



Sguard pro Windows

Sguard pro Windows je jeden z programů formy [ALWIL Software](#), který je určen pro rychlý test změn jednotlivých souborů. Jeho základní určení je v rychlé kontrole základních (hlavně systémových) souborů, např: IO.SYS, MSDOS.SYS, COMMAND.COM nebo WIN.COM. Program není samozřejmě omezen jenom na vyjmenované soubory, ale je do něj možno zařadit libovolný soubor, který je v okamžiku spuštění programu dosažitelný.

Základní informace

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

Historie

- [Verze 7.70](#)
- [Verze 7.50](#)
- [Verze 7.0](#)
- [Původ programu](#)

Přílohy

- [Likvidace virů](#)
- [Požadavky pro práci](#)
- [Varování a chybová hlášení](#)



Instalace programu

Program Sguard pro Windows 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.



Princip práce

Princip práce programu je velice jednoduchý. Program si přečte soubory uvedené na příkazové řádce nebo v [konfiguračním souboru](#) systému AVAST!, spočte si jejich kontrolní součty a zkontroluje s údaji zjištěnými dříve nebo uvedenými na příkazové řádce společně se jmény souborů.

Program je schopen zpracovat soubory uvedená na příkazové řádce, nebo je schopen práce v interaktivním režimu, kdy je možné zadat jména kontrolovaných souborů v [přehledném dialogu](#).

- [Spouštění programu](#)
- [Pracovní soubory](#)



Parametry programu

Program Sguard pro Windows je schopen zpracovat několik různých parametrů na příkazové řádce a jeden speciální parametr. Parametry, které program nezná, jednoduše ignoruje bez jakýchkoli chybových hlášení. V případě, že program nenajde soubor uvedený na příkazové řádce, ignoruje jej také.

Jednotlivé parametry

- [Parametry příkazové řádky](#)
- [Speciální parametry](#)



Ovládání programu

Ovládání programu Sguard pro Windows je stejné, jako ovládání ostatních programů pracujících v systému Windows. Program nepoužívá žádné speciální způsoby obsluhy a nevyžaduje žádné speciální nebo nezvyklé znalosti.

Práce s jednotlivými typy dialogů

- [Práce s dialogem pro interaktivní nastavení](#)
- [Práce s dialogem chybových hlášení a zpráv](#)
- [Práce s dialogem pro dotazy](#)



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 například 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 způsobem vysvětlit (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 měl 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 odstraňování 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 měla být chránìna proti zápisu a spusťte program Lguard, například:

```
A:  
LGuard C:
```

Program Lguard nejdøíve prohledává operaèní pamìť, zda v ní nenajde aktivní virus. Pokud je nějaký 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 Sguard pro Windows pro svou práci požaduje:

1. Microsoft Windows 3.xx, Microsoft Windows for Workgroups 3.xx.
2. Systém s procesorem minimálně 80386sx nebo kompatibilním.



Varování a chyby

Program Sguard 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.

- [Špatný kontrolní součet.](#)
- [Smazat soubor 'ANYFILE' z konfiguračního souboru ?](#)
-
- [Nedostatek paměti.](#)
- [Chyba otevření souboru.](#)
- [Soubory pro kontrolu nenalezeny.](#)
- [Špatná struktura příkazové řádky.](#)

Špatný kontrolní součet. Soubor 'ANYFILE' má kontrolní součet 99998. Kontrolní součet v konfiguračním souboru je 99999. Je tato změna v pořádku ?

Toto varování je zobrazeno v případě, že kontrolní součet souboru nesouhlasí s daty uvedenými na příkazové řádce nebo v [konfiguračním souboru](#). Varování má dvě podoby. V případě kontroly souboru z [příkazové řádky](#) je zobrazeno ve formě varování. V případě kontroly souboru z [konfiguračního souboru](#) má formu dotazu, kde můžete určit, zda je nová kontrolní suma v pořádku (změna souboru je legální) nebo ne. Pokud je změna v pořádku, je nová hodnota kontrolní sumy zaznamenána do [konfiguračního souboru](#).

Smazat soubor 'ANYFILE' z konfiguračního souboru ? Pokud tento soubor smažete, nebude se vícekrát testovat.

