



AVG Internet Security 2011

Používateľská príručka

Revízia dokumentu 2011.21 (16.5.2011)

Copyright AVG Technologies CZ, s.r.o. Všetky práva vyhradené.
Všetky ostatné ochranné známky sú vlastníctvom príslušných vlastníkov.

Tento produkt používa algoritmus MD5 Message-Digest spoločnosti RSA Data Security, Inc., Copyright (C) 1991 – 1992, RSA Data Security, Inc. spoločnosť bola založená v roku 1991.

Tento produkt používa kód z knižnice C-SaCzech, Copyright (c) 1996 – 2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Tento produkt používa knižnicu kompresie zlib, Copyright (c) 1995 – 2002 Jean-loup Gailly a Mark Adler.

Tento produkt používa knižnicu kompresie libbzip2, Copyright (c) 1996 – 2002 Julian R Seward.



Obsah

1. Úvod	8
2. Požiadavky na inštaláciu produktu AVG	9
2.1 Podporované operačné systémy	9
2.2 Minimálne a odporúčané hardvérové požiadavky	9
3. Možnosti inštalácie produktu AVG	10
4. Proces inštalácie produktu AVG	11
4.1 Vitajte!	11
4.2 Aktivovanie licencie AVG	12
4.3 Výber typu inštalácie	13
4.4 Vlastné možnosti	14
4.5 Inštalácia panela AVG Security Toolbar	15
4.6 Pribeh inštalácie	16
4.7 Inštalácia prebehla úspešne	16
5. Po inštalácii	18
5.1 Registrácia produktu	18
5.2 Otvorenie používateľského rozhrania	18
5.3 Kontrola celého počítača	18
5.4 Test EICAR	18
5.5 Predvolená konfigurácia AVG	19
6. Používateľské rozhranie AVG	20
6.1 Hlavná ponuka	21
6.1.1 Súbor	21
6.1.2 Súčasti	21
6.1.3 História	21
6.1.4 Nástroje	21
6.1.5 Pomocník	21
6.2 Informácie o stave zabezpečenia	24
6.3 Rýchle odkazy	25
6.4 Prehľad súčastí	25
6.5 Štatistika	27
6.6 Ikona na paneli úloh	27
6.7 Mini-aplikácia AVG	28

7. Súčasti AVG	31
7.1 Anti-Virus	31
7.1.1 Princíp fungovania súčasti Anti-Virus	31
7.1.2 Rozhranie súčasti Anti-Virus	31
7.2 Anti-Spyware	32
7.2.1 Princíp fungovania súčasti Anti-Spyware	32
7.2.2 Rozhranie súčasti Anti-Spyware	32
7.3 Anti-Spam	34
7.3.1 Princíp fungovania súčasti Anti-Spam	34
7.3.2 Rozhranie súčasti Anti-Spam	34
7.4 Firewall	35
7.4.1 Princíp fungovania súčasti Firewall	35
7.4.2 Profily súčasti Firewall	35
7.4.3 Rozhranie súčasti Firewall	35
7.5 LinkScanner	39
7.5.1 Princíp fungovania súčasti LinkScanner	39
7.5.2 Rozhranie súčasti LinkScanner	39
7.5.3 Search-Shield	39
7.5.4 Surf-Shield	39
7.6 Rezidentný štít	43
7.6.1 Princíp fungovania súčasti Rezidentný štít	43
7.6.2 Rozhranie súčasti Rezidentný štít	43
7.6.3 Detekcia súčasti Rezidentný štít	43
7.7 Family Safety	48
7.8 AVG LiveKive	48
7.9 E-mail Scanner	48
7.9.1 Princíp fungovania súčasti E-mail Scanner	48
7.9.2 Rozhranie súčasti E-mail Scanner	48
7.9.3 Detekcia súčasti E-mail Scanner	48
7.10 Update Manager	52
7.10.1 Princíp fungovania súčasti Update Manager	52
7.10.2 Rozhranie súčasti Update Manager	52
7.11 Licencia	54
7.12 Remote Administration	55
7.13 Webový štít	56
7.13.1 Princíp fungovania súčasti Webový štít	56
7.13.2 Rozhranie súčasti Webový štít	56

7.13.3 Detekcia súčasti Webový štít	56
7.14 Anti-Rootkit	59
7.14.1 Princíp fungovania súčasti Anti-Rootkit	59
7.14.2 Rozhranie súčasti Anti-Rootkit	59
7.15 System Tools	61
7.15.1 Procesy	61
7.15.2 Sieťové pripojenia	61
7.15.3 Automatické spúšťanie	61
7.15.4 Rozšírenia prehliadača	61
7.15.5 Prehliadač LSP	61
7.16 PC Analyzer	66
7.17 ID Protection	68
7.17.1 Princípy fungovania súčasti ID Protection	68
7.17.2 Rozhranie súčasti ID Protection	68
7.18 Security Toolbar	70
8. AVG Security Toolbar	72
8.1 Rozhranie súčasti AVG Security Toolbar	72
8.1.1 Tlačidlo s logom AVG	72
8.1.2 Vyhľadávacie okienko AVG Secure Search (powered by Google) powered	72
8.1.3 Stav stránky	72
8.1.4 Novinky od AVG	72
8.1.5 Správy	72
8.1.6 Vymazanie histórie	72
8.1.7 Upozornenie na nové e-maily	72
8.1.8 Informácie o počasí	72
8.1.9 Facebook	72
8.2 Možnosti panela AVG Security Toolbar	79
8.2.1 Karta Všeobecné	79
8.2.2 Karta Užitočné tlačidlá	79
8.2.3 Karta Zabezpečenie	79
8.2.4 Karta Rozšírené možnosti	79
9. Rozšírené nastavenia programu AVG	84
9.1 Vzhľad	84
9.2 Zvuky	86
9.3 Ignorovanie chybového stavu	88
9.4 Identity Protection	89
9.4.1 Nastavenia súčasti Identity Protection	89

9.4.2 Zoznam povolených	89
9.5 Vírusový trezor	93
9.6 Výnimky z PNP	93
9.7 Anti-Spam	95
9.7.1 Nastavenia	95
9.7.2 Výkon	95
9.7.3 RBL	95
9.7.4 Zoznam povolených	95
9.7.5 Zoznam blokovanych	95
9.7.6 Rozšírené nastavenia	95
9.8 Webový štít	106
9.8.1 Webová ochrana	106
9.8.2 Okamžité správy	106
9.9 LinkScanner	110
9.10 Kontroly	111
9.10.1 Kontrola celého počítača	111
9.10.2 Kontrola zo správcu súborov	111
9.10.3 Kontrola špecifických súborov alebo priečinkov	111
9.10.4 Kontrola vymeniteľných zariadení	111
9.11 Plány	116
9.11.1 Plánovaná kontrola	116
9.11.2 Plán aktualizácie vírusovej databázy	116
9.11.3 Plán aktualizácie programu	116
9.11.4 Plán aktualizácie súčasti Anti-Spam	116
9.12 E-mail Scanner	127
9.12.1 Certifikácia	127
9.12.2 Filtrovanie pošty	127
9.12.3 Servery	127
9.13 Rezidentný štít	136
9.13.1 Rozšírené nastavenia	136
9.13.2 Vylúčené položky	136
9.14 Vyrovnávací server	140
9.15 Anti-Rootkit	141
9.16 Aktualizácia	142
9.16.1 Proxy	142
9.16.2 Vytáčané pripojenie	142
9.16.3 Adresa URL	142
9.16.4 Správa	142



