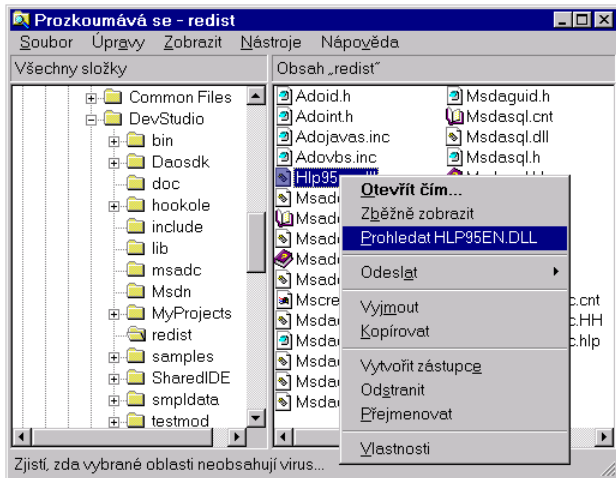


obr. 22

## 2.3 Jsou zde nějaké viry?

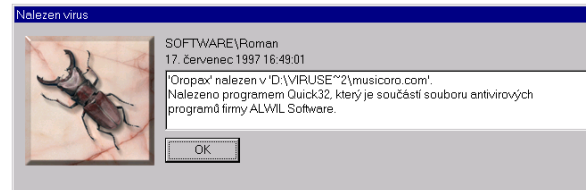
Chcete-li pouze zjistit, zda jsou na Vašem počítači nějaké viry, poklepejte levým tlačítkem myši na položce „Hledání: lokální pevné disky“. Spustíte tím úlohu, která zkontroluje všechny soubory na Vašich pevných discích a nevynechá ani operační paměť počítače. Že úloha opravdu běží, poznáte podle ikony vedle jména úlohy, která bude mít podobu podle obr. 18.

Jestliže AVAST32 v nějakém souboru najde virus, pak každý takovýto nález ohlásí uživateli (obr. 19, bližší popis obsahuje kapitola 5.4). Nebyli žádný virus nalezen, úloha je normálně ukončena; ikona vedle jména úlohy bude vypadat opět jako ikony u jmen úloh na obr. 17.



obr. 23

Potřebujete-li zjistit, zda je nějaký soubor nakažen, není potřeba spouštět kvůli tomu celý program AVAST32. Stačí Vám když se v programu „Průzkumník“ (jeho spuštění je popsáno v kapitole 2.1) dostanete do složky s příslušným souborem a stisknete na jeho jménu pravé tlačítko myši. V místní nabídce, která se objeví, pak zvolíte položku „Prohledat <jméno programu> ...“ (obr. 23). Příslušný soubor bude zkontrolován, zda neobsahuje nějaký virus. Pokud ano, obdržíte varovné hlášení, které ukazuje obr. 24 (hlášení popisuje kapitola 10).



obr. 24

Stejným způsobem je možné prohledat i celé složky, bez nutnosti spouštět celý program AVAST32. Opět na jménu příslušné složky stisknete pravé tlačítko myši a z místní nabídky vyberte funkci „Prohledat <jméno složky>“. Pokud prohledávaná složka obsahuje vnořené složky, budou prohledány i soubory v těchto složkách.

## 2.4 Jak se bránit makrovirům

Závažným problémem v poslední době jsou tzv. „makroviry“. Jedná se o viry, které se šíří v podobě maker v dokumentech aplikací jako jsou MS Word, MS Excel, apod. Před otevřením dokumentu, který byl byť jen otevřen na nějakém cizím počítači, je potřeba jej na přítomnost makrovirů zkontrolovat.

Přinesete-li si dokument na disketu, je výhodné spustit úlohu „Hledání: disketa A:“, která zkontroluje všechny dokumenty a soubory na disketě, zda neobsahují virus. Byl-li v nějakém dokumentu či v souboru nalezen virus, program zobrazí

varovné hlášení (obr. 19). Jak v takovém případě postupovat je popsáno v příloze B.

Jestliže chcete zkontrolovat na přítomnost viru pouze určitý dokument, proveďte to způsobem popsaným v kapitole 2.3.

Potřebujete-li si nahrát dokumenty např. odněkud ze sítě, a nemáte jistotu, že dokumenty jsou čisté (a tu nemáte prakticky nikdy), je tyto dokumenty potřeba také zkontrolovat. Poklepejte levým tlačítkem myši na jméno úlohy „Hledání: zvolit složky“. Po spuštění úlohy, které je indikováno změnou ikony vedle jejího jména, se objeví dialog, ve kterém je potřeba určit složku s kontrolovanými soubory (kapitola 5.5). Dialog i jeho ovládání je velmi podobné standardnímu systémovému dialogu na otevírání souborů.

## 2.5 Jak objevit i dosud neznámý virus

Protože naprostá většina virů mění nějakým způsobem data na pevném disku, je vhodné změny na Vašich discích průběžně hlídat. Potřebujete-li tedy zjistit, zda nějaký soubor na Vašem pevném disku byl změněn, spusťte úlohu „Integrita: lokální pevné disky“ (poklepejte levým tlačítkem myši na jméno úlohy). Spuštěná úloha prohledá všechny pevné disky a zapamatuje si

každý nalezený soubor a stav, v jakém se právě na disku nachází.

Jestliže byl nějaký soubor změněn, pak po dokončení úlohy program zobrazí hlášením s dotazem, zda chcete zobrazit výsledky úlohy (obr. 20). Po stisku tlačítka „Ano“ se před Vámi objeví struktura Vašeho počítače se všemi soubory, které byly od poslední kontroly změněny. Bližší popis zobrazených výsledků je uveden v kapitole 5.3.2; interpretací zobrazených výsledků se zabývá kapitola 7.

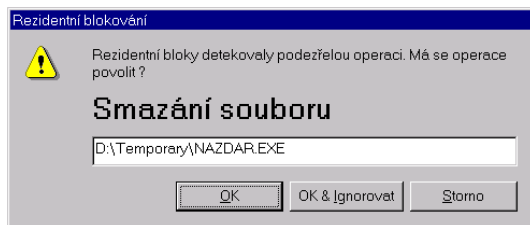
Aby program mohl určit, který soubor byl změněn a který nikoli, je zapotřebí, aby byla vytvořena databáze souborů. Jak databázi souborů vytvořit je popsáno v kapitole 2.2.

Pravidelná kontrola testu integrity dat na Vašich pevných discích je velmi důležitá, důležitější než hledání virů. Ušetří Vám řadu problémů, a proto Vám doporučujeme, abyste jí věnovali náležitou pozornost!!!

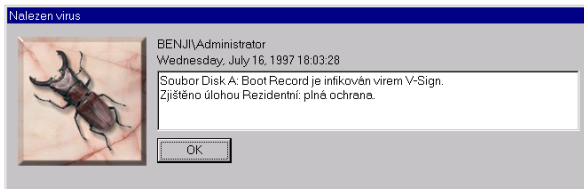
## 2.6 Jak zabránit průniku viru do systému

Aby byl Váš počítač co možná nejlépe ochráněn, je dobré před vlastní prací na počítači spouštět úlohu „Rezidentní: plná ochrana“ (spustíte ji opět poklepnutím levým tlačítkem myši na jméno úlohy). Úloha bude monitorovat takřka všechny

činnosti probíhající uvnitř Vašeho počítače. V případě pokusu o provedení nějaké podezřelé operace nebo pokud program najde virus ve spuštěném programu nebo v systémové oblasti vložené diskety, zobrazí varovné hlášení (mohou vypadat jako hlášení na obr. 25 a obr. 26). Úloha zabrání průniku viru do systému však pouze v případě, že běží (vedle jejího jména je ikona zobrazená na obr. 18). Po jejím ukončení systém již není chráněn.



obr. 25



obr. 26

Po instalaci programu AVAST32 na Váš počítač je úloha „Rezidentní: plná ochrana“ spuštěna automaticky po každém spuštění operačního systému, takže odpadá nutnost spouštět ji před vlastní prací „ručně“. Jak tuto možnost vypnout, naleznete v kapitole 2.8 (běžným uživatelům však doporučujeme nechat rezidentní ochranu zapnutou !!!).

## 2.7 Než začnete pracovat s cizí disketou

Pokud má být ochrana Vašeho počítače účinná, je, kromě pravidelného spuštění úloh hledajících viry, pravidelné aktualizace databáze souborů a pravidelného zálohování důležitých dat, potřeba získat určité návyky při práci s počítačem. Jedním z nich je, že dříve než na svůj počítač zkopírujete cokoli z diskety, o které stoprocentně nevíte, že nemohla přijít do styku s virem (což jsou všechny diskety, které byly alespoň chvíli v jiném počítači), tak zmíněnou disketu na přítomnost viru otestujete.

Zmíněnou činnost provádí úloha „Hledání: disketa A:“, kterou spustíte jako každou jinou úlohu, tedy poklepáním levým tlačítkem myši na jméno úlohy. Úloha „Hledání: disketa A:“ nejprve zkontroluje systémovou oblast diskety (tzv. boot sektor), zda v ní není přítomen nějaký virus a potom

prohledá všechny složky diskety a zkontroluje soubory a dokumenty, které zde nalezne. Obsahuje-li nějaký soubor virus (a je jedno, zda se jedná o makrovirus nebo virus napadající programy), zobrazí AVAST32 varovné hlášení (obr. 19), jinak úloha svou činnost normálně ukončí.

Dalším důležitým zvykem je nenechávat diskety v mechanice déle, než je nutné. Zabráníte nechtěnému natažení systému ze zavirované diskety, a následnému nakažení Vašeho počítače. Většina dnes vyráběných počítačů umožňuje vypnout možnost bootování systému z diskety v tzv. SETUP-u. Jestliže vám pojem SETUP nic neříká, kontaktujte administrátora Vaší sítě.

## 2.8 Návrhy pro práci s AVAST32

Tato kapitola obsahuje několik rad ohledně používání programu AVAST32 a některých jeho částí.

### Vytvoření zástupce na pracovní ploše

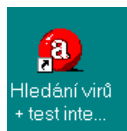
Spouštíte-li pravidelně jednu úlohu, je možné si pro ni vytvořit zástupce na pracovní ploše. Po poklepání levým tlačítkem myši na zástupci se automaticky spustí AVAST32 s příslušnou úlohou. Nebude tedy nejprve potřeba spustit AVAST32 a potom spouštět danou úlohu. Zástupce úlohy na pracovní ploše vytvoříte tak, že na jméno příslušné úlohy stisknete pravé tlačítko myši a z místní

nabídky zvolíte funkci „Vytvořit zástupce“ (obr. 27).



obr. 27

Na pracovní ploše se vytvoří zástupce, který se bude jmenovat stejně jako úloha, na které jste právě tlačítko myši stiskli. Zástupce úlohy „Hledání virů + test integrity“ ukazuje obr. 28.



obr. 28

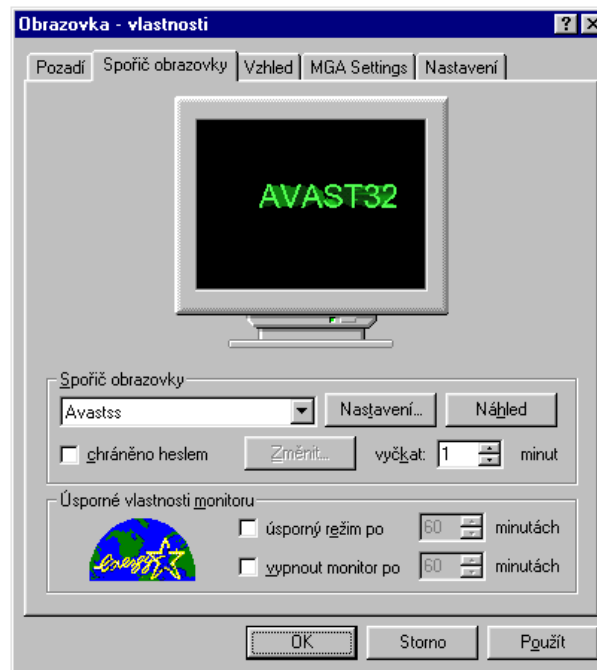
Díky nové architektuře programu AVAST32 nemusíte čekat se spuštěním nové úlohy, až běžící úloha skončí. Program je schopen zpracovávat několik úloh naráz. Rychlost zpracovávaných úloh však závisí na vybavení Vašeho počítače.

### Používání spořiče obrazovky

Hledání virů je poměrně náročná činnost, a to jak na čas, tak i na vybevení počítače, ovšem je potřeba provádět ji průběžně. Proto je součástí programu AVAST32 i spořič obrazovky, který umí hledat viry na pozadí Vašeho oblíbeného spořiče. Uživatel je informován o průběhu hledání virů a samozřejmě též i o jejich nalezení. Podrobný popis spořiče obrazovky naleznete v [kapitole 12](#).

Chcete-li jej používat, klepněte na hlavním panelu na tlačítko „Start“. Ve složce „Nastavení“ zvolte položku „Ovládací panely“ a v okně, které se objeví poklepejte na položce „Obrazovka“. Zobrazí se dialog sloužící pro nastavení parametrů obrazovky. V něm klepněte na jméno stránky „Spořič obrazovky“ (obr. 29).

Používáte-li operační systém Windows 95 pak vyberte z kombinovaného pole v rámečku „Spořič obrazovky“ položku „AvastSS“ (obr. 29). Pod operačním systémem Windows NT ze seznamu vyberte položku „Anti-virus Avast32“.



obr. 29

Do textového pole „vyčkat:“ запиšte dobu v minutách, po které má být spořič obrazovky aktivován od poslední akce uživatele (stisk klávesy, pohyb myši, apod.).

Po stisku tlačítka „Nastavení...“ je možné nastavit různé parametry spořiče obrazovky (viz kapitola 12.1). Chcete-li vidět, jak bude spořič obrazovky vypadat a pracovat, stiskněte tlačítko „Náhled“.

Jste-li s nastavením spořiče obrazovky spokojeni, tlačítkem „OK“ jej potvrdíte a při dalším startu spořiče obrazovky již budou hledány i viry.

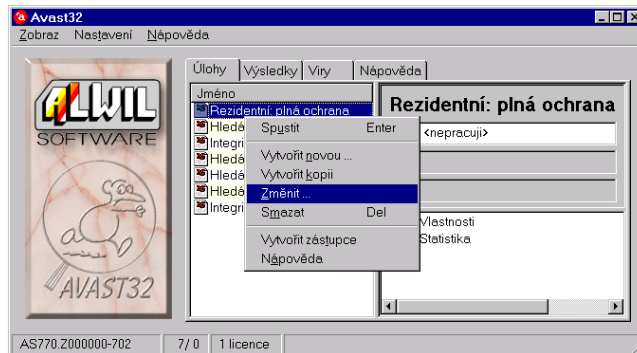
### Spouštění úlohy po spuštění systému

Úlohy, které spouštíte po Vašem každém přihlášení do systému (podobně jako úlohu „Rezidentní: plná ochrana“, viz kapitola 2.6), nechat spouštět automaticky. V nabídce „Zobraz“ vyberte položku „Rozšířené ovládání“. Zde se přepněte na stránku „Úlohy“ (klepněte na stejnojmenný nápis ve vrchní části okna).

Nejprve se přesvědčte, že příslušná úloha neběží ani není pozastavena. Jestliže je úloha pozastavena (vedle jména má kuličku červenou) musíte ji opět spustit - klepněte na ni pravým tlačítkem myši a z menu vyberte položku „Pokračovat“. Běžící úloha (vedle jejího jména je zelená kulička - obr. 18) je potřeba ji zastavit - klepněte na její

jméno pravým tlačítkem myši a vyberte příkaz „Stop“.

Pokud program po provedení výše popsanych úkonů zobrazí hlášení zobrazené na obr. 20, klepněte v něm na tlačítko „Ne“.



obr. 30

Stiskněte pravé tlačítko myši na jménu úlohy, která má být automaticky spouštěna a z nabídky, která se objeví, zvolte funkci „Změnit ...“ (obr. 30). Objeví se okno tzv. průvodce. Obsahuje tlačítko „Další >>“, jehož postupným stiskáváním se dostaňte až na stránku, která ve své vrchní části obsahuje text „Společné ovládací prvky pro všechny druhy úloh“ (obr. 45). Zde zaškrtněte pole „Spustit úlohu s operačním systémem“ a stiskněte tlačítko „OK“ (bližší popis stránky obsahuje

kapitola 4.4.6). Po Vašem dalším přihlášení se do systému bude tato úloha automaticky spuštěna.

Chcete-li naopak automatické spouštění úlohy odstranit, postupujte stejným způsobem a zaškrtnutí zmíněného pole zrušte.

Ovládání programu je však opět přepnuto do své „rozšířené“ podoby, a proto pokud chcete opět pracovat v původním jednoduchém ovládání, vyberte z menu „Zobraz“ položku „Jednoduché ovládání“ (obr. 22).



## 3. Základní popis programu

AVAST32 nabízí komplexní antivirovou ochranu osobního počítače pracujícího pod operačním systémem Windows 95 nebo Windows NT. Program umožňuje provádět činnosti pokrývající prakticky všechny oblasti antivirové ochrany.

Kromě dnes již klasického programu pro vyhledávání známých virů, obsahuje AVAST32 i prostředky umožňující odhalit i tzv. makroviry a polymorfní viry a dokonce může odhalit i činnost virů dosud neznámých.

Pomocí rezidentních testů je možné kontrolovat, zda v systému neproběhly nějaké operace, které by mohly být způsobeny činností viru. Program AVAST32 též umožňuje sledovat veškeré operace probíhající v systému a v případě podezření operaci zablokovat a podat uživateli zprávu. Sledovat lze i spouštěné soubory, a předejít tak virové nákaze.

Uživatelské rozhraní programu AVAST32 naprosto zapadá do prostředí operačních systémů Windows 95 a NT a plně se podřizuje zavedeným standardům. Uživatel pracující v tomto prostředí nebude proto mít s osvojením programu žádné problémy.

Aby se uživatel s programem příjemně pracovalo, obsahuje široké možnosti nastavení a dva druhy ovládání. Rozdělením ovládání se zabývají kapitoly 3.3, 3.4, 3.5 a 5.

### 3.1 Vlastnosti a výhody AVAST32

AVAST32 je antivirový program, určený pro operační systémy Microsoft Windows 95 a Microsoft Windows NT. Rozdíly jeho činnosti pod těmito operačními systémy jsou velmi malé a vyplývají pouze z rozdílné architektury operačních systémů, takže uživatel pracující s programem AVAST32 pod jedním systémem nebude mít s jeho obsluhou pod druhým systémem naprosto žádné problémy.

Hlavní výhodou programu AVAST32 je rychlé a především důkladné otestování Vašeho systému a všech jeho částí. Použité algoritmy, jak potvrzují nezávislé testy, jsou natolik účinné, že virus je rozpoznán až ve stech případech ze sta! Testovat můžete nejen přítomnost viru, ale i to, zda neproběhly v počítači od poslední kontroly nějaké změny. Můžete tak odhalit i virus dosud ještě neznámý!

Hledat viry je možné i ve chvílích, kdy je počítač nejméně vytížen, tedy ve chvíli, kdy s ním nikdo nepracuje. Jedná se konkrétně o spořič obrazovky, který na pozadí uživatelem vybraného spořiče obrazovky hledá viry. Spořič obrazovky programu AVAST32 lze plně nastavit podle přání a potřeb uživatele jako kteroukoli jinou část programu. Spořičem obrazovky se zabývá [kapitola 12](#).

Bude-li nějaký soubor nakažen či poškozen a pokud budete udržovat databázi souborů, můžete se jej programem AVAST32 pokusit obnovit. Úspěšnost obnovování souboru je až devadesát pět procent a správnost obnovení je program AVAST32 schopen zjistit se stoprocentní přesností!

Program AVAST32 umí využívat prostředků síťové komunikace. V případě nalezení viru tak mohou být včas uvědoměni všichni zvolení uživatelé dané sítě. Tato vlastnost umožňuje podstatným způsobem snížit riziko ztráty dat a předejít rozšíření virové nákazy.

AVAST32 využívá všech výhod moderních operačních systémů jako jsou např. dlouhá jména souborů (až 256 znaků), nové ovládací prvky, nebo možnost provádět více činností programu najednou. Uživatel tak již není omezován a může plně využít času stráveného u počítače a jeho výkonu.

Ovládání programu si může uživatel plně přizpůsobit svým potřebám a schopnostem. Začátečníci jistě ocení možnost pracovat s programem bez nutnosti učit se podrobnosti o jeho práci a odborníci jistě uvítají možnost detailního nastavení činnosti programu a jeho reakcí na určité události.

AVAST32 používá k zobrazení nápovědy program Acrobat Reader, tedy velmi kvalitní a uživatelsky přívětivý nástroj, který je v současné době velmi populární. Program Acrobat Reader je však používán tak, že se jeví jako součást programu AVAST32. Umožní Vám velmi jednoduchým způsobem procházet nápovědou a dostat se rychle k té její části, která Vás momentálně zajímá.

## 3.2 Základní funkce programu

Klasickou částí většiny antivirových programů, včetně programu AVAST32, je hledání známých virů (někdy je tato činnost označovaná jako scanování). Program zkontroluje testovaný soubor na přítomnost určitého sledu bytů, který identifikuje jednotlivé viry.

Program AVAST32 odhalí tímto způsobem velké množství virů, ale protože nové viry se objevují velmi často a pravidelně, je zapotřebí, aby databáze známých virů byla pravidelně aktualizována (viz [kapitola 1.6](#)). Program AVAST32 umí rozpoznat i tzv. polymorfní viry, které během svého působení

mění sami sebe a je tudíž velmi těžké je odhalit. Náš produkt rozpozná i tzv. makroviry, což jsou viry šířící se v podobě maker v OLE dokumentech (např. dokument aplikace MS Word nebo MS Excel).

Méně rozšířeným způsobem odhalování virů je tzv. testování integrity dat. Vychází z předpokladu, že virus musí být v době, kdy je počítač vypnut, uložen v nějaké permanentní paměti. V současné době je takovou nejrozšířenější pamětí pevný disk počítače. Z toho vyplývá, že pokud budeme sledovat změny souborů, můžeme tak odhalit i virus, který není doposud znám, stejně dobře jako známý virus.

Jestliže byl například změněn nějaký textový soubor (soubor s příponou TXT), lze z devadesáti devíti procent říci, že to nezpůsobil virus. Pokud se ale změnil nějaký program nebo dokonce systémový soubor, je pravděpodobnost nakažení virem velmi vysoká.

Abyste mohli být sledovány změny jednotlivých souborů je zapotřebí uchovávat informace o stavu, v jakém se nacházeli před určitou dobou. Porovnáním aktuálního stavu souboru se stavem uloženým v databázi lze spolehlivě určit, zda byl soubor změněn, či nikoli. Bude-li se tedy test integrity dat provádět např. každý týden, bude uživatel vědět o všech změnách, které byly s jeho soubory provedeny za poslední týden.

Informace o souborech, uložené v databázi souborů, může program AVAST32 kromě testování integrity použít i na obnovení původního stavu souborů. Budete-li tedy databázi souborů pravidelně udržovat, můžete se v případě napadení Vašich souborů pokusit o jejich obnovení. Zda byl soubor obnoven úspěšně, lze na základě databáze souborů určit zcela přesně.

Program AVAST32 nabízí i možnost sledovat veškeré podezřelé operace se soubory a systémovými oblastmi disků v systému, a před jejich provedením informovat uživatele. Uživatel má pak možnost provedení operace povolit, nebo naopak její provedení zakázat. Uvedená rezidentní ochrana se jmenuje „Rezidentní bloky“ a vychází z faktu, že naprostá většina virů během své činnosti provádí nějaké operace se soubory, a to ať už je napadá nebo nějakým způsobem poškozují.

Virus může být sice v počítači, ten ale přesto nemusí být infikován. K tomu, aby se virus stal aktivním, je zapotřebí, aby byl spuštěn. Většina virů proto napadá spustitelné soubory, tzn. hlavně programy. AVAST32 nabízí rezidentní činnost jménem „Rezidentní sledování“, která provádí test všech programů spouštěných na Vašem počítači. Pokud budete tedy chtít spustit nějaký program, AVAST32 jej nejprve zkontroluje, zda neobsahuje nějaký virus. Jestliže je vše v pořádku, bude program normálním způsobem spuštěn. Byl-li však

v programu objeven virus, obdržíte varovné hlášení a program nebude bez Vašeho svolení spuštěn.

Další poměrně rozšířenou skupinou virů jsou viry šířící se v systémových oblastech disků, tedy hlavně v boot sektoru disket. Počítač se sice nemůže pouhým vložením infikované diskety nakazit, ale může dojít k nechtěnému zavedení systému ze zapomenuté diskety v mechanice a nakažení počítače. AVAST32 obsahuje rezidentní činnost jménem „Sledování boot sektoru“, která při prvním přístupu k jakékoli disketě nejprve zkontroluje její boot sektor, jestli neobsahuje virus. Je-li virus nalezen, program informuje uživatele o nálezů varovným hlášením. Pokud virus není nalezen, je možné s disketou normálně pracovat.

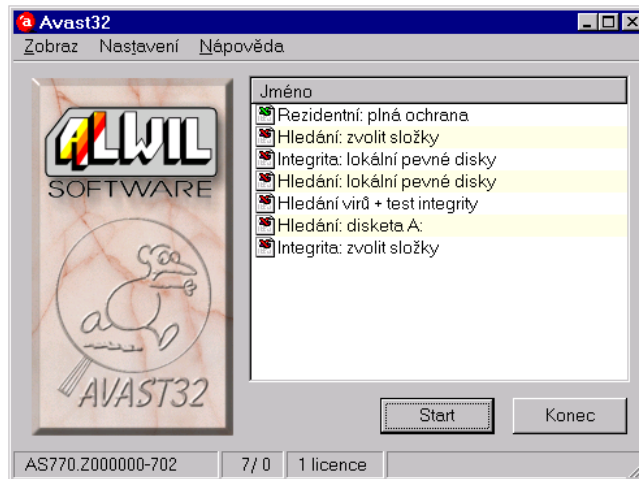
### 3.3 Jednoduché versus rozšířené ovládání

Ovládání programu AVAST32 může mít dvě základní podoby, které se liší především množstvím svých ovládacích prvků a tím i složitostí vlastního ovládání. Z toho pak vyplývá i cílová skupina uživatelů, pro kterou je dané ovládání určeno.

První možná podoba ovládání programu AVAST32 je vidět na obr. 31. Tomuto ovládání říkáme „jednoduché“, protože obsahuje pouze nej-

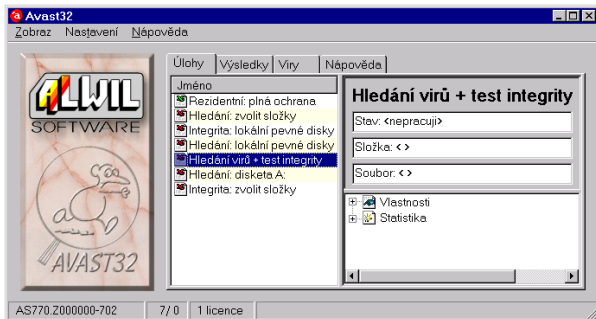
důležitější ovládací prvky programu a chrání tak uživatele před množstvím ovládacích prvků, se kterými většinou nepracuje.

V jednoduchém ovládání lze provádět pouze nejzákladnější činnosti a operace s úlohami.



obr. 31

Ovládání programu AVAST32 může však mít i podobu, kterou ukazuje obr. 32. Rozšířené ovládání, jak jej nazýváme, obsahuje všechny ovládací prvky programu. Uživatel má tak přístup ke všem funkcím a nastavením, které program AVAST32 nabízí.



obr. 32

Rozšířené ovládání je vzhledem ke svému rozsahu rozděleno do několika základních stránek, které obsahují vlastní funkce a parametry. Mezi jednotlivými stránkami se lze pohybovat stiskem levého tlačítka myši na jménu příslušné stránky.

Použité ovládání záleží na aktuálním nastavení programu; implicitně je nastaveno jednoduché ovládání. Podrobný popis jednotlivých ovládání programu AVAST32 a přepínání mezi nimi obsahuje [kapitola 5](#).

### 3.4 Jaké ovládání používat?

K rozdělení ovládání programu AVAST32 nás vedl fakt, že uživatele pracující s programem lze rozdělit podle činností, které s ním vykonávají. Jsou to na jedné straně odborníci (jako např. admi-

nistrátoři sítí, kteří se starají o její správný běh a nastavení), a na druhé straně běžní uživatelé.

Běžný uživatel většinou nepotřebuje množství parametrů - jeho hlavním požadavkem bývá co možná nejjednodušší ovládání, bez nutnosti učit se nastavovat a ovládat další program. Těmto uživatelům doporučujeme používat jednoduché ovládání programu, neboť těmto požadavkům svou koncepcí naprosto vyhovuje.

Administrátoři sítí a zkušenější uživatelé naopak tomu potřebují přesně nastavit činnost a chování programu. Pro ně je určeno rozšířené ovládání programu AVAST32, které zpřístupňuje všechny funkce a ovládací prvky programu a tím umožňuje přizpůsobit program požadavkům uživatele.

Každý z uživatelů pracujících na daném počítači má možnost vybrat si ovládání, které mu vyhovuje, a v něm potom pracovat. Použité ovládání si totiž program „pamatuje“ pro každého uživatele zvlášť.

### 3.5 Možnosti jednotlivých ovládání

Co vše se dá v jednotlivých ovládaních udělat, souvisí s jejich určením.

Jednoduché ovládání je určeno pro běžného uživatele, který potřebuje mít možnost provést nějakou úlohu (tedy otestovat určitou část systému) bez nutnosti zabývat se podrobnostmi

činnosti a nastavením programu. K tomu bylo přihlédnuto, a tak jednoduché ovládání umožňuje provádět velmi jednoduše základní operace s úlohami.

V jednoduchém ovládání může uživatel úlohy spouštět nebo jejich činnost naopak ukončit nebo pozastavit. V případě, že úloha našla virus, bude uživatel upozorněn. Jednoduché ovládání však neumožňuje zobrazit podrobnosti výsledků úloh, tedy ani zjistit, který z testovaných souborů byl nakažen či změněn.

Dále jednoduché ovládání umožňuje provádět základní funkce jako ukončit program, vyvolat nápovědu programu, nebo vytvořit zástupce na pracovní ploše. Jednoduché ovládání samozřejmě umožňuje i přepnutí do ovládání rozšířeného.

Úkolem rozšířeného ovládání je zpřístupnit vše, co program AVAST32 nabízí. Kromě základních operací s úlohami, tak, jak byly zmíněny u jednoduchého ovládání, může uživatel měnit parametry jednotlivých úloh nebo je dokonce smazat. Lze samozřejmě i vytvářet úlohy nové.

Uživatel má k dispozici kompletní výsledky všech dosud proběhlých úloh a nástroje, které mu umožňují na výsledky úloh reagovat. Lze tedy např. výsledky úloh akceptovat, nebo se pokusit změněné soubory opravit. Je možné též podezřelé či nakažené soubory smazat nebo je prostě pře-

jmenovat a přesunout do jiné, k tomu určené složky.

Rozšířené ovládání umožňuje i možnost nastavení prostředí jednotlivých částí programu i programu AVAST32 jako celku. K dispozici jsou ovládací prvky, které dávají každému uživateli možnost přizpůsobit si vlastnosti programu svým potřebám. Nastavení prostředí programu obsahuje i možnost přepnutí ovládání programu do jeho jednoduché podoby.

Součástí rozšířeného ovládání jsou i stručné charakteristiky virů z aktuálního souboru VPS, informace o jeho verzi, i o verzi programu a dále pak informace o vlastníku licence. Tyto informace jsou důležité zejména ve chvíli, kdy je potřeba kontaktovat pracovníky naší firmy.

### **3.6 Úloha jako základní prvek**

Základní prvek, se kterým program AVAST32 pracuje, je „úloha“. Pod tímto pojmem se rozumí podrobný popis všech činností, které se budou po spuštění úlohy provádět. U jednotlivých činností je pak možné nastavit i řadu parametrů, které blíže určují chování úlohy.

Každá úloha musí mít své jméno a musí obsahovat nějakou činnost. Činností pak může být např. kontrola souborů na pevném disku na přítomnost virů či průběžné monitorování systému. Úloha může provádět i více činností naráz; je

možné například testovat přítomnost virů a přitom provádět kontrolu změny dat (tzv. test integrity dat).

Úlohy mohou být privátní, sdílené nebo pouze pro čtení. Sdílené úlohy jsou přístupné všem uživatelům pracujícím na daném počítači, na rozdíl od privátních, které jsou přístupné pouze jejich vlastníkovvi, tedy uživateli, který je vytvořil. Bude-li úloha privátní nebo sdílená, určuje uživatel při jejím vytváření. Úlohy pouze pro čtení jsou zvláštním typem sdílených úloh - jsou přístupné všem uživatelům, ovšem nelze je žádným způsobem změnit (jedná se především o úlohy dodávané s programem).

Všechny úlohy, které jsou momentálně dostupné, jsou uvedeny v seznamu úloh, který je součástí jak jednoduchého tak rozšířeného ovládání.

Vytváření nových úloh je podrobně popsáno v [kapitole 4](#).

### 3.7 Dodávané úlohy

Součástí instalace programu AVAST32 je i několik již vytvořených úloh, které umožňují uživateli program používat ihned po jeho instalaci. Jednotlivé úlohy si popíšeme v následujících odstavcích.

Všechny dodávané úlohy, pokud u nich není uvedeno jinak, jsou pouze pro čtení, tzn. že je

nelze měnit ani mazat.

#### Úloha „Hledání: lokální pevné disky“

Úloha prohledá všechny spustitelné soubory a OLE dokumenty na všech lokálních pevných discích počítače. V případě, že program AVAST32 nějaký virus nalezne, dá to najevo varovným hlášením o nálezů a zvukovým efektem (pokud je v počítači nainstalovaná zvuková karta). Úloha ohlásí každý nalezený virus. Kontrolovány budou i zkomprimované soubory a operační paměť počítače. U každého disku bude také zkontrolována systémová oblast.

#### Úloha „Hledání: zvolit složky“

Úloha provede naprosto stejné kontroly na přítomnost virů jako předchozí úloha, ale před vlastní kontrolou bude mít uživatel možnost vybrat oblasti, které mají být zkontrolovány. Vybrat lze pochopitelně i více oblastí najednou (viz [kapitola 5.5](#)).

U vybraných složek je možné určit, zda si přejete, aby byly zkontrolovány i složky vnořené.

#### Úloha „Hledání: disketa A:“

Úloha provádí stejné kontroly jako dvě předešlé úlohy, ale na disketě v mechanice A:. Tuto úlohu doporučujeme provádět se všemi potencionálně nakaženými disketami. Jedná se především o dis-

kety, které byly používány na jiných počítačích nebo jinými uživateli. U diskety bude zkontrolována i její systémová oblast, tedy boot sektor.

Pokud si zvyknete každou cizí disketu před jejím použitím nejprve zkontrolovat, podstatným způsobem tak snížíte riziko nakažení Vašeho počítače.

#### Úloha „Integrita: lokální pevné disky“

Úloha zkontroluje, jestli nebyly změněny nějaké spustitelné soubory a OLE dokumenty na všech lokálních pevných discích od poslední kontroly. Obsah souborů bude zkontrolován pouze tehdy, byl-li od poslední kontroly změněn nějaký parametr souboru, například atributy, jeho velikost, apod. Výsledky budou zaznamenány v přehledné stromové struktuře (viz kapitola 5.3.2). Úloha také zkontroluje, zda od poslední kontroly nedošlo ke změně systémových oblastí kontrolovaných disků.