Toto varování je zobrazeno v okamžiku, kdy je požadováno smazání některého souboru ze seznamu uvedeného v [konfiguračním souboru](#). Toto varování je zobrazeno ve formě dotazu, zda tento soubor chcete opravdu trvale smazat. Pokud odpovíte kladně, soubor bude smazán se seznamu a až do opětovného zařazení nebude testován.

**Nedostatek paměti. Lituji, ale program nemá k dispozici dostatek paměti.
Požadovaná služba nemůže být provedena.**

Tato chyba se zobrazí v okamžiku, když program narazí na nedostatek paměti pro svou práci. Program Sguard pro Windows používá pro svou práci jenom naprosté minimum paměti (asi 10 kB), které by měly být k dispozici v každém případě. Pokud Vám program zobrazí tuto chybu, spojte se s vaším dodavatelem systému AVAST! nebo přímo s firmou ALWIL Software a informujte jej o této skutečnosti.

Chyba otevření souboru. Program není schopen otevřít soubor ANYFILE. Soubor bude vyřazen ze seznamu.

Program Sguard pro Windows potřebuje otevřít každý testovaný soubor. program jej otevírá pouze pro čtení a zároveň nastavuje příznak, že soubor může být jinými procesy čten, ale ne zapisován. V případě, že je testovaný soubor již otevřen exkluzivním způsobem nebo operační systém nemůže tento soubor zpřístupnit z jakýchkoli jiných důvodů, je ohlášena tato chyba. Jako reakci na tento typ chyby doporučujeme zkontrolovat, zda testovaný soubor skutečně existuje a zda jej právě nepoužívá jiná spuštěná aplikace.

**Soubory pro kontrolu nenalezeny. Parametry souboru AVAST!.INI nejsou správné.
Opravit konfigurační soubor ?**

Program zobrazí tuto chybu jako reakci na špatný obsah konfiguračního souboru. Jedná se o případ, že proměnná NumberFiles obsahuje větší počet souborů pro testování než se v konfiguračním souboru skutečně nachází (proměnné FileXXX). Tato chyba je zobrazena ve formě dotazu, zda chcete opravit konfigurační soubor. Před zobrazením této chyby může dojít k poměrně značné prodlevě v práci programu, která je uvedena zmínou kurzoru na tvar přesýpacích hodin. Tato prodleva je způsobena intenzivním prohledáváním konfiguračního souboru a hledáním chybějících souborů pro testování.

Špatná struktura příkazové řádky. Příkazová řádka nemůže obsahovat přepínače '/A' a '/D' najednou.

Tato chyba je zobrazena jako reakce programu na špatnou strukturu příkazové řádky.



Verze 7.70

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



Verze 7.50

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



Verze 7.0

Program Sguard pro Windows ve své verzi 7.00 je první implementací pro systém Windows. Je součástí systému AVAST! od verze 7.00 a číslování jeho verzí je stejné jako číslování verzí systému AVAST!.



Původ programu

Program Sguard pro Windows odvozuje svůj původ od programu Sguard pro DOS, který je součástí systému AVAST! již od verze 3.0. Při své práci používá stejné interní algoritmy pro zjišťování kontrolních sum souborů, takže čísla, které můžete při práci s programem nebo jeho pracovními soubory spatřit jsou stejná, jako ty, která produkuje program Sguard pro DOS.

Program má téměř stejné schopnosti, jako jeho DOSový protějšek s několika změnami.

1. Program pracuje výhradně v systému Windows.
2. Program obsahuje interaktivní nastavování testovaných souborů.
3. Program neobsahuje možnost testování kontrolní sumy paměti, protože tato schopnost je v systému Windows zbytečná.
4. Program ve své současné verzi neobsahuje možnost testování systémových oblastí jednotlivých disků.



Spouštění programu

Program Sguard pro Windows je možné spouštět několika různými způsoby. Program je schopen akceptovat několik parametrů na [příkazové řádce](#), je možné jej spouštět bez jakýchkoli parametrů.