9.17 Dočasné vypnutie ochrany AVG	149
9.18 Program zlepšovania produktov	149
10. Nastavenia súčasti Firewall	152
10.1 Všeobecné informácie	152
10.2 Zabezpečenie	153
10.3 Profily oblastí a sieťových kariet	154
10.4 IDS	155
10.5 Protokoly	157
10.6 Profily	159
11. Kontrola AVG	161
11.1 Rozhranie kontroly	161
11.2 Preddefinované kontroly	162
11.2.1 Kontrola celého počítača	162
11.2.2 Kontrola špecifických súborov alebo priečinkov	162
11.2.3 Kontrola súčasťou Anti-Rootkit	162
11.3 Kontrola v Prieskumníkovi	172
11.4 Kontrola z príkazového riadka	173
11.4.1 Parametre kontroly z príkazového riadka	173
11.5 Plánovanie kontroly	175
11.5.1 Nastavenia plánu	175
11.5.2 Ako kontrolovať	175
11.5.3 Čo kontrolovať	175
11.6 Prehľad výsledkov kontroly	185
11.7 Podrobné výsledky kontroly	186
11.7.1 Karta Prehľad výsledkov	186
11.7.2 Karta Infekcie	186
11.7.3 Karta Spyware	186
11.7.4 Karta Upozornenia	186
11.7.5 Karta Rootkity	186
11.7.6 Karta Informácie	186
11.8 Vírusový trezor	194
12. Aktualizácie AVG	196
12.1 Úrovne aktualizácie	196
12.2 Typy aktualizácie	196
12.3 Proces aktualizácie	196



13. História udalostí	198
14. FAQ a technická podpora	200



1. Úvod

Táto príručka podrobne dokumentuje produkt **AVG Internet Security 2011**.

Gratulujeme vám ku kúpe produktu AVG Internet Security 2011!

AVG Internet Security 2011 je jeden z radu ocenených produktov AVG, ktorých účelom je priniesť vám pokoj na mysli a zabezpečiť úplnú ochranu vášho počítača. Rovnako ako všetky produkty AVG, aj program **AVG Internet Security 2011** je úplne prerobený od základov a prináša povestnú a všeobecne uznávanú bezpečnostnú ochranu od AVG v ľahšie ovládateľnej a účinnejšej podobe. Váš nový produkt **AVG Internet Security 2011** má zjednodušené rozhranie a používa agresívnejšie a rýchlejšie prehľadávanie. Automatizovali sme väčšinu bezpečnostných funkcií a vytvorili sme nové inteligentné používateľské nastavenia, aby ste mohli prispôsobiť bezpečnostné funkcie vášmu spôsobu života. Už žiaden kompromis medzi použiteľnosťou a zabezpečením!

Produkty AVG boli navrhnuté a vyrobené s cieľom chrániť váš počítač a prácu v sieti. Využívajte úplnú ochranu od AVG.

Všetky produkty AVG prinášajú

- Ochranu, ktorá zodpovedá spôsobu, akým používate počítač a internet: Internet banking a nakupovanie, surfovanie a vyhľadávanie na internete, chatovanie a používanie e-mailu, alebo preberanie súborov a používanie sociálnych sietí – AVG má pre vás ten správny bezpečnostný produkt.
- Bezproblémová ochrana, ktorej dôveruje viac ako 110 miliónov ľudí na celom svete, a za ktorou stojí globálna sieť veľmi skúsených výskumníkov.
- Ochranu posilnenú nonstop odbornou pomocou.



2. Požiadavky na inštaláciu produktu AVG

2.1. Podporované operačné systémy

AVG Internet Security 2011 sa používa na ochranu počítačov s týmito operačnými systémami:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (32-bitová a 64-bitová verzia, všetky edície)
- Windows 7 (32-bitová a 64-bitová verzia, všetky edície)

(a prípadne novšie balíky Service Pack pre konkrétne operačné systémy)

Poznámka: Súčasť [ID Protection](#) nepodporuje 64-bitové operačné systémy Windows XP. Produkt AVG Internet Security 2011 sa môže inštalovať pod týmto operačným systémom, ale bez súčasti IDP.

2.2. Minimálne a odporúčané hardvérové požiadavky

Minimálne hardvérové požiadavky pre produkt **AVG Internet Security 2011**:

- Procesor Intel Pentium 1,5 GHz
- 512 MB pamäte RAM
- 750 MB voľného miesta na pevnom disku (na účely inštalácie)

Odporúčané hardvérové požiadavky pre produkt **AVG Internet Security 2011**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB pamäte RAM
- 1400 MB voľného miesta na pevnom disku (na účely inštalácie)



3. Možnosti inštalácie produktu AVG

AVG umožňuje inštaláciu buď z inštalačného súboru, ktorý sa nachádza na inštalačnom disku CD, alebo prevzatím najnovšieho inštalačného súboru z internetových stránok AVG (<http://www.avg.com/>).

Pred začatím inštalácie programu AVG vám odporúčame, aby ste navštívili internetové stránky AVG (<http://www.avg.com/>) a vyhľadali nový inštalačný súbor. Prevzatím nového inštalačného súboru sa zabezpečí nainštalovanie najnovšej ponúkanej verzie programu AVG Internet Security 2011.

Počas procesu inštalácie vás program požiada, aby ste vložili licenčné alebo predajné číslo. Pripravte si ho ešte pred spustením inštalácie. Predajné číslo je uvedené na obale disku CD. Ak ste si zakúpili produkt AVG online, potom ste licenčné číslo dostali e-mailom.



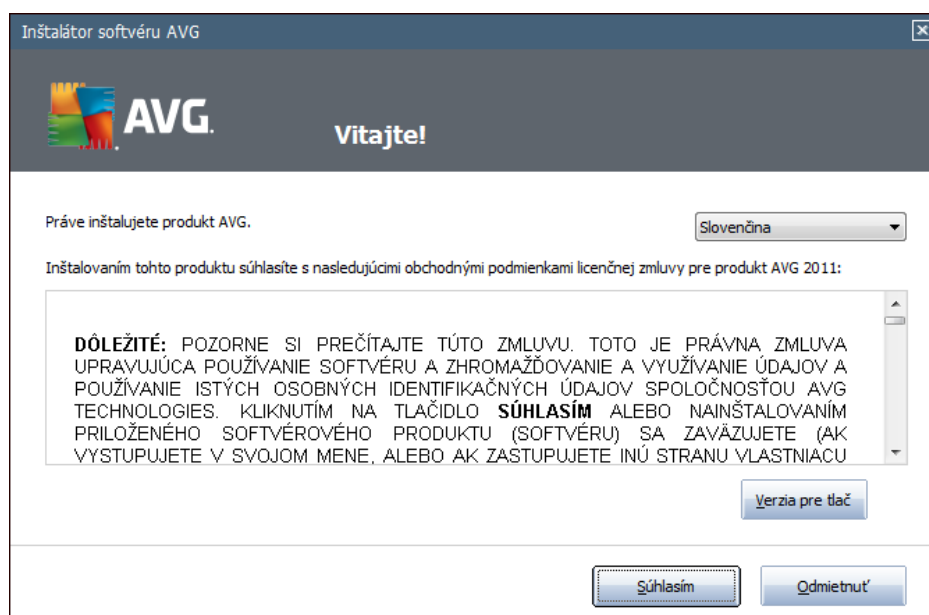
4. Proces inštalácie produktu AVG

Na nainštalovanie programu **AVG Internet Security 2011** do počítača sa musí použiť najnovší inštalračný súbor. Môžete použiť inštalračný súbor z CD, ktorý je súčasťou vašej krabicovej edície, tento súbor však môže byť zastaralý. Preto odporúčame stiahnuť si najnovší inštalračný súbor online. Súbor sa nachádza na webových stránkach AVG (<http://www.avg.com/>) v časti [Stredisko podpory/Na prevzatie](#).

