



## Fguard pro Windows

Fguard pro Windows je jeden z antivirových programů firmy [ALWIL Software](#), který je určen pro hlídání systému Windows 3.1 a novější v reálném čase.

Program řeší jeden z nejkritičtějších problémů Windows, tzn. ochranu systému proti neočekávaným nebo neoprávněným projevům činnosti virů nebo uživatele. Jedná se o jedinečný program, který je schopen řešit i takové problémy, jako je ochrana proti systému při pokusu o formátování disku, pokusy o čtení tabulky rozdělení pevných disků a mnohé jiné kritické činnosti, které jiné antivirové systémy v oblasti Windows neberou v úvahu.

### Základní informace

- [Instalace programu](#)
- [Princip práce](#)
- [Parametry programu](#)
- [Ovládání programu](#)

### Historie

- [Verze 7.70](#)
- [Verze 7.50](#)
- [Verze 7.0](#)
- [Změny proti starším verzím](#)
- [Původ programu](#)

### Přílohy

- [Likvidace virů](#)
- [Požadavky pro práci](#)
- [Chyby a fatální chyby](#)



## **Instalace programu**

Program se instaluje v průběhu instalace systému AVAST!. Jeho samostatná instalace není možná z důvodů komprimace jednotlivých souborů na distribučních disketách.

Instalace samotná probíhá ve dvou krocích. První z nich je program pracující v DOSu, který instaluje programy pracující v systému DOS. Po kladné odpovědi na dotaz, zda chcete instalovat i programy pro Windows, se instalují i soubory, které jsou nutné pro dokončení instalace v systému Windows.

Vlastní instalace v systému Windows spočívá ve spuštění instalačního programu SETUP.EXE, který je standardní součástí dodávky a je připraven po instalaci systému AVAST! pro DOS.

V této části instalace bude program Fguard pro Windows zařazen do skupiny AVAST!, která je automaticky vytvořena, a do startovací skupiny Windows.



## Princip práce

Program Fguard pro Windows z uživatelského hlediska pracuje stejně, jako program [Fguard pro DOS](#). Jeho interní činnost je však od programu pro DOS úplně odlišná.

Fguard pro Windows není ve skutečnosti pouze jeden program. Je to označení pro několik souborů a částí kódu, které spolu komunikují a jsou na sobě plně závislé.

Na straně operačního systému DOS jsou to programy [Fguard](#) a [Rguard](#), které obsahují některé části kódu nutné pro správnou inicializaci a vzájemnou komunikaci obou systémů. Střední článkem tvoří soubor AVAST.386, 32 bitový program, který plní funkce spojení mezi operačními systémy a v některých případech vypisuje hlášení o prováděné operaci. Poslední částí je program FGW.EXE, 16-bitový program pro systém Windows, který má na starosti komunikaci s uživatelem prostřednictvím standardního rozhraní systému. Svou roli hraje i dynamická knihovna FGWLIB.DLL, která obsahuje správu některých přerušování a rutiny, které musejí být neustále v paměti.

Fguard pro Windows pro svou práci vyžaduje přítomnost rezidentních programů v paměti před spuštěním systému Windows. Podle toho, co chcete v systému chránit, to musí být [Fguard](#) nebo [Rguard](#) nebo oba společně.

Veškerou ochranu v systému Windows 3.x mají na starosti programy pracující v DOSu. Tato skutečnost vyplývá ze skutečnosti, že Windows 3.x prakticky úplně závisí na systému souborů DOSu. Všechny ostatní uvedené programy slouží pro rychlé a bezpečné přenesení informace do Windows, zobrazení zprávy a odeslání odpovědi nazpátek programu v DOSu.

- [Spouštění programu](#)
- [Spouštění systému Windows](#)
- [Ukončení programu](#)
- [Spolupráce se systémem DOS](#)



## Spouštění programu

Fguard pro Windows je standardní program systému Windows, který je možné spustit jako každý jiný program určený pro toto prostředí. Pokud se ho pokusíte spustit z DOSu, program vypíše hlavičku a informuje Vás o této skutečnosti.

Při spuštění programu byste měl mít v DOSu instalovaný program [Fguard pro DOS](#), [Rguard pro DOS](#) nebo oba společně, jinak Fguard pro Windows vypíše chybové hlášení a ukončí svou práci. Všechny tyto programy musí mít stejné číslo verze, jinak se program neodstartuje.

Pokud chcete používat tuto nápovědu, musíte mít příslušný soubor nápovědy (FGW.HLP) umístěn ve stejném adresáři jako vlastní program. Pokud používáte instalační program, nemusíte se o tuto podmínku starat, všechny soubory se nainstalují do jednoho adresáře.