Program ve standardním režimu nevytváří žádné okno, ale přes to všechno zjišťuje, zda je spouštěn s požadavkem na zobrazení ve standardním tvaru s rozvinutým oknem, nebo má být spuštěn ve tvaru ikony. Bližší informace naleznete v popisu [speciálních parametrů](#).

Program je možné spustit všemi způsoby, které akceptují všechny normální 16-bitové EXE programy ve Windows.



Pracovní soubory

Program potřebuje pro svou práci několik souborů. Některé z nich potřebuje, aby se vůbec spustil (dynamické knihovny) a [konfigurační soubor](#), který si čte i zapisuje. V případě, že tento soubor neexistuje, program si ho vytvoří v adresáři, ze kterého byl spuštěn.

Jednotlivé pracovní soubory

- [Konfigurační soubor](#)



Konfigurační soubor

Program Sguard pro Windows používá soubor AVAST!.INI k ukládání potřebných údajů. Tento soubor má standardní formát všech [konfiguračních souborů](#) systému Windows a je umístěn v adresáři, odkud byl program spuštěn.

Pro svou práci program používá skupinu [SGUARD].

Jednotlivé parametry

- [Parametr FileXXX](#)
- [Parametr NumberFiles](#)



Parametry příkazové řádky

Obecný tvar příkazové řádky programu Sguard pro Windows je:

```
SGW [soubor [suma] [soubor [suma] ...] [/-][A|a] [/-][D|d] [/-][M|m]]
```

kde **soubor** představuje plné jméno souboru pro kontrolu, **suma** jeho kontrolní sumu zapsanou v desítkové soustavě. Kontrolní sumu je nutné zadat v případě, že ji znáte. Pokud ji neznáte a zapíšete příkazovou řádku například ve tvaru:

```
SGW c:\command.com c:\io.sys c:\msdos.sys
```

program Sguard pro Windows spočte kontrolní sumu pro každý soubor a ohlásí chybu, protože nenašel žádné číslo, se kterým by spočtenou kontrolní sumu porovnal. Výše uvedený zápis má smysl pouze v případě, že do příkazové řádky zadáte jeden z přepínačů **/A** nebo **/D**. Pokud znáte kontrolní součet jednotlivých souborů, můžete zadat stejný příkazový řádek ve tvaru:

```
SGW c:\command.com 12345 c:\io.sys 23456 c:\msdos.sys 34567
```

Význam jednotlivých přepínačů je následovný:

- /A přidá všechny soubory nalezené na příkazové řádce do [konfiguračního souboru](#). Pokud je na příkazové řádce uvedena taky kontrolní suma, přidá ji do [konfiguračního souboru](#) také.
- /D smaže soubory nalezené na příkazové řádce z [konfiguračního souboru](#). Uvedení kontrolní sumy nemá žádný vliv na další práci.
- /M přepne program do interaktivního režimu práce, přičemž nejprve zpracuje všechny ostatní parametry příkazové řádky a po jejich zpracování zobrazí [konfigurační dialog](#).

Parametry /A a /D nemohou být na příkazové řádce uvedeny najednou. Pokud se tak stane, program ohlásí chybu [špatná struktura příkazové řádky](#).

Pokud při použití parametru /A není uvedena kontrolní suma pro některý nebo všechny soubory, jsou tyto přidány do [konfiguračního souboru](#) a kontrolní suma je spočtena při prvním dalším spuštění programu. Tato skutečnost není žádným způsobem ohlášena a probíhá plně bez zásahů uživatele.

Všechny přepínače příkazové řádky mohou být uvedeny znaky '/' nebo '-' a mohou být napsány velkým nebo malým písmenem.



Speciální parametry

Program akceptuje jeden parametr, který se nezadává z příkazové řádky, ale z vlastností ikony spouštěcího programu, který určuje, zda spustit program v minimalizované formě nebo ne.

Pokud je program spuštěn s označením tlačítka **Run Minimized**, zkontroluje stav souborů uvedených na příkazové řádce a uvedených v [konfiguračním souboru](#) v tomto pořadí. Pokud toto tlačítko není označeno, program tento stav považuje za stejný, jako by byl na příkazové řádce uveden parametr **/M** a je spuštěn v interaktivním režimu.