Proces inštalácie je tvorený sledom dialógových okien so stručným opisom toho, čo sa má v každom kroku urobiť. V nasledujúcej časti sa nachádza vysvetlenie každého dialógového okna:

4.1. Vitajte!

Proces inštalácie sa spustí otvorením dialógového okna **Vitajte!**. Tu môžete vybrať jazyk, ktorý sa použije v procese inštalácie, a predvolený jazyk používateľského rozhrania AVG. V hornej časti dialógového okna sa nachádza rozbaľovacia ponuka so zoznamom jazykov, z ktorých si môžete vybrať:



Pozor: Tu sa nastavuje jazyk procesu inštalácie. Vybraný jazyk sa nainštaluje ako predvolený jazyk používateľského rozhrania AVG spolu s angličtinou, ktorá sa nainštaluje automaticky. Ak si želáte nainštalovať ďalšie jazyky používateľského rozhrania, vyberte ich v jednom z uvedených dialógových okien konfigurácie s názvom [Vlastné možnosti](#).

V dialógovom okne sa ďalej nachádza úplne znenie licenčnej zmluvy AVG. Pozorne si prečítajte celú zmluvu. Na potvrdenie, že ste si prečítali a pochopili zmluvu a súhlasíte s jej znením stlačte tlačidlo **Súhlasím**. Ak nesúhlasíte s licenčnou zmluvou, stlačte tlačidlo **Odmietnuť** a proces inštalácie sa ihneď ukončí.



4.2. Aktivovanie licencie AVG

V dialógovom okne **Aktivovanie licencie** zadajte vaše licenčné číslo do príslušného textového poľa.

Predajné číslo sa nachádza na obale disku CD v škatuli produktu **AVG Internet Security 2011**. Licenčné číslo sa nachádza v e-mailovej správe s potvrdením, ktorú ste dostali po zakúpení produktu **AVG Internet Security 2011** online. Číslo sa musí zadať presne tak, ako je uvedené. Ak máte k dispozícii licenčné číslo v digitálnej podobe (v *e-mailovej správe*), na jeho vloženie vám odporúčame použiť funkciu kopírovať a prilepiť.

Pokračujte v procese inštalácie stlačením tlačidla **Ďalšie**.

4.3. Výber typu inštalácie



Dialógové okno **Výber typu inštalácie** ponúka na výber dve možnosti inštalácie: **rýchlu inštaláciu** a **vlastnú inštaláciu**.

Väčšine používateľov odporúčame, aby použili **rýchlu inštaláciu**, ktorá nainštaluje program AVG v úplne automatickom režime s nastaveniami preddefinovanými dodávateľom programu. Táto konfigurácia poskytuje maximálne zabezpečenie pri optimálnom využívaní zdrojov. V budúcnosti budete môcť vždy zmeniť konfiguráciu priamo v aplikácii AVG. Ak ste vybrali možnosť **Rýchla inštalácia**, potom stlačením tlačidla **Ďalšie** prejdete na ďalšie dialógové okno [Inštalácia súčasti AVG Security Toolbar](#).

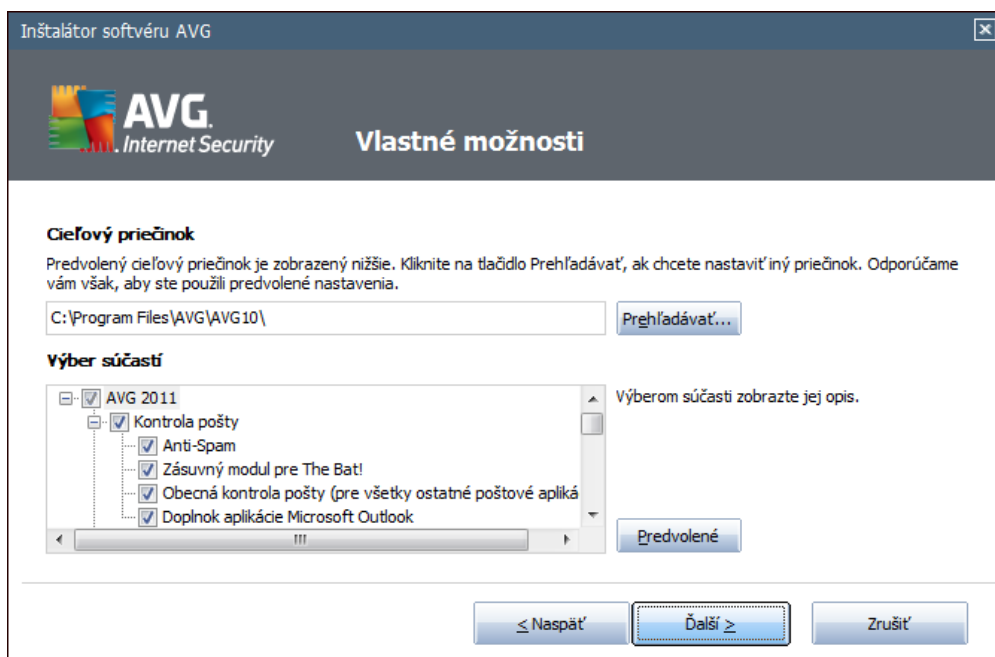
Vlastnú inštaláciu by mali používať len skúsení používatelia, ktorí majú skutočný dôvod inštalovať AVG s neštandardnými nastaveniami, napr. na účely prispôsobenia konkrétnym systémovým požiadavkám. Po výbere tejto možnosti stlačte tlačidlo **Ďalšie**. Otvorí sa dialógové okno [Vlastné možnosti](#).

V pravej časti dialógového okna vyhľadajte začiarkovacie okienko, ktoré súvisí s [mini-aplikáciou AVG](#) (len pod operačnými systémami Windows Vista a Windows 7). Ak si želáte nainštalovať túto mini-aplikáciu, začiarknite príslušné začiarkovacie okienko. [Mini-aplikácia AVG](#) sa bude potom nachádzať na bočnom paneli systému Windows a umožní okamžitý prístup k najdôležitejším funkciám produktu **AVG Internet Security 2011**, t. j. [prehľadávaniu](#) a [aktualizácii](#).



4.4. Vlastné možnosti

Dialógové okno **Vlastné možnosti** umožňuje nastaviť dva parametre inštalácie:



Cieľový priečinok

V časti **Cieľový priečinok** nastavte umiestnenie, do ktorého sa má nainštalovať **AVG Internet Security 2011**. AVG sa štandardne inštaluje do priečinka Program files na disku C:. Ak chcete zmeniť toto umiestnenie, použite tlačidlo **Prehľadávať** na otvorenie prehľadu diskových jednotiek a vyberte príslušný priečinok.

Výber súčastí

V časti **Výber súčastí** sa nachádza prehľad všetkých súčastí programu **AVG Internet Security 2011**, ktoré je možné inštalovať. Ak vám predvolené nastavenia nevyhovujú, môžete odstrániť alebo pridať konkrétne súčasti.

Môžete však vybrať len tie súčasti, ktoré sú súčasťou edície AVG, ktorú ste si zakúpili!