Program Fguard pro Windows Vám doporučujeme spustit automaticky se startem systému Windows, což zaručí správnou funkci programu [Fguard](#) a [Rguard](#) i se systémem Windows a znemožní zablokování systému a z toho vyplývající ztrátu dat.



## Spouštění systému Windows

Soubory programu Fguard pro Windows nijak neovlivňují spuštění systému Windows ve standardním a reálném režimu práce a není je možné v těchto režimech vůbec použít. Soubor AVAST.386 není vůbec systémem rozeznáván jako součást Windows a program FGW.EXE při startu testuje konfiguraci systému a v těchto režimech odmítne pracovat.

Pro rozšířený režim je nutné dodržet několik podmínek. Pokud máte v paměti DOSu instalován program [Fguard](#), [Rguard](#) nebo oba společně je nutné je mít ve stejném adresáři a v něm mít taky soubor AVAST.386. Pokud tomu tak není, jeden z programu vypíše varovné hlášení a Windows nebudou v rozšířeném režimu spuštěny. Program Fguard pro Windows je možné umístit do libovolného adresáře. Je ho možné spustit jenom za předpokladu, že Windows pracují v rozšířeném režimu a při startu Windows byl úspěšně instalován program AVAST.386.



## Ukonèení programu

Fguard pro Windows mùžete ukonèit jako každý jiný program v systému Windows. Jelokož se tento program skládá ze dvou èástí a dùležitìjší z nich, soubor AVAST.386, zùstává v pamìti po celou dobu práce systému je po ukonèení programu Váš poèítaè stále stoprocentnì chránìn. Není-li však systém instalován kompletnì, ztrácíte:

- Možnost interaktivní zmìny konfigurace ochrany poèítaèe,
- Grafický režim zobrazování varovných hlášení. Veškerá varování budou zobrazována v textovém režimu (stejný režim používají kritická varování systému Windows, napøíklad pro varování pøed resetováním poèítaèe z klávesnice),
- Možnost testování spouštìných programù na pøítomnost virù.

Všechny ostatní parametry ochrany zùstávají zachovány. Pro správnou funkci programu Vám doporuèujeme nechat program pracovat po celou dobu práce Windows.



## Spolupráce se systémem DOS

Antivirová ochrana zajiřovaná programem Fguard pro Windows používá pro svou práci stejná data jako systém DOS. Toto řešení má své výhody i nevýhody. Výhodou je, že v každém okamžiku jsou konfigurační data jednoznačně určena a systém není v žádném okamžiku zbaven kontroly. Uživatel rovněž ví, že se změnami operačního systému zůstávají všechny parametry ochrany nezmeněny.

Na tyto skutečnosti se však můžeme podívat i z opačného hlediska. Nikdy může být výhodné mít jinou konfiguraci pro DOS a jinou pro Windows. Tato koncepce však se sebou nese vysoký stupeň nekonzistence. Pokud při práci ve Windows nepočítáme se spuštěním aplikací DOSu, je řešení velice jednoduché. Stačí při spuštění Windows nahradit konfigurační data DOSu daty pro systém Windows a problém by byl vyřešen. Co však dělat, pokud chceme spustit jednu aplikaci DOSu? Musíme zajistit, aby jeden program, který je instalován před spuštěním Windows, měl zároveň k dispozici dvě sady konfiguračních dat a zároveň v reálném čase zjiřovat, která data mají být použita bez jakékoli znalosti přičiny (Windows nebo DOS), která reakci programu vyvolala a to všechno ještě například v přerušení BIOSu při pokusu o formátování disku. Řešení není triviální a situace není ještě stále tak jednoduchá. Aplikací DOSu může být spuštěno více a každá z nich může měnit konfiguraci rezidentních programů podle své libovůle (přesněji dle libovůle uživatele).