Z předchozího textu vyplývá, že změny souborů se dají hlídat pouze mezi dvěma testy integrity dat. Výsledkem prvního spuštění úlohy bude hlášení, že „přibily“ všechny soubory na kontrolovaném disku. Proto je nutné stav souborů zaznamenat do interní databáze, aby při dalších testech bylo možno porovnat aktuální stav souborů s předcházejícím. Jak databázi souborů vytvořit je popsáno v kapitole 2.2.

#### Úloha „Integrita: zvolit složky“

Úloha provede stejné kontroly jako úloha předcházející, ale na oblasti, které se mají kontrolovat, se dotáže uživatele. Pro vybrání testovaných složek slouží dialog, který je popsán v kapitole 5.5. I u tohoto testu platí, že pokud mají být výsledky použitelné, je třeba nejprve naplnit databázi souborů.

#### Úloha „Rezidentní: plná ochrana“

Ochrana prováděná úlohou vychází ze dvou faktů. Pokud má virus napadnout počítač, musí se nejdříve spustit (tj. musí mu být předáno řízení), a proto je vhodné kontrolovat všechny spouštěné soubory a zaváděcí sektory (tzv. boot sektory) vkládaných disket. Druhým předpokladem je, že virus se v počítači projevuje nějakou činností: zapisuje do spustitelného souboru, do boot sektoru disket a nebo se dokonce snaží přeformátovat určitou část disku.

Všechny uvedené činnosti hlídá tato úloha a při pokusu o provedení nějaké potencionálně nebezpečné operace se nejprve zeptá uživatele, zda smí být příslušná operace provedena. Bez jeho svolení nebude provedení operace povoleno.

Doporučujeme tuto úlohu spouštět vždy po startu operačního systému, nebo ještě lépe nastavit jeho automatické spuštění se startem operačního systému nebo umístit jejího zástupce



do složky spustit při startu. Pokud má být úloha a její ochrany účinné, je nutné ji nechat běžet!

Úloha „Rezidentní: plná ochrana“ je sdílená.

### Úloha „Hledání virů + test integrity“

Úloha je kombinací úloh „Hledání: lokální pevné disky“ a „Integrita: lokální pevné disky“. Pokud tedy potřebujete provést obě úlohy, je rychlejší (i z hlediska provádění) spustit úlohu „Hledání virů + test integrity“. O úloze platí vše, co bylo napsáno o zmíněných dvou úlohách.

### Speciální úlohy

Jedná se úlohy, které mají v programu AVAST32 zvláštní význam. Jsou to úlohy „Quick32“ (viz [kapitola 10.1](#)) a „Spořič obrazovky“ (viz [kapitola 12.1](#)).

Všechny speciální úlohy jsou privátní a jsou přístupné pouze přes „Ovládací panely“ (viz [kapitola 6.7](#)).

## 3.8 Základní způsoby ovládání programu

Ovládání programu AVAST32 bylo navrženo tak, aby co nejvíce odpovídalo zavedeným standardům v této oblasti. Proto jsou pro ovládání programu AVAST32 použity pouze standardní systémové ovládací prvky.

V zásadě lze program ovládat dvojím způsobem; pomocí klávesnice nebo myši. Pro rychlejší práci s programem doporučujeme pro jeho ovládní používat myš a klávesnici používat pouze pro vkládání textů. Podrobný popis použití myši i klávesnice je uveden v manuálu nebo v nápovědě operačního systému.

V následujícím textu budeme pojmem „aktivní prvek“ označovat ten prvek, který je nějakým způsobem zvýrazněn. Na [obr. 31](#) je aktivní např. tlačítko „Start“, na [obr. 32](#) je aktivní úloha „Hledání virů + test integrity“. Jakou barvou bude prvek zvýrazněn, záleží na aktuálním nastavení prostředí Vašeho operačního systému (složka „Ovládací panely“, prvek „Obrazovka“).

K ovládání programu slouží ovládací prvky. Mezi nejdůležitější patří tzv. záložkový seznam, který je vidět na [obr. 33](#). Obsahuje vždy několik stránek s různým obsahem a funkcí, kdy viditelná v danou chvíli je pouze jediná stránka. Zviditelnit jakoukoli stránku můžete tak, že klepnete levým tlačítkem myši na jméno příslušné stránky, na tzv. „oušku“.



obr. 33

Pomocí klávesnice se můžete posouvat po jednotlivých stránkách aktivací záložkového seznamu a použitím kláves pro posun kurzoru doleva a doprava. Tímto způsobem aktivujete stránku vlevo či vpravo.

Dalším velmi důležitým ovládacím prvek je tzv. strom. Ten zobrazuje hierarchicky složenou strukturu, která může mít libovolný obsah. Může se jednat například o stromovou strukturu složek uložených na disku (tak strom používá program „Průzkumník“), nebo o informace o aktuálním stavu (obr. 32).

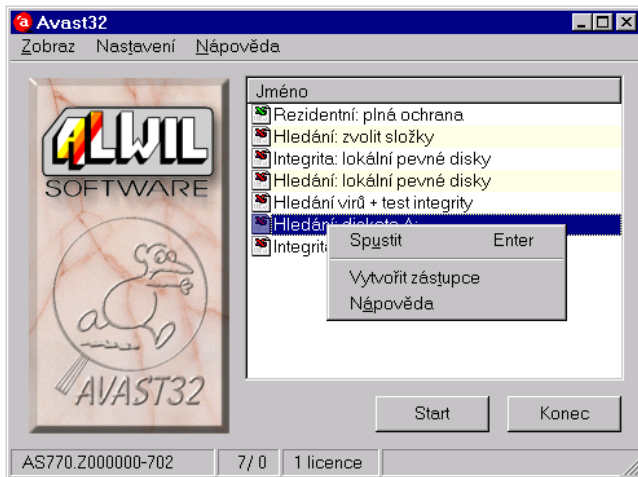
Stromová struktura obsahuje položky. Chcete-li „rozbalit“ nějakou položku, poklepejte levým tlačítkem myši na ikonu, zobrazenou před jménem příslušné položky. Při použití klávesnice musíte položku nejprve aktivovat a potom použít klávesu „Enter“. Položku opět „zabalíte“ stejným způsobem. Je možné též použít kláves pro posun kurzoru doleva (pro „zabalení“ položky) a pro posun kurzoru doprava (pro „rozbalení“ položky).

Prvek, se kterým program AVAST32 také pracuje, je seznam. Na obr. 31 je vidět seznam dostupných úloh, ale samozřejmě, že seznam je použit i jinde. Může obsahovat i více sloupců, jejichž význam je vždy popsán v prvním řádku. Šířku jednotlivých sloupců seznamu pak lze libovolně měnit. To provedete tak, že na pravém okraji jména sloupce stisknete levé tlačítko myši a ne-

cháte je stisknuté. Pohybem ukazovátka myši nastavíte potřebnou šířku sloupce a tlačítko myši uvolníte.

Jeden prvek seznamu je zvýrazněn - říkáme, že je aktivní. Aby se prvek stal aktivní, je potřeba na něj klepnout levým tlačítkem myši, nebo jej zvýraznit pomocí kláves pro pohyb kurzoru nahoru a dolů. Obsahuje-li seznam příliš mnoho prvků, je možné se v něm pohybovat i po „stránkách“ klávesami „PgUp“ a „PgDn“.

Pravé tlačítko myši slouží v operačních systémech Microsoft Windows k vyvolání tzv. místní nabídky (obr. 34). Nejinak je tomu i u programu AVAST32. Funkce místní nabídky se vztahují vždy k prvku, na kterém bylo pravé tlačítko myši stisknuto (na obr. 34 je to úloha „Hledání: disketa A:“) a obsahuje operace, které lze s daným prvkem provádět. Funkci, kterou chcete spustit vyberete stiskem levého tlačítka nad jejím jménem. Nabídka může obsahovat nejen funkce, ale i další složky, ve kterých mohou být opět uloženy funkce nebo další složky, atd.

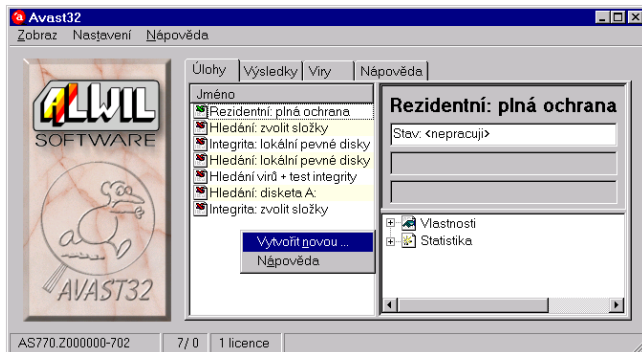


obr. 34

Pro ovládání programu AVAST32 je místní nabídka využívána velmi často, a proto doporučujeme zvláště začínajícím uživatelům, aby si na používání pravého tlačítka myši zvykli. Některé části programu lze totiž ovládat pouze prostřednictvím místní nabídky nebo s použitím klávesnice.

## 4. Vytváření nových úloh

Součástí instalace programu AVAST32 je i několik již vytvořených úloh ([kapitola 3.7](#)), které umožňují okamžité používání programu po jeho instalaci a využití většiny jeho funkcí. Po čase však většina uživatelů pocítí potřebu vytvořit si úlohy vlastní, které budou vyhovovat právě jejich požadavkům a potřebám.



obr. 35

Novou úlohu lze vytvořit pouze v rozšířeném prostředí nebo pomocí „Ovládacích panelů“ (viz [kapitola 6.7](#)). Jestliže tedy pracujete v jednoduchém prostředí, vyberte z nabídky „Zobraz“

položku „Rozšířené prostředí“. V rozšířeném prostředí se přepněte na stránku „Úlohy“, kde stisknete na seznamu úloh pravé tlačítko myši. V místní nabídce potom vyberte funkci „Vytvořit novou ...“ (obr. 35).

Chcete-li změnit nastavení jakékoli úlohy nebo chcete vytvořit novou úlohu a nemáte program AVAST32 spuštěn, můžete tak provést přes „Ovládací panely“. Podrobný popis je uveden v [kapitole 6.7](#).

Podrobný popis postupu vytváření nových úloh najdete právě v této kapitole. Uvedeme nejen popis jednotlivých ovládacích prvků, ale i doporučení, která by měli respektovat zejména méně zkušené uživatelé osobních počítačů.

### 4.1 Privátní nebo sdílená?

Před vytvořením vlastní úlohy by si měl uživatel promyslet, k jakému účelu má nová úloha sloužit a kdo ji má používat. Některé úlohy by měly být přístupné všem uživatelům konkrétního počítačového systému; např. otestování diskety v mechanice A:, či test systému jako takového. Naproti tomu mohou být úlohy přístupné pouze jednomu

uživateli. Jako příklad uvedme otestování soukromých dokumentů a aplikací.

Takové rozdělení úloh je velmi výhodné, neboť jednak odpadá vytváření naprosto shodných úloh zvláště pro každého uživatele a přitom je uživateli ponechána možnost vytvořit si úlohu vlastní, vyhovující jeho potřebám.

Úlohám, ke kterým mají přístup všichni uživatelé daného systému, říkáme „sdílené“. Jedná se o úlohy, které se objeví v seznamu úloh všech uživatelů. Jejich služeb mohou tedy využívat všichni uživatelé. Sdílené úlohy jsou v seznamu úloh označené ikonou, která je vidět na obr. 36.



obr. 36

Sdílené úlohy by na počítači, kde pracuje více uživatelů, měla vytvářet osoba, která má daný počítač na starost. Ve většině případů půjde o administrátora sítě. S tím souvisí i možnost chránit sdílené úlohy heslem. Je-li ochrana heslem nastavena, bude uživateli bez znalosti hesla umožněno pouze danou úlohu spustit, ukončit její činnost a vytvořit si privátní kopii úlohy. Při všech ostatních manipulacích bude po uživateli vyžadováno heslo (viz kapitola 6.1.2).

Jako „privátní“ označujeme ty úlohy, které jsou přístupné pouze tomu uživateli, který je vytvořil. Takové úlohy se neobjeví v seznamu úloh jiných uživatelů a žádný jiný uživatel tedy s nimi nemůže provádět jakékoli operace. Privátní úlohy mají vedle svého jména v seznamu úloh ikonu vyobrazenou na obr. 37.



obr. 37

Bude-li nová úloha sdílená nebo privátní, určí uživatel při jejím vytváření (viz kapitola 4.4.1). Později lze toto nastavení kdykoli změnit (v případě sdílených úloh a zapnuté ochraně je pochopitelně potřebná znalost hesla).

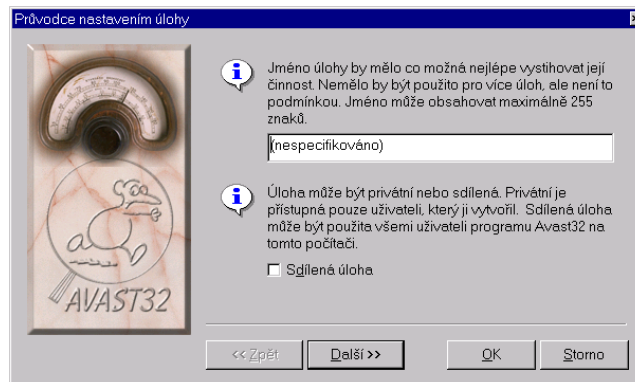
## 4.2 S průvodcem nebo bez něj?

Ovládání programu AVAST32 bylo navrženo s ohledem na všechny uživatele, kteří s ním budou pracovat. Jak jsme se již zmínili, je možné s programem pracovat v jeho jednoduchém či rozšířeném ovládání. Rozdělení ovládání má za úkol především pomoci běžným uživatelům s ovládnutím programu a nezatěžovat je přílišnými podrobnostmi a na druhé straně umožnit odborníkům jeho komplexní ovládání a nastavení.

Podobně je tomu i při vytváření nové úlohy, kdy lze použít tzv. průvodce nebo klasický záložkový seznam. Rozdíl mezi oběma ovládaními pro vytváření nové úlohy je především v přístupu k uživateli. Zatímco při použití průvodce je program vlastně jakýmsi pomocníkem, je záložkový seznam pouze nástrojem pro vytvoření nové úlohy. Ovládací prvky jsou však v obou ovládaních shodné.

Průvodce pro vytváření nové úlohy lze zapnout zaškrtnutím pole „Používat průvodce při vytváření nové úlohy“ na stránce „Základní“ v nabídce „Nastavení/Hlavní konzole ...“ (viz kapitola 6.1.1).

Použije-li uživatel průvodce (obr. 38), je programem při vytváření nové úlohy veden. Postupně stránku za stránkou prochází celým procesem vytváření nové úlohy a nastavuje ovládací prvky na jednotlivých stránkách. Uživatel může kdykoli přejít na další stránku, je-li s nastavením spokojen, nebo se vrátit ke stránce předchozí. K tomu slouží tlačítka „Další >>“ a „<< Zpět“. Je též možné vytváření nové úlohy kdykoli přerušit tlačítkem „Storno“ nebo klávesou „Esc“. Úlohu lze také vytvořit pouze na základě dosud nastavených parametrů tlačítkem „OK“. V takovém případě se pro nenastavené parametry použijí jejich implicitní hodnoty.

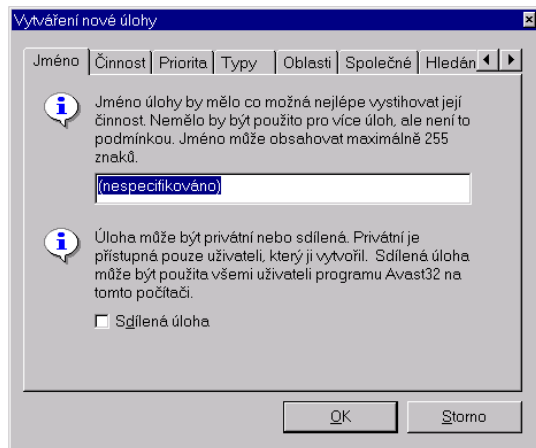


obr. 38

Použití průvodce doporučujeme zejména uživatelům, kteří se s programem AVAST32 teprve učí pracovat. Jeho použití je snadné a prakticky vylučuje přehlédnutí nějakého důležitého ovládacího prvku. Uživatel se tak učí jednotlivé možnosti nastavení i jejich rozmístění na jednotlivých stránkách.

Jestliže je používání průvodce vypnuto, budou se všechny dostupné stránky nacházet v klasickém záložkovém seznamu (obr. 39), jehož ovládaní je popsáno v kapitole 3.8. Ten umožňuje uživateli přejít přímo na stránku s potřebnými ovládacími prvky bez nutnosti procházet všechny stránky předchozí. Stejně jako v případě použití průvodce je možné vytváření úlohy kdykoli pře-

rušit tlačítkem „Storno“ nebo naopak požádat o vytvoření úlohy z dosud zadaných hodnot tlačítkem „OK“, kdy pro nezadané parametry se použijí jejich implicitní hodnoty.



obr. 39

Po záložkovém seznamu zřejmě sáhnou zkušenější uživatelé a to především z důvodu jeho rychlejší obsluhy. Uživatel nastaví pouze to, co nastavit potřebuje, a může rovnou přikročit k vytvoření nové úlohy (tento způsob příliš nedoporučujeme méně zkušeným uživatelům). Záložkový seznam je zvláště výhodný pro modifikaci parametrů již existující úlohy.

Implicitně je nastaveno používání průvodce jak pro vytváření nové úlohy, tak pro změnu již existující.

Změna parametrů existujících úloh probíhá ve stejném prostředí jako vytváření úloh nových. Proto vše, co je zde napsáno o vytváření úloh nových, platí i pro změnu jejich parametrů. Jediným rozdílem je, že pokud během změny parametrů úlohy stisknete tlačítko „Storno“, budou hodnoty všech parametrů ponechány beze změny a úloha jako taková samozřejmě také.

Průvodce pro změnu existujících úloh lze zapnout zaškrtnutím pole „Používat průvodce při změně úlohy“ na stránce „Základní“ v nabídce „Nastavení/Hlavní konzole ...“ hlavního okna (viz kapitola 6.1.1).

### 4.3 Co úloha obsahuje?

Úloha je základním prvkem, se kterým program AVAST32 pracuje. Každá úloha má své jméno a obsahuje podrobný popis všech činností a jejich vlastností, které budou po jejím spuštění prováděny. Obsahuje též i informaci o své důležitosti, resp. o své prioritě.

Činnostmi, které může úloha provádět, jsou v zásadě tři: test přítomnosti známých virů, test integrity dat a různé rezidentní testy. Uvedené základní testy lze většinou ještě dále dělit, ale v zásadě to není nutné. Každou z uvedených

činností je možné nastavit přesně podle potřeb uživatele.

Navíc lze uvedené činnosti téměř libovolně kombinovat, což v konečném důsledku znamená urychlení celkového procesu testování. Např. pokud nastavíte testování přítomnosti virů a zároveň test integrity dat, budou se uvedené testy na jednotlivých souborech provádět naráz, takže soubory nebude potřeba z disku načítat vícekrát, apod.

Součástí úlohy je i informace o době jejího spuštění. Lze nastavit, aby byla úloha spuštěna automaticky po startu operačního systému a chránit tak počítač prakticky po celou dobu jeho činnosti. To je velmi praktické u rezidentních testů, kdy je potřeba, aby byl počítač „pod kontrolou“ co možná nejdéle. Je možné též nastavit spouštění úloh se spuštěním programu AVAST32 nebo nechat spuštění úlohy pouze na uživateli.

Úloha obsahuje také způsob, jakým bude uživatel na případný virus upozorněn. Program AVAST32 umožňuje vložení textu chybového hlášení a je možné také zvolit i zvuk, který bude hlášení doprovázet.

## 4.4 Popis stránek konfigurace úlohy

V následujícím textu budou popsány jednotlivé stránky s ovládacími prvky. Uvedeme vždy popis všech ovládacích prvků na stránce a jejich implicitní hodnoty. Obrázky, které jsou u jednotlivých stránek, ukazují stránky při použití průvodce. Při použití záložkového seznamu je podoba okna jiná, ovládací prvky a jejich význam jsou však tytéž (viz rozdíl mezi [obr. 38](#) a [obr. 39](#)).

Je nutné upozornit, že počet aktuálně dosažitelných stránek závisí na zvolených činnostech úlohy a při jejím vytváření se může měnit. Obecně platí pravidlo, že pro tu činnost, která není v úloze použita, se nezobrazí stránka s jejím nastavením. Uživatel je tak ušetřen přeskakování přebytečných stránek, které nemají žádný vliv na průběh úlohy.

### 4.4.1 Stránka „Jméno“

Na stránce „Jméno“ je programem požadováno vložení jména vytvářené úlohy ([obr. 38](#) a [obr. 39](#)). To by mělo být co možná nejnvýstižnější a nemělo by být kvůli přehlednosti shodné s některým jménem již existující úlohy, i když program umí pracovat i s úlohami se stejným jménem. Jestliže nezadáte žádné jméno, nebude nová úloha vyt-



vořena. Implicitně textové pole obsahuje „(nespecifikováno)“.

Pomocí zaškrtačacího pole „Sdílená úloha“ lze nastavit, zda má být úloha sdílená či privátní. Sdílené úlohy mohou používat všichni uživatelé daného počítače na rozdíl od privátních, které mohou být použity pouze jejich tvůrcem. Pokud pole zůstane nezaškrtnuto, bude nově vytvořená úloha privátní, což je i implicitní nastavení.

Stránka „Jméno“ je přítomna u každé varianty vytvářené úlohy.

#### 4.4.2 Stránka „Činnost“

Stránka „Činnost“ obsahuje ovládací prvky, kterými se určí vlastní činnost úlohy (obr. 40). Lze nastavit, že úloha bude vykonávat i více činností najednou. Nastavení ovládacích prvků na této stránce má zásadní vliv na počet následně dosažitelných stránek. Pokud nezvolíte ani jedinou činnost, nebude vytvoření nové úlohy povoleno.

Zaškrtačací pole „Hledání virů“ zapíná kontrolu přítomnosti známých virů. V každém vybraném souboru pak budou mimo jiné postupně hledány všechny známé viry a jejich případná přítomnost bude oznámena uživateli. Implicitně je hledání virů zapnuto.



obr. 40

Zaškrtačací pole „Testování integrity“ slouží k zapnutí testování integrity dat. U každého vybraného souboru pak bude mimo jiné otestováno, zda nebyl od poslední kontroly změněn a pokud ano, tak jakým způsobem. Pole není implicitně zaškrtnuto.

Zaškrtačací pole „Zjednodušené testování integrity“, stejně jako pole předchozí, zapíná test integrity dat. Na rozdíl od něj však u souborů budou pouze vypočítány zjednodušené kontrolní součty jejich obsahů, atributy souborů se nebudou testovat. Kontrola změny souboru tak bude rychlejší. Zjednodušené testování není implicitně zapnuto.

Uvedené činnosti nazýváme nerezidentními. Následující pak řadíme mezi rezidentní. Podle typu prováděných činností pak hovoříme i o rezidentních a nerezidentních úlohách. Zda právě vytvářená úloha bude rezidentní či nikoli, záleží na tom, jestli je povolena nějaká nerezidentní činnost. Pokud ano, bude úloha nerezidentní a nastavení ovládacích prvků rezidentních činností bude ignorováno. Není-li zaškrtnuta ani jedna nerezidentní činnost, bude úloha rezidentní.

Pole „Testování integrity“ nemůže být zaškrtnuto zároveň s polem „Zjednodušené testování integrity“ (konečně, nemá to ani význam). Pokud zaškrtnete obě pole, program AVAST32 ponechá zaškrtnuté pouze posledně zaškrtnuté pole. Jinak řečeno, AVAST32 změní nastavení zaškrťávacích polí tak, aby bylo přípustné.

Zaškrtnutím pole „Rezidentní bloky“ uživatel zapne pro danou úlohu rezidentní blokování podezřelých operací. To spočívá ve sledování systému a následném blokování potenciálně nebezpečných akcí. Jedná se o některé souborové operace a operaci formátování disků. Je-li blokování povoleno, je uživatel na každou takovou akci upozorněn a dotázán, zda má být daná operace opravdu provedena. Pole je implicitně zaškrtnuto.

Zaškrťávací pole „Sledování boot sektoru“ umožňuje mezi činnosti prováděné úlohou zařadit

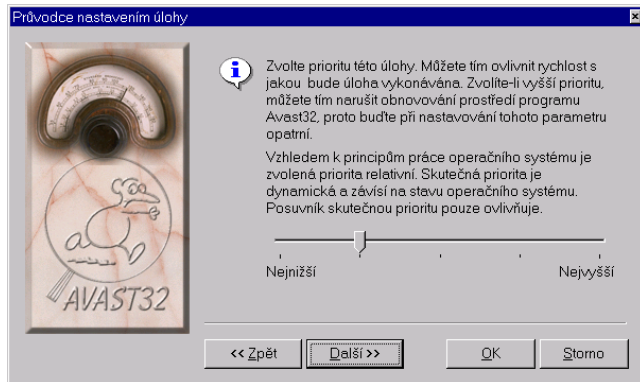
i sledování boot sektoru vkládaných disket, ze kterého se zavádí operační systém počítače. Jedná se o tzv. boot sektor. Pole je implicitně zaškrtnuto.

Zaškrťávací pole „Rezidentní sledování“ pro danou úlohu zapíná kontrolu spouštěných programů a dokumentů. Každý program, který má být spuštěn, bude nejprve zkontrolován, zda neobsahuje některý ze známých virů. Pokud je virus nalezen, program není spuštěn a uživatel obdrží varovné hlášení. Jinak je program normálním způsobem spuštěn. Sledování programů je implicitně zapnuto.

Stránka „Činnost“ je přítomna u každé varianty vytvářené úlohy.

#### 4.4.3 Stránka „Priorita“

Každá nerezidentní úloha umožňuje nastavit svou prioritu provádění. Jedná se vlastně o to, že uživatel sdělí operačnímu systému, jak důležitá je pro něj daná úloha. Čím vyšší má úloha prioritu, tím dostane více času procesoru a tím také poběží rychleji. Je nutné si uvědomit, že rychlost provádění úlohy záleží nejen na její prioritě, ale i na aktuálním stavu systému a prioritách všech ostatních právě běžících programů. Implicitně má úloha nastavenou prioritu menší, než je priorita samotného programu AVAST32.

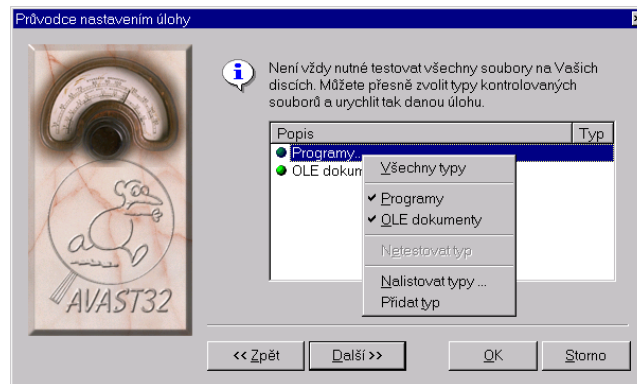


obr. 41

K nastavení priority slouží právě tato stránka (obr. 41). Obsahuje pouze posuvník, jehož nastavením lze měnit vlastní prioritu úlohy. Čím více je táhlo posuvníku vlevo, tím je priorita úlohy nižší a naopak. Protože se jedná o zásah do plánování úloh operačního systému, doporučujeme měnit pozici posuvníku pouze uživatelům, kteří vědí, co činí. Běžnému uživateli bude v naprosté většině případů vyhovovat přednastavená hodnota. Pokud bude nastavená priorita úlohy příliš velká, může dojít ke zpomalenému obnovování uživatelského prostředí programu. To není chyba programu, ale pouze důsledek faktu, že úloha má vyšší prioritu než uživatelské prostředí programu AVAST32.

Stránka „Priorita“ je přítomna pouze tehdy, je-li povoleno hledání virů nebo testování integrity dat a to ať už normální nebo zjednodušené, tedy pokud úloha obsahuje nerezidentní činnosti.

#### 4.4.4 Stránka „Typy“



obr. 42

Stránka „Typy“ slouží k určení typů souborů, které se ve vybraných složkách mají testovat (obr. 42). Většinou totiž není nutné testovat všechny soubory, protože viry napadají pouze některé z nich. Je například zbytečné testovat textové soubory (soubory s příponou TXT), protože i kdyby v nich virus byl, operační systém spuštění textového souboru nepovolí a virus se tak nikdy

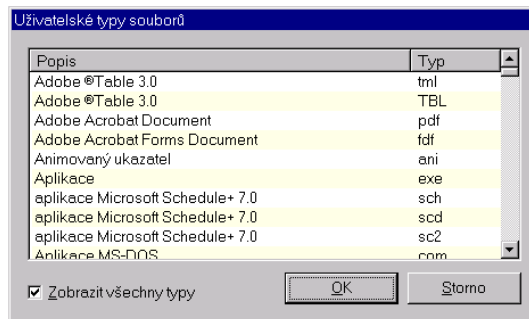
nestane aktivním. Omezením počtu testovaných souborů zrychlíte běh úlohy.

Všechny typy souborů, které se budou testovat, jsou vidět v seznamu na této stránce. Seznam obsahuje stručný popis typu souborů a případně i jeho příponu. Přípona souboru může obsahovat i zástupné znaky „\*“ (hvězdičku) a „?“ (otazník), jejichž význam je stejný, jako při použití kdekoli v operačním systému.

Přidat další typ do seznamu kontrolovaných typů je možné přes místní nabídku (obr. 42). Ta se zobrazí po stisku pravého tlačítka myši na seznamu typů. První tři položky nabídky jsou přednastavené typy, jejichž zatržením se daný typ umístí i do seznamu typů. Jedná se o položky „Všechny typy“ - zapne kontrolu úplně všech zvolených souborů, „Programy“ - kontrolovány budou pouze soubory, které lze spustit (včetně knihoven), a o položku „OLE dokumenty“, která zapne kontrolu dokumentů vytvořených technologií OLE. Je-li jejich zatržení zrušeno, jsou automaticky odstraněny i ze seznamu testovaných typů.

Do seznamu typů lze přidat i typy z databáze známých typů. K tomu slouží funkce „Nalistovat typy ...“ v místní nabídce. Po jejím vybrání se zobrazí dialog obsahující databázi známých typů souborů (obr. 43). Ta může obsahovat buďto nejdůležitější typy souborů nebo po zaškrtnutí pole

„Zobrazit všechny typy“ bude obsahovat úplně všechny známé typy souborů. Chcete-li nějaký typ zařadit do seznamu kontrolovaných typů, pak jej nejprve aktivujte a potom stisknete tlačítko „OK“. Po stisku tlačítka „Storno“ bude dialog zavřen a seznam zůstane beze změny.



obr. 43

Funkce „Přidat typ“ slouží k přímému zadání typu kontrolovaných souborů. Po jejím zvolení je uživateli umožněno zapsání přípony typu, která může obsahovat i zástupné znaky „\*“ (hvězdičku) a „?“ (otazník). Po jejím zapsání a stisku klávesy „Enter“ je nový typ přidán do seznamu.

Uživatelem vložené typy je možné kdykoli pozměnit - po klepnutí levým tlačítkem myši na příslušný typ Vám bude umožněna jeho editace. Pracujete-li s operačním systémem Windows

NT 3.51, pak poklepejte levým tlačítkem myši na jménu typu.

Vedle jména kontrolovaného typu souboru je ikona, znázorňující způsob práce s typem:

- soubory tohoto typu budou kontrolovány. Implicitně jsou tak označeny všechny nově přidané typy, včetně předvolených.
- soubory takto označeného typu kontrolovány nebudou. Lze tak programu sdělit, aby např. zkontroloval „Všechny soubory“ kromě souborů typu TXT apod. Označení typu provedete zaškrtnutím položky „Netestovat typ“ v místní nabídce. Vyjmout z kontroly však nelze přednastavené typy.

Pokud bude v seznamu nějaký z typů označen, že nemá být kontrolován, může to způsobit mírné zpomalení běhu úlohy. Program pak bude muset kontrolovat nejenom, zda má být soubor tohoto typu kontrolován, ale také zda nemá být z kontroly vyjmut. Na druhé straně, tím že nějaký typ souboru vyjmete z kontroly, můžete značně urychlit běh úlohy. Konkrétní situace záleží na vzorku kontrolovaných souborů, obecně lze však říci, že kvůli např. kontrole jednoho souboru navíc se nevyplatí vyjmout jeho typ ze seznamu kontrolovaných typů.

Typ souboru lze odstranit ze seznamu jeho vybráním a stiskem klávesy „Del“, nebo jestliže se

jedná o předvolený typ (viz výše), je možné zrušit jeho zatržení v místní nabídce.

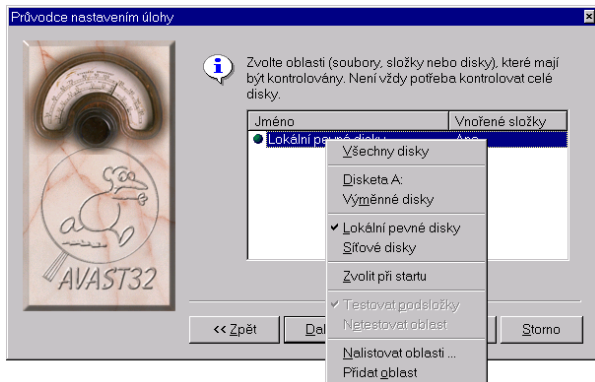
Při provádění úlohy se u každého zvoleného souboru nejprve otestuje jeho typ. Jestliže je typ uveden v seznamu na této stránce a je označen zelenou kuličkou, pak se s ním provedou všechny zvolené činnosti. Jinak se soubor jednoduše přeskočí. Implicitně je nastaven test programů (resp. spustitelných souborů) a OLE dokumentů.

Pokud úloha bude provádět rezidentní bloky, pak se budou kontrolovat pouze operace se soubory, jejichž typ je uveden na této stránce. Položky „Všechny typy“, „OLE dokumenty“ a typy, které mají být z kontroly vyjmuty (tj. typy označené červenou kuličkou), budou ignorovány, to znamená, že jejich přítomnost v seznamu nemá na rezidentní bloky pražádný vliv.

Stránka „Typy“ je přítomna pouze tehdy, obsahuje-li úloha alespoň jednu z následujících činností: hledání virů, testování integrity dat (normální nebo zjednodušené) nebo rezidentní bloky.

#### 4.4.5 Stránka „Oblasti“

Stránka „Oblasti“ umožňuje uživateli nastavit, které disky, příp. složky má nově vytvářená úloha kontrolovat (obr. 44). Lze tak přesně určit pouze ty složky, které mají být kontrolovány a urychlit běh úlohy vynecháním složek, které je zbytečné kontrolovat.



obr. 44

Všechny kontrolované oblasti nebo složky jsou zobrazeny v seznamu na této stránce. Přidat nějakou oblast lze přes místní nabídku. Ta obsahuje předvolené oblasti „Všechny disky“, „Disketa A:“, „Výměnné disky“, „Lokální pevné disky“, „Síťové disky“ a „Zvolit při startu“. Poslední položka znamená, že před zahájením vlastní úlohy bude uživatel dotázán na další kontrolované složky, které budou zkontrolovány spolu s těmi v seznamu. Zaškrtnutím oblasti v místní nabídce se tato objeví i v seznamu prohledávaných oblastí.

Zaškrtnutím položky „Testovat podsložky“ místní nabídky můžete určit, jestli u zvolené oblasti mají být prohledány i všechny jejich vnořené složky. Není-li položka zaškrtnuta, budou zkon-

trolovány pouze soubory ve vybrané složce či disku - případně vnořené složky prohledány nebudou. Položku je možné nastavit pro každou prohledávanou oblast zvlášť. Implicitně je prohledávání vnořných složek povoleno.