Zvýraznite položku v zozname **Výber súčastí** a na pravej strane v tejto časti sa zobrazia stručné informácie o príslušnej súčasti. Ďalšie informácie o funkcionalite jednotlivých súčastí sa nachádzajú v kapitole [Prehľad súčastí](#) v tejto dokumentácii. Na obnovenie predvolenej konfigurácie nastavení dodávateľom softvéru použite tlačidlo **Predvolené**.

Pokračujte stlačením tlačidla **Ďalšie**.

4.5. Inštalácia panela AVG Security Toolbar

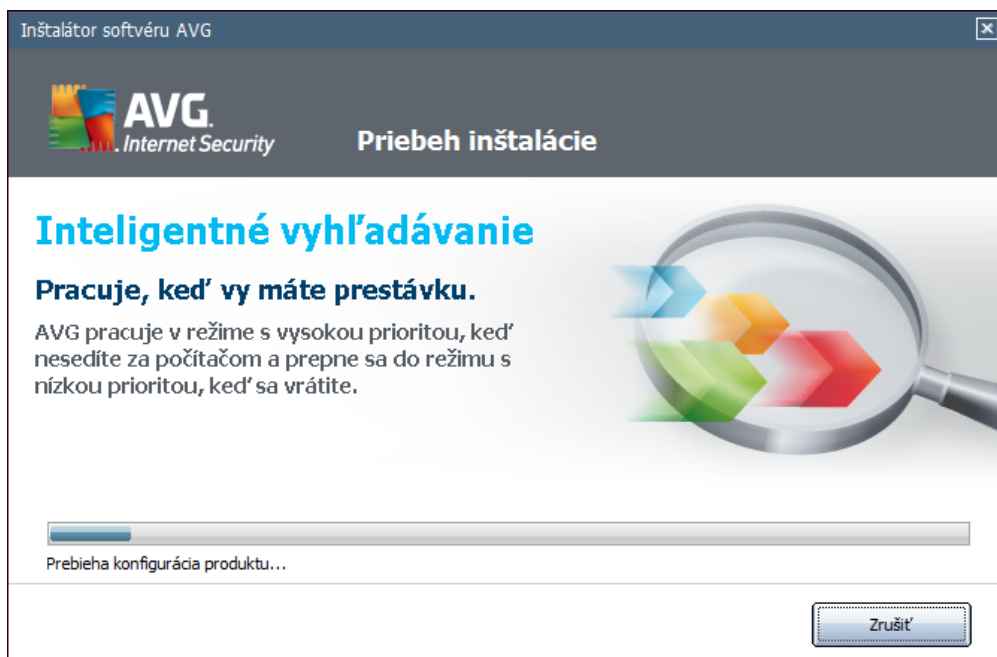


V dialógovom okne **Inštalácia súčasti AVG Security Toolbar** nastavte, či sa má nainštalovať súčasť **AVG Security Toolbar**. Ak nezmeníte predvolené nastavenia, potom sa táto súčasť nainštaluje automaticky do internetového prehliadača (v súčasnosti sú podporované prehliadače Microsoft Internet Explorer v. 6.0 a novšie a Mozilla Firefox v. 3.0 a novšie) a bude sa starať o komplexnú ochranu počas surfovania na internete.

Zároveň môžete rozhodnúť, či sa má služba AVG Secure Search (powered by Google) nastaviť ako predvolený vyhľadávač. Ak ju chcete nastaviť ako predvolenú, nechajte príslušné začiarkovacie okienko označené.

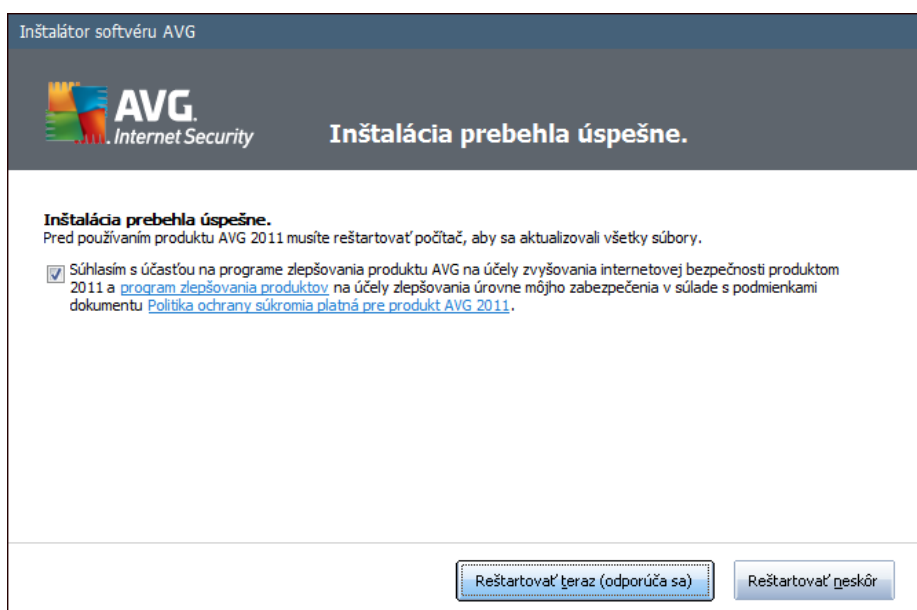
4.6. Priebek inštalácie

Dialógové okno **Priebek inštalácie** informuje o priebehu procesu inštalácie a používateľ v ňom nemusí nič robiť:



Po dokončení inštalácie sa otvorí ďalšie dialógové okno.

4.7. Inštalácia prebehla úspešne





Dialógové okno **Inštalácia prebehla úspešne** potvrdí, že sa program **AVG Internet Security 2011** celý nainštaloval a nastavil.

V tomto dialógovom okne uveďte vaše kontaktné informácie, aby ste mohli prijímať všetky informácie a novinky súvisiace s produktom. Pod registračným formulárom sa nachádzajú tieto dve možnosti:

- **Áno, chcem dostávať e-maily s bezpečnostnými novinkami a špeciálnymi ponukami súvisiacimi s produktom AVG 2011** – začiarňte toto okienko, ak chcete byť informovaný o tom, čo je nové v oblasti internetovej bezpečnosti, a chcete dostávať informácie o špeciálnych ponukách, vylepšeniach a aktualizáciách produktov AVG atď.
- **Súhlasím s účasťou v programe internetovej bezpečnosti a zlepšovania produktu AVG 2011...** – začiarňte toto okienko, ak súhlasíte s účasťou v programe zlepšovania produktov (podrobné informácie sa nachádzajú v kapitole [Rozšírené nastavenia programu AVG/Program zlepšovania produktov](#)), v rámci ktorého sa zhromažďujú anonymné informácie o detegovaných hrozbách na zvýšenie celkovej úrovne bezpečnosti internetu.

Na dokončenie procesu inštalácie je potrebné reštartovať počítač: rozhodnite, či chcete **reštartovať teraz**, alebo odložiť túto akciu – **Reštartovať neskôr**.

Poznámka: Ak používate podnikovú licenciu AVG a ak ste predtým nenainštalovali súčasť Remote Administration (pozri [Vlastné možnosti](#)), otvorí sa dialógové okno úspešnej inštalácie s týmto rozhraním:

Musíte nastaviť parametre databázy AVG DataCenter – zadajte informácie o pripojení v časti AVG DataCenter v tvare server:port. Ak tieto informácie momentálne nepoznáte, nechajte pole prázdne a konfiguráciu budete môcť nastaviť neskôr v dialógovom okne **Rozšírené nastavenia/Remote Administration**. Podrobné informácie o súčasti AVG Remote Administration sa nachádzajú v používateľskej príručke produktu AVG Business Edition; príručku si môžete prevziať na internetových stránkach AVG (<http://www.avg.com/>).