Z těchto důvodů jsme si vybrali první řešení a všechny aplikace ([Fguard](#), [Rguard](#), FGW i AVAST.386) pracují se stejnými daty. Každá změna konfiguračních dat se promítá do obou prostředí. Vlastní změna konfiguračních dat je okamžitá, bez ohledu na to, ze kterého prostředí ji uskutečníme. Na druhou stranu může nějakou dobu trvat, než se změna dat uskuteční v DOSu "vizuálně" promítne do systému Windows. Tato prodleva je způsobena charakterem systému Windows, který je víceúlohový a není možné zaručit okamžitě zpracování zprávy ze systému DOS do systému Windows (obecně vzato žádné zprávy). Změna se "vizuálně" projeví za několik okamžiků i když vlastní změna dat a tím pádem i ochrana je provedena okamžitě přímým zápisem do paměti. Tuto vlastnost systému můžeme nejlépe dokumentovat na použití "horké" klávesy v DOSu pro program [Fguard](#). Pokud si spustíte DOS v okně Windows a máte instalovaný program FGW.EXE, pak po stlačení klávesy CTRL-5 (přesný význam naleznete v popisu programu Fguard) uslyšíte zvukové znamení přepnutí aktivity programu a po kratším nebo delším časovém okamžiku (dle využívání systému a počtu spuštěných programů) uvidíte, že ikona programu FGW nebo obsah rozvinutého okna se automaticky změní. Tato změna však není z výše uvedených důvodů okamžitá.



## **Verze 7.70**

Program ve své verzi 7.70 obsahuje pouze minimální změny proti verzi 7.50.





## **Verze 7.50**

Program ve své verzi 7.50 obsahuje pouze minimální změny proti verzi 7.0.



## **Verze 7.0**

Program ve své verzi 7.0 je již trvalou součástí antivirového systému AVAST!. Verze 7.0 přináší mírné rozšíření uživatelského rozhraní a několik interních změn, které zlepšují stabilitu programu v mezních podmínkách.



## Změny proti starším verzím.

### Změny verze 7.0 proti verzi 6.2

Ve verzi 7.0 byla instalována schopnost ukrýt ikonu programu tak, že nemusí být po dobu činnosti systému Windows viditelná.

Všechny ostatní změny programu se týkají pouze interních částí, které nejsou viditelné pro uživatele.

### Změny verze 6.2 proti verzi 6.0.

Ve verzi 6.2 byla plně implementována spolupráce programu Fguard pro Windows s programem [Rguard pro DOS](#) - implementace testování spouštěných programů na přítomnost virů. V návaznosti na tuto změnu program rozeznává dva parametry příkazové řádky:

/SB Program 'zasekne' počítá v případě zjištění BOOT viru na disketě.  
/SE Program 'zasekne' počítá v případě zjištění viru ve spouštěném programu.

Nová verze má nepatrně změněno uživatelské rozhraní a při zobrazování varování upozorňuje na skutečnost, že odpověď je nevyhnutelně zadat z klávesnice.

### Změny verze 6.0 proti verzi 5.1.

Ve verzi 6.0 byla změněna práce s jazykovou mutací češtiny. Program je schopen automaticky nastavovat potřebnou jazykovou mutaci. Toto zjišťování spočívá v testování proměnné **sCountry** z oblasti **[intl]** souboru WIN.INI. Pokud proměnná obsahuje čítec 'CZECH' nebo 'Ěesk' psaný libovolnou kombinací velkých a malých písmen, program používá kódovou stránku 1250. Pokud proměnná tento čítec neobsahuje, program automaticky konvertuje všechny potřebná data z kódové stránky 1250 do češtiny bez diakritiky. Pro tuto konverzi se používá dynamická knihovna AWLANG.DLL, která je součástí dodávky systému AVAST! pro české zákazníky.

Byl změněn tvar okna pro varování, které již neobsahuje tlačítka. Tato změna byla provedena, protože program není schopen z principiálních důvodů konstrukce systému Windows používat myš na odpověď ve varovném okně.

Hlášené REPORT není nadále vypisováno přímo do plochy hlavního okna, ale do samostatného okna, které již nadále nepřepisuje obsah obrazovky. Toto okno je umístěno v pravém horním rohu vždy nad všemi aktivními aplikacemi.

Program FGW.EXE rozeznává jeden parametr příkazové řádky, který může být psán libovolnou kombinací velkých a malých písmen. Parametr musí být uveden znakem '/' nebo '-'. Rozeznávaný parametr je:

/SB Program 'zasekne' počítá v případě zjištění BOOT viru na disketě.

### Změny verze 5.1 proti verzi 5.0.

Ve verzi 5.1 je program určen jenom pro práci v tzv. rozšířeném režimu práce Windows. Toto omezení však není tak svazující, jak se může na první pohled zdát. Systém Windows lze sice používat i na počítačích s procesorem 80286 a pamětí 1 MB, ale vlastní práce s

podobným hardwarem připomíná spíše pomalou demonstraci než cokoli jiného. Druhým důvodem omezení je to, že systém Windows pracující ve standardním režimu není schopen komunikace s DOSem a naopak. Tento režim připomíná (a ve své podstatě je) pouhý přepínač mezi DOSem a systémem Windows. Toto tvrzení samozřejmě neplatí o provozování úloh Windows, ale pouze o spolupráci úloh DOSu a Windows. V rozšířeném režimu práce je již možné zajistit plnohodnotnou a spolehlivou ochranu systému před napadením nebo vlastní nepozorností uživatele bez ohledu na počet a typ úloh, které jsou právě zpracovávány.