Vedle jména kontrolované oblasti je ikona, znázorňující způsob práce s oblastí:



oblast bude zkontrolována. Takto jsou implicitně označeny všechny nově přidávané oblasti, včetně předvolených.



takto označené oblasti kontrolovány nebudou. Lze tak programu sdělit, aby např. zkontroloval „Lokální pevné disky“ kromě složky „C:\Známé\_viry“ apod. Označení typu provedete zaškrtnutím položky „Netestovat oblast“ v místní nabídce. Vyjmout z kontroly však nelze přednastavené oblasti.

Funkce „Nalistovat oblasti“ místní nabídky slouží k přímému zvolení oblastí, které mají být prohledány. Po jejich zvolení se objeví standardní dialog umožňující zvolit i více oblastí najednou. Oblasti vybrané v tomto dialogu budou zařazeny do seznamu.

Funkce „Přidat oblast“ slouží k přímému zadání oblasti z klávesnice. Po jejím zadání bude do seznamu kontrolovaných oblastí přidána položka „Vlož jméno oblasti ...“ a bude umožněna její editace. Po zadání oblasti stisknete klávesu „Enter“.

Ve jménu oblasti je možné použít i zástupné znaky „\*“ (hvězdička) a „?“ (otazník) a specifikovat tak více složek najednou.

Uživatelé vložené oblasti je možné kdykoli pozměnit - po klepnutí levým tlačítkem myši na příslušnou oblast Vám bude umožněna jeho editace. Pracujete-li s operačním systémem Windows NT 3.51, pak poklepejte levým tlačítkem myši na jméno oblasti.

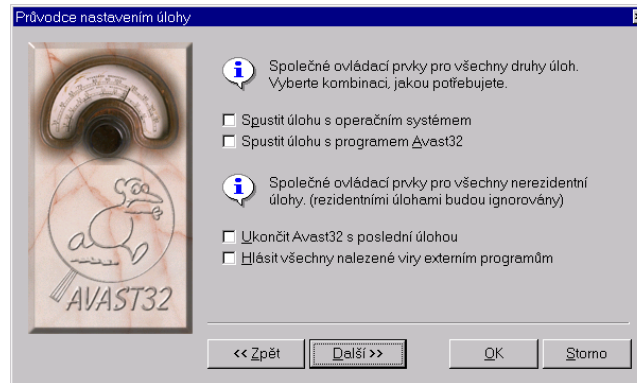
Chcete-li nějakou oblast ze seznamu odstranit, pak ji nejprve vyberte levým tlačítkem myši a potom stiskněte klávesu „Del“. Předvolené oblasti lze ze seznamu odstranit i tak, že zrušíte jejich zatržení v místní nabídce.

Stránka „Typy“ je přítomna pouze tehdy, je-li povoleno hledání virů nebo testování integrity dat a to ať už normální nebo zjednodušené.

#### 4.4.6 Stránka „Společné“

Stránka „Společné“ obsahuje ovládací prvky parametrů, které se svou povahou nedají zařadit na žádnou jinou stránku (obr. 45).

Zaškrtnutím pole „Spustit úlohu s operačním systémem“ uživatel sdělí programu, že vytvářená úloha má být spuštěna ihned po přihlášení uživatele. Implicitně není pole zaškrtnuto. Pokud je úloha sdílená a pole je zaškrtnuto, pak se úloha bude spouštět každému uživateli daného počítače ihned po jeho přihlášení do systému.



obr. 45

Zaškrťovací pole „Spustit úlohu s programem Avast32“ zapíná spouštění úlohy automaticky po startu programu AVAST32. Jestliže je úloha sdílená, bude se automaticky spouštět všem uživatelům, jinak pouze uživateli, který úlohu vytvořil. Spouštění úlohy zároveň s programem AVAST32 je implicitně vypnuto.

Následující dvě zaškrťovací pole mají vliv pouze na nerezidentní úlohy, což jsou úlohy obsahující hledání virů nebo test integrity dat (normální nebo zjednodušený). Jejich nastavení bude rezidentními úlohami ignorováno.

Zaškrťovací pole „Ukončit Avast32 s poslední úlohou“ zapíná automatické ukončování programu AVAST32, po skončení poslední běžící úlo-

hy. Tuto možnost je výhodné použít zejména u úloh, které se spouštějí jinak než přímo z programy AVAST32, např. pomocí zástupce na pracovní ploše. Pole není implicitně zaškrtnuto.

Zaškrtnuté pole „Hlásit všechny nalezené viry externím programům“ dává uživateli možnost nastavit, zda mají být externí programy (tedy programy, které nejsou součástí AVAST32) informovány pouze o prvním nalezeném viru během jedné úlohy (pole není zaškrtnuto) nebo o všech nalezených virech (pole je zaškrtnuto). Implicitně není pole zaškrtnuto. Bližší informace o systému informování externích programů o nalezených virech jsou uvedeny v [příloze F.1](#).

Stránka „Společně“ je přítomna u každé varianty vytvářené úlohy.

#### 4.4.7 Stránka „Hledání virů“

Jednou z hlavních činností programu AVAST32 je vyhledávání známých virů. Stránka „Hledání virů“ (obr. 46) slouží k nastavení té části programu AVAST32, která má právě hledání virů na starost.

Zaškrtnutým polem „Testovat operační paměť“ má uživatel možnost nastavit, zda se při hledání virů má také zkontrolovat operační paměť počítače. Tak je možné odhalit virus, který počítač již napadl. Implicitně se test paměti bude provádět.



obr. 46

Pod operačním systémem Windows NT, vzhledem k jeho architektuře, nemá test operační paměti smysl, a proto pracujete-li pod systémem Windows NT, nebude Vám tato možnost nabídnuta. Stránka „Hledání virů“ tedy v operačním systému Windows NT neobsahuje zaškrtnuté pole „Testovat operační paměť“.

Zaškrtnuté pole „Ignorovat charakteristiku virů“ slouží k zapnutí kontroly souborů na přítomnost všech virů v databázi. Pokud není pole zaškrtnuto, jsou soubory testovány pouze na přítomnost virů, které napadají daný typ souborů. Takže pokud je soubor typu COM, nebude testován na přítomnost virů, které napadají pouze soubory typu EXE apod. Zaškrtnutím tohoto pole



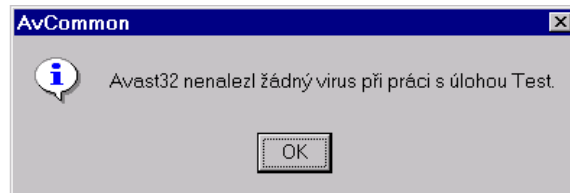
zajistíte, aby byly soubory testovány na přítomnost všech virů, bez ohledu na typ, který napadají. Implicitně je pole zaškrtnuto.

Zaškrťovací pole „Testovat celé soubory“ určuje, zda se na přítomnost virů mají testovat celé soubory. Jestliže pole není zaškrtnuto, program AVAST32 bude testovat pouze některé oblasti souborů. To je výhodné zvláště z hlediska rychlosti úlohy. Program přitom vychází z faktu, že naprostá většina virů napadajících soubory se přidává na konec souboru nebo přemazává jeho začátek, takže většinou bývá zbytečné testovat celý soubor. Pole není implicitně zaškrtnuto.

Pomocí zaškrťovacího pole „Testovat komprimované soubory“ lze zapnout kontrolu zkomprimovaných souborů. Zkomprimované soubory mohou být totiž napadeny dvojnásobem: před komprimací a po komprimaci. Jestliže byl soubor napaden až po komprimaci, objeví ho program AVAST32 bez nutnosti jej dekomprimovat. Aby však bylo možné odhalit i virus, který soubor napadl už před komprimací, je potřeba soubor nejprve dekomprimovat a potom teprve zkontrolovat.

Po zaškrtnutí pole bude program AVAST32 soubory kontrolovat nejprve zkomprimované, potom soubory vnitřně dekomprimuje (soubory na disku zůstanou zkomprimované) a výsledek znovu zkontroluje.

V současné době program AVAST32 podporuje komprimační programy Diet, Lzexe, Pklite a Ice. Testování komprimovaných souborů je implicitně povoleno.



obr. 47

Zaškrtnutí pole „Zobrazit informaci, pokud nebyl nalezen žádný virus“ způsobí, že AVAST32 bude zobrazovat hlášení o skončení hledání virů i v případě, že žádný vir nebyl nalezen (obr. 47). Tato možnost je implicitně vypnutá.

Dále si můžete zvolit, kdy chcete být informováni o nalezení viru. Výběr provedete zvolením jednoho z následujících přepínačů:

- zvolení přepínače „Hlásit všechny objevené viry“ způsobí, že program AVAST32 pro každý virus, který nalezne, zobrazí varovné hlášení (kapitola 5.4) a počká na reakci uživatele.
- přepínač „Hlásit pouze první virus“ zapne zobrazování varovného hlášení podobně jako předchozí přepínač, ale pouze pro první nalezený virus. Jestliže uživatel potřebuje

pouze informaci o tom, zda je jeho počítač nakažen nebo ne, je výhodné zvolit tento přepínač. Pokud po skončení testu bude potřeba zjistit všechny nakažené soubory, stačí si prohlédnout stránku „Výsledky“ rozšířeného ovládání.

- přepínač „Nehlásit nalezené viry“ slouží k potlačení zobrazování hlášení o nalezených virech. Je-li přepínač zvolen, nebude uživatel informován o žádném z nalezených virů. Protože hrozí nebezpečí, že případné nalezení viru v systému bude přehlédnuto, doporučujeme používat tuto možnost v součinnosti například s hlášením o nalezení viru po přihlášení uživatele (kapitola 6.5.1, zaškrťovací pole „Zobrazovat hlášení o viru po přihlášení“).

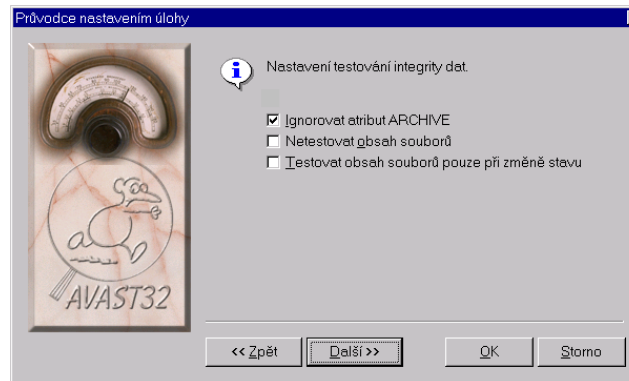
Implicitně je zvoleno hlášení všech nalezených virů.

Stránka „Hledání virů“ je dosažitelná pouze tehdy, má-li daná úloha viry vyhledávat, tzn. že je zvolena činnost hledání virů na stránce „Činnost“ (viz kapitola 4.4.2).

#### 4.4.8 Stránka „Integrita“

Stránka „Integrita“ (obr. 48) slouží k nastavení parametrů testování integrity dat na Vašich discích. Pod pojmem testování integrity dat si lze představit sledování změn, které byly provedeny s jednotlivými soubory od poslední kontroly.

Uživatel tak má možnost odhalit činnost virů, a to i včetně těch dosud neznámých.



obr. 48

Zaškrtnutím pole „Ignorovat atribut ARCHIVE“ informujete program, že má ignorovat změnu atributu ARCHIVE u kontrolovaných souborů. Atribut je využíván převážně zálohovacími programy k rozeznání souborů, které mají být archivovány. Operační systém tento atribut nastavuje při jakémkoli zápisu do souboru.

Jestliže je pole zaškrtnuto, nebude test integrity dat hlásit změnu tohoto atributu, tzn. že soubor, u kterého se změnil od poslední kontroly pouze atribut ARCHIVE, nebude zařazen do seznamu

změněných souborů. Pole je implicitně zaškrtnuto.

Zaškrtnutím pole „Netestovat obsah souborů“ je možné zakázat testování změny obsahu souborů. Soubory se pak budou kontrolovat pouze podle svých parametrů jako je datum poslední změny, velikost, atributy atd., ale nebudou se vytvářet kontrolní součty jejich obsahu. Zaškrtnutím pole urychlíte běh úlohy, ale z důvodu větší bezpečnosti Vašeho systému doporučujeme nechat testování obsahu souborů zapnuté. Implicitně se obsah souborů bude testovat.

Zaškrtnutím pole „Testovat obsah souborů pouze při změně stavu“ má uživatel možnost nastavit, aby se obsah souborů kontroloval pouze tehdy, došlo-li ke změně základních vlastností souboru (atributů, datumu poslední změny, apod.). Tato možnost vychází z předpokladu, že pokud bylo manipulováno s obsahem souboru, byly změněny i parametry souboru. Zaškrtnutím pole lze urychlit běh úlohy. Implicitně není pole zaškrtnuto.

Stránka „Integrita“ je přítomna pouze v případě, že jedna z činností, které mají být prováděny je i testování integrity dat, a to ať už normální nebo zjednodušené (viz [kapitola 4.4.2](#)).

#### 4.4.9 Stránka „Pokračuj“

Stránka „Pokračuj“ umožňuje uživateli vybrat úlohu, která má být spuštěna po dokončení právě vytvářené úlohy (obr. 49)



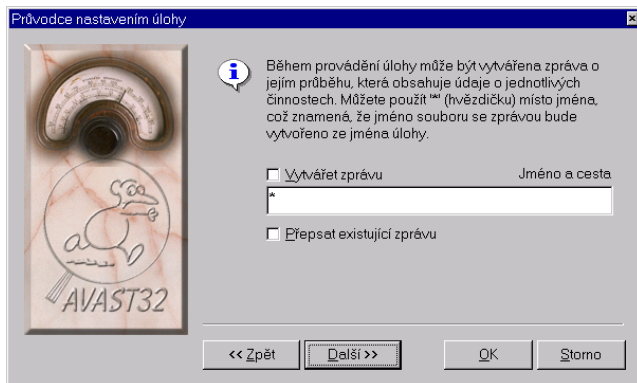
obr. 49

Jméno takové úlohy je potřeba zapsat do textového pole „Jméno úlohy“ nebo je možné jej vybrat ze seznamu dosud vytvořených úloh. Seznam úloh se objeví po klepnutí levým tlačítkem myši na šipku vpravo od textového pole. Implicitně textové pole neobsahuje žádné jméno úlohy.

Stránka „Pokračuj“ je přístupná pouze pro nerezidentní úlohy, tzn. je-li na stránce „Činnost“ zvolena alespoň jedna nerezidentní činnost.

#### 4.4.10 Stránka „Zpráva“

Během provádění úlohy může být programem AVAST32 vytvořen soubor s podrobnou zprávou o její činnosti a výsledcích. Povolení vytváření této zprávy a nastavení jejího jména obsahuje právě stránka „Zpráva“ (obr. 50). Zpráva o průběhu úlohy je ukládána v podobě čistého ASCII textu do zvoleného souboru (viz dále). Obsahuje informace o souborech, které byly testovány, o nalezených virech a jiné důležité informace, včetně statistik testování systému.



obr. 50

Zaškrtnuté pole „Vytvářet zprávu“ zapíná vytváření souboru se zprávou o činnosti úlohy. Impli-

citně se soubor se zprávou nebude vytvářet.

Pod předchozím ovládacím prvkem se nalézá textové pole, do něhož lze zapsat složku a jméno souboru, do kterého se zpráva bude zapisovat. Zadá-li uživatel místo jména „\*“ (hvězdičku), bude se soubor se zprávou jmenovat stejně jako úloha, pouze přípona souboru bude RPT. Pokud u jména souboru není uvedena přípona, použije se automaticky zmíněná přípona RPT. Implicitně textové pole obsahuje „\*“.

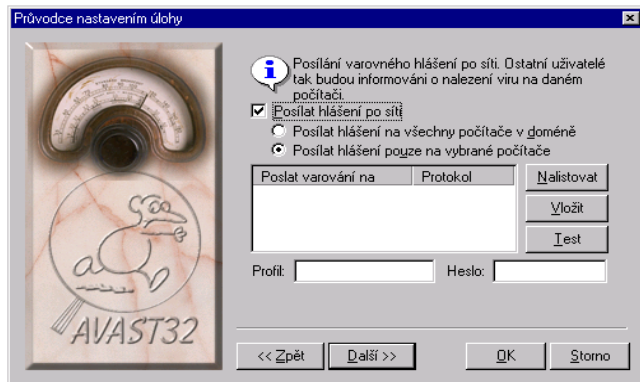
Zaškrtnuté pole „Přepsat existující zprávu“ říká programu, že pokud již existuje soubor se zprávou daného jména, má být přepsán. Jestliže přepsání není povoleno a soubor se zprávou již existuje, potom bude zpráva o činnosti této úlohy přidána k již existujícímu souboru. Implicitně není pole zaškrtnuto.

Stránka „Zpráva“ je dosažitelná pouze v případě, že úloha obsahuje alespoň jednu nerezidentní činnost, tzn. alespoň hledání virů nebo test integrity dat.

#### 4.4.11 Stránka „Síťové varování“

Stránka „Síťové varování“ (obr. 51) obsahuje ovládací prvky pro nastavení parametrů posílání varovných hlášení po síti. Program AVAST32 totiž umožňuje v případě nalezení viru zaslat na počítače dosažitelné lokální sítě varovné hlášení

o hrozícím nebezpečí a předejít tak hromadnému rozšíření viru.



obr. 51

Zaškrtnuté pole „Posílat hlášení po síti“ zapne posílání varovného hlášení prostřednictvím sítě. Implicitně posílání hlášení po síti není povoleno.

Pokud jste posílání varovného hlášení po síti povolili, musíte dále určit, kam má být v případě nalezení viru hlášení zasláno. To provedete zvolením jednoho z následujících přepínačů:

- přepínačem „Posílat hlášení na všechny počítače v doméně“ nastavíte posílání varovného hlášení o nalezení viru na všechny počítače, které budou v danou chvíli připojeny k aktuální doméně,

- přepínač „Posílat hlášení pouze na vybrané počítače“ způsobí, že hlášení bude zasláno pouze na počítače, které jsou uvedeny v seznamu na této stránce.

Implicitně je nastaveno posílání varovného hlášení pouze na vybrané počítače.

Je-li posílání hlášení po síti povoleno a je zvoleno posílání hlášení pouze na vybrané počítače, je potřeba tyto počítače určit. Seznam vybraných počítačů se nachází pod uvedenými ovládacími prvky.

Počítač, na který má být hlášení o nalezení viru zasláno, je možné určit přímým zapsáním jeho jména do seznamu vybraných počítačů. Stiskem tlačítka „Vložit“ zobrazíte místní nabídku s několika protokoly:

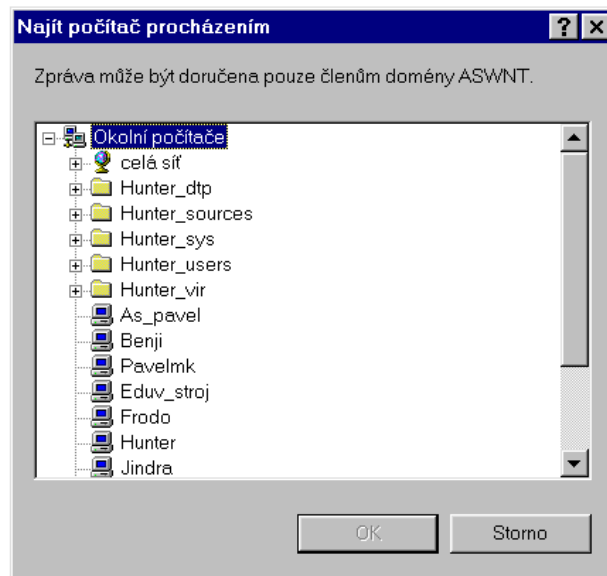
- položka „Internet“ určuje, že počítač, na který bude varovná zpráva zaslána, je určen pomocí standardní URL adresy. Pro doručení zprávy bude použit protokol SMTP (Internet Mail),
- položkou „Microsoft“ sdělíte programu, že daný počítač je přístupný přes poštu Microsoft Mail,
- položka „Základní“ umožňuje uživateli zapsat libovolnou adresu včetně specifikace protokolu, který má být použit. Např. adresa „SMTP:novak@aaa.cz“ tohoto protokolu je stejná jako adresa „novak@aaa.cz“ protokolu „Internet“ apod.,

- položka „Interní“ znamená, že pro přístup na zvolený počítač bude použit protokol pro lokální síť (daný počítač, musí být samozřejmě přes lokální síť dostupný).

Po zvolení příslušného protokolu bude přidána do seznamu položka jménem „Vlož platnou adresu/jméno ...“. Klepnete-li na ní levým tlačítkem myši, bude Vám umožněna její editace. Po zapsání jména počítače stiskněte klávesu „Enter“.

Vložené jména počítačů je možné kdykoli pozměnit - po klepnutí levým tlačítkem myši na příslušné jméno Vám bude umožněna jeho editace. Pracujete-li s operačním systémem Windows NT 3.51, pak poklepejte levým tlačítkem myši na jménu počítače.

Po stisku tlačítka „Nalistovat“ se opět objeví místní nabídka s protokoly (v současné době obsahuje pouze položku „Interní“, viz výše). Počítač, dostupný přes lokální síť, můžete vybrat pomocí dialogu, který ukazuje obr. 52. Postupně prohledejte všechny části sítě až naleznete požadovaný počítač. Do seznamu zvolených počítačů jej zařadíte tak, že jej nejprve označíte a stisknete tlačítko „OK“. Stiskem tlačítka „Storno“ dialog zavřete a seznam počítačů zůstane beze změny.



obr. 52

Počítač můžete ze seznamu odstranit tak, že jej nejprve aktivujete a poté stisknete klávesu „Del“.

Parametry položek v seznamu, resp. vybraných počítačů, je možné dodatečně změnit. Chcete-li změnit přístupový protokol na daný počítač, klepněte do sloupce „Protokol“ příslušného počítače. Z místní nabídky poté vyberte nový protokol. Podobným způsobem změníte i jméno/adre-

su počítače: po klepnutí levým tlačítkem myši Vám bude umožněna jeho editace.

Pokud si nejste doručením varovné zprávy jisti, můžete „spojení“ vyzkoušet tlačítkem „Test“. Na každý vybraný počítač pak bude zasláno zkušební hlášení.

Budete-li posílat zprávu prostřednictvím jiného protokolu než „Interní“, je potřeba zapsat jméno profilu, který se má použít, popř. jeho heslo, do příslušných textových polí. Pokud necháte textové pole „Profil:“ nevyplněné použije se profil, zadaný pro použití všemi úlohami (viz kapitola 6.1.4). Pokud i zde není žádný profil zadán a v danou chvíli žádný profil nepoužíváte (tzn. nemáte spuštěn např. program Microsoft Outlook), budete na jméno profilu dotázáni.

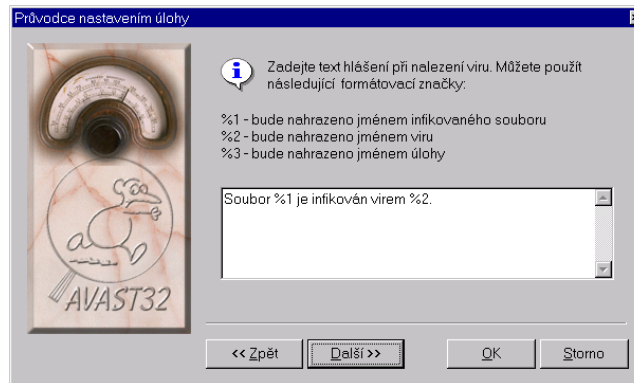
Zadáte-li profil na této stránce a současně zadáte jiný profil pro použití všemi úlohami, použije se profil zadaný na této stránce (tj. profil úlohy).

Jestliže pracujete pod operačním systémem Windows NT, musíte mít spuštěny služby „Alert“ a „Messenger“ (složka „Ovládací panely“, prvek „Služby“), abyste mohli odesílat a přijímat síťová hlášení. Nemáte-li práva potřebná k jejich používání, kontaktujte administrátora Vaší sítě. Pracujete-li ve Windows 95 a chcete-li, aby posílání varovných zpráv po síti pracovalo, musíte mít spuštěn program „WinPopUp“.

Varovné hlášení může na zvolený počítač přijít i vícekrát. Nejedná se o chybu programu, ale o systémovou záležitost. Počet zaslaných kopií hlášení záleží na počtu instalovaných síťových protokolů.

Stránka „Síťové varování“ je přítomna, je-li zvolena alespoň jedna z následujících činností: hledání virů, sledování boot sektoru nebo rezidentní sledování.

#### 4.4.12 Stránka „Hlášení“



obr. 53

Stránka slouží k editaci textu hlášení, které bude zobrazeno při nalezení viru (obr. 53). Je-li povoleno posílání zpráv po síti, pak bude toto

hlášení zasláno i na všechny zvolené počítače (viz kapitola 4.4.11).

K dispozici je textové pole, které umožňuje zapsání vlastního textu hlášení. Pomocí formátovacích značek je do něj možné vkládat i proměnné parametry, jako je jméno souboru, úlohy apod. Příslušná formátovací značka pak bude nahrazena daným jménem. Význam formátovacích značek je následující:

- %1 - jméno infikovaného souboru,
- %2 - jméno viru, který soubor napadl,
- %3 - jméno úlohy, která virus objevila.

Pokud byl například nalezen úlohou „Vlastní“ virus „OneHalf“ v souboru „D:\PRG.EXE“ a vložený text bude mít tvar „Pozor! Byl nalezen virus %2 v souboru %1. Použita úloha %3.“ bude výsledné hlášení vypadat takto: „Pozor! Byl nalezen virus OneHalf v souboru D:\PRG.EXE. Použita úloha Vlastní.“

Implicitně textové pole obsahuje zprávu ve tvaru:

Soubor %1 je infikován virem %2.

Stránka „Hlášení“ je přítomna tehdy, je-li zvolena alespoň jedna z následujících činností: hledání virů, sledování boot sektoru a rezidentní sledování.

#### 4.4.13 Stránka „Zvuky“

Nalezení viru může dát program AVAST32 najevo i zvukově. Chcete-li tuto možnost využít, pak na stránce „Zvuky“ (obr. 54) stisknete tlačítko „Nastavit ...“ a v zobrazeném dialogu nastavit příslušný zvuk (podrobný popis je uveden dále).

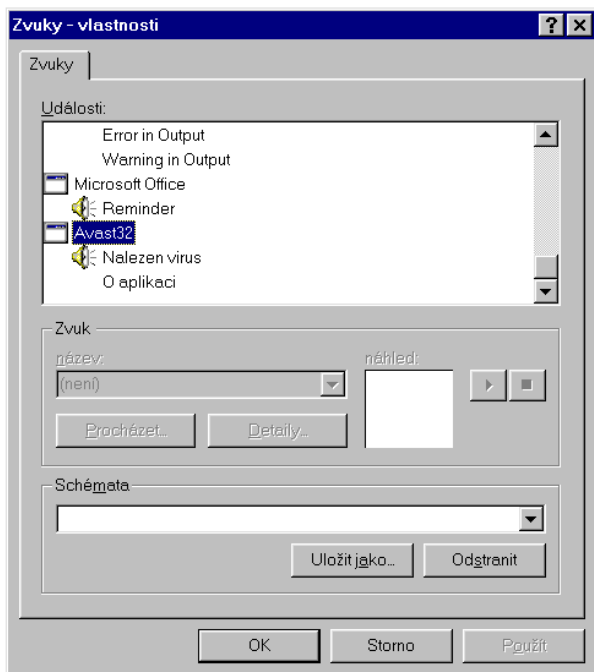


obr. 54

Program AVAST32 pro nastavení zvuku pro oznámení nalezení viru využívá systémový ovládací panel „Zvuky“ (obr. 55).

Nejprve v seznamu „Události“ naleznete položku „Avast32“ a označte její podpoložku „Nalezen virus“.





obr. 55

Složku a jméno souboru se zvukem můžete buďto zapsat přímo do textového pole nebo jej můžete vybrat pomocí standardním dialogu pro otevírání souborů. Ten se zobrazí po stisku tlačítka „Procházet ...“. Podrobný popis tohoto dialogu

je uveden v manuálu nebo nápovědě operačního systému.

Příslušný zvukový soubor můžete také vybrat z nabídky, která se objeví po stisku šipky vedle textového pole „název :“.

Zvuky programu AVAST32 pro různé události je možné nastavit díky využití ovládacího panelu „Zvuky“ i není-li AVAST32 spuštěn - viz [kapitola 6.7.3](#).

Abyste mohl být soubor na Vašem počítači přehrán, musí být Váš počítač vybaven zvukovou kartou a příslušnými ovladači! Samotná přítomnost zvukové karty a jejich ovladačů v počítači však nestačí! Je potřeba, aby karta i ovladače byly správně nainstalovány a pracovaly. Pokud Váš operační systém zvuky přehrává (např. při startu, pokud nejsou vypnuty), pak je bezproblémově přehraje i program AVAST32!

Stránka „Zvuky“ je přítomna, je-li pro danou úlohu zvolena jedna z následujících činností: hledání virů, sledování boot sektoru nebo rezidentní sledování.

#### 4.4.14 Stránka „Sledování“

Stránka „Sledování“ obsahuje ovládací prvky, které slouží k bližšímu určení souborů, které mají být kontrolovány před svým spuštěním (obr. 56). V poslední době se objevil nový typ virů, který nenapadá spustitelné soubory ani boot sektory

disků, ale nově datové soubory, konkrétně OLE dokumenty. Jedná se o tzv. makroviry. Program AVAST32 proto obsahuje možnost průběžně kontrolovat i otevírané OLE dokumenty. Omezením počtu kontrolovaných souborů lze urychlit spouštění jednotlivých programů a otevírání OLE dokumentů.



obr. 56

Při každém pokusu spustit nějaký program či otevřít dokument, jej program AVAST32 nejprve prohlédne, zda není infikován nějakým známým virem. Pokud ne, bude soubor spuštěn, v opačném případě bude uživatel informován. Soubory obsahující OLE dokumenty však budou kontrolovány pouze v případě, kdy jsou otevírány po-

mocí OLE funkcí. Při standardních operacích se soubory, jako je jejich kopírování apod. nebude dokument kontrolován.

Spustitelné soubory a OLE dokumenty jsou kontrolovány ve chvíli, kdy je požadováno jejich spuštění nebo otevření pomocí OLE funkcí. Z toho vyplývá, že k mírnému snížení rychlosti může dojít pouze při startu kontrolované aplikace nebo při zmíněném otevírání OLE dokumentu - nikoli však během vlastní práce se spuštěnou aplikací ani s otevřeným dokumentem.

Kontrolovat lze OLE dokumenty, 16-bitové aplikace pro Windows 3.1, aplikace MS-DOSu a samozřejmě 32-bitové programy. Zda se příslušný typ souboru bude kontrolovat, určíte zaškrtnutím příslušného pole. 32-bitové aplikace (tedy aplikace určené pro operační systémy Windows 95 a NT) se budou kontrolovat vždy. Je možné označit libovolnou kombinaci sledovaných programů. Implicitně jsou zaškrtnuty všechny položky.

Dále má uživatel možnost určit, zda se budou při spuštění programu kontrolovat všechny jeho soubory, tedy včetně všech knihoven, nebo všechny soubory s výjimkou systémových knihoven a nebo všechny soubory kromě knihoven. Výběr se provede zvolením jednoho z uvedených přepínačů.

Zvolené nastavení má velký vliv na rychlost spouštění aplikací, zvláště pokud používají stále stejné knihovny. Jestliže tedy pravidelně provádíte kontrolu Vašeho systému, je z hlediska rychlosti výhodné vypnout kontrolu alespoň systémových knihoven. Naopak, pokud si hodláte nainstalovat program s neznámým původem, doporučujeme zapnout kontrolu všech spustitelných souborů včetně jeho knihoven.

Implicitně je nastavena kontrola naprosto všech spouštěných souborů, včetně knihoven s výjimkou systémových.

Stránka „Sledování“ je přítomna pouze v případě, že mezi činnosti prováděné úlohou patří i sledování spouštěných programů (viz kapitola 4.4.2).

#### 4.4.15 Stránka „Rezidentní bloky“

Stránka „Rezidentní bloky“ obsahuje ovládací prvky pro nastavení další možné činnosti úloh a tou je blokování potenciálně nebezpečných operací (obr. 57). Při každém pokusu o provedení takovéto operace bude uživatel upozorněn a operace bude provedena pouze s jeho svolením.

Při tomto přístupu však může být uživatel často obtěžován zbytečnými dotazy, a proto program AVAST32 nabízí možnost zvolit pouze ty operace, které mají být sledovány.



obr. 57

Zaškrtnutí pole „Souborové operace MS-DOSu“ způsobí, že AVAST32 bude kontrolovat potenciálně nebezpečné operace se soubory, které se snaží vykonat aplikace určené pro operační systém MS-DOS. Implicitně je pole zaškrtnuto.

Zaškrťovací pole „Souborové operace Windows“ slouží k zapnutí kontroly potenciálně nebezpečných operací se soubory, které se pokusí vykonat aplikace určené pro operační systémy Windows 95 a Windows NT. Implicitně je pole zaškrtnuto.

Pracujete-li v operačním systému Windows 95, pak stránka „Blokování“ obsahuje i zaškrťovací pole „Formátování“. Jeho zaškrtnutím zapnete kontrolu formátovacích operací na Vašem počítačovém systému. Pole doporučujeme nechat

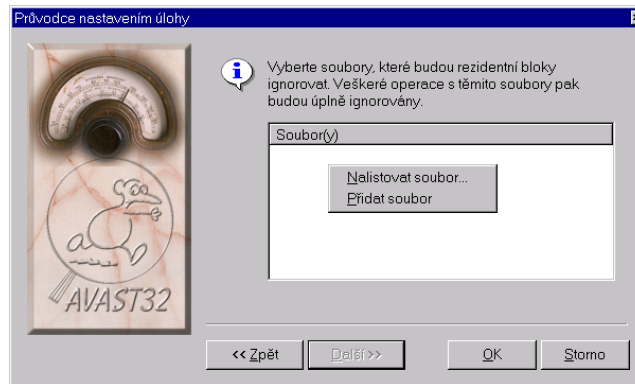
zaškrtnuté, protože viry používající tuto systémovou službu jsou obzvláště nebezpečné - v lepším případě totiž můžete přijít o určitou část Vašeho pevného disku, v horším o celý jeho obsah. Implicitně není pole zaškrtnuto.

V prostředí operačního systému Windows NT stránka obsahuje pouze zaškrtačkové pole „Souborové operace MS-DOSu“ a „Souborové operace Windows“.

Stránka „Rezidentní bloky“ je dosažitelná pouze v případě, že jednou z činností úlohy je i blokování potenciálně nebezpečných operací (viz kapitola 4.4.2).

#### 4.4.16 Stránka „Ignorovat“

Stránka umožňuje uživateli specifikovat soubory, se kterými budou všechny operace (MS-DOSu i Windows) programem AVAST32 při zapnutém blokování nebezpečných operací úplně ignorovány (obr. 58). Tato možnost byla do programu začleněna hlavně proto, že existuje celá řada běžných programů, o kterých je známo, že si během své činnosti do sebe ukládají nejrůznější informace. Hlášení takové činnosti programu může být nepříjemné a časově náročné.



obr. 58

Stránka obsahuje seznam souborů, u kterých nebudou hlídány žádné operace. Pokud úloha obsahuje i jiné činnosti, než je blokování, pak tyto činnosti budou prováděny i se soubory uvedenými v tomto seznamu. Implicitně je seznam souborů prázdný. Chcete-li do seznamu nějaký soubor přidat, použijte místní nabídku:

- funkce „Přidat soubor“ přidá do seznamu souborů položku jménem „Vlož platné jméno souboru ...“ a umožní uživateli její editaci. Po vložení jména souboru stiskněte klávesu „Enter“.
- funkce „Nalistovat soubor...“ otevře standardní dialog na otvírání souborů (obr. 88) a umožní uživateli vybrat požadovaný soubor. Vybraný

soubor pak bude přemístěn do seznamu souborů.