5. Po inštalácii

5.1. Registrácia produktu

Po dokončení inštalácie produktu **AVG Internet Security 2011** si zaregistrujte produkt online na internetových stránkach AVG (<http://www.avg.com/>) na stránke **Registrácia** (*postupujte podľa pokynov uvedených priamo na tejto stránke*). Registráciu získate úplný prístup k vášmu používateľskému účtu AVG, informáciám o aktualizáciách AVG a ďalším službám poskytovaným výhradne registrovaným používateľom.

5.2. Otvorenie používateľského rozhrania

Používateľské rozhranie AVG sa otvára niekoľkými spôsobmi:

- Dvakrát kliknite na ikonu AVG na paneli úloh
- Dvakrát kliknite na ikonu AVG na pracovnej ploche.
- Dvakrát kliknite na stavový riadok v spodnej časti mini-aplikácie AVG (ak je nainštalovaná; platí pre Windows Vista/Windows 7)
- V ponuke **Štart/Programy/AVG 2011/Používateľské rozhranie AVG**
- Na paneli nástrojov AVG Security Toolbar pomocou možnosti **Spustiť AVG**

5.3. Kontrola celého počítača

Existuje potenciálne riziko, že sa do vášho počítača dostal počítačový vírus ešte pred nainštalovaním produktu **AVG Internet Security 2011**. Z tohto dôvodu by ste mali spustiť prehľadávanie celého počítača, aby sa vylúčila možnosť existencie infekcie v počítači.

Pokyny na spustenie prehľadávania celého počítača sa nachádzajú v kapitole Prehľadávanie programom AVG.

5.4. Test EICAR

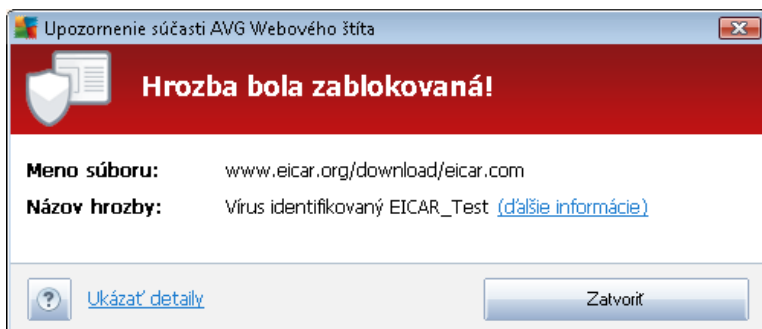
Na kontrolu, či sa program **AVG Internet Security 2011** nainštaloval správne, môžete použiť test EICAR.

Test EICAR je štandardná a absolútne bezpečná metóda, ktorá sa používa na testovanie fungovania antivírusového programu. Je bezpečná, pretože v skutočnosti nejde o vírus a neobsahuje žiadne fragmenty vírusového kódu. Väčšina produktov naň reaguje ako na vírus (*aj keď ho obvyčajne označí jednoznačným názvom, ako napríklad „EICAR-AV-Test“*). Vírus EICAR si môžete prevziať na internetových stránkach EICAR na adrese www.eicar.com, kde nájdete aj všetky potrebné informácie o teste EICAR.

Preveďte si súbor **eicar.com** a uložte ho na pevný disk počítača. Ihneď po potvrdení preberania testovacieho súboru zobrazí Webový štít upozornenie na túto skutočnosť. Zobrazenie tohto



oznámenia znamenajú, že je program AVG správne nainštalovaný v počítači.



Na internetových stránkach <http://www.eicar.com> si môžete prevziať aj komprimovanú verziu „vírusu“ EICAR (napr. s názvom *eicar_com.zip*). **Webový štít** vám umožní prevziať tento súbor a uložiť ho na pevný disk počítača, ale súčasť **Rezidentný štít** deteguje „vírus“, keď sa ho pokúsite rozbaľiť. **Ak sa programu AVG nepodarí identifikovať testovací súbor EICAR ako vírus, skontrolujte ešte raz konfiguráciu programu!**

5.5. Predvolená konfigurácia AVG

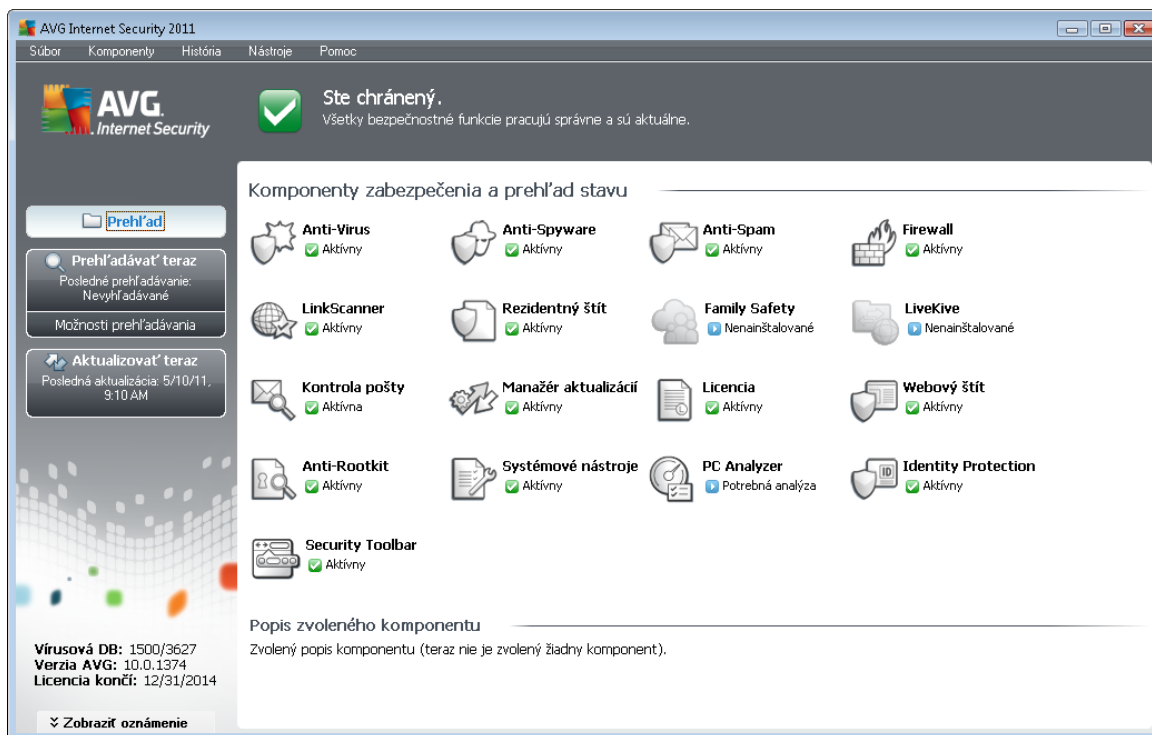
Predvolenú konfiguráciu (t. j. nastavenie aplikácie bezprostredne po inštalácii) produktu **AVG Internet Security 2011** nastavil dodávateľ softvéru tak, aby všetky súčasti a funkcie fungovali optimálnym spôsobom.