Program FGW se ve verzi 5.10 skládá ze dvou hlavních částí, souborů AVAST.386 a FGW.EXE. První z nich, tzv. virtuální driver, je 32 bitová knihovna, která obsahuje kritické části programu nutné pro spolupráci systému DOS a Windows. Tvoří spojovací články mezi rezidentními programy [Fguard](#) a [Rguard](#) z DOSu a programem FGW.

Druhý ze souborů je program FGW.EXE, což je standardní aplikace pro systém Windows, která obsluhuje komunikaci programu s uživatelem. Má za úkol zobrazovat aktuální nastavení ochrany a vypisovat varovná hlášení ve tvaru, který je pro Windows standardem.



## **Původ programu**

Program Fguard pro Windows je součástí systému AVAST! již od verze 5.0. S vývojem antivirového systému se také vyvíjel a nyní již poskytuje stabilní ochranu systému před viry i uživatelem.

Program se vyvinul z programů [Fguard](#) a [Rguard](#) pro DOS, které prozatím stále pro svou práci potřebuje.



## Parametry programu

Program Fguard pro Windows rozeznává dva parametry příkazové řádky, parametry uvedené v [konfiguračním souboru](#) AVAST!.INI a parametry, které si přečte z rezidentních programů v DOSu.

### Jednotlivé parametry:

- [Parametry příkazové řádky](#)
- [Parametry konfiguračního souboru](#)
- [Parametry rezidentních programů](#)



## Parametry příkazové řádky

Program Fguard pro Windows rozeznává dva parametry, které mohou být udávány na příkazové řádce. Parametry mohou být uvedeny znaky '/' nebo '-' a mohou být uvedeny velkými nebo malými písmeny.

### **Jednotlivé parametry jsou:**

/SB Program 'zasekne' poěítaè v pøípadì zjištíní BOOT viru na disketì.

/SE Program 'zasekne' poěítaè v pøípadì zjištíní viru ve spouštíném programu.

Zaseknutí spoěívá v zablokování jakékoli další práce systému, ale obrazovka Windows zůstane nezminìna, takže správce systému se může pokusit identifikovat nakažený program nebo disketu. Pokraèování v práci je možné až po RESETu poěítaèe.



## Parametry konfiguračního souboru

Program Fguard pro Windows pro ukládání parametrů v době mezi jednotlivými spuštěními programu používá soubor [AVAST!.INI](#), který je umístěn v adresáři, odkud byl program spuštěn.

Všechny parametry programu Fguard pro Windows jsou uloženy v skupině [FGUARD]. Soubor [AVAST!.INI](#) používají i další programy systému AVAST.

### **Proměnná TEMP**

Proměnná TEMP slouží pro účely komunikace jednotlivých instancí programu Fguard pro Windows. Její hodnota se mezi jednotlivými běhy programu mění. Je důležité, aby se obsah proměnné během práce programu Fguard pro Windows nezměnil jiným programem, jinak může dojít k zablokování počítače.

### **Proměnná HideIcon**

Proměnná HideIcon obsahuje logickou hodnotu 0 nebo 1. V případě, že proměnná obsahuje hodnotu 1, bude ikona programu po dobu jeho běhu skrytá a program nebude zobrazován ani v seznamu pracujících úloh (standardním Seznamu úloh).





## Parametry rezidentních programů

Program Fguard pro Windows při svém startu zjišťuje přítomnost a nastavení programů [Fguard pro DOS](#) a [Rguard pro DOS](#). Jejich nastavení si čte přímo z jejich interních dat, kam zapisuje také veškeré změny.

V případě, že některý program není zaveden do paměti, jsou příslušné ovládací prvky nepřístupné. Popis jednotlivých parametrů můžete najít v [příslušných kapitolách](#).



## Ovládání programu

Z hlediska ovládání má program dvě zcela samostatné části. Konfigurační okno programu, ve kterém je možné nastavovat konfiguraci a okno varování, které se zobrazí v závislosti na prováděných operacích a nastavené konfiguraci.

Program je možno ovládat pomocí klávesnice nebo pomocí myši stejným způsobem, jako všechny ostatní programy systému Windows. V programu je pouze jedna výjimka a tou je okno varování, které není možno ovládat myší.