Vložené soubory je možné kdykoli pozměnit - po klepnutí levým tlačítkem myši na příslušný soubor Vám bude umožněna jeho editace. Pracujete-li s operačním systémem Windows NT 3.51, pak poklepejte levým tlačítkem myši na jméno souboru.

Jméno souboru nesmí obsahovat zástupné znaky „\*“ (hvězdičku) a „?“ (otazník). Soubor lze ze seznamu smazat obvyklým způsobem, tedy nejprve je potřeba jej vybrat a potom použít klávesu „Del“.

Stránka „Ignorovat“ je dosažitelná pouze v případě, že jednou z činností úlohy je i blokování potenciálně nebezpečných operací (viz [kapitola 4.4.2](#)).

## 4.5 Kontrola vkládaných údajů

Při vytváření nové úlohy program AVAST32 vyžaduje vložení několika údajů a samozřejmě kontroluje jejich správnost a úplnost. Pokud jsou zadané údaje nesprávné, bude na to uživatel upozorněn. Je-li zapnuto používání průvodce pro danou operaci s úlohou, nebude uživateli umožněno ani přejít na následující stránku bez vložení správných údajů.

Jméno úlohy by mělo být pokud možno co nejvýstižnější a z důvodu přehlednosti by nemělo

být použito pro více úloh. Program však vytvoření více úloh se shodným jménem nebrání. Pokud není jméno úlohy zadáno, program AVAST32 nepovolí její vytvoření.

Aby vytvoření nové úlohy mělo smysl, musí obsahovat nějakou činnost. Jednotlivé činnosti, které bude úloha provádět se zadávají na stránce „Činnost“ ([kapitola 4.4.2](#)). Jestliže jste tedy nezadali žádnou činnost úlohy, nebude její vytvoření povoleno.

Program AVAST32 také nedovolí vytvořit novou úlohu, jestliže obsahuje činnost hledání virů nebo test integrity dat a není určen žádný typ souborů, které mají být kontrolovány ([kapitola 4.4.4](#)) nebo nejsou určeny oblasti, které mají být kontrolovány ([kapitola 4.4.5](#)). Jinak řečeno, seznamy na stránkách „Typy“ a „Oblasti“ jsou prázdné.

Program AVAST32 však nekontroluje, zda zadané soubory (např. soubor se zvukem nebo soubory, které mají být ignorovány) existují. Na jejich neexistenci je uživatel upozorněn až v případě jejich potřeby. Taktéž není kontrolována dosažitelnost počítačů uvedených na stránce „Síťové varování“ ([kapitola 4.4.11](#)) - tu můžete otestovat tlačítkem „Test“ na této stránce.

## 5. Popis ovládání programu

Ovládání programu AVAST32 může mít dvě podoby. Tou první je tzv. jednoduché ovládání, které se svou povahou hodí zejména pro uživatele, kteří potřebují provádět běžné funkce bez nutnosti znalosti detailů práce programu a jeho funkce.

Druhé ovládání, tzv. rozšířené, obsahuje rozhraní pro veškeré funkce a možnosti, které program AVAST32 nabízí. Využijí ho zejména odborníci a zkušenější uživatelé, neboť umožňuje přizpůsobit si program vlastním potřebám a využít tak všech jeho funkcí a výhod.

Společným prvkem obou ovládání je, kromě loga firmy ALWIL Software a nabídky okna, která je popsána v následující kapitole, stavový řádek, který se nachází u spodního okraje okna. Obsahuje čtyři kolonky. V první kolonce je uvedeno přesné číslo verze programu AVAST32 včetně čísla jeho překladu. Jestliže kontaktujete pracovníky naší firmy v případě nějakých problémů, pak budete zmíněná čísla potřebovat.

Druhá kolonka obsahuje počet dosažitelných úloh a počet právě běžících úloh. Počet použitých licencí a počet zakoupených licencí je uveden v pořadí třetí kolonce. Poslední kolonka je v současné době nevyužita.

Po prvním startu programu se objeví jednoduché ovládání programu AVAST32.

### 5.1 Nabídka hlavního okna

Dalším prvkem, společným pro jednoduché a rozšířené ovládání, je nabídka okna (obr. 59). Nachází se pod lištou hlavního okna a je dostupná kdykoli během činnosti programu.



obr. 59

#### Nabídka „Zobraz“

Je určena pro přepínání ovládání programu AVAST32. Jejím obsahem jsou položky „Jednoduché ovládání“ a „Rozšířené ovládání“, jejichž zvolením se přepnete do příslušného ovládání programu.

Právě používané ovládání je označeno kuličkou (obr. 59 byl pořízen při zapnutém rozšířeném ovládání).

### Nabídka „Nastavení“

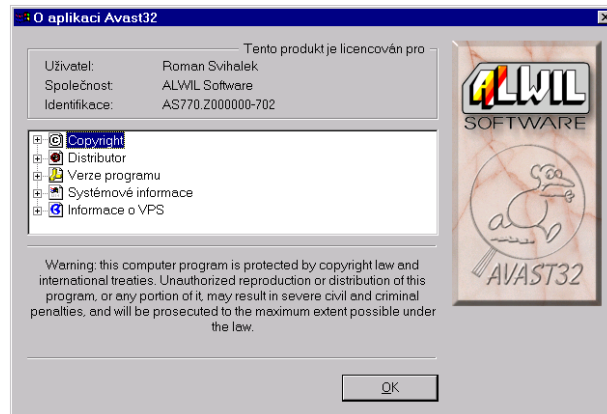
Pomocí položek této nabídky lze přizpůsobit chování programu AVAST32 a všech jeho částí potřebám jednotlivých uživatelů. Obsahují například volbu používání průvodce při vytváření a změnách úloh apod. Součástí nastavení programu je i možnost aktualizace souboru s charakteristikami všech dosud známých virů, tzv. souboru VPS.

Z důvodu rozsáhlosti a důležitosti těchto položek jsme se jim rozhodli věnovat samostatnou kapitolu. Podrobný popis všech částí nastavení programu uživatel nalezne v [kapitole 6](#).

### Nabídka „Nápověda“

Zvolením položky „WEB“ se spustí prohlížeč WWW stránek (pokud je samozřejmě nainstalován) a v případě, že jste napojeni na Internet, zobrazí se Vám stránka firmy ALWIL Software.

Položka „Informace“ této nabídky je určena pro zobrazení informací o programu (obr. 60).



obr. 60

Těmito informacím byste měli věnovat určitou pozornost, protože některé z nich můžete potřebovat obrátíte-li se na naši firmu se žádostí o technickou podporu. Pracovníci technické podpory mohou odmítnout zodpovědět vaše dotazy v případě, že jim tyto informace neposkytnete!

Jsou zde uvedeny informace jako:

- vlastníci autorských práv,
- vlastníci licence a počet licencí dostupných přes síť,
- verze programu AVAST32 a použitých komponent, včetně detailních informací o překladu programu,

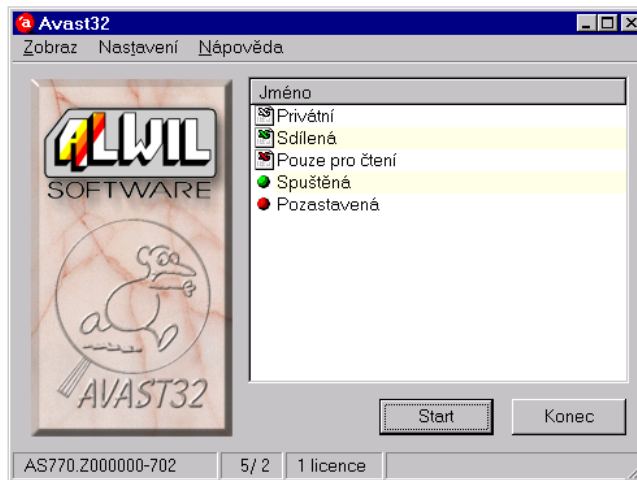
- informace o operačním systému, jeho verzi a o dostupné paměti,
- verze souboru VPS (databáze virů) a informace o jeho překladu.

Číslo verze programu AVAST32 a číslo jeho překladu je uvedeno i v první kolonce stavového řádku hlavního okna programu.

## 5.2 Jednoduché ovládání

Jednoduché ovládání ukazuje obr. 61. Obsahuje seznam dostupných úloh a několik ovládacích tlačítek.

Seznam dostupných úloh obsahuje úlohy, které může uživatel v danou chvíli použít. Vedle jména každé úlohy je ikona znázorňující jeho aktuální stav. Pokud úloha není spuštěna, znázorňuje ikona typ úlohy (na obr. 61 jsou to úlohy „Sdílená“, „Privátní“ a „Pouze pro čtení“). Je-li daná úloha spuštěna, je vedle jejího jména zelená kulička (na obr. 61 je to úloha „Spuštěná“). Jestliže je úloha pozastavena, má kulička barvu červenou (na obr. 61 je to úloha „Pozastavená“).



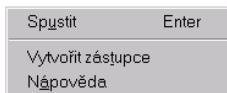
obr. 61

Levé tlačítko slouží ke spuštění nebo zastavení běhu úlohy. Jeho význam se mění vždy podle aktivní úlohy, tedy té úlohy, která je v seznamu dostupných úloh zvýrazněna. Jestliže aktivní úloha není spuštěna, má tlačítko jméno „Start“ a slouží ke spuštění úlohy. Je-li naopak úloha spuštěna, má tlačítko jméno „Stop“ a v tom případě slouží k jejímu ukončení.

Spustit nebo pozastavit (nikoli ukončit) lze úlohu také tak, že ji nejprve aktivujete a potom stisknete klávesu „Enter“ nebo pokleпáte levým tlačítkem myši na jejím jméně.



Tlačítkem „Konec“ ukončíte činnost programu AVAST32. Současně s ním budou ukončeny i všechny nerezidentní úlohy.



obr. 62

Místní nabídku, vyvolanou stiskem pravého tlačítka myši na jméně úlohy, ukazuje obr. 62. Její konkrétní obsah však záleží na aktuálním stavu úlohy. Zvolená funkce se bude provádět s úlohou, na jejímž jméně bylo právě tlačítko myši stisknuto.

Místní nabídka může obsahovat následující funkce:

- funkce „Spustit“ spustí provádění úlohy. Je přístupná pouze u úloh, které právě neběží,
- funkce „Ukončit“ ukončí provádění úlohy. Je přístupná pouze u běžících nebo pozastavených úloh,
- funkce „Pozastavit“ pozastaví úlohu. Je přístupná pouze u běžících úloh,
- funkce „Vytvořit zástupce“ vytvoří na pracovní ploše zástupce úlohy. Zástupce lze potom využít k přímému spouštění úlohy, bez nutnosti nejprve spustit program AVAST32. Funkce je v nabídce obsažena vždy,

- funkce „Nápověda“ vyvolá nápovědu programu AVAST32. K vyvolání nápovědy je též možné použít klávesu „F1“. Tato funkce je v nabídce vždy přítomna.

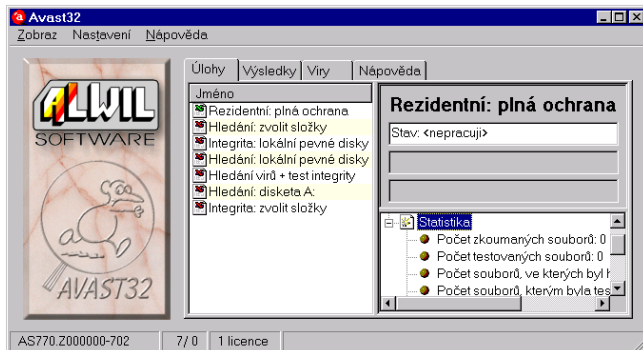
## 5.3 Rozšířené ovládání

Rozšířené ovládání obsahuje uživatelsky příjemné rozhraní pro přístup ke všem funkcím a nastavením, které program AVAST32 nabízí. Protože těchto funkcí a nastavení je příliš mnoho, je rozšířené ovládání organizováno do několika stránek. V následujících kapitolách si jednotlivé stránky podrobně popíšeme.

### 5.3.1 Stránka „Úlohy“

Stránka je rozdělena na dvě části (obr. 63). Levá část obsahuje seznam dostupných úloh, tak jak byl popsán u jednoduchého ovládání. Jeho použití i vlastnosti, až na místní nabídku, jsou naprosto shodné.

V pravé části stránky jsou umístěny informace o stavu aktivní úlohy, jejích vlastnostech a průběhu úlohy. Informace jsou uspořádány do stromové struktury.



obr. 63

Informace o stavu aktivní úlohy jsou umístěny v textových polích ve vrchní části. Prvním textovým polem je pole „Stav“, zobrazující aktuální stav úlohy. Možné stavy jsou tři: úloha není spuštěna („<nepracuji>“), úloha je spuštěna („Pracuji“) a nebo je úloha spuštěna, ale momentálně je její běh pozastaven („<pauza>“). Kompletní cestu k právě prohledávané složce ukazuje v pořadí druhé textové pole - „Složka“ a konečně poslední textové pole obsahuje jméno souboru, který je právě testován. Pokud je aktivní úloha rezidentní (viz kapitola 4.4.2), pak je zobrazena pouze informace o stavu úlohy.

Vlastnosti a statistiky o průběhu úlohy jsou uspořádány ve stromové struktuře, která se nachází pod zmíněnými textovými poli. K jednot-

livým údajům se dostanete „rozbalením“ příslušné položky. To provedete poklepáním levým tlačítkem myši na znaménko před jménem položky.

Informace o vlastníkově úlohy, činnostech vykonávaných během úlohy, datu vytvoření a posledního použití úlohy je uvedena v položce „Vlastnosti“. Je zde též informace o celkovém počtu spuštění úlohy od jejího vytvoření.

Poslední položkou je „Statistika“ (je rozbalena na obr. 63), která informuje uživatele o počtu nalezených souborů, testovaných souborů, souborů testovaných na přítomnost virů, souborů, u kterých byla testována jejich integrita, o počtu netestovaných souborů, infikovaných souborů a o počtu nalezených virů. Všechny položky se vztahují k aktivní úloze. Kontroluje-li aktivní úloha například pouze integritu dat, bude položka o počtu nalezených virů vždy nulová!

Jestliže aktivní úloha (tj. úloha, která je v seznamu úloh vybrána) právě běží, jsou informace v reálném čase aktualizovány a uživatel má tak přehled o jejím průběhu.

### Místní nabídka

Stejně jako jednoduché ovládání, tak i rozšířené ovládání obsahuje místní nabídku, která se zobrazí po stisku pravého tlačítka myši na jméno příslušné úlohy (obr. 64). Kromě funkcí na spuš-

tění, pozastavení a ukončení úlohy obsahuje níže popsané funkce.

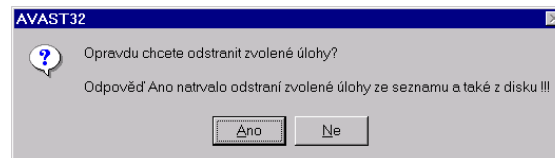


obr. 64

- funkce „Vytvořit novou ...“ slouží k vytváření nových úloh. Její podrobný popis je uveden v kapitole 4,
- funkcí „Vytvořit kopii“ lze vytvořit přesnou kopii dané úlohy. Nová úloha bude obsahovat naprosto shodné nastavení všech parametrů jako zvolená úloha. Jméno nové úlohy však bude ve tvaru „Kopie <jméno zvolené úlohy>“, Pokud chce uživatel vytvořit kopii ze sdílené úlohy a jsou-li sdílené úlohy chráněny jemu neznámým heslem, pak nově vytvořená úloha bude privátní. Veškeré ostatní nastavení zůstanou zachovány,
- funkce „Změnit ...“ umožňuje uživateli změnit nastavení parametrů úlohy. Změna úlohy probíhá v naprosto stejném prostředí jako vytváření úlohy.

váření úlohy. Proto vše, co bylo napsáno v kapitole 4 o vytváření nových úloh, platí i pro jejich změnu. Jestliže v okně změny ovládacích prvků úlohy stisknete tlačítko „OK“, a pokud provedené změny splňují podmínky uvedené v kapitole 4.5, bude změna úlohy provedena. Stisknete-li však tlačítko „Storno“, změna úlohy se neprovede a nastavení všech jejích parametrů zůstane nezměněno,

- funkce „Smazat“ slouží k odstranění příslušné úlohy ze seznamu úloh a zároveň i z pevného disku. Po jejím zvolení bude uživatel dotázán, zda to s odstraněním úlohy myslí opravdu vážně (obr. 65). Po stisku tlačítka „Ano“ bude zvolená úloha neobnovitelně odstraněna ze seznamu dostupných úloh a z pevného disku počítače,

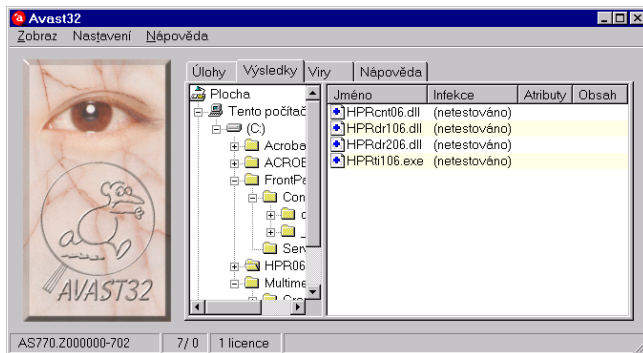


obr. 65

- funkce „Vytvořit zástupce“ vytvoří, stejně jako u jednoduchého ovládání, zástupce úlohy na pracovní ploše počítače. Tohoto zástupce lze

- potom využít k přímému spouštění úlohy bez nutnosti nejprve spustit program AVAST32,
- funkce „Nápověda“ zobrazí nápovědu programu AVAST32. Nápovědu je též možné zobrazit klávesou „F1“.

### 5.3.2 Stránka „Výsledky“



obr. 66

Stránka „Výsledky“ obsahuje výsledky všech úloh, které obsahovaly činnosti hledání známých virů nebo testování integrity dat (obr. 66). Ovládání této stránky je velmi podobné ovládání programu „Průzkumník“. Tato kapitola popisuje pouze ovládání a význam jednotlivých skutečností, které stránka „Výsledky“ obsahuje. Interpretaci těchto skutečností se zabývá až [kapitola 7](#).

Výsledky úloh jsou shrnuty do jediného stromu složek, díky čemuž má uživatel přehled o výsledcích všech úloh, které byly provedeny od spuštění programu. Do stromu složek program AVAST32 však zařadí pouze soubory, které vykazují známky infekce virem nebo byly od minulé kontroly nějakým způsobem změněny. Jinými slovy, zde budou všechny podezřelé soubory.

Zařazeny sem budou také soubory nové, přesněji řečeno ty, které program AVAST32 nenašel ve své interní databázi souborů, a najdete zde i jména souborů, které byly smazány či přesunuty. S boot sektory disků a s pamětí se zachází jako se soubory, takže v případě jejich změny budou do stromové struktury zařazeny také. Budou zařazeny přímo do složky „Tento počítač“.

Podezřelé soubory jsou do stromové struktury zařazeny podle své skutečné cesty. Pokud tedy strom obsahuje nějakou složku, zcela určitě tato složka (nebo některá její vnořená složka) obsahuje podezřelý soubor. Chcete-li tedy zjistit obsah některé ze složek, aktivujte ji a v pravé části stránky se objeví podezřelé soubory (pokud zde nějaké jsou). Před jménem každého souboru může být ikona znázorňující akci, která byla se souborem provedena.



obr. 67

Je-li zde modré znaménko plus (obr. 67) znamená to, že soubor je nový, tedy přibyl zde od poslední kontroly. Jestliže jste test integrity dat spustili poprvé, budou jako nové označeny všechny nalezené soubory, protože interní databáze souborů je doposud prázdná a je potřeba ji teprve naplnit.



obr. 68

Zelené znaménko mínus (obr. 68) signalizuje, že zde soubor daného jména naopak chybí. Je dobré si uvědomit, co jste s počítačem dělali. Pokud jste například od minulé kontroly vysypávali koš, je samozřejmé, že program ohlásí chybějící soubory na příslušném disku ve složce „RECYCLED“, stejně tak budete pravděpodobně informováni o zmizení dočasných souborů apod.



obr. 69

Další znak, který se může objevit u jména souboru, je červený vykřičník (obr. 69). AVAST32 tak dává najevo, že je soubor nakažen, nebo že při práci se souborem došlo k nějaké chybě.

Je-li soubor nakažen, je ve sloupci „Infekce“ uvedeno jméno viru. Jestliže je sloupec prázdný, pak při práci se souborem došlo k chybě. Ta mohla nastat z různých důvodů, nejčastěji však zřejmě půjde o chybu sdílení souboru, tzn. že soubor je používán jinou aplikací.



obr. 70

Pokud jste provedli opravu OLE dokumentu (viz dále), může se objevit vedle jména opraveného souboru žlutý otazník (obr. 70). AVAST32 tak signalizuje, že po provedení operace opravení, resp. odstranění makroviru ze souboru, je jeho stav neznámý. Potřebujete-li zjistit, zda se stav takto označeného souboru odlišuje od stavu, který je uložen v databázi, proveďte test integrity souboru znovu.

Zelená kulička (obr. 18) se může objevit, podobně jako otazník, u souborů, které byly opraveny. Na rozdíl od otazníku se však objeví pouze u souborů, které nejsou OLE dokumenty a jejich oprava proběhla úspěšně. Takto označené soubory

se tedy nachází ve stavu, jaký je zaznamenán v databázi souborů.



obr. 71

Jestliže u souboru je ikona z obr. 71, byl soubor nějakým způsobem změněn. Přesnější informace o změně souboru jsou uvedeny ve sloupcích za jeho jménem, které jsou popsány v následujících odstavcích:

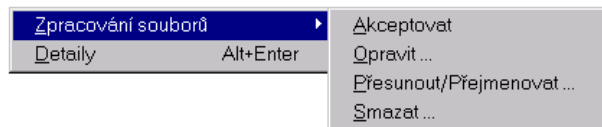
- sloupec „Infekce“ obsahuje jméno viru, kterým je soubor pravděpodobně nakažen. Sloupec má však význam pouze ve chvíli, jestliže byl daný soubor na přítomnost viru testován. Pokud ano a sloupec je prázdný, nebyl v daném souboru žádný ze známých virů nalezen. Obsahuje-li však sloupec jméno viru, je soubor s největší pravděpodobností nakažen! Jestliže soubor nebyl testován, obsahuje sloupec text „(netestováno)“,
- sloupec „Atributy“ informuje uživatele o změně atributů a o změně data a času posledního zápisu do souboru. Pod operačním systémem Windows NT bude sloupec také indikovat změnu zabezpečovacích informací souboru. Pokud byla u souboru testována integrita, a sloupec je prázdný, pak uvedené parametry

příslušného souboru nebyly od poslední kontroly změněny. V opačném případě sloupec obsahuje „!!!“ (tři vykřičníky),

- sloupec „Obsah“ oznamuje uživateli, že byl změněn obsah, popř. velikost souboru. Pokud je sloupec prázdný a u souboru byla testována integrita dat, obsah souboru nedoznal od poslední kontroly žádných změn. Jinak sloupec obsahuje „!!!“ (tři vykřičníky).

Znovu upozorňujeme, že pokud je sloupec „Infekce“ prázdný, nemusí to znamenat, že soubor není infikován. Pokud byl daný soubor testován na přítomnost viru a sloupec je prázdný, pak to znamená, že v souboru nebyl při daném nastavení programu objeven žádný známý virus!

### Místní nabídka



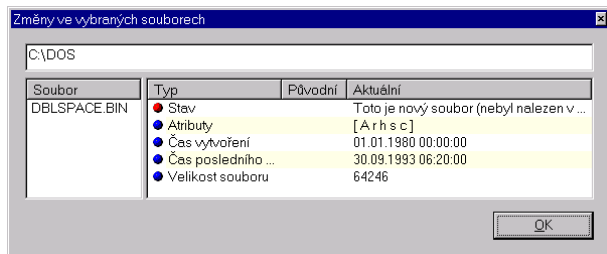
obr. 72

Místní nabídka (obr. 72) se vztahuje vždy k souborům, které byly označeny. Stejná nabídka je použita i pro složky v levé části stránky. Funkce zvolená pro příslušnou složku se provede se všemi

soubory, které obsahuje, i se soubory ve všech vnořených složkách.

Funkce „Detaily“ slouží k zobrazení dialogu s přesnějšími informacemi o charakteru změny souboru (obr. 73). Jsou zde uvedeny informace o zvoleném souboru, jako jeho stav, atributy, datum vytvoření a poslední modifikace a samozřejmě i délka souboru, příp. i jméno viru, který soubor napadl. To vše je zobrazeno pro původní stav souboru (je uložen v interní databázi) i pro aktuální stav souboru, v jakém se nachází na disku.

Pro zobrazení dialogu lze také použít klávesovou zkratku „Alt + Enter“.



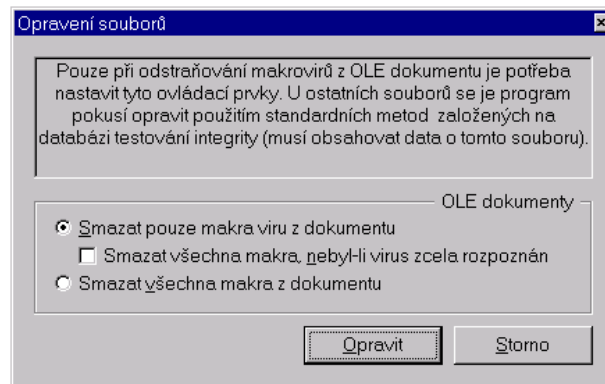
obr. 73

Místní nabídka obsahuje složku „Zpracování souboru“, která obsahuje funkce pro práci s podezřelými soubory:

### Akceptování souborů

Funkce „Akceptovat“ sdělí programu AVAST32, že o změnách v souborech víte a že je již nemá hlásit. Takto ošetřené soubory zmizí ze seznamu podezřelých souborů a pokud by složka, ve které byly umístěny, zůstala prázdná, potom zmizí i ona. Funkce vlastně zapíše aktuální stav souborů do interní databáze, takže při další kontrole se bude jevit jako výchozí.

### Opravení souborů



obr. 74

Funkce „Opravit ...“ se pokusí vrátit označené soubory do původního stavu. Po jejím zvolení se objeví dialog, který je vidět na obr. 74. Jestliže je

opravovaným souborem OLE dokument, má uživatel možnost nastavit některé parametry. V opačném případě nemá jejich nastavení smysl a budou ignorovány.

Přepínačem „Smazat pouze makra viru z dokumentu“ je možné nastavit, aby z dokumentu byla odstraněna pouze makra, ve kterých byl nalezen virus. Ostatní makra zůstanou nedotčena.

Přepínač „Smazat všechna makra z dokumentu“ způsobí, že z OLE dokumentu budou odstraněna všechna makra, ať už virus obsahují či nikoliv.

Implicitně je nastaveno odstranění pouze maker obsahujících virus.

Zaškrtnutím pole „Smazat všechna makra, nebyl-li virus zcela rozpoznán“ sdělíte programu, že pokud virus nebyl rozpoznán zcela přesně (u některých makrovirů je detekce velmi obtížná), mají být z dokumentu odstraněna všechna makra.

Má-li být opraven soubor, který neobsahuje OLE dokument, pokusí se program AVAST32 soubor opravit metodou založenou na testování integrity dat. Program AVAST32 si totiž udržuje interní databázi souborů, do které si zaznamenává důležité informace o stavu jednotlivých souborů a pomocí kontrolních součtů i o jejich obsahu. S využitím těchto informací se AVAST32 pokusí obnovit zvolený soubor. Opravit lze až devadesát pět procent infikovaných souborů. Zda byl soubor

obnoven, dokáže AVAST32 určit se stoprocentní přesností.

Z předchozího textu vyplývá, že pokud budete chtít soubory úspěšně obnovit, budete potřebovat pravidelně aktualizovanou databázi souborů na Vašich discích. Tuto databázi je nutné udržovat, jinými slovy je potřeba průběžně provádět kontrolu integrity dat a legální změny souborů zapisovat do interní databáze funkcí „Akceptovat“.

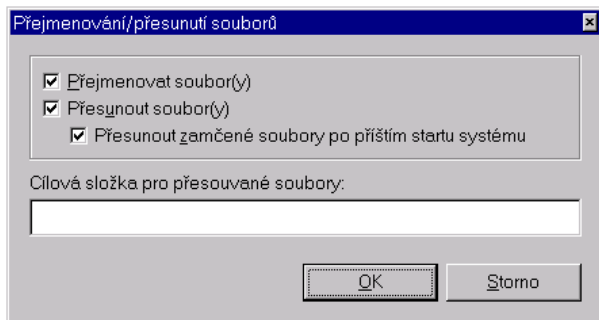
Algoritmy pro obnovování souborů použité v programu AVAST32 jsou určeny výhradně pro obnovu souborů napadených nějakým virem. Pro obnovení přepsaných nebo editovaných souborů je tedy nelze použít. Nastavení ovládacích prvků dialogu se pro soubory neobsahující OLE dokumenty ignoruje.

Stiskem tlačítka „Opravit“ se spustí vlastní proces opravy souboru. Tlačítkem „Storno“ zavřete dialog a s označenými soubory nebude manipulováno.

### **Přejmenování a přesunutí souborů**

Funkce „Přesunout/Přejmenovat ...“ umožňuje podezřelé soubory přesunout do jiné složky nebo je přejmenovat. Funkce zobrazí dialog, který je vidět na obr. 75.





obr. 75

Zaškrťací pole „Přejmenovat soubory“ umožňuje u označených souborů změnit jejich příponu. Takto přejmenované soubory budou odlišeny od ostatních a u spustitelných souborů se tak předejde i jejich nechtěnému spuštění. To by v případě, že soubor obsahuje virus, vedlo k nakažení počítače (pokud již k němu nedošlo). U souboru bude stávající přípona nahrazena přednastavenou příponou (viz [kapitola 6.1.3](#)). Vlastní jméno souboru zůstane nedotčeno.

Najde-li program během přejmenovávání nějaký neznámý typ souboru, zeptá se uživatele, jak má být pozměněna přípona nalezeného souboru. Zapsanou příponu si program zapamatuje, a až příště nalezne soubor stejného typu, tak tuto příponu automaticky použije.

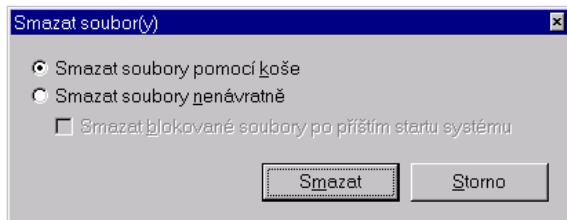
Zaškrtnutím pole „Přesunout soubory“ zapnete přesunutí označených souborů do zvolené složky. Jméno složky, do které se budou označené soubory přesouvat, a cesta k ní se zapíše do textového pole „Cílová složka pro přesouvané soubory:“.

Jestliže je zapnuto přesouvání souborů, je možné zaškrtnutím pole „Přesunout zamčené soubory po příštím startu systému“ určit, že pokud se souborem nelze v danou chvíli manipulovat (např. je využíván jinou aplikací), je možné jeho přesunutí odložit do příštího startu operačního systému. Nemůže sa Vám tak stát, že byste daný soubor zapomněli přesunout - program se o vše postará sám.

Implicitně je zapnuto jak přejmenování souborů, tak i jejich přesun včetně možnosti odložit jejich přesun až do příštího startu operačního systému.

### Smazání souborů

Poslední funkcí ve složce „Zpracování souboru“ je funkce „Smazat ...“. Po jejím zvolení se zobrazí dialog, ve kterém si uživatel může vybrat způsob smazání souborů (obr. 76).



obr. 76

Zvolením přepínače „Smazat soubory pomocí koše“ určíte, že označené soubory budou smazány přemístěním do odpadkového koše. Smazané soubory se tak dají kdykoli bez problémů obnovit a z tohoto důvodu tento způsob doporučujeme zejména méně zkušeným uživatelům osobních počítačů.

Jestliže používáte operační systém Windows NT verze 3.51 pak tento přepínač bude pro Vás nedostupný. Potom musíte použít následující způsob.

Přepínač „Smazat soubory nenávratně“ zapne přímé odstranění souborů z disku, bez možnosti jejich obnovení.

Je-li přepínač zvolen, můžete zaškrtnutím polem „Smazat blokováné soubory po příštím startu systému“ určit, že pokud se souborem nelze právě manipulovat (např. je využíván jinou aplikací), je možné jeho smazání odložit do příštího startu

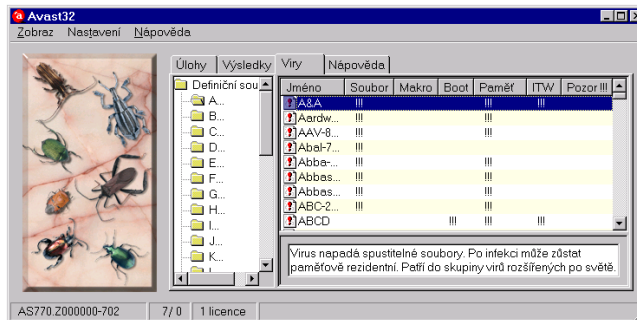
operačního systému. Pole není implicitně zaškrtnuto.

Implicitně je zvolen přepínač „Smazat soubory pomocí koše“.

Po stisku tlačítka „Smazat“ se provede smazání všech označených souborů zvoleným způsobem. Tlačítko „Storno“ dialog zavře.

### 5.3.3 Stránka „Viry“

Pokud Vás zajímají bližší informace o všech virech, které program AVAST32 v současné době zná, klepněte na „ouško“ stránky „Viry“. Na této stránce máte k dispozici kompletní, abecedně seřazený seznam všech základních typů virů (obr. 77).



obr. 77

Podobně jako všechny ostatní stránky, je i tato rozdělena na dvě části. Vlevo má uživatel možnost zvolit si počáteční písmeno nebo číslici jména viru, o kterém se chce dozvědět podrobnější informace. Viry, jejichž jména začínají zvoleným znakem, se objeví spolu se svou charakteristikou v pravé části stránky.

Viry se mohou šířit v zásadě těmito způsoby: jako součást nějakého spustitelného souboru, jako makro určitého dokumentu (tzv. makroviry), nebo přepsáním tzv. boot sektoru (sektor, který je načítán při inicializaci systému) nějakého disku.

Všem výše uvedeným způsobům odpovídají první tři sloupce, uvedené za jménem viru. Jestliže tedy nějaký sloupec u příslušného viru obsahuje „!!!“ (tři vykřičníky) znamená to, že tento virus napadá počítačový systém daným způsobem.

Sloupec „Paměť“ říká, může-li být virus dlouhodobě přítomný v operační paměti nakaženého počítače (říkáme, že je rezidentní). Další sloupec obsahuje informaci, zda je virus na seznamu ITW, což je seznam nejrozšířenějších virů. Poslední sloupec, označený „Pozor !!!“, informuje o nebezpečnosti viru. Pokud u viru naleznete označení „!!!“ (tři vykřičníky), je lépe si s ním nezahrávat. Takto označené viry jdou totiž zpravidla z počítače velmi těžko odstranit nebo mohou napáchat škody na Vašich datech. Odstranění tako-

vých virů by měl provádět někdo opravdu zkušený!