Nemeňte konfiguráciu AVG, ak na to nemáte vážny dôvod! Zmenu nastavení odporúčame robiť len skúseným používateľom.

Niektoré menšie zmeny nastavenia **súčastí AVG** je možné robiť priamo v používateľskom rozhraní konkrétnych súčastí. Ak máte pocit, že je potrebné zmeniť konfiguráciu AVG takým spôsobom, aby bola lepšie prispôbena vašim potrebám, otvorte **rozšírené nastavenia AVG**: vyberte položku v systémovej ponuke **Nástroje/Rozšírené nastavenia** a zmeňte konfiguráciu AVG v novo otvorenom dialógovom okne **Rozšírené nastavenia AVG**.

6. Používateľské rozhranie AVG

AVG Internet Security 2011 sa otvára v hlavnom okne:



Hlavné okno je rozdelené na niekoľko častí:

- **Systémová ponuka** (horný riadok v okne) je štandardná štruktúrovaná ponuka, ktorá umožňuje prístup ku všetkým súčastiam, službám a funkciám programu AVG – [podrobnosti >>](#).
- **Informácie o stave zabezpečenia** (horná časť okna) informuje o momentálnom stave nainštalovaného programu AVG – [podrobnosti >>](#)
- **Rýchle odkazy** (ľavá časť okna) umožňuje rýchly prístup k najdôležitejším a najčastejšie používaným úlohám programu AVG – [podrobnosti >>](#)
- **Prehľad súčastí** (stredná časť okna) poskytuje prehľad všetkých nainštalovaných súčastí AVG – [podrobnosti >>](#)
- **Štatistika** (ľavá spodná časť okna) poskytuje všetky štatistické informácie o fungovaní programu – [podrobnosti >>](#)
- **Ikona na paneli úloh** (pravý spodný roh monitora, na paneli úloh) informuje o momentálnom stave programu AVG – [podrobnosti >>](#)
- **Mini-aplikácia AVG** (bočný panel systému Windows, v operačných systémoch Windows Vista/7) umožňuje rýchly prístup k prehľadávaniu a aktualizáciám programu AVG – [podrobnosti >>](#)



6.1. Hlavná ponuka

Hlavná ponuka je štandardná ponuka, ktorá sa používa vo všetkých aplikáciách v operačnom systéme Windows. Je umiestnená horizontálne v hornej časti hlavného okna programu **AVG Internet Security 2011**. Hlavná ponuka sa používa na sprístupnenie konkrétnych súčastí, funkcií a služieb AVG.

Hlavná ponuka je rozdelená na päť hlavných častí:

6.1.1. Súbor

- **Ukončiť**: Zatvorí používateľské rozhranie programu **AVG Internet Security 2011**. Aplikácia AVG sa však bude aj naďalej spúšťať na pozadí a počítač bude stále chránený!

6.1.2. Súčasti

Položka **Súčasti** v ponuke programu obsahuje odkazy na všetky nainštalované súčasti AVG, ktoré otvárajú hlavné dialógové okno v používateľskom rozhraní:

- **Prehľad systému** – používa sa na otvorenie hlavného používateľského rozhrania s [prehľadom všetkých nainštalovaných súčastí a ich stavu](#).
- **Anti-Virus** chráni pred vírusmi, ktoré sa pokúšajú preniknúť do počítača – [podrobnosti >>](#)
- **Anti-Spyware** chráni počítač pred spywarom a adwarom – [podrobnosti >>](#)
- **Anti-Spam** kontroluje všetky prichádzajúce e-mailové správy a označí nežiaduce e-maily ako SPAM – [podrobnosti >>](#)
- **Firewall** kontroluje, akým spôsobom si počítač vymieňa dáta s ostatnými počítačmi na internete alebo v miestnej sieti – [podrobnosti >>](#)
- **LinkScanner** kontroluje výsledky vyhľadávania zobrazené v internetovom prehliadači – [podrobnosti >>](#)
- **E-mail Scanner** kontroluje všetky prichádzajúce a odchádzajúce správy, či neobsahujú vírusy – [podrobnosti >>](#)
- **Family Safety** pomáha monitorovať online aktivity vašich detí a chráni ich pred nevhodným obsahom internetových stránok – [podrobnosti >>](#)
- **LiveKive** zabezpečuje automatické zálohovanie vašich dát online – [podrobnosti >>](#)
- **Rezidentný štít** beží na pozadí a kontroluje kopírované, otvárané a ukladané súbory – [podrobnosti >>](#)
- **Update Manager** riadi všetky aktualizácie programu AVG – [podrobnosti >>](#)
- **Licencia** informuje o čísle, type a dátume expirácie licencie – [podrobnosti >>](#)
- **Webový štít** kontroluje všetky dáta prevzaté internetovým prehliadačom – [podrobnosti >>](#)



- **Anti-Rootkit** deteguje programy a technológie, ktoré sa pokúšajú maskovať škodlivý kód – [podrobnosti >>](#)
- **System Tools** uvádza podrobný prehľad prostredia AVG a informácie o operačnom systéme – [podrobnosti >>](#)
- **PC Analyzer** poskytuje informácie o stave počítača – [podrobnosti >>](#)
- **Identity Protection** je súčasť, ktorá chráni pred škodlivým softvérom a znemožní zlodejom identitu odčudziť vaše cenné osobné digitálne dáta – [podrobnosti >>](#)
- **Security Toolbar** umožňuje používať vybrané funkcie produktu AVG priamo v internetovom prehliadači – [podrobnosti >>](#)
- Σ \ασ Remote Administration sa nachádza len v sieťových edíciách AVG Business Editions, a to len v prípade, ak ste ju nainštalovali počas [inštalácie](#).

6.1.3. História

- **Výsledky kontroly:** Prepne sa testovacie rozhranie AVG, konkrétne na dialógové okno [Prehľad výsledkov kontroly](#).
- **Detekcia súčasti Rezidentný štít** – otvorí dialógové okno s prehľadom hrozieb detegovaných súčastou [Rezidentný štít](#)
- **Detekcia súčasti E-mail Scanner** – otvorí dialógové okno s prehľadom príloh e-mailových správ označených súčastou [E-mail Scanner](#) ako nebezpečné.
- **Nálezy súčasti Webový štít:** Otvorí dialógové okno s prehľadom hrozieb zistených súčastou [Webový štít](#)
- **Vírusový trezor:** Otvorí rozhranie úložiska karantény ([Vírusový trezor](#)), do ktorého AVG odstraňuje všetky detegované infekcie, ktoré sa z rôznych dôvodov nedajú automaticky vyliečiť. V tejto karanténe sú infikované súbory izolované, aby bolo možné garantovať bezpečnosť počítača. Infikované súbory sú zároveň uložené pre prípad, ak by sa dali v budúcnosti opraviť.
- **Protokol histórie udalostí** – otvára rozhranie protokolu histórie s prehľadom všetkých zaznamenaných činností aplikácie **AVG Internet Security 2011**.
- **Firewall** – otvára rozhranie s nastaveniami súčasti Firewall na karte [Protokoly](#) s podrobným prehľadom všetkých činností súčasti Firewall.

6.1.4. Nástroje

- **Kontrola počítača** – otvorí [rozhranie kontroly programom AVG](#) a spustí kontrolu celého počítača.
- **Kontrola vybraného priečinka** – otvorí [rozhranie kontroly programom AVG](#) a pomocou stromovej štruktúry počítača umožní definovať súbory a priečinky, ktoré majú byť skontrolované.