### Ovládání jednotlivých částí programu

- [Konfigurační okno](#)
- [Okno varování](#)
- [Report okno](#)



## Konfigurační okno

Konfigurační okno programu Fguard pro Windows je hlavní a jediné okno, které pracuje standardním způsobem oken systému Windows. Je to dialogové okno, které obsahuje několik skupin ovládacích prvků různých typů a různého určení. Ovládací prvky jsou od rozděleny do tří skupin podle svého určení třírozměrným efektem. Vrchní část je určena pro obsluhu programu Rguard a spodní pro obsluhu programu Fguard. Na kraji okna je umístěna skupina tlačítek pro společné použití. Podle konfigurace Vašeho systému, nemusí být všechny ovládací prvky aktivní.

### Jednotlivé ovládací prvky:

- [Ovládání programu Rguard](#)
- [Ovládání programu Fguard](#)
- [Společné ovládací prvky](#)



## **Okno varování**

Okno varování má pro každé varování rozdílný obsah, který dostatečně výstižně vyjadřuje příčinu jeho zobrazení i způsob odpovědi nebo jiné reakce. Jeho ovládání je velice jednoduché. Je možné použít jenom klávesy, které jsou v okně uvedeny nebo klávesy Enter (Return), která má stejný účinek jako první ze zobrazených voleb.



## Report okno

Report okno je velice jednoduché okno, které se zobrazuje na dobu asi 10 vteřin v pravém horním rohu obrazovky. Okno zobrazuje krátký text, který vyjadøuje pøíèinu jeho zobrazení. Okno je naprosto samostatné a nemá žádný vliv na ostatní okna Windows. Ono je zobrazeno nad všemi ostatními okny a není s ním možno pohybovat.



## Ovládání programu Rguard

Práce programu Rguard je ovlivňována dvěma parametry v horní části konfiguračního okna.

### **Testuj BOOT sektor disket**

Parametr určuje, zda bude BOOT sektor každé diskety otestován na viry při přístupu na disketu. V případě, že BOOT sektor diskety obsahuje virus, je zobrazeno varování a v práci je možné pokračovat nebo přístup na disketu nepovolit.

### **Testuj spouštěcí programy**

Parametr určuje, zda budou všechny spouštěcí programy testovány na přítomnost virů. Pokud je vzorek viru ve spouštěcím programu nalezen, je možné zakázat spuštění programu. Spouštěcí programy jsou testovány jako jeden celek ve tvaru, v jakém se nacházejí na disku. Z toho vyplývá, že test může nějakou dobu trvat, zvláště při programech s délkou nad 1 MB (QPro 5.0, MS Word, ...) na počítačích s malou vyrovnávací pamětí procesoru a nízkou frekvencí. Dle velikosti programu je nutné počítat až s prodlevou 30 vteřin.



## Ovládání programu Fguard

Práce programu Fguard je ovlivňována parametry uvedenými ve spodní části konfiguračního okna.

Pokud je některý parametr označen šedivým čtvercem, program sleduje pokusy uvedenou činností, ale uživatelé o jejím průběhu pouze informuje pomocí REPORT okna.

### **Program je aktivní**

Parametr určuje, zda budou nebo nebudou sledovány všechny činnosti programu Fguard. Pokud není parametr označen, program Fguard je vypnut.

### **Pokus o formátování stopy**

Parametr určuje, zda program sleduje nebo nesleduje pokusy o formátování některého z přístupných disků nebo disket.

### **Manipulace se soubory**

Parametr určuje, zda program sleduje nebo nesleduje pokusy o otevírání souborů, jejich mazání a další podobné činnosti s celými soubory.

### **Přímý zápis pomocí DOSu**

Parametr určuje, zda program sleduje nebo nesleduje pokusy o přímý zápis na pevné disky nebo diskety DOSem (přerušení 25h), který obchází standardní metody ukládání dat.

### **Přímý zápis pomocí BIOSu**

Parametr určuje, zda program sleduje nebo nesleduje pokusy o přímý zápis na pevné disky nebo diskety BIOSem (přerušení 13h), který obchází standardní metody ukládání dat. Protože i legální zápisy jsou ve své konečné podobě transformovány na zápis pomocí BIOSu, použití tohoto přepínače může vést k záplavě varovných hlášení. Doporučujeme Vám tento přepínač aktivovat až v případě podezření na nákazu virem.

### **Změna obsahu CMOS paměti**

Parametr určuje, zda program periodicky sleduje nebo nesleduje změny obsahu konfigurační paměti CMOS. Některé programy nebo systémy pravidelně mění její obsah. V těchto případech je sledování změn prakticky neproveditelné. Těchto programů nebo systémů je však minimum.