Označíte-li nějaký virus v seznamu na pravé části stránky „Viry“, objeví se v textovém poli ve spodní části jeho stručná charakteristika. Jedná se vlastně o srozumitelné vypsání obsahu jednotlivých sloupců tak, jak jsme si je popsali.

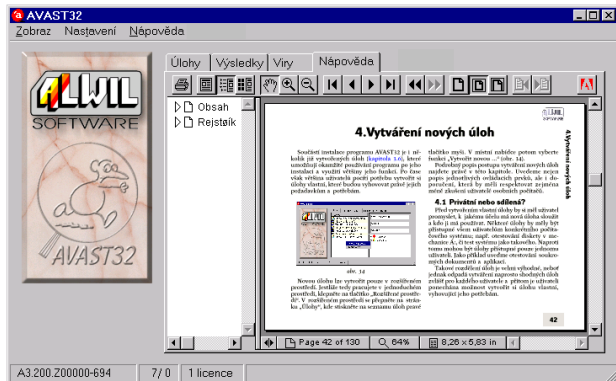
Levá část stránky „Viry“ obsahuje kromě písmen abecedy, číslic a ostatních znaků také dvě speciální položky. Položkou „ITW“ lze v pravé části stránky zobrazit seznam všech virů z aktuálního souboru VPS, které jsou na seznamu ITW. Podobně pracuje i položka „Pozor !!!“ s tím, že v seznamu na pravé části stránky se objeví zvlášť nebezpečné viry. Viry budou v obou případech abecedně seřazeny.

Protože pro vytvoření seznamu pro výše zmíněné dvě položky je potřeba prohledat celý soubor VPS, může jejich zobrazení nějakou chvíli trvat.

Podrobnější popis všech známých virů, jejich činnosti a zvláštností není k dispozici. Není únosné ani účelné zjišťovat veškeré podrobnosti o každém viru hlavně z důvodu jejich obrovského množství. Případní zájemci o podrobnější informace o určitém viru nechtě se obrátit na pracovníky naší firmy, kteří jim požadované informace rádi poskytnou.

### 5.3.4 Stránka „Nápověda“

Stránka „Nápověda“ (obr. 78) slouží uživateli jako útočiště před případnými problémy při práci s programem. Obsahuje totiž nápovědu programu AVAST32.

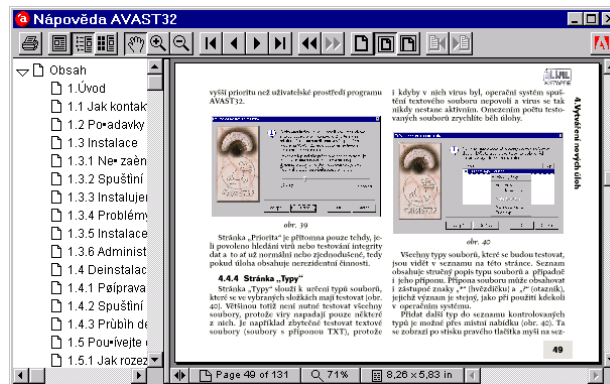


obr. 78

Při jakýchkoli problémech s programem prosíme, abyste nejprve nahlédli do nápovědy programu AVAST32 a pokud zde nenajdete to, co hledáte, teprve potom kontaktovali naši technickou podporu.

Jestliže na Vašem počítači není nainstalován program Acrobat Reader, nebude možné nápovědu programu AVAST32 zobrazit. V takovém

případě musíte AVAST32 ukončit, program Acrobat Reader nainstalovat (viz kapitola 1.3.1) a potom AVAST32 znovu spustit.



obr. 79

Nápověda programu AVAST32 může být buďto součástí stránky „Nápověda“, tak jak ukazuje obr. 78 nebo může být „plovoucí“. Pod pojmem plovoucí nápověda se skrývá okno s nápovědou, volně pohyblivé po pracovní ploše (obr. 79). Nápověda není tedy vázána na stránku „Nápověda“, ale je možné ji umístit kamkoli a mít ji tak neustále k dispozici.

Plovoucí nápovědu lze vyvolat kdykoli během činnosti programu AVAST32 a to buďto z místní nabídky, a nebo způsobem běžným v prostředí

operačních systémů Windows 95 a NT, tedy stiskem klávesy „F1“. Zavřete ji potom klávesou „Esc“.

Je-li zobrazena plovoucí nápověda, stránka „Nápověda“ již nápovědu neobsahuje. Jinak řečeno, lze mít zobrazenou vždy pouze jednu nápovědu.

Ať už je nápověda umístěná na uvedené stránce a nebo je plovoucí, ovládání je vždy stejné, protože k zobrazení nápovědy je v obou případech použit oblíbený program Acrobat Reader. Je však použit takovým způsobem, že se jeví jako nedělitelná součást programu AVAST32.

V následujících odstavcích si popíšeme ovládání nápovědy.



Tlačítko slouží k vytištění nápovědy nebo její části. Po jeho stisku se objeví dialog, který umožňuje nastavit parametry, kvalitu a rozsah tisku.

Následující tři tlačítka určují možnosti procházení nápovědou:



Je-li stisknuto toto tlačítko, bude okno s nápovědou obsahovat pouze část zobrazující vlastní nápovědu. Část usnadňující pohyb v nápovědě nebude zobrazena.



Je-li stisknuto toto tlačítko, bude okno s nápovědou obsahovat vedle části zobrazující nápovědu i část, ve které bude zobrazen obsah nápovědy (obr. 79). Stiskem levého tlačítka myši na položce obsahu se



lze přesunout na příslušnou část nápovědy.

Tlačítko zapíná zobrazení jednotlivých očíslovaných stránek vedle vlastní nápovědy. Stiskem levého tlačítka myši na příslušné stránce se lze přesunout na stránku s příslušným číslem.

Následující tři tlačítka určují způsob práce s nápovědou (ukazovátka myši bude mít podobu, kterou ukazuje zvolené tlačítko):



Jestliže je stisknuto toto tlačítko, potom po klepnutí levým tlačítkem myši nad nápovědou je možné s právě zobrazenou stránkou nápovědy libovolně pohybovat a zobrazit tu její část, kterou uživatel potřebuje vidět.







Je-li stisknuto toto tlačítko, provede se po stisku levého tlačítka myši nad nápovědou dvojnásobné zvětšení dané části nápovědy.





Je-li stisknuto toto tlačítko, pak po stisku levého tlačítka myši nad nápovědou se dokument dvojnásobně zmenší, tzn. že bude vidět jeho větší část, ale s menšími detaily.


Následující čtyři tlačítka slouží pro pohyb v nápovědě (ostatní parametry, jako např. lupa, zůstanou nezměněny):

-  Tlačítko slouží pro přesun na první stránku nápovědy.
-  Stiskem tohoto tlačítka se lze přesunout na předcházející stránku nápovědy.
-  Tímto tlačítkem se přesunete na následující stránku nápovědy.
-  Po stisku tohoto tlačítka bude zobrazena poslední stránka nápovědy.


Další dvě tlačítka umožňují procházet dosud provedenými kroky:


-  Tlačítko zruší posledně provedený příkaz, tzn. vrátí okno s nápovědou do stavu, v jakém se nacházelo před jeho provedením. Takto se např. lze vracet na všechny dosud shlédnuté stránky nápovědy.
-  Pokud jste se předchozím tlačítkem vrátili o jeden krok zpět, lze se tímto tlačítkem naopak posunout o jeden krok dopředu. Jinými slovy provedete tutéž operaci, kterou jste předchozím tlačítkem odvolali. Tlačítko lze použít, pokud po stisku předchozího tlačítka nebyla provedena žádná operace.

Následující tři tlačítka slouží k rychlému nastavení lupy podle zobrazené stránky:

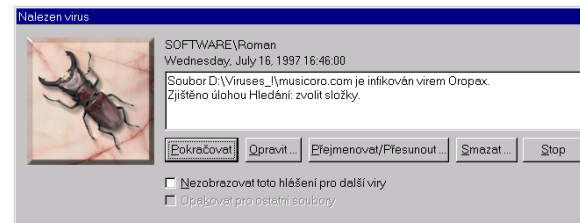
-  Tlačítko nastaví zobrazení stránky v její skutečné velikosti, tzn. že nastaví hodnotu lupy na sto procent. Je možné, že zobrazená stránka bude větší nebo

naopak menší než je část okna vyhrazená pro její zobrazení.

-  Po stisku tohoto tlačítka bude nastavena velikost lupy na takovou hodnotu, aby byla vidět vždy kompletní stránka nápovědy. Při změně rozměru okna se změní i velikost stránky.

-  Tímto tlačítkem nastavíte hodnotu lupy na takovou hodnotu, aby šířka stránky odpovídala šířce okna s nápovědou. Na výšku stránky nebude brán zřetel. Při změně šířky okna se změní i šířka zobrazení stránky.

## 5.4 Hlášení o nalezení viru



obr. 80

Jestliže byl během provádění úlohy objeven nějaký virus, zobrazí program AVAST32 varovné hlášení (obr. 80). Text uvedený v tomto hlášení

záleží na nastavení úlohy, která virus objevila (viz [kapitola 4.4.12](#)).

Tlačítkem „Pokračovat“ sdělíte programu, že má v dané úloze pokračovat. Infikovaný soubor lze ošetřit později na stránce „Výsledky“ ([kapitola 5.3.2](#)).

Tlačítko „Opravit ...“ slouží k okamžité opravě nakaženého souboru. Bude vyvolán naprosto stejný dialog jako v případě funkce „Opravit ...“ v místní nabídce na stránce „Výsledky“ rozšířeného ovládacího programu. Podrobný popis dialogu je uveden v [kapitole 5.3.2](#). Po opravě souboru se bude pokračovat v provádění úlohy.

Tlačítko „Přesunout/Přejmenovat“ umožňuje uživateli nakažený soubor přesunout do jiné složky a/nebo změnit jeho příponu. Podrobný popis je uveden u stejnojmenné funkce v [kapitole 5.3.2](#). Po přesunutí a přejmenování souboru bude úloha pokračovat.

Tlačítko „Smazat ...“ slouží ke smazání nakaženého souboru z disku. Podrobný popis dialogu, který se objeví je uveden u funkce „Smazat ...“ v [kapitole 5.3.2](#). Po jeho zavření se bude pokračovat v provádění úlohy, která virus objevila.

Tlačítkem „Stop“ ukončíte běh úlohy, která virus objevila.

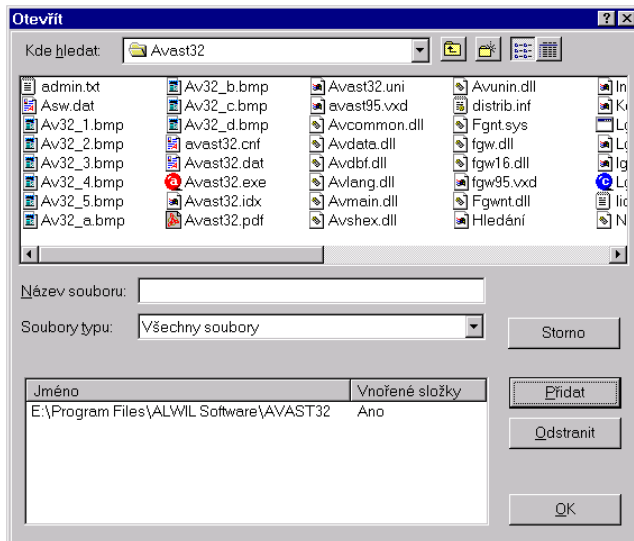
Hlášení o nalezení viru obsahuje i dva ovládací prvky.

Zaškrtnutím pole „Nehlásit další nalezené viry“ sdělíte programu, že pokud během provádění aktuální úlohy najde další virus, nemá již varovné hlášení zobrazovat. Implicitně není pole zaškrtnuto.

Zaškrtnutím pole „Opakovat pro ostatní soubory“ říkáte programu, že pokud najde další nakažený soubor, má s ním provést naprosto stejnou operaci, jaká bude provedena s tímto souborem. Pole je přístupné pouze tehdy, jestliže je pole „Nehlásit další nalezené viry“ zaškrtnuto. Tato možnost není implicitně povolena.

## 5.5 Vybrání testovaných oblastí

Program AVAST32 potřebuje na několika místech určit, které oblasti, tedy soubory, složky, popř. celé disky, mají být zkontrolovány. Proto obsahuje dialog, který tuto činnost ulehčuje (obr. 81). Umožňuje vybrat i více složek či disků naráz, čímž velmi usnadňuje práci s programem.



obr. 81

Vrchní část dialogu je prakticky stejná jako u standardního dialogu na otevírání souborů, který je součástí operačního systému. Zde uživatel běžným způsobem zvolí potřebný soubor, složku, popř. celý disk, který chce vybrat, a stiskem tlačítka „Přidat“ zvolenou položku přidá do seznamu ve spodní části dialogu. Takto uživatel bude postupovat do té doby, než bude seznam obsahovat všechny oblasti, které je potřeba zkontrolovat.

Jestliže jste se při výběru zmýlili, nebo prostě již některou z vybraných oblastí kontrolovat nechcete, pak ji jednoduše ze seznamu odstraňte. To provedete tak, že jí nejprve vyberete a stiskem tlačítka „Odstranit“ ji odstraníte ze seznamu vybraných oblastí. S oblastí odstraněnou ze seznamu pak příslušná operace prováděna nebude.

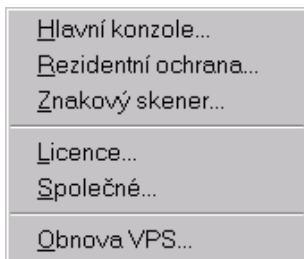
Vedle jména oblasti je napsáno, zda se mají testovat i její složky. Chcete-li toto nastavení změnit, poklepejte levým tlačítkem myši na jméno oblasti. Test podsložek je u nově přidávaných oblastí implicitně povolen.

Pokud jste vybrali všechny požadované oblasti, stiskem tlačítka „OK“ spustíte provádění příslušné operace. Stisknete-li tlačítko „Storno“ (nebo dialog zavřete jiným způsobem), pak se provedení zvolené operace zruší a vybrané soubory budou ignorovány.



## 6. Nastavení programu

Nabídka „Nastavení“ (obr. 82) slouží k přizpůsobení funkcí a vlastností programu AVAST32.



obr. 82

Po zvolení jakékoli položky se objeví dialog, ve kterém lze příslušné ovládací prvky nastavit dle potřeby. Všechny dialogy jsou, podobně jako hlavní okno programu AVAST32, rozděleny do několika stránek, mezi kterými je možné přepínat pomocí záložkového seznamu.

Stránky jsou označeny kuličkami různé barvy. Má-li kulička barvu modrou, jsou ovládací prvky na příslušné stránce určeny i pro běžného uživatele - jejich nastavení nemá zásadní vliv na činnost a funkčnost programu. Je-li však kulička červená, ovládací prvky by měl měnit pouze zku-

šený uživatel, který přesně ví, co danou změnou způsobí. Stránky, označené červenou kuličkou jsou proto dosažitelné pouze pro uživatele s právy administrátora - ostatním uživatelům se jednoduše nezobrazí.

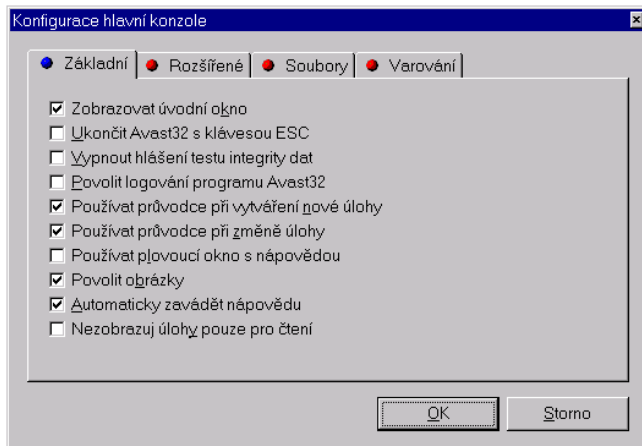
V následujících kapitolách si podrobně popíšeme jednotlivé položky nabídky „Nastavení“ hlavního okna.

### 6.1 Položka „Hlavní konzole ...“

Dialog, který se objeví po zvolení po vybrání této položky, obsahuje na několika stránkách ovládací prvky pro nastavení programu AVAST32 a jeho prostředí.

#### 6.1.1 Stránka „Základní“

Stránka „Základní“ umožňuje uživateli přizpůsobit si chování programu jeho potřebám (obr. 83). Všechny ovládací prvky na této stránce se uchovávají zvlášť pro každého uživatele, což umožňuje individuální nastavení chování programu AVAST32. Jejich změna se projeví až po dalším spuštění programu.



obr. 83

Zaškrtnutím pole „Zobrazovat úvodní okno“ zapnete zobrazování loga programu AVAST32 při jeho spuštění. Pokud Vás logo ruší, či chcete mírně zrychlit start programu, potom pole nezaškrtněte. Implicitně je pole zaškrtnuto.

Zaškrtnutím pole „Ukončit Avast32 s klávesou ESC“ určuje, zda je možné ukončit program AVAST32 stiskem klávesy „Esc“. To je výhodné zejména pro zkušenější uživatele, kteří programy raději ovládají pomocí klávesových zkratk. Běžný uživatel by pole zřejmě zatrhávat neměl, aby tak předešel nechtěnému ukončení programu. Implicitně není pole zaškrtnuto.

Zaškrtnutím pole „Vypnout hlášení testu integrity dat“ vypíná zobrazování hlášení o dokončení testu integrity dat (obr. 20). Nezáleží přitom, jestli se jedná o normální nebo zjednodušený test.

Zpráva bude zobrazena pouze tehdy, byl-li nějaký z testovaných souborů změněn. Obsahuje i dotaz, zda si uživatel přeje zobrazit výsledky úlohy. Po kladné odpovědi, tedy po stisku tlačítka „Ano“, se aktivuje stránka „Výsledky“ rozšířeného ovládání (pracujete-li v jednoduchém ovládání, pak se program automaticky přepne do rozšířeného ovládání). Implicitně je zobrazování hlášení povoleno.

Zaškrtnutím pole „Povolit logování programu Avast32“ zapíná tzv. logování. Ve Windows 95 logování spočívá v tom, že se ve složce programu AVAST32 vytvoří textový soubor s názvem „AVAST32.log“, do kterého se budou zapisovat všechny programem prováděné činnosti. Dále do něj budou zapisovány informace o nalezených virech, uživatelích pracujících s programem apod. Velikost logovacího souboru je dána hodnotou zapsanou na stránce „Soubory“ (kapitola 6.1.3) do textového pole „Velikost log. souboru“. Implicitně je logování vypnuto.

Pod operačním systémem Windows NT se program pokusí zapisovat logovací informace do systémového logovacího souboru. Ten je možné si prohlédnout pomocí programu „Prohlížeč

událostí", který lze spustit vybráním stejnojmenné položky ze složky „Programy/Administrátorské nástroje“. Jestliže z jakéhokoli důvodu nemůže logovací informace do zmíněného souboru zapsat, bude postupovat jako v případě Windows 95.

Používání logování je vhodné zejména v síťovém prostředí, kde tak lze kontrolovat činnost jednotlivých uživatelů.

Zaškrťovací pole „Používat průvodce při vytváření nové úlohy“ aktivuje tzv. „průvodce“, který Vás bude provázet tvorbou nové úlohy (viz [kapitola 4](#)). Doporučujeme zaškrťávat toto pole, zejména pak začínajícím uživatelům. Implicitně je pole zaškrtnuto.

Zaškrťovací pole „Používat průvodce při změně úlohy“ aktivuje, podobně jako pole předcházející, průvodce, tentokrát však pro použití při změně existujících úloh (viz [kapitola 4](#)). Implicitně je používání průvodce nastaveno.

Zaškrťovacím polem „Používat plovoucí okno s nápovědou“ lze nastavit, aby nápověda programu AVAST32 mohla mít libovolnou pozici na obrazovce a nebyla tedy vázána na stránku „Nápověda“ ([kapitola 5.3.4](#)). Implicitně není pole zaškrtnuto.

Zaškrťovací pole „Povolit obrázky“ zapne zobrazování obrázků v hlavním okně programu AVAST32. Obrázky ilustrují prováděnou činnost a zpřijemňují práci s programem. Jejich používá-

ní však vyžaduje operační paměť počítače, a proto máte-li jí nedostatek, nebo obrázky prostě nechcete, pole nezaškrťávejte. Implicitně je používání obrázků povoleno.

Zaškrťovací pole má vliv pouze na program AVAST32 - obrázky z dialogů programů WARN32 a QUICK32 odstraněny nebudou.

Zaškrťovací pole „Automaticky zavádět nápovědu“ slouží k tomu, aby soubor s nápovědou programu AVAST32 byl po jeho startu automaticky zaveden a při každém vyvolání nápovědy nebylo potřeba jej znovu zavádět z disku. Jestliže pole není zaškrtnuto, bude se soubor s nápovědou zavádět až na žádost uživatele, tedy po zaškrtnutí příslušné položky nabídky nebo po stisku klávesy „F1“. Implicitně je pole zaškrtnuto.

Pokud máte dostatek operační paměti a často nahlížíte do nápovědy, doporučujeme Vám pole zaškrtnout. Urychlíte tak zobrazování nápovědy.

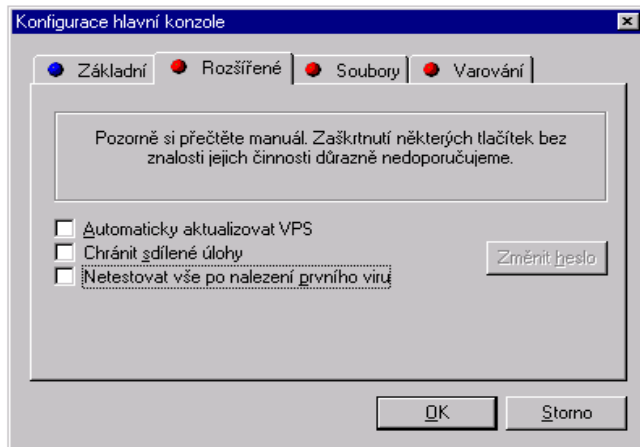
Zaškrtnutím pole „Nezobrazuj úlohy pouze pro čtení“ způsobíte, že v seznamu úloh (a to ať již rozšířeného nebo jednoduchého ovládní) nebudou zobrazeny úlohy pouze pro čtení - většinou se jedná o úlohy dodávané s programem. Implicitně není pole zaškrtnuto.

### **6.1.2 Stránka „Rozšířené“**

Ovládací prvky na stránce „Rozšířené“ ukazuje obr. 84. Jejich změna ovlivní všechny uživatele

pracující s programem, protože nastavení těchto ovládacích prvků se ukládá pro program AVAST32 jako celek.

Změna ovládacích prvků se projeví až po dalším spuštění programu.

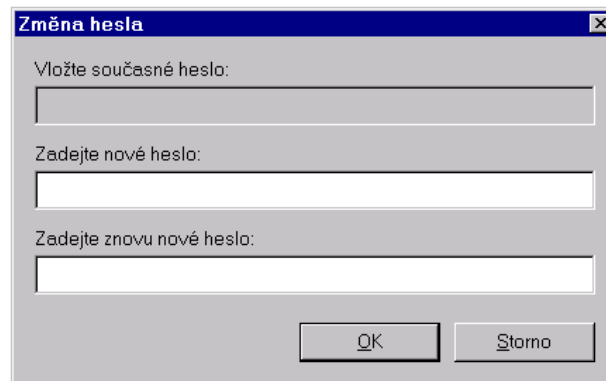


obr. 84

Zaškrtnuté pole „Automaticky aktualizovat VPS“ slouží k povolení automatické aktualizace souboru VPS, který obsahuje databázi známých virů. Je-li pole zaškrtnuto, program AVAST32 po svém startu automaticky prohledá nastavenou složku (kapitola 6.6, textové pole „Cesta pro aktualizaci“). Najde-li novější soubor VPS než je stáva-

ající, bude stávající soubor VPS automaticky nahrazen novějším. V opačném případě se se stávajícím souborem VPS nebude nic dělat.

Implicitně není automatická aktualizace souboru VPS povolena.

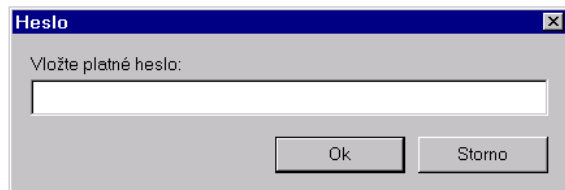


obr. 85

Zaškrtnuté pole „Chránit sdílené úlohy“ umožňuje chránit sdílené úlohy před změnou heslem. Po jeho zaškrtnutí se objeví dialog umožňující zadání hesla (obr. 85). Heslo je potřeba zapsat dvakrát a to nejprve do textového pole „Zadejte nové heslo“ a pro kontrolu i do textového pole „Zadejte znovu nové heslo“. Jestliže bylo heslo do obou polí zapsáno shodně, bude použito. V opačném případě budete upozorněni a bude

Vám dána možnost heslo zapsat znovu. Zaškrtnutí pole lze zrušit pouze se znalostí právě platného hesla.

Pokud jsou sdílené úlohy chráněny heslem, pak bez jeho znalosti nebudou kromě operací spuštění, pozastavení, ukončení úlohy, vytvoření privátní kopie a vytvoření jejího zástupce na ploše, povoleny žádné další operace se sdílenými úlohami.



obr. 86

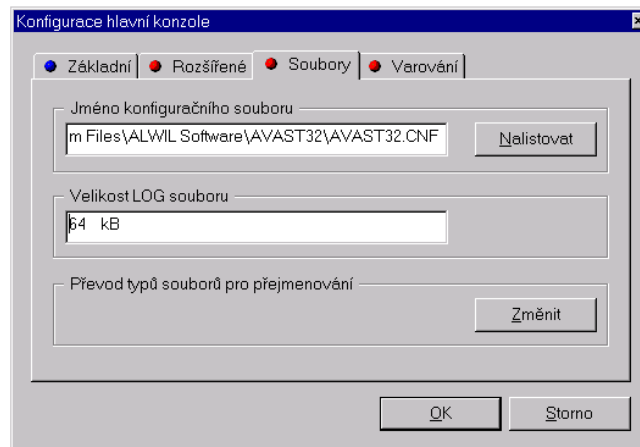
Na obr. 86 je vidět dialog, který je zobrazen vždy, když je potřeba zadat heslo. Jestliže je zadané heslo správné, bude uživateli příslušná operace s úlohou umožněna. Vložení hesla je po uživateli požadováno pouze jednou - program si správné heslo pamatuje a jeho opětovné vložení bude vyžadovat až po dalším startu programu AVAST32 nebo po změně hesla.

Ke změně stávajícího hesla slouží tlačítko „Změnit heslo“. Po jeho stisku se objeví stejný dialog jako v případě, když byla ochrana sdílených úloh

zapnuta. Před zapsáním nového hesla je potřeba do textového pole „Vložte současné heslo“ zapsat heslo dosavadní, a to i v tom případě, že uživatel během činnosti programu již heslo zadal. Bez jeho správného zadání nebude heslo změněno!

### 6.1.3 Stránka „Soubory“

Stránka „Soubory“ dává uživateli možnost blíže určit soubory, se kterými program AVAST32 pracuje (obr. 87).

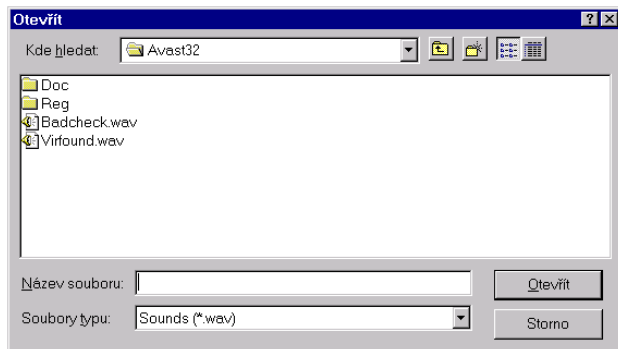


obr. 87

Nastavení ovládacích prvků na této stránce se uchovávají pro program jako celek, takže jejich

změna ovlivní všechny uživatele. Provedené změny budou brány na zřetel až po dalším startu programu AVAST32.

Textovým polem „Jméno konfiguračního souboru“ má uživatel možnost zadat jméno konfiguračního souboru (\*.CNF) programu AVAST32, včetně cesty k němu. Takto specifikovaný konfigurační soubor se bude používat místo dosavadního.



obr. 88

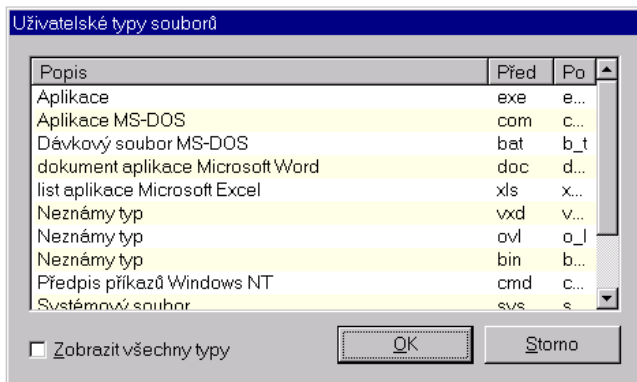
Tlačítko „Nalistovat CNF“ slouží k určení konfiguračního souboru pomocí standardního systémového dialogu pro otevírání souborů (obr. 88). Jméno vybraného souboru se automaticky umístí do výše uvedeného textového pole. Implicitně je

používán konfigurační soubor ze složky programu AVAST32.

V textovém poli „Velikost log. souboru“ je možné nastavit maximální velikost logovacího souboru. Velikost souboru se udává v KB (v kilobytech). Jestliže logovací soubor dosáhne udané velikosti, bude jeho zhruba první třetina smazána. Tím dojde k odstranění nejstarších údajů ze souboru a k vytvoření místa pro údaje nové. Implicitní maximální velikost logovacího souboru je 64 KB.

Hodnota v textovém poli má smysl pouze ve Windows 95 a to tehdy, je-li logování povoleno (bližší informace viz kapitola 6.1.1, zaškrtačací pole „Povolit logování programu AVAST32“).

Tlačítko „Změnit“ slouží k vyvolání dialogu, ve kterém lze nastavit novou příponu pro daný typ souboru (obr. 89). Dialog obsahuje seznam známých typů souborů a jejich přípon (sloupec „Před“). Sloupec „Po“ obsahuje přípony, které při přejmenovávání daného typu souborů nahradí příponu stávající. Dialog může obsahovat pouze ty nejdůležitější přípony nebo všechny známé přípony - to lze zvolit zaškrtnutím pole „Ukaž všechny typy“.



obr. 89

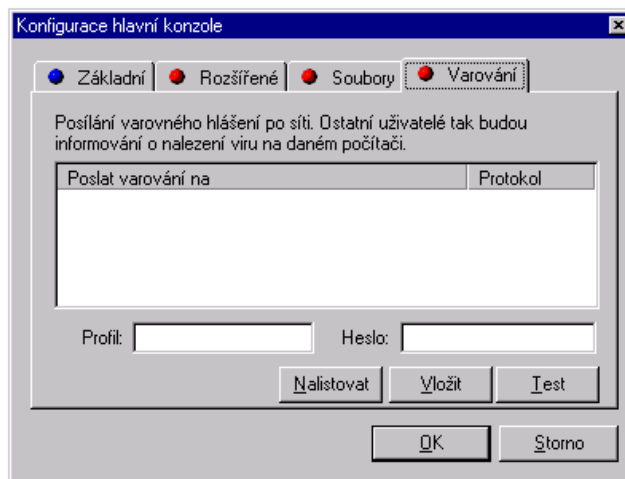
Přípony uvedené v tomto dialogu se použijí při přejmenování souboru na stránce „Výsledky“ (kapitola 5.3.2). Soubory uvedené ve stromové struktuře na této stránce byly nějakým způsobem změněny nebo program v nějakém z nich dokonce rozpoznal virus. V takovém případě je vhodné (zejména u spustitelných souborů) je přejmenovat, aby nemohlo dojít ani k jejich nechtěnému spuštění.

Pokud chcete změnit příponu nějakého typu souborů, nejprve ji vyberte a potom na ni klepněte levým tlačítkem myši. Bude Vám umožněna její editace. Novou příponu potvrďte klávesou „Enter“.

Jste-li spokojeni se změnami, které jste provedli s příponami souborů, stiskněte tlačítko „OK“.

Nové přípony souborů budou používány při dalším přejmenování souborů, bez nutnosti nového spuštění programu. Jestliže raději chcete používat přípony, které byly používány doposud, použijte tlačítko „Storno“.

### 6.1.4 Stránka „Varování“



obr. 90

Stránka „Varování“ slouží k vybrání počítačů (obr. 90), na které bude v případě nalezení viru zasláno varovné hlášení. Uživatelé těchto počítačů budou informováni spolu s těmi, jejichž počítače

byly vybrány během vytváření úlohy (kapitola 4.4.11), která virus našla.

Seznam vybraných počítačů se uchovává pro program AVAST32 jako celek, takže jeho změna ovlivní všechny uživatele. Změny však vejdou v platnost až po dalším spuštění programu AVAST32.

Počítač, na který má být hlášení o nalezení viru zasláno, je možné určit přímým zapsáním jeho jména do seznamu vybraných počítačů. Stiskem tlačítka „Vložit“ zobrazíte místní nabídku s několika protokoly:

- položka „Internet“ určuje, že počítač, na který bude varovná zpráva zaslána, je určen pomocí standardní URL adresy. Pro doručení zprávy bude použit protokol SMTP (Internet Mail),
- položkou „Microsoft“ sdělíte programu, že daný počítač je přístupný přes poštu Microsoft Mail,
- položka „Základní“ umožňuje uživateli zapsat libovolnou adresu včetně specifikace protokolu, který má být použit. Např. adresa „SMTP:novak@aaa.cz“ tohoto protokolu je stejná jako adresa „novak@aaa.cz“ protokolu „Internet“ apod.,
- položka „Interní“ znamená, že pro přístup na zvolený počítač bude použit protokol pro lokální síť (daný počítač, musí být samozřejmě přes lokální síť dostupný).

Po zvolení příslušného protokolu bude přidána do seznamu položka jménem „Vlož platnou adresu/jméno ...“. Klepnete-li na ní levým tlačítkem myši, bude Vám umožněna její editace. Po zapsání jména počítače stisknete klávesu „Enter“.

Po stisku tlačítka „Nalistovat“ se opět objeví místní nabídka s protokoly (v současné době obsahuje pouze položku „Interní“, viz výše). Počítač, dostupný přes lokální síť, můžete vybrat pomocí dialogu, který ukazuje obr. 52.

Jméno počítače můžete ze seznamu odstranit tak, že jej nejprve vyberete a poté stisknete klávesu „Del“.

Budete-li posílat zprávu prostřednictvím jiného protokolu než „Interní“, je potřeba zapsat jméno profilu, který se má použít, popř. jeho heslo, do příslušných textových polí. Pokud necháte textové pole „Profil:“ nevyplněné (nebo zadané jméno profilu je neplatné), a program se pokusí zaslat varovné hlášení, budete na jméno profilu dotázáni.

Parametry položek v seznamu, resp. vybraných počítačů, je možné dodatečně změnit. Chcete-li změnit přístupový protokol na daný počítač, klepněte do sloupce „Protokol“ příslušného počítače. Z místní nabídky poté vyberte nový protokol. Podobným způsobem změníte i jméno/adre-



su počítače: po klepnutí levým tlačítkem myši Vám bude umožněna jeho editace.