- **Kontrola súboru** – používa sa na skontrolovanie jedného súboru vybraného v stromovej štruktúre disku.
- **Aktualizácia** – automaticky spustí proces aktualizácie produktu **AVG Internet Security 2011**.
- **Aktualizácia z adresára** – spustí proces aktualizácie z aktualizáčnych súborov, ktoré sa nachádzajú v nastavenom priečinku na disku počítača. Túto možnosť vám však odporúčame použiť len ako núdzové riešenie, napr. v situáciách, keď nie je vytvorené pripojenie na internet (*napríklad počítač je infikovaný a odpojený od internetu; počítač je pripojený k sieti bez prístupu na internet a pod.*). V novo otvorenom okne vyberte priečinok, do ktorého ste predtým uložili aktualizáčny súbor a spustíte proces aktualizácie.
- **Rozšírené nastavenia** – otvorí dialógové okno **Rozšírené nastavenia programu AVG**, ktoré vám umožní editovať konfiguráciu produktu **AVG Internet Security 2011**. Odporúčame vám, aby ste nemenili predvolené nastavenia aplikácie definované dodávateľom softvéru.
- **Nastavenia súčasti Firewall** – otvára samostatné dialógové okno s rozšírenou konfiguráciou súčasti **Firewall**.

6.1.5. Pomocník

- **Obsah**: Otvorí súbory pomocníka AVG.
- **Získať pomoc online**: Otvorí webové stránky AVG (<http://www.avg.com/>) na stránke strediska podpory zákazníkov.
- **Webové stránky vášho produktu AVG**: Otvorí webové stránky AVG (<http://www.avg.com/>).
- **O vírusoch a hrozbách**: Otvorí online **Vírusovú encyklopédiu**, v ktorej si môžete vyhľadať podrobné informácie o identifikovanom víruse.
- **Znova aktivovať**: Otvorí dialógové okno **Aktivácia produktu AVG** s údajmi, ktoré ste vložili v dialógovom okne **Prispôbiť AVG** v **processe inštalácie**. Toto dialógové okno sa používa na vloženie licenčného čísla, buď pri nahradení predajného čísla (*číslo, s ktorým ste nainštalovali AVG*), alebo pri nahradení starého licenčného čísla (*napr. pri upgradovaní na nový produkt AVG*).
- **Registrovať teraz**: Vytvorí pripojenie na registračnú stránku na webových stránkach AVG (<http://www.avg.com/>). Vyplňte svoje registračné údaje; nárok na bezplatnú technickú podporu získajú len zákazníci, ktorí si svoj produkt AVG zaregistrujú.

Poznámka: Ak používate skúšobnú verziu produktu **AVG Internet Security 2011**, uvedené dve položky sa zobrazia v podobe **Kúpiť teraz** a **Aktivovať** a umožnia vám ihneď zakúpiť úplnú verziu programu. Ak je produkt **AVG Internet Security 2011** nainštalovaný pomocou predajného čísla, položky sa zobrazia v podobe **Registrovať** a **Aktivovať**. Ďalšie informácie sa nachádzajú v časti **Licencia** v tejto dokumentácii.

- **O produkte AVG**: Otvorí dialógové okno **Informácie** s piatimi kartami, na ktorých sa nachádzajú informácie o názve programu, verzii programu a vírusovej databázy, systémové

informácie, informácie o licenčnej zmluve a kontaktné informácie spoločnosti **AVG Technologies CZ**.

6.2. Informácie o stave zabezpečenia

Časť **informácie o stave zabezpečenia** sa nachádza v hornej časti hlavného okna AVG. V tejto časti sa vždy nachádzajú informácie o momentálnom stave zabezpečenia programom **AVG Internet Security 2011**. Pozrite si prehľad ikon, ktoré sa môžu nachádzať v tejto časti, a ich význam:



– Zelená ikona znamená, že je program AVG úplne funkčný. Počítač je úplne chránený, aktualizovaný a všetky nainštalované súčasti fungujú správne.



– Oranžová ikona upozorňuje, že jedna alebo niekoľko súčastí je nesprávne nakonfigurovaných a je potrebné venovať pozornosť ich vlastnostiam alebo nastaveniam. Newskytuje sa žiaden kritický problém programu AVG a pravdepodobne ste sa z nejakého dôvodu rozhodli niektorú súčasť vypnúť. Stále ste chránený programom AVG. Venujte však pozornosť nastaveniam problémovej súčasti! Jej názov bude uvedený v časti **Informácie o stave zabezpečenia**.

Táto ikona sa zobrazí aj vtedy, keď sa z nejakého dôvodu rozhodnete [ignorovať chybový stav súčasti](#) (možnosť „Ignorovať stav súčasti“ sa nachádza v kontextovej ponuke, ktorá sa otvára kliknutím pravým tlačidlom myši na ikone príslušnej súčasti v prehľade súčastí v hlavnom okne programu AVG). Môže sa vyskytnúť situácia, keď bude potrebné použiť túto možnosť; dôrazne vám však odporúčame, aby ste funkciu „**Ignorovať stav súčasti**“ čo najskôr znova vyplli.



– Červená ikona informuje o kritickom stave programu AVG! Jedna alebo niekoľko súčastí nefunguje správne a AVG nedokáže chrániť počítač. Venujte okamžitú pozornosť odstráneniu uvedeného problému. Ak nedokázate odstrániť chybu sami, kontaktujte tím [technickej podpory AVG](#).

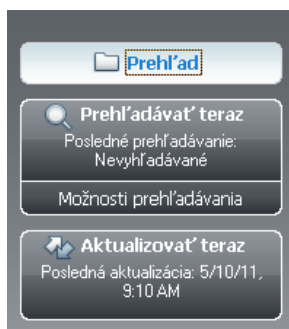
Ak nie je program AVG nastavený tak, aby poskytoval optimálny výkon, potom sa vedľa informácie o stave zabezpečenia nachádza nové tlačidlo s názvom Opraviť (alebo Opraviť všetko, ak sa problém týka viac ako jednej súčasti). Stlačením tlačidla spustíte automatický proces kontroly a konfigurácie programu. Je to jednoduchý spôsob ako nastaviť optimálny výkon programu AVG a dosiahnuť maximálnu úroveň zabezpečenia!

Odporúčame vám, aby ste venovali pozornosť **informáciám o stave zabezpečenia** a v prípade, že správa upozorňuje na problém, pokúsili sa ho ihneď odstrániť. V opačnom prípade počítač nebude dokonale chránený!

Poznámka: Informáciu o stave programu AVG získate kedykoľvek pohľadom na [ikonu na paneli úloh](#).

6.3. Rýchle odkazy

Rýchle odkazy (v ľavej časti [používateľského rozhrania AVG](#)) umožňujú získať okamžitý prístup k najdôležitejším a najčastejšie používaným funkciám programu AVG:



- **Prehľad** – tento odkaz sa používa na prepnutie práve otvoreného rozhrania AVG na hlavné rozhranie s prehľadom všetkých nainštalovaných súčastí – pozri kapitolu [Prehľad súčastí >>](#)
- **Kontrolovať teraz** – štandardne toto tlačidlo zobrazí informácie (typ kontroly, dátum posledného spustenia) o poslednej spustenej kontrole. Môžete buď spustiť príkaz **Kontrolovať teraz** na opakované spustenie rovnakej kontroly, alebo kliknutím na odkaz **Možnosti kontroly** otvoriť rozhranie kontrol programom AVG, ktoré umožňuje spustiť kontroly, naplánovať kontroly a editovať ich parametre – pozri kapitolu [Kontrola programom AVG >>](#)
- **Aktualizovať teraz** – odkaz zobrazí dátum posledného spustenia aktualizácie. Stlačením tohto tlačidla sa otvorí rozhranie aktualizácie a ihneď sa spustí proces aktualizácie programu AVG – pozri kapitolu [Aktualizácia AVG >>](#)

Tieto odkazy sa vždy nachádzajú v používateľskom rozhraní. Ak použijete rýchly odkaz na spustenie konkrétneho procesu, potom sa v grafickom používateľskom rozhraní otvorí nové dialógové okno, ale rýchle odkazy budú stále dostupné. Okrem toho sa prebiehajúci proces znázorní aj v grafickej podobe.