### **Změna vektorů přerušení**

Parametr určuje, zda program periodicky sleduje nebo nesleduje pokusy o změny vybraných vektorů přerušení, což je jedna ze standardních činností mnoha virů, ale i mnoha programů. Tomuto hlášení je vhodné věnovat zvýšenou pozornost.

### **Krokování přerušení**

Parametr určuje, zda program sleduje nebo nesleduje pokusy o krokování (tunelování) přerušení, což je jedna ze obvyklých činností moderních virů. Pravděpodobnost, že by normální program vykonával tuto činnost je velice malá a proto hlášení o pokusu o krokování přerušení věnujte maximální pozornost.

### **Editační okna**

Editační okna obsahují až 10 různých typů souborů, které může program Fguard pro Windows sledovat. Pokud potřebujete pracovat s více typy souborů můžete použít standardních znaků systému DOS pro určení více typů jedním šetizcem (tzv. wildchars). Typ

souboru je urèen øetìzcem maximální tøj znakù.





## Spoleèné ovládací prvky

Spoleèné ovládací prvky slouží pro práci se samotným programem Fguard pro Windows. Tyto prvky nejsou uzavøeny v žádném grafickém prvku.

### **Skrýt ikonu programu**

Parametr urøuje, zda bude ikona programu viditelná nebo ne.

### **OK**

Tlaèítko OK slouží pro uložení zmìnìných informací do pamìti rezidentních programù instalovaných v systému DOS a jejich okamžitou aktivaci. Po jeho stisku se okno programu zmenší do tvaru ikony.

### **Zruš**

Tlaèítko Zruš slouží pro zrušení zmìn všech parametrù zmìnìných od posledního stisku tlaèítka OK. Po jeho stisku se okno programu zmenší do tvaru ikony.

### **Nápovìda**

Tlaèítko Nápovìda slouží pro vyvolání této nápovìdy na stránce [Konfiguraèní okno](#).

### **Report**

Tlaèítko Report slouží pro pøepnutí všech parametrù do režimu REPORT a zpìt. Obìma smìry jsou pøepnuta všechna tlaèítka, která mají tøi stavy.



## Likvidace virù

Podle mnoha průzkumù se již milióny uživatelù výpoèetní techniky po celém svìtì setkali s viry, a tak je bohužel vysoká pravdìpodobnost, že pøes veškerá preventivní opatøení se to může jednou pøihodit i Vám.

Nejdùležitìjší v takovém okamžiku je nepropadnout panice a zachovat klid. Jelikož jste jisti uživatel, který nerad riskuje, máte jisti všechna důležitá data a programy zálohovány, takže ani kompletní znièení obsahu Vašeho disku by Vás jisti pøíliš nezaskoèilo. Navíc jste jisti uživatel pozorný a peèlivý, takže pøítomnost viru jste odhalil pomìrnì vèas, tedy døíve, než mohl napáchat velké škody. Odhalit virus můžete napøíklad pozorováním neobvyklého chování systému (grafické a zvukové efekty, neobvyklé chybové hlášení, neznámá aktivita disku, chyby dosud bezvadnì fungujících programù apod.) nebo pomocí pravidelného a peèlivého používání antivirového systému AVAST!.

Pokud tedy zjistíte nesrovnalosti, které nelze nijakým racionálním zpùsobem vysvìtlit (zmìna délky nebo obsahu souboru, nepovolená manipulace se soubory, podivné diskové operace, zmìny v operaèní pamìti atd.), je tøeba nejprve pomocí programu Lguard a Vguard zjistit, zda v systému není pøítomen nikterý ze známých virù, které umí tyto programy odhalit. Program Lguard by si mìl poradit s naprostou vìtšinou dnešních virù. Pokud ani jeden z těchto programù virus nenalezne, použijte program Aguard, který je schopen zachytit všechny zmìny, ke kterým na disku došlo od jeho posledního spuštìní. Program Aguard obsahuje i možnost otestovat zmìněné soubory na pøítomnost virù a pøípadnì tyto viry ze souborù odstranit. Pøi jejich odstraòování nepotøebuje žádné informace o typu virù a tak je velice úèinný i proti novým nebo neznámým typùm.