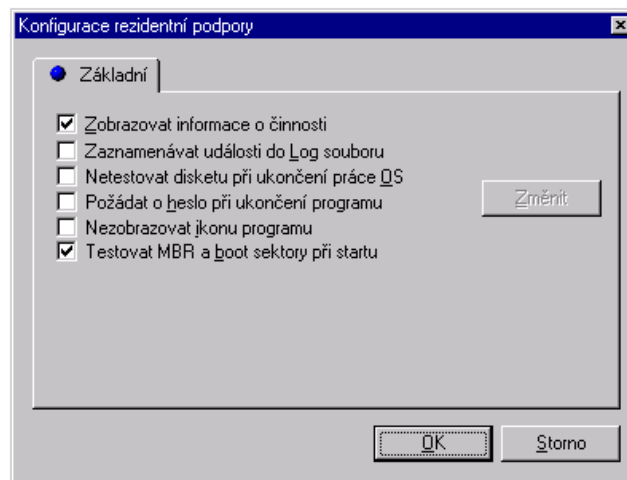
Pokud si nejste doručení varovného hlášení jisti, můžete „spojení“ vyzkoušet tlačítkem „Test“. Na každý vybraný počítač bude zasláno zkušební hlášení. Implicitně je seznam počítačů, na které budou zaslány varovné hlášení, prázdný.

## 6.2 Položka „Rezidentní ochrana ...“

Zvolením této položky se zobrazí dialog, který je vidět na obr. 91. Obsahuje ovládací prvky pro nastavení části zajišťující rezidentní ochrany (jedná se o program RGW32, viz kapitola 9).

Změna nastavení ovládacích prvků se projeví až po dalším spuštění programu RGW32.

Zaškrťovací pole „Zobrazovat informace o činnosti“ určuje, zda bude si uživatel přeje být informován o probíhajících rezidentních činnostech. Je-li pole zaškrtnuto, bude se vpravo dole na pracovní ploše zobrazovat stručná informace o právě probíhající rezidentní činnosti. Není-li pole zaškrtnuto, žádná informace zobrazena nebude, což je i implicitní nastavení.



obr. 91

Zaškrtnutím pole „Zaznamenávat události do Log souboru“ může uživatel programu sdělit, že chce, aby o činnosti rezidentních ochran byly zapisovány informace do tzv. logovacího souboru (bližší popis je uveden v kapitole 6.1.1, u zaškrťovacího pole „Povolit logování programu Avast32“).

Pomocí zaškrťovacího pole „Netestovat disketu při ukončování práce OS“ zamezíte rezidentní části programu AVAST32, aby během ukončování práce operačního systému testovala disketu.

Pokud by byla vložená disketa infikována a pokud by zůstala v mechanice, došlo by při násle-

dujícím startu operačního systému k nakažení počítače (pokud ovšem nemáte v SETUP zakázáno zavádění systému z mechaniky). Je-li ale v mechanice objevena disketa a pole není zaškrtnuto, bude zobrazeno hlášení, kterým se zabývá kapitola 9.3. Implicitně není pole zaškrtnuto.

Zaškrťovací pole „Požádat o heslo při ukončení programu“ umožňuje zamezit ukončení rezidentů a tím ochránit, např. méně zkušené uživatele před virovou nákazou. Při každém pokusu o ukončení programu RGW32 se objeví dialog zobrazený na obr. 86 a bez zadání správného hesla nebude možné program ukončit.

Po zaškrtnutí pole se objeví dialog, který je vidět na obr. 85. Zaškrtnutí pole nelze samozřejmě bez znalosti hesla zrušit. Implicitně není pole zatrženo.

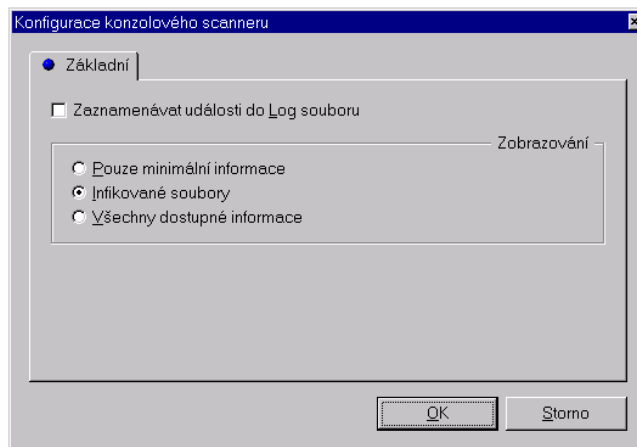
Tlačítkem „Změnit“ můžete měnit heslo programu RGW32 - pokud znáte současné heslo. Změnu hesla provedete v dialogu na obr. 85.

Zaškrtnutím pole „Nezobrazovat ikonu programu“ způsobíte, že program RGW32 nebude během své činnosti zobrazovat malou ikonu na hlavním panelu (obr. 103). Běžným uživatelům doporučujeme pole nezaškrťovat. Implicitně není pole zaškrtnuto.

Zaškrťovací pole „Testovat MBR a boot sektory při startu“ umožňuje, aby program RGW32 ihned po svém startu otestoval systémové oblasti lokálních pevných disků. Implicitně je pole zaškrtnuto.

Pracujete-li v operačním systému Windows 95 obsahuje dialog i pole „Testovat paměť při startu“, jehož zaškrtnutím způsobíte, že program RGW32 při svém startu zkontroluje operační paměť počítače.

### 6.3 Položka „Znakový scanner ...“



obr. 92

Po zvolení položky „Znakový scanner ...“ se objeví dialog, který ukazuje obr. 92. Obsahuje ovládací prvky pro základní nastavení tzv. znakového scanneru, tedy programu pro hledání virů,

kteřý je spouštěn z příkazové řádky (jedná se o program LGW32, viz [kapitola 8](#)).

Pomocí zaškrťovacího pole „Zaznamenávat události do Log souboru“ může uživatel programu sdělit, že si přeje o činnosti znakového scanneru zapisovat informace do logovacího souboru (bližší popis je uveden v [kapitole 6.1.1](#), u zaškrťovacího pole „Povolit logování programu Avast32“).

Dialog také obsahuje přepínače, pomocí kterých může uživatel nastavit množství informací zobrazovaných na standartním výstupu (obvykle se jedná o okno příkazové řádky):

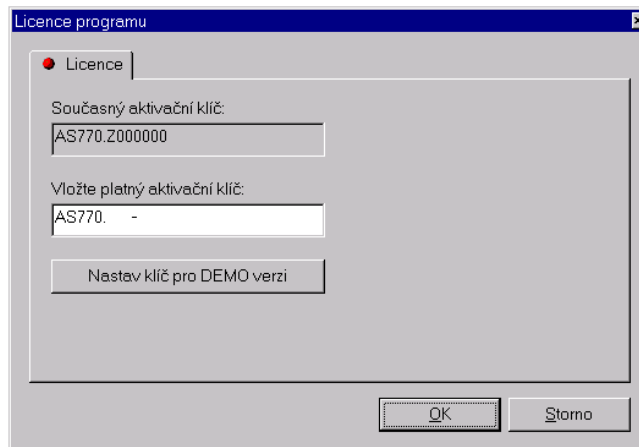
- přepínač „Pouze minimální informace“ způsobí, že znakový scanner bude vypisovat pouze svoji hlavičku,
- po zvolení přepínače „Infikované soubory“ bude zobrazována hlavička znakového scanneru, informace o případných nakažených souborech a virech, kterými jsou nakaženy. Zobrazena bude také tabulka s celkovou statistikou o průběhu testu,
- přepínačem „Všechny dostupné informace“ uživatel sdělí znakovému scanneru, že si přeje být informován o všem, co právě dělá a o výsledcích jeho činnosti.

Množství informací zobrazovaných znakovým scannerem lze také nastavit pomocí parametrů na příkazové řádce (viz [kapitola 8](#), parametr /V). V

takovém případě se na nastavení na této stránce nebere zřetel.

## 6.4 Položka „Licence ...“

Dialog ukrývající se pod položkou „Licence“ umožňuje uživateli změnit aktivační klíč programu (obr. 93). Ten obsahuje mimo jiné i informaci o počtu zakoupených licencí, takže pokud se rozhodnete dokoupit další licence, nebudete muset instalaci programu AVAST32 opakovat. Pouze změníte aktivační klíč na této stránce a bude hotovo.



obr. 93

Stránka obsahuje současný aktivační klíč. Pod ním je umístěno textové pole umožňující vložit nový aktivační klíč. Tlačítkem „OK“ provedete vlastní změnu aktivačního klíče. Jestliže vložený aktivační klíč je neplatný, obdržíte chybové hlášení a aktivační klíč nebude změněn.

Tlačítkem „Nastav klíč pro DEMO verzi“ nastavíte aktivační klíč tzv. demoverze programu. S tímto aktivačním klíčem bude program funkční pouze tři měsíce od nastavení aktivačního klíče (samozřejmě, pokud nebude nastaven platný aktivační klíč).

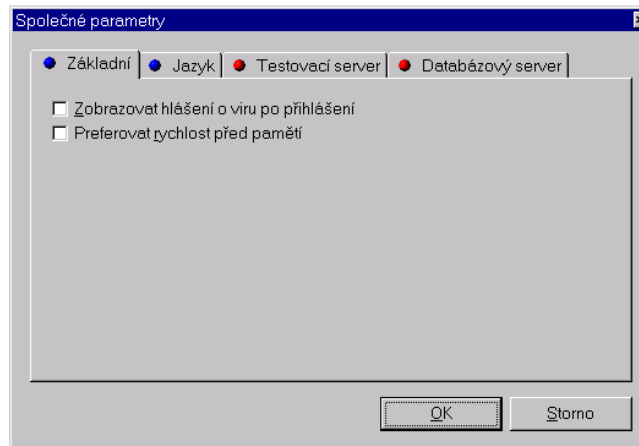
Význam jednotlivých částí aktivačního klíče je uveden v [příloze D](#).

## 6.5 Položka „Společné ...“

Dialog, který se objeví po zvolení této položky, obsahuje stránky s ovládacími prvky společnými pro všechny části programu AVAST32.

### 6.5.1 Stránka „Základní“

Tato stránka obsahuje ovládací prvky pro základní nastavení všech částí programu AVAST32 (obr. 94). Nastavení ovládacích prvků na této stránce se uchovává pro program jako celek, takže jejich změna ovlivní všechny uživatele. Změny provedené na této stránce se však projeví až po dalším startu programu AVAST32.



obr. 94

Zaškrtnuté pole „Zobrazovat hlášení o viru po přihlášení“ slouží k povolení zobrazování varovné zprávy po přihlášení se uživatele do systému. Varovné hlášení bude zobrazeno pouze tehdy, byl-li během posledního spuštění počítače nalezen virus. Uživatel je tak informován, že pracuje s nakaženým počítačem. Implicitně není pole zaškrtnuto.

Pro zobrazování varovné zprávy je používán program WARN32, který je podrobně popsán v [kapitole 11](#).

Zaškrtnuté pole „Preferovat rychlost před pamětí“ říká programu, za jakých okolností má být

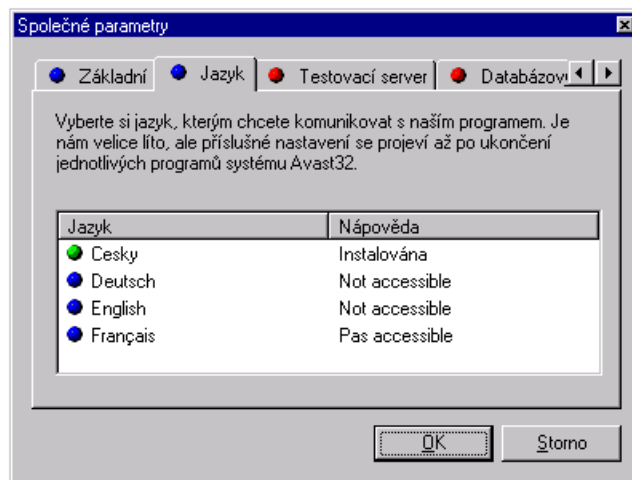
testovací server (soubor „VPS32.DLL“, viz [příloha A](#)) přítomen v paměti. Jestliže pole není zaškrtnuto, bude testovací server v paměti přítomen od svého prvního použití a nebude z ní odstraněn ani při ukončení své poslední činnosti. Je-li pole zaškrtnuto, bude testovací server z operační paměti počítače odstraněn ihned, jakmile ho nebude zapotřebí, tj. po skončení poslední běžící úlohy. Po spuštění další úlohy se bude testovací server zavádět z disku znovu.

Máte-li dostatek operační paměti, doporučujeme pole nezaškrtnávat. Urychlíte tak běh programu AVAST32. V případě, že máte operační paměti nedostatek, pole raději zaškrtnávejte - budete se ale muset smířit s pomalejší odezvou programu. Implicitně není pole zaškrtnuto.

### 6.5.2 Stránka „Jazyk“

Stránka „Jazyk“ umožňuje uživateli přepínat mezi jazyky, které program AVAST32 podporuje (obr. 95). Jazyky jsou umístěny v seznamu v prvním sloupci na stránce. Jazyk, ve kterém program právě komunikuje je označen zelenou kuličkou, ostatní pak kuličkou modrou.

Druhý sloupec seznamu informuje uživatele o přístupnosti dokumentace v daném jazyce, tj. zda je příslušná dokumentace nainstalována, či nikoli.



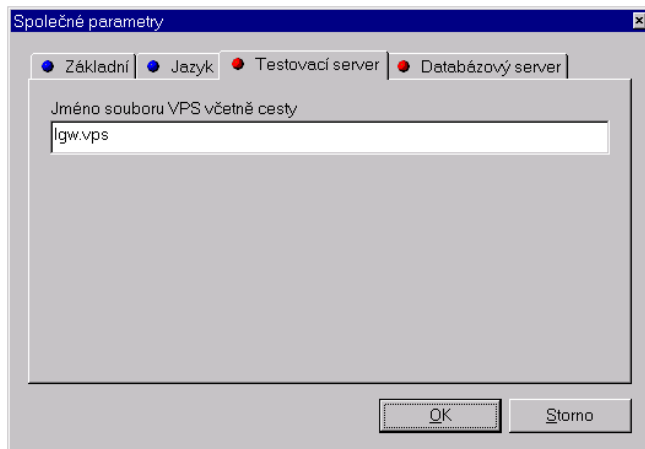
obr. 95

Chcete-li změnit jazyk programu AVAST32, poklepejte na něm levým tlačítkem myši. Změna jazyka se projeví až po dalším spuštění programu. AVAST32 si nastavený jazyk „pamatuje“ pro každého uživatele zvlášť, takže jeho změna ovlivní pouze nastavení programu pro uživatele, který ji provedl.

Implicitně je nastaven jazyk, který uživatel vybral před vlastní instalací programu ([obr. 3](#)).

### 6.5.3 Stránka „Testovací server“

Stránka „Testovací server“ umožňuje uživateli nastavit základní parametry tzv. testovacího serveru (obr. 96). Ten je používán všemi částmi programu AVAST32, takže zde provedené změny ovlivní každou jeho část a každého uživatele, pracujícího s programem AVAST32 na daném počítači (bližší informace o testovacím serveru jsou uvedeny v příloze A).

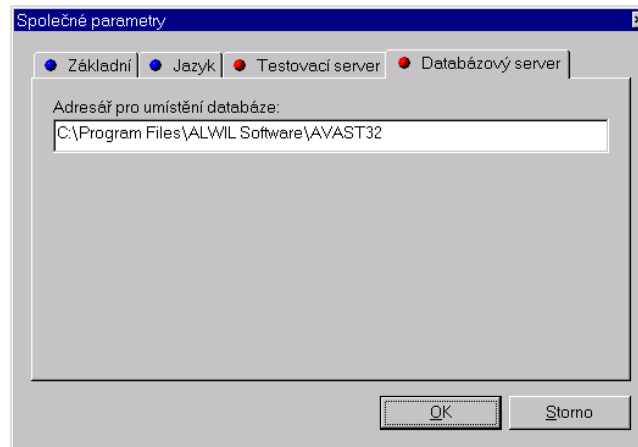


obr. 96

Textové pole „Jméno souboru VPS včetně cesty“ obsahuje jméno souboru VPS, tedy souboru

s databází známých virů, včetně kompletní cesty k němu. Protože se jedná o velmi důležitý soubor, měl by si uživatel uvědomit, že udáním špatného souboru VPS se vystavuje nebezpečí nerozpoznání virů nebo naopak hlášení falešných poplachů. Implicitně textové pole obsahuje jméno souboru „lgw.vps“ ze složky programu AVAST32.

### 6.5.4 Stránka „Databázový server“



obr. 97

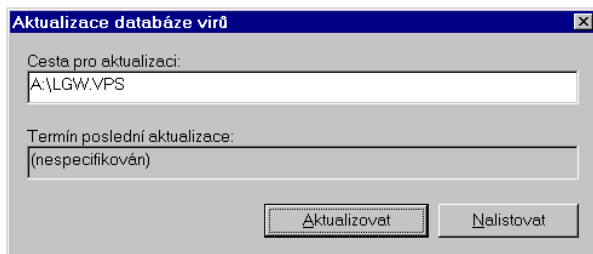
Pomocí textového pole „Složka pro umístění databáze:“ této stránky (obr. 97) můžete nastavit, do jaké složky si má AVAST32 ukládat své data-

bázové soubory. Jedná se především o databázi souborů na Vašich pevných discích, která je používána při testu integrity dat.

## 6.6 Položka „Obnova VPS ...“

Program AVAST32 umožňuje jednoduchou aktualizaci databáze známých virů. Stačí pouze stávající soubor LGW.VPS nahradit novějším; není tedy potřeba přeinstalovávat program jako takový.

Můžete soubor LGW.VPS zkopírovat ručně (tento postup však příliš nedoporučujeme) nebo můžete zvolit tuto položku. Po jejím zvolení se objeví dialog, který je vidět na obr. 98.



obr. 98

Textové pole „Cesta pro aktualizaci VPS“ obsahuje cestu ke složce, ve které bude hledán novější soubor VPS. Aktualizace souboru VPS je též možné provádět automaticky, viz kapitola 6.1.2, zaškrtnuté pole „Automaticky aktualizovat VPS“.

Pokud jste program AVAST32 instalovali z disku CD-ROM, bude textové pole implicitně obsahovat cestu „<cd>:\AVS\LGW.VPS“, kde místo <cd> je označení Vaší jednotky CD-ROM. Při instalaci z disket zde bude implicitně uvedena cesta „A:\LGW.VPS“.

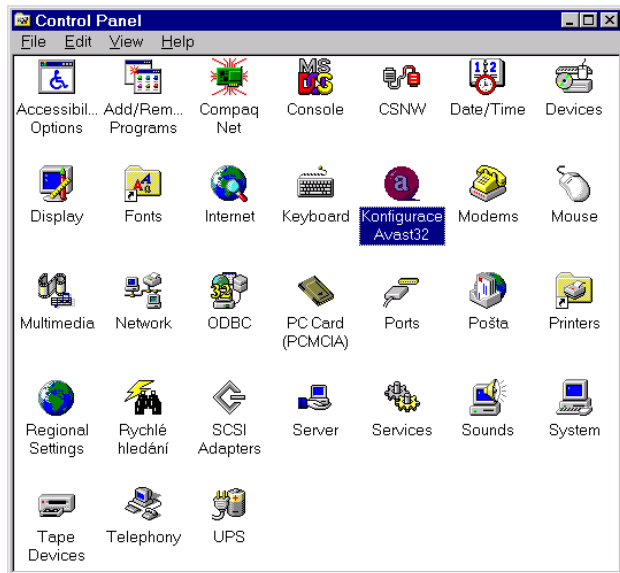
Potřebnou složku lze také specifikovat pomocí standardního dialogu na otevírání souborů (obr. 88), který se objeví po klepnutí na tlačítko „Nalistovat“.

Textové pole „Termín poslední aktualizace“ obsahuje datum a čas poslední provedené aktualizace souboru VPS (pokud byla nějaká provedena).

Tlačítkem „Aktualizovat“ spustíte vlastní aktualizaci souboru LGW.VPS. Aktualizace však bude provedena pouze tehdy, je-li specifikovaný soubor LGW.VPS novější než ten, který je právě používán.

## 6.7 Nastavení programu přes „Ovládací panely“

Nastavení všech částí programu AVAST32 lze provádět i bez nutnosti spouštět hlavní program. Stačí vybrat ze složky „Nastavení“ nabídky tlačítka „Start“ položku „Ovládací panely“.



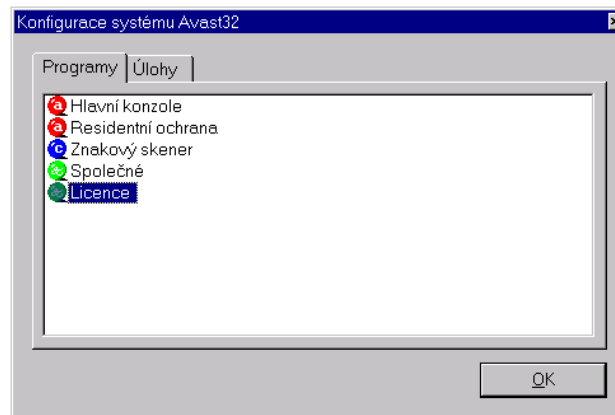
obr. 99

V okně, které se objeví, poklepejte na položku „Konfigurace AVAST32“ (obr. 99). Objeví se okno se stránkami, mezi kterými můžete přepínat pomocí záložkového seznamu. V následujících kapitolách si popíšeme jednotlivé stránky.

### 6.7.1 Stránka „Programy“

Stránka „Programy“ slouží pro vybrání části programu, kterou chcete nastavit (obr. 100). Po-

klepáním na příslušnou položku vyvoláte dialog, ve kterém pomocí ovládacích prvků změníte nastavení příslušné části programu.



obr. 100

Seznam na této stránce obsahuje následující položky:

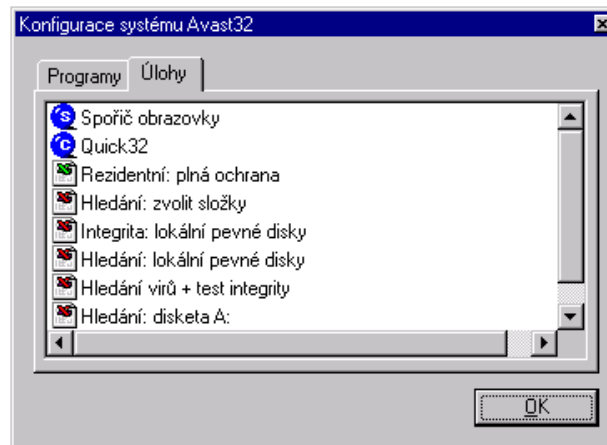
- položka „Hlavní konzole“ vyvolá dialog pro nastavení programu AVAST32 jako takového. Zobrazený dialog je podrobně popsán v kapitole 6.1,
- položkou „Rezidentní ochrana“ můžete změnit nastavení části programu, která se stará o rezidentní činnosti (program RGW32, viz kapi-



- tola 9). Popis zobrazeného dialogu naleznete v kapitole 6.2,
- položka „Znakový scanner“ slouží k základnímu nastavení programu pro hledání známých virů, který je určen pro příkazovou řádku (program LGW32, viz kapitola 8). Příslušný dialog je popsán v kapitole 6.3,
  - pomocí položky „Společné“ je možné nastavit nejrůznější parametry, které jsou společné pro všechny části programu AVAST32. Bližší informace o zobrazeném dialogu naleznete v kapitole 6.5,
  - poslední položka „Licence“ Vám umožňuje změnit aktivační klíč Vaší kopie programu. Tímto způsobem můžete změnit počet dostupných licencí bez nutnosti nové instalace celého programu, viz kapitola 6.4.

### 6.7.2 Stránka „Úlohy“

Z této stránky můžete vyvolat dialogy pro modifikaci jednotlivých úloh programu AVAST32 (obr. 101). Seznam na této stránce je velmi podobný seznamu úloh jednoduchého a rozšířeného ovládání. Poklepete-li na jméno úlohy, kterou chcete změnit, objeví se dialog, který je podrobně popsán v kapitole 4 (popis jednotlivých stránek dialogů obsahují kapitoly 4.4.1 až 4.4.16).

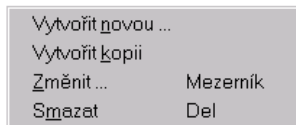


obr. 101

Seznam kromě úloh běžných úloh obsahuje i dvě speciální úlohy, které mají zvláštní význam. Úloha „Spořič obrazovky“ je popsána v kapitole 12.1, úloha „Quick32“ potom v kapitole 10.1.

### Místní nabídka

Místní nabídku, vyvolanou stiskem pravého tlačítka myši nad seznamem úloh stránky „Úlohy“, ukazuje obr. 102.



obr. 102

- položka „Vytvořit novou ...“ slouží pro vytvoření nové úlohy programu AVAST32 (viz [kapitola 4](#)), bez nutnosti jej spouštět,
- pomocí položky „Vytvořit kopii“ může uživatel vytvořit kopii úlohy. Kopie úlohy bude mít naprosto stejné nastavení parametrů jako úloha, nad kterou bylo právě tlačítko myši stisknuto. Pouze je-li úloha sdílená a uživatel nezná správné heslo, pak bude nově vytvořená úloha privátní,
- položka „Změnit ...“, stejně jako poklepání na jméno úlohy, vyvolá dialog pro změnu nastavení dané úlohy (viz výše),
- zvolením položky „Smazat ...“ lze příslušnou úlohu natrvalo odstranit ze seznamu úloh. Nejprve je však potřeba smazání úlohy potvrdit stiskem tlačítka „Ano“ v dialogu, který se objeví po zvolení položky ([obr. 65](#)).

Jestliže provedete jakékoli změny s úlohami přes „Ovládací panely“ a přitom máte spuštěn program AVAST32, pak provedené změny se v programu objeví až při jeho opětovném spuštění!!!

### 6.7.3 Nastavení zvuku

AVAST32 umožňuje pro své události nastavit i zvukový soubor, který bude přehrán vždy, když ke zvolené události dojde.

Zvuky lze zvolit v ovládacím panelu „Zvuky“, který je vidět na [obr. 55](#). Díky tomu, že pro nastavení zvuku je použit standardní systémový prostředek, není při nastavování zvuku (stejně jako při nastavování ostatních částí programu AVAST32) potřeba, aby byl vlastní program spuštěn.

V seznamu „Události“ najdete položku „Avast32“ a vyberte událost, pro kterou chcete změnit nastavený zvuk. Způsob, jak nastavit zvukový soubor pro určitou událost je popsán v [kapitole 4.4.13](#).

## 7. Interpretace výsledků

Doporučujeme Vám si tuto kapitolu důkladně přečíst a trochu se nad ní zamyslet. Možná zde budeme pouze opakovat staré známé pravdy, ale opatrnosti není nikdy dost. Zejména méně zkušení uživatelé osobních počítačů by měli zbystrit a rozhodně kapitolu nepřeskakovat.

Základní skutečností, kterou se musíte řídit je, že platí přímá úměra mezi prací, znalostmi, zkušeností a bezpečností Vašeho počítače. Možná se Vám to bude zdát divné, ale dokud nebudete věnovat soustavnou pozornost tomu co děláte i z hlediska možné virové infekce, sebelepší anti-virový program Vám nepomůže. Zároveň pokud Vás nezajímají počítače a jste lékař, ekonom nebo právník a nemáte čas se starat o „podružné“ věci jako je bezpečnost počítače a Vašich dat, musíme Vás zklamat. Opravdu se mýlíte. A pokud ani nechcete dát na naši radu a nechcete se naučit ani základům, doporučujeme Vám vrátit náš program prodejci, který Vám vrátí peníze. Ušetříte sobě i nám mnoho starostí. Aby jste mohli dobře vykonávat Vaši práci, potřebujete znát český pravopis a gramatiku. Stejně tak práce s počítačem vyžaduje určité základní znalosti, bez kterých se můžete obejít opravdu jenom stěží.

Je možné napsat program pro editaci textu, databázi nebo tabulkový procesor, který bude plně uživatelsky přívětivý a nebude prakticky vyžadovat žádné speciální znalosti nebo Vás popřípadě potřebné věci naučí. Problematika bezpečnosti a anti-virové ochrany je ale opravdu odlišná. Snažně Vás žádáme, věnujte jí potřebný čas a pozornost.

### 7.1 AVAST32 nalezl viry

Tato část je poměrně jednoduchá, i když ne úplně triviální. Pokud Avast32 hlásí, že nalezl virus, ještě to neznamená, že zde opravdu virus je. A i když zde opravdu virus je, ještě to neznamená, že máte zavirován počítač. I tento text byl psán na počítači, který obsahuje několik desítek různých virů a přece je autor úplně klidný, protože tyto viry nejsou aktivní.

Podrobný popis co s informací o nalezeném viru je uveden v [příloze B](#), kterou Vám doporučujeme důkladně si prostudovat.

## 7.2 AVAST32 nalezl změny v souborech

Tady je situace trochu složitější, ale ne neřešitelná. Nicméně pouze zkušenosti s pravidelnou prací s programem AVAST32 a testováním integrity dat Vám mohou přinést očekávané výsledky.

Interpretace výsledků není jednoduchá. Ne snad proto, že by program poskytoval složité informace nebo šifry, ale protože každý z Vás dostane při každém spuštění testů integrity jiné informace a jejich zpracování se může lišit případ od případu. Z těchto důvodů není možné zde napsat obecně platnou „kuchařku“, která uspokojí všechny uživatele. Můžeme zde uvést pouze několik obecných rad, návrhů a postupů, které doporučujeme aplikovat. Nicméně detaily a podrobnosti si musíte vyvodit sami.

### 7.2.1 Nové soubory

Pokud AVAST32 ohlásí, že nalezl nové soubory, může se jednat o několik případů. Nejjednodušší z nich je ten, že se jedná opravdu o nový soubor pocházející z legálního zdroje. Řešení je jednoduché, prostě jej akceptujte a tím se uloží do databáze souborů. Co je to legální zdroj je ovšem složitější. Například, opravdu legální zdroj jsou instalační média programu, který jste nedávno nainsta-

lovali. Zmíněný program mohl nainstalovat Váš kolega nebo administrátor sítě. Máte-li ve Vaší firmě dobré vztahy, pak Vás o této skutečnosti jistě informovali a Vy můžete rozhodnout o tom, zda je soubor v pořádku či nikoli.

Může se také jednat o dočasný soubor, který si některý program vytvořil pro svou potřebu a právě jej používá nebo jej „zapomněl“ smazat. To je také pravděpodobně v pořádku, ale soubor tohoto typu si mohl vytvořit i virus. Rozhodnutí může být těžké a je pouze na Vás.

Také použití „Košé“ pro mazání souborů způsobí detekci nových souborů v příslušné složce.

Nedejte se zmást, že nový soubor vznikl v nějaké složce známého jména, například ve složce operačního systému. Autoři virů znají tyto složky také a s úspěchem je používají.

### 7.2.2 Změněné soubory

Důvodů pro změnu souboru může být opravdu mnoho. I samotný operační systém si „žije vlastním životem“ a používá soubory velice intenzivně. Každé spuštění programu nebo editace dokumentu má za následek stopu, kterou AVAST32 detekuje a oznámí. Zde musíte rozhodnout Vy, která změna je platná a která nikoli. Například změna textových souborů bude na devadesát devět procent způsobena Vámi, zatímco změna souboru COMMAND.COM na

devadesát devět procent nějakým virem. Všimněte si, že nic není stoprocentní, což platí pro celou oblast virové problematiky. Mezi výše uvedenými extrémy leží ostatní typy souborů. Například o dokumentech programu Microsoft Word (\*.doc) je těžké říci, proč se změnily. Mohli jste to být Vy pouhým přečtením jeho obsahu, nebo to mohl být tzv. „makrovirus“, který napadl tento dokument.

Obecně ale platí, že pokud je napaden výkonný program (exe, sys, dll, bin, vxd, scr,...) je změna mnohem podezřelejší, než když je změněn dokument nebo datový soubor. Ale pozor, i zde existují výjimky.

### 7.2.3 Smazané soubory

Zde toho moc nepomůže. Obnova tohoto souboru je možná jenom pomocí speciálních prostředků operačního systému nebo ze záložních kopií. Mimochodem, kdy jste naposledy zálohovali svoje data? Opravdu se chcete spoléhat jenom na náhodu?

### 7.2.4 Speciální případy

Existuje několik speciálních případů, kdy se Vám nepovede se soubory pracovat. V tom případě zjistíte, že AVAST32 signalizuje chybu při práci se souborem ([kapitola 5.3.2](#)).

Ve většině případů nebudete moci zkontrolovat soubor, který právě používá jiný program. Tento soubor je blokován a operační systém Vám k němu nepovolí přístup. To platí jak o operačním systému, který používá soubory sám o sobě, i o pracujících programech. Ty nemusí být po každé viditelné na obrazovce Vašeho počítače. Pokud ale pracují a používají soubory, Avast32 nebude moci tyto soubory zkontrolovat.

Pokud pracujete s operačním systémem, který podporuje bezpečnost na úrovni souborů a používáte systém souborů, který tuto vlastnost podporuje také (Windows NT s NTFS), musíte mít dostatečná práva, abyste mohly zkontrolovat jednotlivé soubory. Pokud Vaše práva dostatečná nejsou, soubor zůstane nezkontrolován.

## 8. Program LGW32

Program slouží k vyhledávání známých virů, včetně virů polymorfních a makrovirů. Jedná se o ekvivalent úlohy, kde bychom testovali pouze přítomnost známých virů v programu AVAST32 a má tedy i velmi podobné možnosti nastavení.

Vzhledem k tomu, že jak program AVAST32 tak program LGW32 používají služby testovacího serveru VPS32, jejich výsledky jsou naprosto totožné. Rozdíl mezi nimi je pouze v tom, že program LGW32 používá pro svou činnost pouze možnosti příkazového řádku, na rozdíl od uživatelsky velmi přívětivého prostředí programu AVAST32.

Příkazová řádka programu LGW32 vypadá takto:

```
LGW32 [@<jméno úlohy> | [+ | -]<jméno
oblasti>[-] [<parametr>, ...]
```

Chcete-li spustit úlohu vytvořenou programem AVAST32, potom za znak „@“ (zavináč) napište její jméno. Obsahuje-li jméno úlohy mezeru, musí být jméno v uvozovkách. Pokud v nich nebude, program úlohu neprovede!

Není-li na příkazové řádce zadáno jméno úlohy, bude program LGW32 kontrolovat zadané oblasti. Jakým způsobem se bude kontrola provádět,

určíte parametry, podobně jako u příkazů operačního systému.

U programu LGW32 je možné nastavit několik parametrů. Podrobný popis těchto parametrů je uveden v [kapitole 6.3](#). Je-li však na příkazové řádce uveden i příslušný přepínač, bude parametr nastaven podle tohoto přepínače.

[+ | -]

- znaménka před jménem oblasti znamenají, zda mají být testovány i vnořené složky. Znaménko plus test vnořených složek povolí, znaménko mínus jej zakáže.

[-]

- znaménko mínus za jménem oblasti způsobí, že oblast nebude testována. Tak lze program LGW32 např. sdílet, aby otestoval celý disk „D:“ kromě složky „D:\Viry“. Má stejný účinek, jako červená kulička u jména kontrolované oblasti v programu AVAST32 (viz [kapitola 4.4.5](#)).

Program LGW32 podporuje následující parametry:

### **/? /H, /HELP**

- program zobrazí nápovědu. Nápověda obsahuje několik stránek, mezi kterými lze přepínat numerickými klávesami, které vždy znamenají číslo stránky, která má být zobrazena. Po stisku jakékoli jiné klávesy dojde k návratu do příkazové řádky.