Práce s dialogem pro interaktivní nastavení

Pokud je při spuštění programu použit parametr /M nebo speciální parametr, je zobrazen dialog pro interaktivní nastavení testovaných programů.

Dialog je modifikovanou verzí standardního dialogu systému Windows pro otevírání souborů. Jeho modifikace spočívá v přidání spodní části, ve které se nachází seznam se jmény souborů, které se při spuštění Sguardu pro Windows testují a dvě tlačítka pro práci s tímto seznamem.

Do seznamu je možno přidat prakticky libovolným množstvím souborů. Jediné omezení je způsobeno systémem Windows, který neumožňuje libovolné množství prvků v seznamu.



Práce s dialogem chybových hlášení a zpráv

Chybová hlášení nebo zprávy jsou programem generovány na podnět událostí, které mají vážný vliv na práci programu nebo jsou důležité pro uživatele.

Tento typ dialogu umožňuje pouze jednu odpověď a program čeká do okamžiku, než uživatel tuto odpověď zadá. Ostatní pracující programy systému Windows nejsou tímto čekáním žádným způsobem ovlivněny a pracují normálně dále.



Práce s dialogem pro dotazy

Dotazy jsou programem generovány v případě, že program potřebuje znát odpověď jak pokračovat dále v práci.

Tento typ dialogu umožňuje odpovědět kladně nebo záporně na otázku, která je zobrazena. Program čeká do okamžiku, než si uživatel vybere jednu z nabízených odpovědí. Ostatní pracující programy systému Windows nejsou tímto čekáním žádným způsobem ovlivněny a pracují normálně dále.



Parametr FileXXX

Parametr FileXXX je určen pro uložení jména testovaného souboru a jeho kontrolní sumy. Soubor znaků 'XXX' je v reálném [konfiguračním souboru](#) nahrazen číslem. Například:

```
File1=c:\command.com,12345
```

Z ukázky je zřejmé, že číslo nahrazující znaky 'XXX' není uvedeno žádnými nulami nebo prázdnými znaky. Kontrolní suma je uvedena ihned za jménem souboru a je od něj oddělena čárkou.

Číslování jednotlivých položek není důležité, je dokonce možné některé z nich vynechat. Při používání interaktivního nastavení program Sguard pro Windows automaticky vzestupně čísluje jednotlivé položky. V případě, že jsou některé z nich smazány, program automaticky použije volné čísla.

Pokud manuálně editujete obsah kontrolního souboru, je nutno přesně dodržet formát parametru. Program nepředpokládá žádné odchylky od zde popsaných pravidel. Položky, které program není schopen identifikovat, ignoruje bez jakýchkoli hlášení.



Parametr NumberFiles

Parametr NumberFiles je určen pro uložení počtu souborů, které má kontrolovat. Počet je uložen jako standardní číslo v desítkové soustavě.

Pokud používáte interaktivní nastavení, program Sguard pro Windows automaticky udržuje hodnotu parametru. Pokud manuálně editujete konfigurační soubor, je potřeba mít na vidomí následující fakta.

Program otestuje jenom ten počet souborů, který je uveden v parametru NumberFiles, přičemž tyto soubory zpracovává v řádkovém pořadí. Všechny ostatní soubory ignoruje.

Pokud je v parametru NumberFiles uvedeno vyšší číslo, než kolik je uvedeno souborů v [konfiguračním souboru](#), program ohlásí chybu [Soubory pro kontrolu nenalezeny](#) a nabídne opravu parametru.

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!.

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
Průběžná 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

PATH je systémová proměnná, která určuje, kde bude operační systém hledat spustitelné programy, když je nenajde v aktuálním adresáři.

Michal Kováčik je pracovníkem firmy ALWIL Software, který se zabývá implementací stávající nabídky do systému Windows. Můžete mu posílat zprávy na BBS firmy ALWIL Software na jméno 'MICHAL KOVACIC', rád Vám odpoví na Vaše dotazy.

BBS je zkratka pro Bulletin Board System, systém pro komunikaci, výměnu zpráv a souborů mezi uživateli. Na naší BBS je také možné získat poslední upgrade antivirového balíku AVAST! v případě, že máte zaplacenou službu AVS a máte přístup k modemu.