Pøi likvidaci napadení vložte do disketové jednotky poèítaèe pracovní disketu, vytvoøenou pøi instalaci systému AVAST!, která by mìla být chránìna proti zápisu a spusťte program Lguard, napøíklad:

**A:  
LGuard C:**

Program Lguard nejdøíve prohledává operaèní pamìì, zda v ní nenajde aktivní virus. Pokud je nijaký virus nalezen, je potøeba ho v pamìti eliminovat, aby pøestal být funkèní. Poté co byl z pamìti virus odstranìn, nehrozí nebezpeèí jeho další aktivity. Dále program testuje systémovou oblast disku a následuje testování souborù. Na závìr program vypíše pøehlednou tabulku s výsledky své èinnosti.

Pro odstranìní neznámého typu viru je potøeba nahrát systém z **èisté** systémové diskety (nejlépe z té, která byla vytvoøena pøi instalaci programového vybavení AVAST!). Programem Aguard snadno odhalíte všechny soubory, které byly virem nelegálnì modifikovány. Jejich seznam lze vytisknout na tiskárnì pøíkazem Print Screen nebo vytvoøit na disku pomocí parametru **"/O"**.

Programy antivirového souboru AVAST! obsahují vlastní mechanismus, který umožňuje zjistit jejich pøípadnou modifikaci virem. Pøi svém spuštìní nejdøíve testují, zda nebyly samy zmìněny, a pokud ano, ohlásí tuto skuteènost uživateli, napø.:

**VGuard.EXE**

**WARNING: This program was modified (maybe by some virus ??) !!**

**Press any key to continue...**

Toto hlášení slouží jako upozornění, že program byl modifikován. Jeho hlavní význam tkví v tom, že uživatel je vás varován. Po stisknutí kterékoli klávesy program pokračuje ve své normální činnosti, je však pravděpodobné, že v tomto okamžiku byl již virus aktivován.

Při napadení systémových oblastí pevných disků je možné v případě používání operačního systému MS-DOS 5.0 a vyšších použít systémový program FDISK s parametrem **"/MBR"**, který obnoví standardní stav systémových oblastí bez vlivu na data, která mohou být na disku uložena. Nevyhnutelnou podmínkou pro použití je nastartování počítače z čisté systémové diskety, jinak je léze neúčetná.

Pro ochranu BOOT sektoru je možné výhodně použít program Bguard, kterým je možno obnovit stav BOOT sektorů pevných disků.

Přejeme Vám, aby se Vám počítačové viry zdaleka vyhnuly. A pokud se přece jen objeví, aby Vám naše programové vybavení pomohlo překonat všechny problémy, které Vám počítačové viry způsobily.

**Pokud si nejste jisti, svěřte odstranění virů odborníkům !!**



## **Požadavky pro práci**

Program Fguard pro Windows potřebuje pro svou práci:

- Windows 3.1 nebo novější 16-bitový systém (Windows 3.11, Windows for Workgroups 3.1, 3.11) pracující v rozšířeném režimu.
- VGA video adaptér nebo lepší.
- Disketová jednotka pro instalaci systému.
- Pevný disk pro uložení programů.



## Chyby a fatální chyby

Program Fguard pro Windows je schopen zobrazit několik různých druhů varování a chybových hlášení, která zobrazuje v různé formě. Jejich seznam a bližší informace o možných variantách jsou uvedeny níže.

- [Nekompatibilita verzí.](#)
- [Program není instalován.](#)
- [Interní chyba DPML.](#)
- [Interní chyba při změně dat.](#)
- [Chyba inicializace programu.](#)
- [Chyba při vytváření REPORT okna.](#)
- [Chyba alokace paměti.](#)
- [Spouštěcí programy nebudou testovány.](#)
- 
- [Chyba detekce rozšířeného módu.](#)

**Nekompatibilita verzí. Program není schopen pracovat z důvodu nekompatibility s podpůrnou knihovnou (AVAST.386).**

Soubor FGW.EXE a AVAST.386 musí mít stejnou verzi. Tyto dva soubory spolu velice úzce spolupracují proto není možné použít různé kombinace pro práci.

**Program není instalován. V paměti počítače není FGUARD nebo RGUARD pro DOS nebo programy FGUARD nebo RGUARD a FGW nejsou vzájemně kompatibilní.**

Program Fguard pro Windows nevykonává žádné sledování činnosti programů nebo uživatelů ve své vlastní režii. V současné verzi pouze zobrazuje informace předané rezidentními programy z DOSu. V případě, že tyto programy nejsou instalovány nebo nemají stejnou verzi, nemůže Fguard pro Windows pracovat.