### **/A**

- zapne kontrolu souborů na přítomnost všech virů včetně těch, které daný typ soubory ne- napadají. Potom bude např. soubor s příponou COM kontrolován i na přítomnost virů, které napadají pouze EXE soubory.

### **/C[+]**

- zapíná kontrolu celých souborů (viz [kapitola 4.4.7](#)). Do tohoto režimu se program sám automaticky přepne po nalezení libovolného viru. Znak „+“ (plus) způsobí, že budou kontrolovány i komprimované soubory.

### **/E[A|E|O]<typ>**

- informuje program, které typy souborů se mají kontrolovat (viz [kapitola 4.4.4](#)). Písmeno „A“ znamená, že budou kontrolovány všechny soubory, písmeno „E“ označuje spustitelné soubory a konečně písmeno „O“ znamená OLE dokumenty. Můžete také přímo specifikovat

typy kontrolovaných souborů. Jejich počet není omezen, a vzájemně musí být odděleny čárkou. Pokud není parametr uveden, budou se testovat pouze spustitelné soubory a OLE dokumenty.

### **/X[typy]**

- uvedené typy souborů nebudou kontrolovány. Tímto způsobem je možné zařídit, aby byly např. kontrolovány všechny soubory, kromě textových (přípona TXT). Parametr má stejný účinek jako červená kulička u jména typu v seznamu kontrolovaných typů v programu AVAST32 (viz [kapitola 4.4.4](#)).

### **/L[-]**

- pro danou operaci zapíná logování. Podrobný popis mechanismu logování je uveden v [kapitole 6.1.1](#), u zaškrtačovacího pole “Povolit logování programu Avast32”.

### **/M**

- zapne test operační paměti. Kromě paměti však nebude již nic dalšího testováno.

### **/R[<jméno>]**

- při provádění kontroly bude vytvořen soubor se zprávou o průběhu kontroly (viz [kapitola 4.4.10](#)). Pokud není uvedeno jméno souboru,

protokol bude zapsán do souboru „LGW32.RPT“ v právě platné složce.

### **/S<jméno>**

- specifikuje soubor obsahující zvuk, který bude přehrán po nalezení prvního viru. Aby mohl být zvuk přehrán, musí být v počítači nainstalována zvuková karta a příslušné ovladače.

### **/V[N|I|A]**

- určuje, o jakých souborech se mají vypisovat informace na obrazovku. Písmeno „N“ vypne vypisování, „I“ zapne vypisování pouze infikovaných souborů a „A“ zapne výpis všech nalezených souborů.

### **/U<jméno>[,<jméno>]**

- určuje jméno počítače nebo domény, na kterou se má zaslat hlášení o nalezení viru. Za parametrem musí být zapsáno alespoň jedno jméno.

### **/Z[+|V]**

- zapne automatické odstraňování nalezených makrovirů v OLE dokumentech. Znaménko + způsobí, že pokud virus nebyl v OLE dokumentu rozpoznán zcela přesně, budou smazány všechna makra v dokumentu. Písmeno V zajistí automatické odstranění všech maker z nakaženého dokumentu. Jestliže za

přepínačem není uveden žádný znak, bude z OLE dokumentu odstraněno pouze makro obsahující virus.

V okamžiku ukončení činnosti program LGW32 vrátí operačnímu systému návratový kód. Tento kód může být později testován buď programem, který jej spustil, nebo v příkazové řádce pomocí příkazu IF ERRORLEVEL. Návratový kód programu LGW32 může nabývat pouze následující hodnoty:

- |     |  |
|-----|--|
| 0   | - program byl normálně ukončen, žádný virus nebyl nalezen, |
| 1   | - programem byl nalezen virus,                             |
| 10  | - čas, po který šlo používat demoverzi programu, vypršel,  |
| 11  | - program nelze spustit, zřejmě špatná instalace,          |
| 255 | - závažná chyba při provádění programu.                    |



## 9. Program RGW32

Program se stará o všechny rezidentní činnosti. Pokud tedy například v programu AVAST32 spustíte nějakou rezidentní úlohu, zavolá se právě program RGW32. Jeho přítomnost v paměti je indikována ikonkou v pravé části hlavního panelu (obr. 103). Poklepáním levým tlačítkem myši na tuto ikonku se zobrazí okno programu.

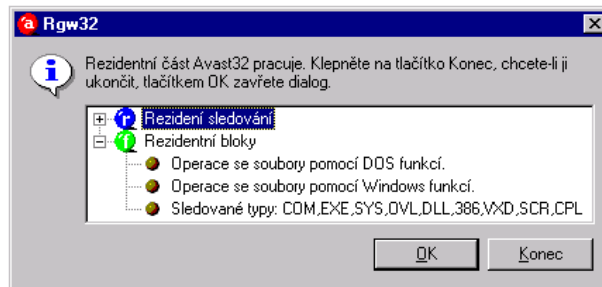
Zobrazení ikonky programu RGW32 je možné vypnout - viz kapitola 6.2, zaškrťovací pole „Nezobrazovat ikonu programu“. Běžným uživatelům ale doporučujeme nechat ikonku viditelnou.



obr. 103

Pomocí tohoto okna (obr. 104) lze program RGW32 a tím i spuštěnou úlohu ukončit. Okno obsahuje strom se dvěma základními skupinami: „Rezidentní sledování“ a „Rezidentní bloky“. Jejich rozbalením zobrazíte jednotlivé činnosti, které program v danou chvíli provádí.

U programu RGW32 je možné nastavit několik parametrů. Podrobný popis těchto parametrů je uveden v kapitole 6.2.



obr. 104

Příkazová řádka programu RGW32 vypadá takto:

```
RGW32 <jméno> | /E
```

Parametr <jméno> specifikuje rezidentní úlohu, která má být spuštěna. Není-li parametr uveden nebo úloha s tímto jménem neexistuje, program zobrazí chybové hlášení. Na jednom počítači může být spuštěna pouze jedna rezidentní úloha. Při spuštění další rezidentní úlohy bude první úloha ukončena.

Jestliže úloha obsahuje i nějaké nerezidentní činnosti, budou tyto činnosti a jejich nastavení ignorovány - vždy budou prováděny pouze zvolené rezidentní testy.

Objahuje-li příkazový řádek místo jména úlohy parametr „/E“ bude aktuální rezidentní úloha ukončena. Tento parametr je vhodný zejména pro ukončování programu RGW32 z dávkových souborů.

Program RGW32 nevrací žádné návratové kódy.

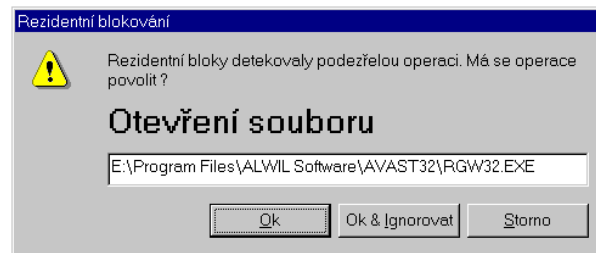
RGW32 může během své činnosti zobrazit několik dalších dialogů. Tyto dialogy oznamují uživateli nebezpečnou operaci se souborem, nález viru v boot sektoru vložené diskety či virus ve spuštěném programu nebo v OLE dokumentu, otevíraného pomocí OLE funkcí. Jejich popis je uveden v následujících kapitolách.

## 9.1 Hlášení nebezpečných operací

Jak jsme se již zmínili, má program RGW32 na starost veškeré rezidentní činnosti, které mohou úlohy provádět. Mezi tyto činnosti patří i rezidentní blokování nebezpečných operací. Jestliže je spuštěna úloha, která v sobě obsahuje i činnost rezidentních bloků, pak jsou sledovány veškeré operace zvoleného operačního systému ([kapitola 4.4.15](#)).

Při pokusu o provedení jakékoli podezřelé operace program RGW32 zobrazí upozornění (obr. 105) a provedení dané operace pozdrží než mu uživatel sdělí, co dělat dál. Upozornění obsahuje textové pole, které obsahuje jméno souboru,

se kterým měla být podezřelá operace provedena. Dále obsahuje tři tlačítka:

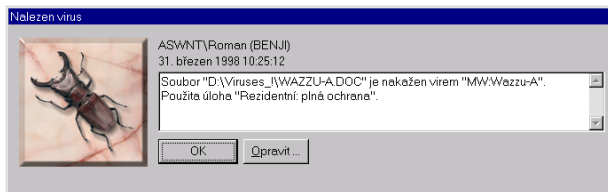


obr. 105

- klepnete-li na tlačítko „OK“, bude operace se souborem provedena. Další případné podezřelé operace se souborem budou také ohlášeny.
- tlačítko „OK & Ignorovat“ uvedenou operaci povolí, a program RGW32 až do svého ukončení a opětovného spuštění nebude uživateli hlásit žádné operace s uvedeným souborem.
- tlačítko „Storno“ sdělí programu, že provedení příslušné operace má potlačit. Po jeho stisku program provedení operace nedovolí, a samozřejmě ohlásí uživateli i každý další pokus o provedení nebezpečné operace s daným souborem.

## 9.2 Hlášení boot viru a viru ve spuštěném souboru nebo otevíraném dokumentu

Program RGW32 může také kontrolovat spuštěné programy, OLE dokumenty otevírané pomocí OLE funkcí a boot sektory vkládaných disket. Zmíněné činnosti bude program RGW32 provádět, jestliže byly zaškrtnuty na stránce „Činnost“ ([kapitola 4.4.2](#)).



obr. 106

Jestliže vložíte do mechaniky disketu, pak při prvním přístupu na ni program zkontroluje boot sektor, zda neobsahuje nějaký virus. Pokud jej nalezne, zobrazí varovné hlášení (obr. 106). S disketou můžete dále pracovat, protože aby se virus stal aktivním musí být nejprve spuštěn a k tomu u boot virů dochází pouze při zavádění systému. Varovné hlášení má za úkol Vás upozornit na číhající nebezpečí.

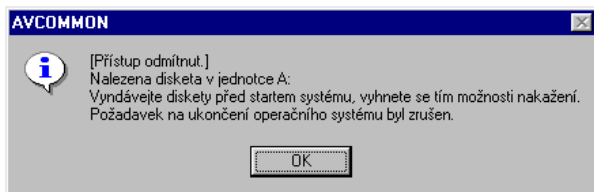
Varovné hlášení na obr. 106 se také zobrazí, byl-li v nějakém spustitelném programu objeven známý virus nebo se uživatel pokusil otevřít OLE dokument obsahující virus. Aby program RGW32 hlášení zobrazil, musí samozřejmě být spuštěna úloha obsahující činnost rezidentního sledování a musí být zvolena kontrola příslušných souborů.

Jestliže byl nalezen makrovirus v nějakém dokumentu, obsahuje hlášení tlačítko „Opravit“ (jako na obr. 106). Klepnutím na toto tlačítko zobrazíte dialog, který ukazuje [obr. 74](#), pomocí něhož můžete nalezený makrovirus z dokumentu odstranit.

Klepnete-li na tlačítko „OK“, můžete pokračovat v práci.

## 9.3 Hlášení přítomnosti diskety před ukončením systému

Je-li program RGW32 spuštěn při ukončování systému zkontroluje, zda jste nezapomněli v mechanice A disketu. Tímto způsobem se totiž viry velmi často dostávají do počítače. Pokud se v mechanice nalézá disketa, program zobrazí chybové hlášení (obr. 107) a proces ukončení operačního systému bude přerušeno. V opačném případě je systém ukončen zcela běžným způsobem.



*obr. 107*

Kontrolu přítomnosti diskety během ukončování operačního systému je možné vypnout - viz [kapitola 6.2](#), zaškrťovací pole „Netestovat disketu při ukončování práce OS“.

# 10. Program QUICK32

Program QUICK32 slouží, podobně jako programy AVAST32 a LGW32, k otestování souboru na přítomnost některého ze známých virů.

Je používán především pro kontrolu souboru vyvolanou přes místní nabídku např. v programu „Průzkumník“ (obr. 23). V jiných případech je daleko vhodnější použít program AVAST32 nebo LGW32.

Implicitně je program QUICK32 nastaven tak, aby otestoval všechny soubory na přítomnost všech virů. Zkomprimované soubory budou kontrolovány nejprve ve své komprimované podobě, potom budou vnitřně dekomprimovány a znovu zkontrolovány.

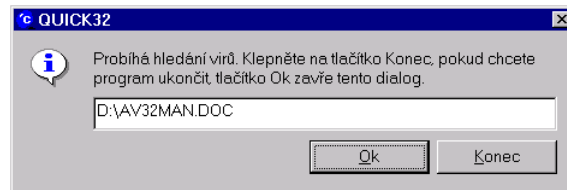
Příkazová řádka programu QUICK32 vypadá takto:

```
QUICK32 <jméno>
```

Parametr <jméno> udává jméno složky nebo souboru, který chceme zkontrolovat, včetně jeho cesty. V případě, že jako parametr byla programu předána složka, prohledány budou i všechny její podsložky.



obr. 108



obr. 109

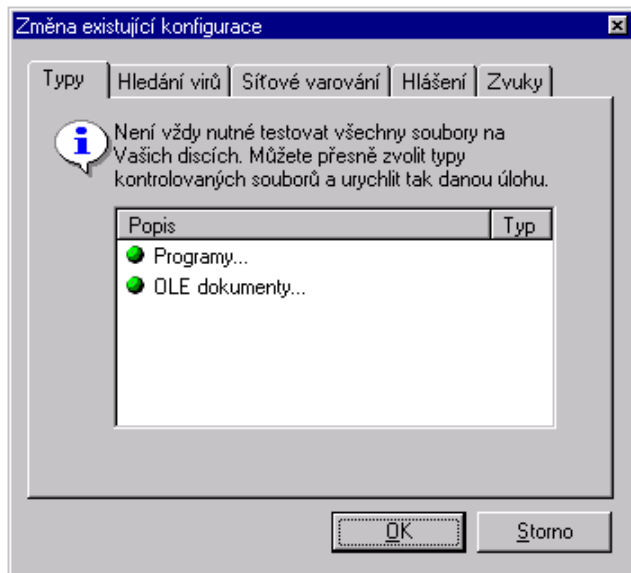
Program uživatele o svém běhu informuje malou ikonou v pravé části hlavního panelu (obr. 108). Po poklepání levým tlačítkem myši na tuto ikonu se objeví okno se jménem právě kontrolovaného souboru (obr. 109). Chcete-li činnost programu předčasně ukončit, stiskněte tlačítko „Konec“. Okno zavřete tlačítkem „OK“.

Jestliže program QUICK32 našel virus, informuje o tom uživatele varovným hlášením (obr. 24). Program však po nalezení a ohlášení prvního viru končí, takže pokud kontrolovaná složka obsahuje

více nakažených souborů, bude uživatel upozorněn pouze na první z nich!

Program QUICK32 navrácí žádné návratové kódy.

## 10.1 Nastavení programu QUICK32



obr. 110

Nastavit parametry programu QUICK32 je možné přes položku „Konfigurace Avast32“

v „Ovládacích panelech“ (viz. [kapitola 6.7](#)). Seznam na stránce „Úlohy“ pak obsahuje položku „Quick32“. Poklepaním levým tlačítkem myši na této položce (nebo výběrem položky „Změnit...“ z místní nabídky) je možné provést příslušná nastavení.

Okno, ve kterém se provádí změna nastavení programu QUICK32 (obr. 110), obsahuje záložkový seznam se stránkami ovládacích prvků:

- stránka „Typy“ umožňuje nastavit, které typy souborů mají být kontrolovány, a které mají být naopak ignorovány (viz [kapitola 4.4.4](#)),
- stránka „Hledání virů“ obsahuje ovládací prvky pro nastavení parametrů hledání virů. Prvky, jejichž nastavení nemá pro program Quick32 význam jsou šedivé a nelze je tudíž nastavit. Podrobně je stránka popsána v [kapitole 4.4.7](#),
- na stránce „Síťové varování“ je možné nastavit, že v případě nalezení viru bude poslána varovná zpráva i na další počítače (viz [kapitola 4.4.11](#)),
- text zprávy, která se zobrazí při nalezení viru obsahuje stránka „Hlášení“ (viz [kapitola 4.4.12](#)),
- stránka „Zvuky“ slouží k přiřazení zvukům jednotlivým událostem programu Avast32 (takovou událostí může být např. nalezení viru). Je podrobně popsána v [kapitole 4.4.13](#).

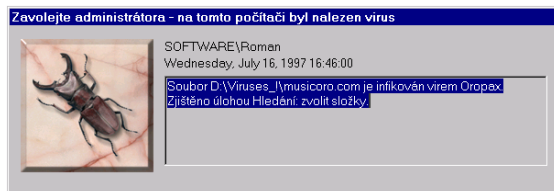
# 11. Program WARN32

Úkolem programu WARN32 je upozornit uživatele na skutečnost, že na daném počítači byl objeven virus. Je automaticky spouštěn po startu operačního systému, jestliže je povoleno zobrazování varovné zprávy (viz kapitola 6.5.1, zaškrtnuté pole „Zobrazovat hlášení o viru po přihlášení“).

Příkazová řádka programu vypadá takto:

WARN32

Jak je vidět, program pro své spuštění nepotřebuje žádné parametry a vzhledem ke své činnosti (viz dále) nevrací ani žádný návratový kód.



obr. 111

Po svém spuštění program nahlédne do registru operačního systému, zda nebyl na tomto počítači objeven nějaký virus (tuto informaci pro WARN32 do registru zaznamenávají programy AVAST32,

LGW32 a QUICK32). Pokud byl nějaký virus objeven, potom program zobrazí varovné hlášení (obr. 111), které se bude pohybovat po pracovní ploše. Varovné hlášení informuje uživatele o posledním nalezeném nakaženém souboru, dále pak o jménu viru, který soubor napadl a o jménu úlohy, která virus objevila.

Pokud nebyl objeven žádný virus, program se ukončí, aniž by o své činnosti dal nějakým způsobem vědět. Uživatel nemusí ani postřehnout, že byl spuštěn.

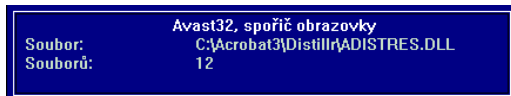
Jestliže program zobrazil varovné hlášení, pak jeho ukončení není jednoduchá záležitost. Z tohoto důvodu by běžný uživatel neměl program WARN32 sám spouštět (ostatně k tomu nemá ani žádný důvod).

Pokud se po přihlášení uživatele do systému objeví varovné hlášení, měl by to neprodleně ohlásit administrátorovi sítě nebo jiné odpovědné osobě!

Samotné odstranění hlášení programu WARN32 z pracovní plochy nestačí, je potřeba též zařídit, aby při dalším startu operačního systému již hlášení programu nebylo zobrazeno!

## 12. Spořič obrazovky

Součástí programu AVAST32 je i spořič obrazovky, který Vám umožní průběžně hledat viry ve chvíli, kdy je počítač nejméně vytížen, tj. když s ním právě nepracujete. Hledání virů probíhá na pozadí spořiče obrazovky, který si vybere uživatel, takže vzhled spořiče má uživatel plně pod kontrolou.



obr. 112

O průběhu testu je uživatel informován v okně pohybujícím po obrazovce (obr. 112). Obsahuje informace o právě testovaném souboru a o počtu již prohledaných souborů. V případě, že byl nalezen virus, je testování přerušeno, a v okně se objeví hlášení o nalezení viru.

Okno může mít několik barev. Máte-li nastaven režim obrazovky s nízkým počtem barev (méně než 65536), je pozadí bílé a text je černý - byl-li nalezen virus pozadí je černé a text bílý. Používáte-li režim s větším počtem barev pozadí bude text

bílý, pozadí pak modré nebo červené (jestliže byl nalezen virus).

Spořič obrazovky se přeruší naprosto běžným způsobem, tedy pohnutím myši, stiskem klávesy apod. Pouze v případě, že byl nalezen virus, bude po přerušení spořiče obrazovky zobrazeno hlášení, které je ukazuje [obr. 106](#).

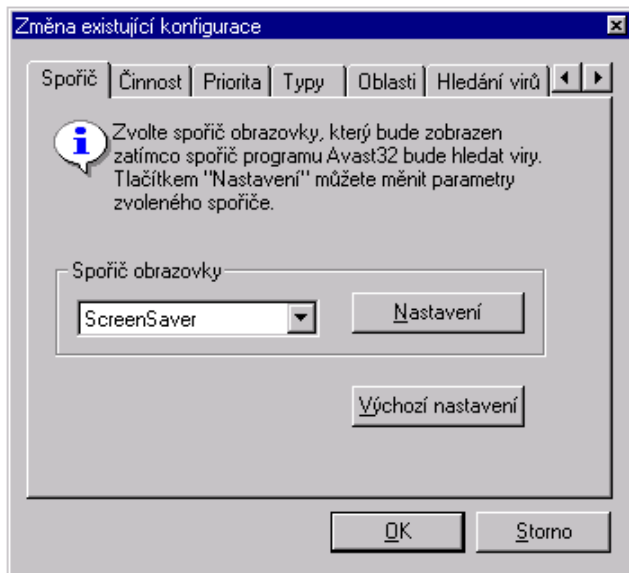
Chcete-li používat spořič obrazovky programu AVAST32, a nevíte jak sdělit operačnímu systému, že jej má používat, nahlédněte do [kapitoly 2.8](#).

### 12.1 Nastavení spořiče obrazovky

Nastavit parametry spořiče je možné přes položku „Konfigurace Avast32“ v „Ovládacích panelech“ (viz. [kapitola 6.7](#)). Seznam na stránce „Úlohy“ pak obsahuje položku „Spořič obrazovky“. Poklepáním levým tlačítkem myši na této položce (nebo výběrem položky „Změnit...“ z místní nabídky) je možné provést příslušná nastavení.

K nastavení spořiče obrazovky se také dostanete, poklepete-li na položce „Obrazovka“ v „Ovládacích panelech“. V dialogu, který se objeví, se přepněte na stránku „Spořič obrazovky“ ([obr. 29](#)) a klepněte na tlačítko „Nastavení“.





obr. 113

Okno, ve kterém se provádí změna nastavení šetřiče obrazovky (obr. 113), obsahuje záložkový seznam se stránkami ovládacích prvků:

- stránka „Spořič“ obsahuje základní ovládací prvky pro nastavení spořiče obrazovky - jejich podrobný je uveden v kapitole 12.1.1,
- stránka „Činnost“ slouží pro podrobnější nastavení činnosti, kterou bude spořič obrazovky provádět (viz kapitola 12.1.2).

Všechny následující stránky jsou přítomny pouze tehdy, je-li zaškrtnuto pole „Hledání virů“ na stránce „Činnost“ (viz kapitola 12.1.2).

- stránka „Priorita“ slouží pro nastavení priority testovacího vlákna (viz kapitola 4.4.3). Pro spořič obrazovky doporučujeme nastavit prioritu větší než u běžných úloh,
- stránka „Typy“ umožňuje nastavit, které typy souborů mají být kontrolovány, a které mají být naopak ignorovány (viz kapitola 4.4.4),
- stránka „Oblasti“ je určena pro nastavení oblastí, ve kterých bude spořič obrazovky hledat viry (viz kapitola 4.4.5),
- stránka „Hledání virů“ obsahuje ovládací prvky pro nastavení parametrů hledání virů. Prvky, jejichž nastavení nemá pro spořič obrazovky význam jsou šedivé a nelze je tudíž nastavit. Podrobně je stránka popsána v kapitole 4.4.7,
- na stránce „Síťové varování“ je možné nastavit, že v případě nalezení viru bude poslána varovná zpráva i na další počítače (viz kapitola 4.4.11),
- text zprávy, která se zobrazí při nalezení viru obsahuje stránka „Hlášení“ (viz kapitola 4.4.12),
- stránka „Zvuky“ slouží k přiřazení zvukům jednotlivým událostem programu Avast32 (takovou událostí může být např. nalezení viru). Je podrobně popsána v kapitole 4.4.13.

### 12.1.1 Stránka „Spořič“

Tato stránka obsahuje základní ovládací prvky pro nastavení spořiče obrazovky (obr. 113).

Kombinované pole v rámečku „Spořič obrazovky“ slouží pro výběr spořiče obrazovky, na jehož pozadí se budou hledat viry. Příslušný spořič vyberte ze seznamu, který se objeví po stisku šipky v pravé části pole. Jestliže nebyl zvolen žádný spořič nebo zvolený spořič je z nějakého důvodu nedosažitelný, program se pokusí najít nějaký jiný vhodný spořič obrazovky.

Tlačítko „Nastavení“ je určeno k nastavení parametrů šetřiče obrazovky, zvoleného ve výše popsaném kombinovaném poli. Jeho funkce tedy závisí na zvoleném spořiči.

Tlačítko „Výchozí nastavení“ umožňuje uživateli vrátit nastavení všech ovládacích prvků na všech stránkách do jejich implicitní polohy.

Stránka „Spořič“ je dosažitelná při jakémkoli nastavení šetřiče obrazovky.

### 12.1.2 Stránka „Činnost“

Stránka „Činnost“ slouží pro podrobnější nastavení činnosti, kterou bude spořič obrazovky provádět (obr. 114).



obr. 114

Zaškrávací pole „Hledání virů“ povoluje hledání virů spořičem programu AVAST32. Jestliže není pole zaškrtnuto, viry nebudou hledány. Implicitně je hledání virů povoleno.

Zaškrtnutím pole „Opakovat hledání“ způsobíte, že po prohledání všech zvolených oblastí (viz kapitola 4.4.5) se bude jejich prohledávání opakovat. Implicitně je pole zaškrtnuto.

Posuvník v rámečku „Rychlost pohybu okna“ umožňuje nastavit rychlost jakou se bude okno spořiče programu AVAST32 pohybovat po pracovní ploše. Implicitně je tato doba nastavena na 5 sekund.

# A. Implementace virových rutin

Informace uvedené v této příloze jsou určeny zejména uživatelům, kteří chtějí optimalizovat práci systému, ve kterém je program AVAST32 nasazen. Jsou zde uvedeny principy práce programu a zběžně popsány některé knihovny. Běžní uživatelé zde uvedené informace zřejmě nevyužijí.

## A.1 Obecné principy

Vzhledem k tomu, že antivirový balík AVAST32 obsahuje několik programů hledající viry, je vlastní testování implementováno jako samostatná část, která je z těchto programů volána. Tím je zabráněno opakování kódu a k němu náležejících dat, které by zbytečně prodlužovaly programy a zabíraly tak místo na Vašem pevném disku a v paměti počítače. Všechny programy, které potřebují zjistit, zda se někde nenachází virus používají stejný postup a stejné knihovny, což má za následek dramatické snížení požadavků na operační paměť počítače.

Také použití dat je optimalizováno. Jak již bylo uvedeno, veškerá data potřebná pro hledání virů jsou umístěna v souboru LGW.VPS. Tento soubor je již dost velký a špatná zpráva pro uživatele je, že vzhledem k neustále zvětšujícímu se počtu

virů, bude neustále narůstat. Pokud jste se do něj podívali, jeho obsah není na první pohled příliš smysluplný, ale pro správnou funkci programu je životně důležitý. Většina informací, které jsou v něm obsaženy, je statická. Může tedy být použita mnoha programy bez nebezpečí přepsání dynamických dat.

## A.2 Vlastní knihovny

Pro vlastní volání antivirových funkcí je použito několik knihoven. První z nich je knihovna AvMain.DLL, což je normální dynamická knihovna, známá již od verze Windows 3.x. Tato knihovna je mimo jiné použita pro inicializaci, „úklid“ a zobecnění volání antivirových služeb z různých druhů programů. Obecně lze říci, že tvoří obálku vlastní implementace.

Vlastní hledání virů se odehrává v knihovně Vps32s.DLL. Tato knihovna je implementována jako „InProc server“ pracující v „Apartment“ modelu práce. Jedná se o tzv. COM server, který se mapuje do adresového prostoru programu, který jej inicializuje. Pokud Vám výše uvedené informace zhola nic neříkají, vůbec nic se neděje a tuto kapitolu můžete s klidným svědomím přeskočit.

K vlastní práci používá tato knihovna ještě několik pomocných (Vps32a.DLL, Vps32e.DLL), ale ty vykonávají speciální činnosti, které nejsou v kontextu této kapitoly zajímavé.

Použitá implementace má jednu vlastnost, která Vám může připadat zajímavá a možná by jste ji rádi použili. COM servery mají totiž interface, který je viditelný zvnějšku v čitelném a srozumitelném tvaru. Tato skutečnost mnohdy svádí k jejich použití i jiným způsobem, než v programu, který je k tomu oprávněn. Rádi bychom Vás před tímto varovali! Máme k tomu dva důvody. Za prvé tento postup není v souladu s právním řádem a pokud to zjistíme, budeme nuceni obrátit se na naše právníky. Druhý, mnohem podstatnější důvod, je ten, že tyto funkce nejsou oficiálně dokumentovány a jejich použití Vám může způsobit **opravdové škody**. Pokud se spolehnete na současnou implementaci, můžete být v budoucnu opravdu nepříjemně překvapeni.

### **A.3 Optimalizace použití**

Ze způsobu implementace virových rutin přímo plyne možnost optimalizace jejich použití. Ve skutečnosti, každý program, který používá tyto funkce musí mít přístup ke všem datům, která jsou umístěna v souboru LGW.VPS. Tento soubor musí být před každým použitím zkontrolován, přečten a analyzován, což trvá relativně dlouho. Proto se

zmíněné operace provádí pouze tehdy, není-li již soubor LGW.VPS používán.

To znamená, že pokud je datový soubor používán jinými programy, pak spuštění dalšího programu z balíku AVAST32 bude rychlejší. K tomuto účelu také dodáváme program Vps32.EXE, který nemá za úkol nic jiného, než držet datový soubor virů v paměti a tím urychlovat jeho použití. Uvedenou vlastnost oceníte zejména v případě, že budete používat kontrolu souborů na Vašem počítači pomocí místní nabídky programu „Průzkumník“, kdy inicializace celého VPS souboru pro každý jednotlivý soubor může být frustrující.

Druhá strana tohoto urychlení je méně volně operační paměti ve Vašem počítači, a to i v době, kdy soubor LGW.VPS není využíván žádnou aplikací.

## B. Co s nalezeným virem

Jestliže Vám kterýkoli z programů z balíku AVAST32 ohlásil přítomnost viru, nemusí to vždy znamenat, že soubor je skutečně nakažen. Jak v takovémto případě postupovat, si popíšeme v následujících kapitolách. I zde však platí, že dále popisované operace by měl provádět uživatel, který má s operačními systémy Windows 95 a NT zkušenosti a ví, co se po provedení jednotlivých operací stane a jaké budou mít následky.

### B.1 Je to falešný poplach?

Před tím, než propadnete panice a začnete mazat detekované soubory, volat antivirovou službu nebo požádáte o časově neomezenou dovolenou, musíte zjistit, zda je detekovaný soubor opravdu napaden nebo zda se jedná o falešný poplach. Ten může být způsoben několika různými příčinami, například:

- poplach způsobený použitím dvou scannerů najednou (viz [příloha B.1.1](#)),
- poplach způsobený imunizací souborů (viz [příloha B.1.2](#)),
- poplach způsobený žertovnými programy (viz [příloha B.1.3](#)),

- poplach způsobený chybou techniky, programového vybavení nebo uživatele (viz [příloha B.1.4](#)),
- poplach způsobený principy práce Windows (viz [příloha B.1.5](#)).

AVAST32 je vytvářen se zřetelem na minimalizaci falešných poplachů. Pravidelné testování proti nim zahrnuje asi 4 GB (4096 MB) souborů různého původu a obsahu. Nicméně i přes takto důkladné testování se může stát, že některý programů z balíku poskytne falešné hlášení. Pokud se tak stane, prosíme, spojte se s námi. Pomůžete nám zlepšit náš produkt a Vy se budete moci cítit bezpečněji.

Pokud nebudete rozumět dalšímu výkladu této kapitoly, nic si z toho nedělejte. Zkušenost v práci s počítačem nepatří mezi vrozené vlastnosti. Pouze se v případě nalezení viru obraťte na skutečné odborníky.

#### B.1.1 Poplach způsobený použitím dvou scannerů virů najednou

Pokud používáte několik různých scannerů najednou nebo těsně po sobě, může se stát, že Vám některý z nich ohlásí virus v paměti. Důvod

pro toto hlášení je jednoduchý. Každý ze scannerů potřebuje alespoň na chvíli mít informace o virech nezakódované a přístupné v paměti. Pokud ve stejném okamžiku testuje tuto paměť jiný scanner nebo pokud je tato paměť přesunuta do virtuální paměti a později použita bez vyčištění, může se stát, že jsou tyto informace příčinou falešného poplachu.

Situace je jednodušší, pokud jsou tyto scannery napsány „špatně“, tzn. tak, že nečistí svou paměť. V tomto případě je velice pravděpodobné, že v paměti naleznete několik (např. 5 a více) různých druhů virů. V tomto případě je situace jasná, jde o falešný poplach.

Horší situace je v případě, že jsou scannery napsány „dobře“ a paměť si po sobě čistí. I v tomto případě se může stát, že naleznete virus v paměti.

Jak zjistit, zda se nejedná o falešný poplach? Je to dost snadné, ale možná časově náročné. Ukončete práci se všemi aplikacemi, ukončete operační systém a vypněte počítač síťovým vypínačem. Znovu jej zapněte a nastartujte operační systém. Spusťte scanner, který Vám hlásil přítomnost viru v paměti. Pokud jej opakovaně nehlásí, pokuste se reprodukovat práci (spouštění programů), kterou jste dělali před spouštěním scannerů a po chvíli znovu spusťte testování proti virům. Pokud ani

v tomto případě není nalezen virus v paměti, jedná se o falešný poplach.

AVAST32 důsledně čistí veškerou používanou paměť a co více, veškeré informace a vzorky virů uchovává pouze v kódovaném stavu. Pouze v okamžiku testování dekóduje informace o jednom viru a po použití tuto informaci smaže. To znamená, že v každém okamžiku může být v paměti maximálně jeden dekódovaný vzorek viru.

### B.1.2 Poplach způsobený imunizací

Existují antivirové prostředky, které nabízejí a pracují s funkcí, kterou nazýváme „**imunizace souborů**“ nebo s funkcí, která nabízí připojení kontrolního součtu k testovanému souboru. Při následujícím testování tyto prostředky jednoduše zkontrolují vloženou informaci s aktuálním stavem a na základě výsledku mohou oznámit podezření z napadení souboru virem. Tento proces je velice rychlý a poměrně jednoduchý pro implementaci.

Ovšem tento poměrně jednoduchý a rychlý proces s sebou nese několik zásadních problémů. Představte si dva produkty takto pracující používané pro testování jednoho souboru. Jejich střídavé používání se navzájem ruší a oba produkty budou hlásit, že soubor byl změněn.

Další problém je skutečnost, že pouhé otestování souboru jej fyzicky změní. Když pomineme problémy autorských práv originálních souborů, vyvstává zde otázka, zda si můžete být jisti, že změněný soubor bude i nadále pracovat tak, jak jeho originál. Pravděpodobně ano, ale existují programy, které se před spuštěním zkontrolují a nebudou pracovat v případě jakékoli změny. Navíc výše uvedené řádky platí pouze pro výkonné soubory. Jakákoli změna datových souborů s sebou nese vysoké riziko havárie programu, který tyto datové soubory používá.

Pokud si myslíte, že se viry nemohou šířit v datových souborech měli jste donedávna pravdu. Dnes již existuje speciální skupina virů („**Makroviry**“), které se šíří výhradně pomocí datových souborů.