**Interní chyba DPMI. Nemohu alokovat struktury nutné pro přístup k datům.  
Program není schopen pracovat. Doporuèuji ukonèit práci ve Windows.**

Program Fguard pro Windows používá k některým operacím prostředkù DPMI. Pokud dojde k chybì při práci s tímto rozhraním, jde s největší pravdìpodobností o vážnou chybu.



**Interní chyba při zmnì dat. Zobrazovaná data neodpovídají datùm, které jsou brány do úvahy při chránìní systému.**

Program zjistil chybu při ukládání zmìnìných konfiguraèních dat do datových oblastí rezidentních programù. Při této chybì může dojít k pøepsání èásti pamìti a èinnost systému může být nestabilní.

**Chyba inicializace programu. Není volný žádný časovač, který je nutný pro práci.  
Ukončete některý program a zkuste znovu.**

Program Fguard pro Windows potřebuje pro svou práci jeden kanál pro získávání informací o změně času. Protože jde o zdroj, který je v 16-bitových Windows limitován, nemusí být pokaždé k dispozici.

**Chyba při vytváření REPORT okna. Hlášení nebude zobrazeno.**

Při vytváření REPORT okna došlo k jakékoli chybě. Protože REPORT okno slouží jenom pro informaci uživatele, tato chyba není příliš závažná.

**Chyba alokace paměti. Nemohu alokovat paměť DOSu. Sledování spuštěných programů je vypnuto.**

Sledování spuštěných programů vyžaduje paměť umístěnou na adrese pod 1 MB (tzv. paměť DOSu). Tato paměť je v 16-bitových Windows velice intenzivně používaná a její množství je limitováno, takže nemusí být pokaždé k dispozici.

**Spouštiné programy nebudou testovány. Knihovna pro jejich testování (AWANTI.386) není instalována.**

Knihovna AWANTI.386 implementuje vlastní podprogramy pro testování dat. Její instalace probíhá při zavádění systému Windows a nemusí pokaždé proběhnout. Například v případě nedostatku paměti nebude tato knihovna instalována.

**Chyba detekce rozšířeného módu. Program není schopen pracovat v jiném módu.  
Ukončete Windows a použijte příkaz 'WIN /3'.**

Program Fguard pro Windows pracuje pouze v rozšířeném režimu systému Windows.

**Konfigurační soubor** je soubor, ve kterém se uchovávají parametry programu v době, kdy je počítač vypnut nebo kdy program nepracuje. Konfigurační soubor pro programy systému AVAST! se nazývá AVAST!.INI a můžete ho najít v adresáři, odkud byl program spuštěn. Je to standardní typ konfiguračního souboru pro programy určené do systému Windows. Před manuálními změnami obsahu tohoto souboru doporučujeme pořídit si jeho zálohu, protože nesprávně provedené změny mohou způsobit nefunkčnost antivirového systému AVAST! nebo zablokování systému.

**FGUARD** je rezidentní antivirový program pro DOS, který v reálném čase hlídá všechny pokusy o modifikaci sledovaných souborů (smazání, otevření pro zápis, zápis, přejmenování, zrušení příznaku "pouze čtení"). Kromě toho je program schopen sledovat i případnou destruktivní činnost viru. Umožňuje hlídat pokusy o formátování, přímý zápis na disk pomocí DOSu či BIOSu, změnu obsahu konfigurace paměti CMOS, krokování přerušování a změny vybraných vektorů přerušování.



**Firma ALWIL Software** a její programové produkty nejsou na trhu žádným nováčkem. Firma samotná byla založena až v dubnu 1991 oddělením od družstva ALWIL, ale kolektiv jejich pracovníků je pospolu již od roku 1988, kdy vznikla první verze souboru antivirových programů AVAST! a Správce uživatelských programů SUP. V tomtéž roce byla na trh uvedena implementace národního prostředí nejen pro osobní počítače kompatibilní s IBM PC a jeho obvyklé periférie, ale i pro laserové tiskárny.

Zůstáváme i nadále věrni své specializaci v oblasti systémových programů, ochrany dat a implementaci národního prostředí pro laserové tiskárny. Poslední novinky z naší produkce jsou například šifrování obsahu pevných disků v reálném čase nebo program Lguard pro Windows.

ALWIL Software  
Průbežná 76, 100 31 Praha 10  
telefon (+422)782 20 50  
  
fax (+42 2)782 25 53  
BBS (+42 2)782 25 50  
BBS (+42 2)782 20 50 (18:00 - 7:00)  
cc:Mail (+42 2)782 2549

**RGUARD** je jeden z rezidentních antivirových programů pro DOS, který zajišťuje antivirové testování spouštěných programů a testování přítomnosti BOOT virů na disketách v prostředí DOSu.