**AVAST32 žádným způsobem nemodifikuje žádný testovaný soubor.** Z důvodů větší bezpečnosti jej dokonce otevírá pouze pro čtení, aby ani náhodou nemohlo dojít k jejich narušení. Pokud si některé součásti AVAST32 ukládají informace o souborech, dělají tak do samostatného souboru.

Pouze ve speciálním případě, a sice při odstraňování nalezených virů, jsou soubory zapisovány, ale i tak je tento proces prováděn na kopii souboru a až po úspěšném dokončení je opravený soubor zapsán s původním jménem.

### B.1.3 Poplach způsobený žertovnými programy

Pokud se Vám stane, že se počítač začne chovat nezvykle až podezřele, nemusí jít o virus. Může se jednat o „žertovný“ program, který Vám nainstaloval na počítač kolega, nebo který je Vám podstrčen s falešnou nebo zavádějící informací o jeho účelu. Příkladem může být instalace předvádění „lechtivých“ obrázků při startu počítače. Slabší povahy nebo méně zkušení uživatelé mohou mít problémy s uvedením do původního stavu a podobný „žert“ mohou považovat za působení zvláště zákeřného viru.

Nicméně nemusí to být pravda. A jak rozeznat „žert“ od opravdového viru? Může to být obtížné. Přesné hranice těchto dvou skupin není možné stanovit. Je zapotřebí vycházet z konkrétní situace. Například viry si nemohou dovolit předvádět nějaké grafické obrázky (navíc v barvách), protože ty jsou dost veliké. Nejdůležitější rozdíl, který ovšem není snadné rozeznat, je to, že se viry množí a „žerty“ ne.



### B.1.4 Poplach způsobený chybou techniky, programu nebo uživatele

Problémy s technikou, instalovanými programy nebo dalšími zařízeními mohou být snadno zaměněny s virovou nákazou. Například častými problémy, které bývají takto zaměňovány, jsou problémy s tiskem, či pevným diskem. Existuje ovšem velice málo virů, které mohou způsobovat tyto problémy.

Na druhou stranu rozlišit hlášení „Memory parity error“ může jenom odborník, protože toto hlášení může být způsobeno vadným paměťovým čipem ale také virem, který jej vypíše na obrazovku. Zde mohou pomoci jenom zkušenosti.

### B.1.5 Poplach způsobený principy operačních systémů Windows

Windows používají takový způsob správy paměti, který Vám umožňuje používat více paměti, než ve skutečnosti máte. To ovšem může způsobit falešný poplach, protože tzv. „signatury“ virů jsou přítomny v paměti „fyzické“ ovšem mohou se objevit i na disku v paměti „virtuální“. Pak se může stát, že najdete virus např. v souboru WIN386.SWP (v systému Windows NT je to soubor PAGEFILE.SYS). Stává se také dost často, že

„normální“ virus se najde v souboru .DOC. Také toto je falešný poplach, kterého se dá zbavit tak, že se soubor otevře ve Wordu, zvolí se „Ulož jako“ a uloží se pod stejným jménem. Pozor! Zde je nutno rozlišit, zda se nejedná o tzv. makrovirus.

## B.2 Je to opravdu virus!!!

Pravděpodobně první, co vás napadne, může být „Proč právě já?!“. Není to nic divného, velká většina uživatelů se již s virem setkala a nebezpečí nehrozí pouze počítačovým „poustevníkům“. Při troše štěstí nemusí nákaza způsobit velkou škodu. **Na druhé straně, štěstí více přejte připraveným!!!**

- První akce (viz [příloha B.2.1](#)),
- Jaký typ viru infikoval můj počítač?(viz [příloha B.3](#)),
- Kombinované (multipartitní) viry (viz [příloha B.3.1](#)),
- Viry, které zůstávají instalované v paměti (viz [příloha B.3.2](#)),
- Viry napadající soubory (viz [příloha B.3.3](#)),
- Viry napadající systémové oblasti disků (viz [příloha B.3.4](#)),
- Makroviry (viz [příloha B.3.5](#)).

### B.2.1 První akce

Základem je nepropadnout panice. Škoda, kterou virus mohl způsobit je zanedbatelná v po-

rovnání s tím, co můžete způsobit vlastní ukvapenou akcí.

Panika je Váš nepřítel. Pokud jste typ, který snadno panikaří, při nalezení viru nechte počítač na pokoji a běžte si dát šálek kávy. Pak zavolejte Vašeho administrátora. Uvidíte, že problém není až tak vážný.

Pokud chcete něco dělat bez pomoci druhých, klidně ukončete práci všech pracujících programů a uložte si svá data. Může se také stát, že musíte dokončit právě prováděný program. Nic se neděje, nechte jej dokončit, co je zapotřebí. Máte čas, jenom nepatrná část virů je závislá na čase, po který jsou aktivní. Vyvarujte se pouze spouštění dalších programů (pokud to jde). V žádném případě nevypínejte počítač síťovým vypínačem. Důsledky by mohly být pro Vaše data na pevném disku katastrofální.

Vypnutí počítače síťovým vypínačem bez předchozího ukončení práce operačního systému („shut down“) je nehezký zvyk, který se Vám zcela jistě vymstí.

Pokud se Vám povedlo ukončit operační systém, vypněte počítač síťovým vypínačem. Odpočiňte si, protože nastala doba přemýšlení, co dělat dále.

Tento čas je zapotřebí využít. Nepotřebujete se jenom zbavit viru, ale potřebujete přesně nebo alespoň s velkou pravděpodobností zjistit zdroj nákazy (pravděpodobně Váš přítel s nejnovější

verzí známé hry). Velice důležitou otázkou je, jak dlouho můžete mít virus v počítači.

Raději buďte pesimističtí, vyplatí se to. Podcenění této doby znamená udělat první krok k opakované infekci!!!

Neméně důležité je promyslet si, zda jste nemohl rozšířit virus dále. Je jedno, zda máte nakažen firemní počítač a Vaše firma rozeslala tisíce nakažených disket, nebo jste pouze věnoval novou verzi hry svému příteli. V obou případech je nejlepší ihned informovat všechny, kterých se může potenciální nákaza týkat. **Udělejte to teď!!!**

Ostuda spojená s rozšířením virové nákazy je mnohem snesitelnější, když na nebezpečí sami upozorníte. V případě firmy jde o důvěru zákazníků, kterou můžete úplně ztratit, pokud zjistí nákazu a zjistí, že jste o ní věděli a neinformovali je (možná si to můžete dovolit).

Jednou z nejdůležitějších věcí, které musíte posoudit je to, zda skutečně máte zálohovaná všechna důležitá data z infikovaného počítače.

Každé odstraňování viru s sebou nese riziko kompletní ztráty dat na vašich pevných discích i v případě, že odstraňování provádí vyškolený a velice zkušený odborník.

Je nám jasné, že o potřebě zálohovat dobře víte. Ale ruku na srdce, kdy naposled jste zálohovali? A pokud to děláte pravidelně, zkusil jste někdy obnovit uložená data nazpátek? A i když obě pod-

mínky splňujete, máte záložní kopii zálohovacího programu jinde než na infikovaném počítači? Co když se na ten počítač již více nedostanete?

Takže, pokud nemáte aktuální zálohu, teď právě je čas ji udělat. Již se nedá nic dělat a musíte ji vykonat s vědomím, že zálohovaná data mohou obsahovat virus a zároveň, že každé další spouštění počítače může zvyšovat stupeň infikování systému. Ale nedá se nic dělat. Záloha je opravdu zapotřebí i v případě, že další práci bude vykonávat někdo úplně jiný (hlavně někdo, kdo nenese žádnou odpovědnost za Vaše data).

Takže malé shrnutí. V případě nákazy virem:

- dokončete práci, zbytečně nespěchejte ale ani neotálejte s dalšími opatřeními,
- zjistěte co nejvíce informací o viru,
- ukončete práci operačního systému,
- vypněte počítač síťovým vypínačem,
- rozmyslete si, jak dlouho můžete mít počítač nakažen a odkud pravděpodobně nákaza přišla,
- informujte všechny, kterým jste mohl nakažená data nebo média rozeslat,
- pokud to je zapotřebí, data zazálohujte. Nenechávejte nic na náhodě!!!

Pokud jste splnil tyto body, můžete přistoupit k další práci. Zde musíte kriticky ohodnotit své vlastní schopnosti a zkušenosti s počítačem. Pokud počítačům moc nerozumíte, nedoporučujeme Vám odstranění viru provádět vlastními silami.

Pokud ale budete rozumět dalšímu výkladu, můžete to zkusit bez odborné pomoci. Jak na to? Na tuto otázku se pokusíme odpovědět.

Dejte si také pozor na různé „odborníky“. Pokud od nich např. uslyšíte výraz „low level format“, rychle utečte. Ve skutečnosti se snaží zničit Vás a Vaše data.

Pokud také pracujete ve větší firmě, kontaktujte jako prvního Vašeho administrátora, popř. člověka, majícího na starosti počítače.

### B.3 Jaký typ viru infikoval můj počítač?

Je důležité vědět, jaký typ viru je přítomen na Vašem počítači. Další postup na tom přímo závisí a zároveň některé jemné nuance určení typu viru mohou postup odstraňování virů zřetelně změnit.

Pokud se někomu bude zdát následující výklad málo odborný, je to způsobeno maximální snahou o zachování čitelnosti této kapitoly i pro ty uživatele, kteří se nesetkávají s viry pravidelně.

Takže základní typy virů jsou:

- kombinované (multipartitní viry),
- viry, které zůstávají instalované v paměti,
- viry napadající soubory,
- viry napadající systémové oblasti disků,
- makroviry.

Pokud narazíte na velice zřídka se vyskytující virus, který mění nebo modifikuje datové soubory, jiné než OLE dokumenty, máte pravděpodobně smůlu v tom, že tato data jsou velice nevěrohodná nebo přímo nepoužitelná. Zároveň neexistuje prostředek, jak zničené datové soubory opravit (snad kromě zálohy statických dat).

V dalším textu budeme předpokládat, že používáte operační systém Microsoft Windows 95 nebo Microsoft Windows NT. Odstraňování virů v systému MS-DOS se může lišit od zde uvedených postupů.

### **B.3.1 Kombinované (multipartitní) viry**

Kombinované viry jsou jednoduše viry, které napadají některou z kombinací souborů, systémových oblastí disků a paměti najednou. Jejich odstraňování je kombinací odstraňování jednoduchých typů virů v přesně určeném pořadí. Pro toto pořadí platí:

- není možné odstraňovat virus z disku, pokud je přítomen v paměti,
- při odstraňování virů z disků je zapotřebí odstranit viry ze systémových oblastí disků jako první,
- viry v jednotlivých souborech se odstraňují až jako poslední.

### **B.3.2 Viry zůstávající instalované v paměti**

Tyto viry nejsou instalované pouze v paměti, ale jistě jsou přítomny i někde na disku.

Pokud Vám některý „odborník“ bude tvrdit, že virus může být v paměti bez toho, aby byl přítomen někde jinde (na pevném disku, disketě nebo jiném médiu podobného typu), obraťte se na někoho jiného. Vaše data budou mnohem bezpečnější.

Virus může být v paměti a zároveň nebyť aktivní. Představte si situaci, že kopírujete infikovaný soubor z diskety na disketu. I v tomto případě je používaná operační paměť počítače a zdrojový i výsledný soubor jsou nahrány v ní. To znamená, že virus může v paměti existovat i po ukončení kopírování jednoduše proto, že není důvod, proč takto použitou paměť čistit. To ovšem neznamená, že virus v této podobě může jakkoli škodit.

Zároveň nemůžete odstraňovat virus z Vašeho systému v okamžiku, kdy je přítomen v operační paměti a je aktivní. Důvod je prostý, virus ihned napadne každý program nebo systémovou oblast disku, kterou se pokusíte vyléčit. S tím neuděláte nic. Obecně platí, že nemůžete eliminovat virus v paměti v době, kdy je v ní přítomen. Samoz-

řejmě, mohou existovat výjimky, ale na to se nemůžete spolehnout.

Zároveň musíme zdůraznit, že viry určené speciálně pro operační systémy Windows 95 a NT dnes prakticky neexistují a z těch několika velice řídkých případů žádný není schopen zůstat rezidentně v paměti. Pokud se situace změní, budeme vás o tom informovat.

Z předchozího odstavce vyplývá, že v paměti může být jenom virus určený pro systém MS-DOS, který se do ní dostal při startu počítače nebo při práci v DOSovém okně. Pokud se zároveň jedná o virus, napadající systémové oblasti disků, můžete přejít přímo ke kapitole o virech tohoto typu. Pokud jde o viry napadající soubory, řešení, jak odstranit virus z paměti, není složité.

Zavedte systém ze systémové diskety. V podstatě můžete použít libovolnou systémovou disketu od MS-DOSu 5.0 a výše. Ovšem doporučujeme Vám použít systémovou disketu pro systém, který máte nainstalován na počítači.

Pokračujte dále podle typu viru.

Pod operačním systémem Windows NT v podstatě není problém s viry v paměti. Jediné viry, které takto mohou tropit neplechu, jsou viry napadající systémové oblasti disku.

### B.3.3 Viry napadající soubory

Odstranění virů ze souborů je jednoduchá a dosti nezáživná práce. Hlavní problém spočívá v rozhodnutí, jak virus odstranit. Máte zase na výběr několik možností.

Stoprocentní obnovení zabezpečí pouze restaurování souborů ze záložních kopií (samozřejmě, pokud zálohu máte a pokud i tato záloha není napadená stejným nebo jiným typem virů). Obnova ze záložních kopií může být jednoduchá a spolehlivá. Pokud pravidelně věnujete čas zálohování, zjistíte, proč se to vyplatí. Práce je to rychlá a pohodlná.

Pokud používáte pravidelně program pro kontrolu integrity a máte k dispozici aktuální verzi databáze, máte také prakticky po starostech. AVAST32 umožní restaurovat soubory napadené prakticky všemi viry (přibližně 95 procent různých druhů virů). Spolehlivost obnovy je stejná jako v případě obnovy souborů ze záložních kopií, protože AVAST32 kontroluje, zda se mu povedlo soubor restaurovat do posledního bitu.

Pokud nic z výše uvedených odstavců nemůžete použít, začíná být situace vážnější. Stále ještě nemusíte přijít o žádné programy. Musíte ale mít k dispozici originální diskety nebo jejich kopie. Znamená to ovšem podstatně více práce, protože nakažené programy musíte odinstalovat a opa-

kovaně nainstalovat, což s sebou nese spoustu známých problémů s uchováním pracně vymyšlených úloh a konfigurací.

Deinstalace programů neznamená jejich prosté smazání z disku. Všechny „solidní“ programy pro operační systémy Windows 95 a NT (včetně programu AVAST32) mají schopnost deinstalace, která má na starost více než pouhé smazání souborů.

Pokud ani tento způsob nemůžete použít, máte problém. Opravdu velký problém, protože Vám doporučíme pouze smazání napadených souborů. Existuje sice ještě jedna potenciální varianta, kterou můžete použít, ale její výsledky mohou být dosti tristní. Jde o to, že se můžete pokusit o odstranění virů ze souborů pomocí některého jiného antivirového programu. Toto odstranění má jednu velkou nevýhodu. Nemůžete zjistit, zda je opravený soubor ve stejném stavu v jakém byl před napadením. To je také hlavní důvod, proč AVAST32 žádnou podobnou vlastnost neobsahuje.

### **B.3.4 Viry napadající systémové oblasti disků počítače**

Existuje obrovské množství virů schopných napadnout systémovou oblast pevných disků. Ovšem jen několik z nich je tzv. „kombinovaných virů“, které jsou schopny napadnout a šířit se

pomocí souborů. Proto s malou výhradou můžeme říci, že pokud jste našli virus v systémové oblasti některého disku, stalo se to tak, že jste se pokoušel nainstalovat počítač z diskety. Je jedno, zda se to povedlo nebo ne. Pokud byl na té disketě virus, napadl Váš počítač bez ohledu na to, jaký operační systém normálně používáte.

Je úplně zbytečné se domnívat nebo dokonce někoho přesvědčovat, že například virus „J&M“ neboli „JiMi“ se dostal do Vašeho počítače pouhým přečtením dat z diskety. Jednoduše to není pravda, ať již Vám to tvrdí kdokoli. Je to prostě nesmysl.

Výjimkou ovšem je například virus „OneHalf“, který se může šířit i pomocí souborů, což znamená, že spuštěním infikovaného souboru dojde k napadení počítače. Podobných virů je ovšem naprosté minimum.

Postup pro odstranění: nainstalovat systém ze systémové diskety a spuštění následujícího programu: `fdisk /MBR` příslušného operačního systému.

Je pouze důležité, aby tato disketa nebyla napadena virem. Po úspěšném provedení těchto příkazů bude virus ze systémových oblastí disku provozujícího Microsoft Windows 95 a NT odstraněn.

Pokud se Vám povede nainstalovat operační systém, máte prakticky vyhráno. Můžete použít

schopností obnovy operačního systému, které jsou v něm zabudovány a ty se postarají o zbytek. Pokud ovšem nenastartujete systém vůbec, je zle.

### **B.3.5 Makroviry**

Jedná se o viry, které se šíří dokumenty. Tyto viry jsou v současné době jedny z nejrozšířenějších virů ve světě a tento trend se pomalu přenáší i k nám. Nejčastěji napadají dokumenty aplikace Microsoft Word, ale poslední dobou již přecházejí i na jiné kancelářské aplikace.

Odstranění se dá provést rovnou z prostředí AVAST32 (viz [kapitola 5.3.2](#)). Stejně ovšem doporučujeme, abyste si zavirované dokumenty někam zazálohovali, originály odvirovali a pak otestovali jejich čitelnost ve Vašich programech. Pokud budou takto odvirované dokumenty v pořádku, je možno smazat jejich zavirované zálohy. Pokud ne, kontaktujte pracovníky naší firmy.

Algoritmy používané programem AVAST32 na vyhledávání a následné odstraňování makrovirů z OLE dokumentů, patří v současné době ke světové špičce, takže Vaše dokumenty budou opravdu v těch správných rukou.

## C.Implicitní nastavení nové úlohy

### Stránka „Jméno“

Textové pole pro zadání jména úlohy obsahuje text „(nespecifikováno)“. Nová úloha je implicitně privátní.

### Stránka „Činnost“

Z nerezidentních činností je zvolena pouze činnost „Hledání virů“. „Testování integrity“ ani „Zjednodušené testování integrity“ zvoleno není. Z rezidentních činností není zaškrtnuta žádná.

### Stránka „Priorita“

Priorita úlohy je nastavena na hodnotu nižší, než je priorita prostředí programu AVAST32.

### Stránka „Typy“

Pro novou úlohu je nastavena kontrola programů (resp. spustitelných souborů) a OLE dokumentů.

### Stránka „Oblasti“

Implicitně je nastavena kontrola všech lokálních pevných disků, tedy všech pevných disků, nainstalovaných přímo ve Vašem počítači. Kontrolovány budou i jejich vnořené složky.

### Stránka „Společné“

Žádné z polí na této stránce není zatrženo, tzn. že nová úloha bude spouštěna přímo uživatelem, program AVAST32 nebude ukončen zároveň s poslední úlohou a externím programům se bude hlásit pouze první virus nalezený úlohou.

### Stránka „Hledání“

Zaškrtnuta jsou pole „Testovat operační paměť“ (pole je viditelné pouze pod Windows 95), „Ignorovat charakteristiku virů“ a „Testovat komprimované soubory“.

Úloha bude pod operačním systémem Windows 95 testovat operační paměť, bude ignorovat charakteristiku virů, bude testovat celé soubory a komprimované soubory zkontroluje jak zkomprimované, tak dekomprimované. Pokud nenajde žádný virus, nezobrazí ani žádné hlášení.

Z přepínačů je implicitně zvolen přepínač „Hlásit všechny objevené viry“.

### Stránka „Integrita“

Na této stránce je zaškrtnuto pouze pole „Ignorovat atribut ARCHIVE“. Test integrity dat bude tedy u kontrolovaných souborů ignorovat atribut



ARCHIVE, a bude pokaždé testovat obsah souborů.

#### **Stránka „Pokračuj“**

V textové pole „Jméno úlohy“ je prázdné; po skončení této úlohy nebude již spouštěna další.

#### **Stránka „Zpráva“**

Pole „Vytvářet soubor se zprávou“ není zaškrtnuté, textové pole „Jméno a cesta souboru“ obsahuje „\*“ (hvězdičku) a pole „Přepsat existující zprávu“ zatrženo není. Nová úloha nebude tedy vytvářet zprávu o své činnosti.

#### **Stránka „Sítové varování“**

Pole „Posílat hlášení po síti“ není zaškrtnuté, takže posílání zpráv po síti není povoleno a nastavení ostatních ovládacích prvků na této stránce je ignorováno. Zvolen je přepínač „Posílat hlášení pouze na vybrané počítače“. Seznam počítačů na této stránce je implicitně prázdný.

#### **Stránka „Hlášení“**

Textové pole pro text hlášení implicitně obsahuje následující text:

Soubor %1 je infikován virem %2.

#### **Stránka „Zvuky“**

Tato stránka neobsahuje žádné ovládací prvky.

#### **Stránka „Sledování“**

Pole „OLE dokumenty“, „16-bitové aplikace Windows“ a „aplikace MS-DOSu“ jsou zaškrtnuty, takže sledovány budou veškeré aplikace běžící na Vašem počítači. Z přepínačů je zvolen přepínač „Prohledávat vše kromě systémových knihoven“.

#### **Stránka „Rezidentní bloky“**

Pole „Souborové operace MS-DOSu“ a „Souborové operace Windows“ jsou zaškrtnuta. Ve Windows 95 pole „Formátování“ zaškrtnuto není. Budou tedy sledovány všechny operace, kromě formátování.

#### **Stránka „Ignoruj“**

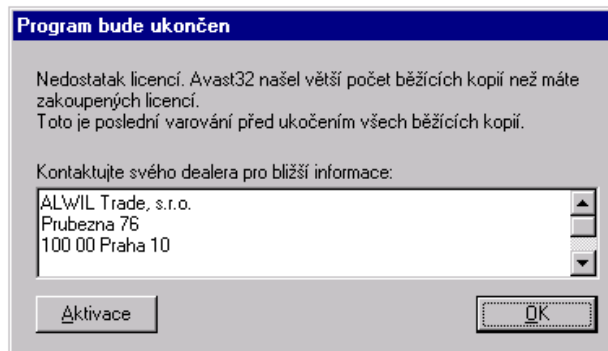
Seznam souborů na této stránce je implicitně prázdný. Budou tedy sledovány podezřelé operace se všemi soubory na Vašem počítači.

## D.Popis aktivačního klíče a licencí

Aktivační klíč je posloupnost znaků ve tvaru AABBB.CDDDDDD-EEEEEE. První část obsahuje identifikaci programu, část BBB určuje číslo verze programu a položka C je znak určující počet dostupných licencí. Je-li zde písmeno „A“, pak je zakoupena pouze jediná licence, je-li zde „B“, pak jsou zakoupeny dvě licence atd. DDDDDD určuje sériové číslo kopie programu a EEEEEEE je kód, kterým se ověřuje pravost celého aktivačního klíče.

Program AVAST32 si hlídá počet momentálně spuštěných kopií v síti. Pokud máte zakoupeno méně než deset licencí, dovolí Vám program spustit vždy o jednu kopii více, než je počet zakoupených licencí. Máte-li zakoupeno alespoň deset licencí, budete moci spustit o dvě kopie programu AVAST32 více, než jste zakoupili licencí.

Na skutečnost, že uživatel spustil více kopií programu než je počet zakoupených licencí, bude upozorněn varovným hlášením (obr. 115). Klepnutím na tlačítko „Aktivace“ zobrazíte dialog, který Vám umožní aktivační klíč změnit (viz kapitola 6.4). Tlačítkem „OK“ dialog ukončíte.



obr. 115

Pokud i přes toto hlášení se pokusí uživatelé spustit další kopie programu AVAST32, budou ukončeny všechny jeho dosud běžící kopie.

Chcete-li zjistit, na kterých počítačích ve Vaší síti běží program AVAST32 s Vaším aktivačním klíčem, klepněte pravým tlačítkem myši na třetí položce stavového řádku v hlavním okně programu AVAST32 (položka obsahuje informaci o dostupných a momentálně používaných licencích).

## E. Síťové vlastnosti a podpora

Program AVAST32 samozřejmě podporuje práci v síti, která je dnes naprosto běžným vybavením řady pracovišť.

AVAST32 umožňuje při nalezení viru zaslat zprávu kterémukoli připojenému uživateli, nejčastěji zřejmě administrátorovi sítě, nebo jiné odpovědné osobě. Program AVAST32 pro tuto činnost používá služeb, které mu poskytují operační systémy Windows, takže není potřeba žádná dodatečná konfigurace.

Při práci v síti je potřeba dodržovat licenční ujednání. Program AVAST32 hlídá počet běžících kopií programu, aby jejich počet nepřesáhl počet zakoupených licencí. Bližší informace v [příloze D](#).

Na síti bývá problémem udržet všechny používané programy v dostatečně aktuální verzi, u antivirových programů to platí dvojnásob. Aby administrátor sítě nemusel aktualizovat databázi virů na každém počítači zvlášť, je do programu AVAST32 zabudována automatizace této činnosti.

Vše, co je potřeba učinit, je vytvořit složku, ze které by mohli číst všichni uživatelé sítě. Tuto složku pak zadat programu AVAST32 jako složku, která má být použita pro automatickou aktualizaci

souboru VPS ([kapitola 6.6](#), textové pole „Cesta pro aktualizaci“) a samozřejmě povolit vlastní automatickou aktualizaci ([kapitola 6.1.2](#), zaškrtačkové pole „Automaticky aktualizovat VPS“).

Potom stačí každou novou aktualizaci souboru VPS (tzv. malá aktualizace) zkopírovat do vytvořené složky, a aktualizace se provede automaticky po celé síti. Program AVAST32 totiž po svém startu zkontroluje, zda zvolená složka neobsahuje novější soubor VPS. Jestliže jej obsahuje, potom svůj dosavadní soubor VPS odstraní a nahradí jej novějším.

# F.Vlastnosti pro programátory

AVAST32 je orientován hlavně uživatelským směrem, má však i několik vlastností, které využijí zejména programátoři. Nejdůležitější z nich je popsána v následující kapitole.

Jestliže kdekoli v programu AVAST32 zadáváte cestu, může jméno obsahovat i jméno systémové proměnné, uzavřené mezi dva znaky „%“ (procento). Na kořenovou složku systému se tedy lze odkázat např. takto „%SystemRoot%“. Jestliže systémová proměnná uvedeného jména neexistuje, pak bude tato část cesty ignorována.

## F.1 Posílání zpráv o nalezených virech

Program AVAST32 disponuje mechanismem, který umožňuje informovat externí programy o nalezených virech. K tomuto účelu byla zřízena schránka jménem

„\\.\mailslots\AVAST32\VIRUSFOUND“, do které jsou zapisovány informace o prvním viru nalezeném rezidentním programem a informace o všech virech nalezených rezidentními programy. Je možné nastavit, aby do schránky byly posílány

informace o všech nalezených virech ([kapitola 4.4.6](#)).

Zpráva o nalezeném viru obsahuje jméno domény, počítače, uživatele, nakaženého souboru a viru, který soubor napadl. Údaje jsou do schránky zapsány ve formátu řetězce, vzájemně oddělené nulovým znakem.

# Rejstřík

## A

- Acrobat Reader 34, 84, 85
  - instalace 9
- administrátor 29, 63, 119, 130, 131, 139
  - instalace 17, 18
  - práva 8, 17
- aktivační klíč 13, 16, 138
  - změna 99
- ALWIL Software 6, 12, 20, 71
- ALWIL Trade 6, 7, 17, 20
- AVAST32 20, 39
  - deinstalace. *Viz* deinstalace
  - informace 71
  - instalace 8, 17
    - administrátorská. *Viz* administrátor: instalace
    - problémy 16
    - průběh 10
    - příprava 8
    - spuštění 9
  - licence. *Viz* licence
  - logování. *Viz* logování
  - optimalizace 125
  - požadavky na systém 7
  - spuštění 21, 90

- ukončení 55, 73, 90
- verze 8, 70, 71, 138
- vlastnosti 33, 140
  - síťové. *Viz* síťové: vlastnosti
- základní funkce 33, 34
- zástupce 21, 22
- AVAST32.CNF 18, 94
- AVS 7, 20

## B

- boot sektor 28, 35, 36, 40, 76, 83, 114, 115
  - sledování 36, 50
- boot viry 134
  - hlášení. *Viz* hlášení: boot viru

## C

- CD-ROM 8, 9, 17, 20, 103

## D

- databázový server 102
- deinstalace 8, 18, 19, 134
- dialog
  - opravení souboru 79
  - otevírání souboru 94
  - přesunutí/přejmenování souboru 80

seznam typů 52  
 smazání souboru 81  
 vybrání oblastí 54, 87  
 zadání hesla 92, 93  
 změna přípony 94  
 změna souboru 79  
 Diet 57  
 disketa  
     26, 28, 39, 40, 54, 114, 115, 132, 133, 134  
 dodávané úlohy 39

## E

Excel 26, 35  
 externí programy 56, 140

## F

falešný poplach 102, 126, 127, 129  
 formátovací značky 64

## H

heslo 92  
     změna 93  
 hlášení  
     boot viru 115  
     nebezpečných operací 114  
     viru 115  
 hledání virů 34, 39, 49, 69, 124  
 implementace 124  
 nastavení 56

výsledky 76

## I

Ice 57  
 ikona  
     kulička 53, 54, 72, 77, 101  
     mínus 77  
     otazník 77  
     plus 77  
     vykřičník 77  
 instalace  
     Acrobat Reader. *Viz* Acrobat Reader: Instalace  
     AVAST32. *Viz* AVAST32: Instalace

## K

klávesnice 7, 41, 42, 43, 54  
 komprimační programy 57  
 kontrola. *Viz* test  
 koš 17, 77, 82, 108

## L

LGW32 110  
 LGW.VPS. *Viz* soubor VPS  
 licence 12, 99, 138  
 logování 90  
     velikost souboru 94  
 Lzexe 57

## M

makroviry 26, 66, 80, 83, 112, 115, 128, 135  
malá aktualizace 20  
Micronic 7  
Microsoft Mail 61  
Microsoft Outlook 63  
místní nabídka 42, 43  
jednoduché ovládání 73  
Průzkumník 26, 117  
stránka  
„Oblasti“ 54  
„Typy“ 52  
„Úlohy“ 74  
„Výsledky“ 78  
MS-DOS 66, 67, 133

## N

nabídka. *Viz* místní nabídka  
nápověda 73, 76, 84, 91  
LGW32 111  
ovládání 85  
plovoucí 84, 91  
nastavení programu 89  
Ovládací panely 103  
položka „Hlavní konzole“ 89  
stránka „Rozšíření“ 91  
stránka „Soubory“ 93  
stránka „Varování“ 95

stránka „Základní“ 89  
položka „Licence“ 99  
položka „Obnova VPS ...“ 103  
položka „Rezidentní ochrana“ 97  
položka „Společné“ 100  
stránka „Databázový server“ 102  
stránka „Jazyk“ 101  
stránka „Testovací server“ 102  
stránka „Základní“ 100  
položka „Znakový scanner“ 98  
zvuky. *Viz* zvuky

## O

OLE dokumenty 52, 66, 80, 112, 115  
Ovládací panely 9, 18, 63, 103  
ovládání 36, 41, 45, 70  
jednoduché 36, 72  
přepnutí 25, 70  
rozšířené 25, 36, 73  
stránka „Nápověda“ 84  
stránka „Úlohy“ 73  
stránka „Viry“ 82  
stránka „Výsledky“ 76

## P

pevné disky 23, 39, 54  
Pklite 57  
pracovní plocha 21, 22, 29, 75, 84  
průvodce 46, 47, 48, 91

Průzkumník 22, 26, 117

První kroky 21

Přidat nebo ubrat programy 10, 18

příkazový řádek 110

## Q

QUICK32 117

nastavení 118

## R

README.TXT 12

rezidentní bloky 35, 50, 53, 67, 68

rezidentní sledování 50, 65, 115

RGW32 113

nastavení 97

## S

seznam

oblastí 54

počítačů 61, 96

souborů 68

typů 52, 94

úloh 59, 72, 73, 105

síťové

disky 54

varování 60

vlastnosti 139

sloupec

„Atributy“ 78

„Infekce“ 78

„Obsah“ 78

služby

„Alerter“ 63

„Messenger“ 63

soubor VPS 20, 102

aktualizace 103

automatická 92

soubory

akceptování 79

atributy 40, 49, 78, 79

ARCHIVE 58

blokované 77, 82

dlouhá jména 34

nové 77, 108

oprava 79, 87

přejmenování/přesunutí 80, 87

smazané 77, 109

smazání 81, 87

stav 79

typy 51, 111

změna 94

změněné 79, 108

spořič obrazovky 30, 34, 120

nastavení 120

stavový řádek 70

stránka

„Činnost“ 49

„Hlášení“ 63



„Hledání“ 56  
 „Ignorovat“ 68  
 „Integrita“ 58  
 „Jméno“ 48  
 „Oblasti“ 53  
 „Pokračuj“ 59  
 „Priorita“ 50  
 „Rezidentní bloky“ 67  
 „Síťové varování“ 60  
 „Sledování“ 65  
 „Společné“ 55  
 „Typy“ 51  
 „Zpráva“ 60  
 „Zvuky“ 64  
 stromová struktura 42

## T

technická podpora 71, 84  
 test  
   celých souborů 57, 111  
   komprimovaných souborů 57, 111  
   obsahu souborů 59  
   paměti 24, 39, 56, 111, 127  
 test integrity 27, 35, 40, 49, 69, 77, 80, 133  
   hlášení 90  
   nastavení 58  
   výsledky 76, 108  
   vytvoření databáze 23

## U

úloha 38, 44, 47  
   činnost 48, 49  
   Hledání virů + test integrity 23, 24, 41  
   Hledání: disketa A: 28, 39  
   Hledání: lokální pevné disky 25, 39  
   Hledání: zvolit složky 39  
   implicitní nastavení 136  
   Integrita: lokální pevné disky 27, 80  
   Integrita: zvolit složky 40  
   konfigurace 48  
   odstranění 75, 106  
   pouze pro čtení 39, 72, 91  
   pozastavení 72, 73  
   priorita 50  
   privátní 39, 45, 49  
   průběh 60, 111  
   Quick32 118  
   Rezidentní: plná ochrana 28, 40  
   sdílená 39, 45, 49  
     ochrana 92  
   spuštění 55, 59, 72, 73  
   stav 74  
   Šetříč obrazovky 120  
   ukončení 72, 73, 75  
   výsledky. Viz výsledky  
   vytvoření 44, 69, 75, 106  
     kopie 75, 106

zástupce 29, 73, 75  
 změna 75, 106  
 úvodní okno 90

## V

viry 82, 129  
   hlášení 56  
   hlášení o nalezení 63, 86  
   charakteristika 56, 83  
   kombinované 132  
   nalezení 57, 63, 107, 126, 140  
   napadající soubory 133  
   rezidentní 132  
   typy 131  
 výměnné disky 54  
 výsledky 76  
   interpretace 107  
 vytvoření zástupce  
   AVAST32. *Viz* AVAST32: zástupce  
   úlohy. *Viz* úloha: vytvoření zástupce

## W

WARN32 119  
 Windows 66, 67, 129, 133  
   Windows NT 8, 17, 56, 63, 68, 90  
     3.51 21, 52, 55, 62, 69, 82  
   Windows 95 30, 67, 90, 94  
 Word 26, 35  
 WWW 20, 71

## Z

záložkový seznam 41, 46  
 zástupné znaky 52, 55, 69  
 zjednodušené testování integrity 49  
 zvuky 64, 106, 112

## Symboly

80386 7