6.4. Prehľad súčastí

Časť **Prehľad súčastí** sa nachádza v strede [používateľského rozhrania AVG](#). Táto časť je rozdelená na dve oblasti:

- Prehľad všetkých nainštalovaných súčastí, ktorý je tvorený panelom s ikonami súčastí a informáciou o tom, či je príslušná súčasť zapnutá alebo vypnutá.
- Opis vybranej súčasti

V programe **AVG Internet Security 2011** sa v časti **Prehľad súčastí** nachádzajú informácie o týchto súčastiach:

- **Anti-Virus** chráni pred vírusmi, ktoré sa pokúšajú preniknúť do počítača – [podrobnosti >>](#).



- **Anti-Spyware** chráni počítač pred spywarom a adwarom – [podrobnosti >>](#)
- **Anti-Spam** kontroluje všetky prichádzajúce e-mailové správy a označí nežiaduce e-maily ako SPAM – [podrobnosti >>](#)
- **Firewall** kontroluje, akým spôsobom si počítač vymieňa dáta s ostatnými počítačmi na internete alebo v miestnej sieti – [podrobnosti >>](#)
- **LinkScanner** kontroluje výsledky vyhľadávania zobrazené v internetovom prehliadači – [podrobnosti >>](#)
- **E-mail Scanner** kontroluje všetky prichádzajúce a odchádzajúce správy, či neobsahujú vírusy – [podrobnosti >>](#)
- **Rezidentný štít** beží na pozadí a kontroluje kopírované, otvárané a ukladané súbory – [podrobnosti >>](#)
- **Family Safety** pomáha monitorovať online aktivity vašich detí a chráni ich pred nevhodným obsahom internetových stránok – [podrobnosti >>](#)
- **LiveKive** zabezpečuje automatické zálohovanie vašich dát online – [podrobnosti >>](#)
- **Update Manager** riadi všetky aktualizácie programu AVG – [podrobnosti >>](#)
- **Licencia** informuje o čísle, type a dátume expirácie licencie – [podrobnosti >>](#)
- **Webový štít** kontroluje všetky dáta prevzaté internetovým prehliadačom – [podrobnosti >>](#)
- **Anti-Rootkit** deteguje programy a technológie, ktoré sa pokúšajú maskovať škodlivý kód – [podrobnosti >>](#)
- **System Tools** uvádza podrobný prehľad prostredia AVG a informácie o operačnom systéme – [podrobnosti >>](#)
- **PC Analyzer** poskytuje informácie o stave počítača – [podrobnosti >>](#)
- **Identity Protection** je súčasť, ktorá chráni pred škodlivým softvérom a znemožní zlodejom identitu odčudzit' vaše cenné osobné digitálne dáta – [podrobnosti >>](#)
- **Security Toolbar** umožňuje používať vybrané funkcie produktu AVG priamo v internetovom prehliadači – [podrobnosti >>](#)
- **Σ Remote Administration** sa nachádza len v sieťových edíciách AVG Business Editions, a to len v prípade, ak ste ju nainštalovali počas [inštalácie](#).

Jedným kliknutím na ikonu ktorejkoľvek súčasti zvýrazníte súčasť v prehľade súčastí. V spodnej časti používateľského rozhrania sa zároveň zobrazí opis základných funkcií súčasti. Dvojším kliknutím na ikonu otvorte rozhranie konkrétnej súčasti so základnými štatistickými informáciami.

Kliknutím pravým tlačidlom na ikonu súčasti otvorte kontextovú ponuku; okrem toho, že sa otvorí



grafické rozhranie súčasti, môžete použiť aj možnosť **Ignorovať stav súčasti**. Vyberte túto možnosť, ak ste si vedomý [chybového stavu súčasti](#), ale z nejakého dôvodu si želáte nechať program AVG v tomto stave a nechcete byť informovaný pomocou [ikony na paneli úloh](#).

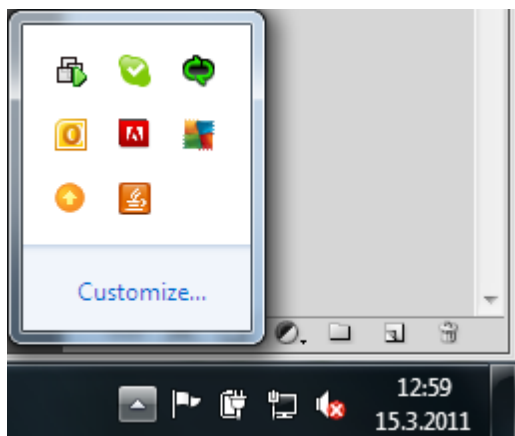
6.5. Štatistika

Časť **Štatistika** sa nachádza v ľavej spodnej časti [používateľského rozhrania AVG](#). Nachádzajú sa v nej informácie o činnosti programu:

- **Vírusová databáza** – informuje o momentálne nainštalovanej verzii vírusovej databázy.
- **Verzia AVG** – informuje o nainštalovanej verzii produktu AVG (číslo je v tvare 10.0.xxxx, kde 10.0 je verzia produktového radu a xxxx znamená číslo zostavy).
- **Platnosť licencie vyprší** – informuje o dátume vypršania platnosti vašej licencie AVG.

6.6. Ikona na paneli úloh

Ikona na paneli úloh (na paneli úloh operačného systému Windows) informuje o momentálnom stave produktu **AVG Internet Security 2011**. Vždy sa nachádza na paneli úloh, bez ohľadu na to, či je hlavného okna programu AVG otvorené alebo zatvorené:



Farebná  **ikona na paneli úloh** informuje, že sú všetky súčasti AVG zapnuté a úplne funkčné. Ikona AVG na paneli úloh sa zobrazí v úplných farbách aj v prípade, keď sa vyskytne chybový stav programu AVG, ale ste si úplne vedomý tejto situácie a vedome ste sa rozhodli [ignorovať stav súčasti](#). Ikona s výkričníkom  informuje o výskyte problému (vypnutá súčasť, chybový stav a pod.). Dvojitým kliknutím na **ikonu na paneli úloh** otvorte hlavné okno, ktoré vám umožní zmeniť nastavenia súčasti.

Ikona na paneli úloh ďalej informuje o prebiehajúcich aktivitách programu AVG a možných zmenách stavu programu (napr. automatickom spustení naplánovanej kontroly alebo aktualizácie, prepnutí profilu súčasti Firewall, zmene stavu súčasti, výskyte chybového stavu...) pomocou prekryvacieho okna, ktoré sa otvorí na ikone AVG na paneli úloh:



Ikona na paneli úloh sa môže použiť aj ako rýchly odkaz na otvorenie hlavného okna programu AVG – dvakrát kliknite na túto ikonu. Kliknutím pravým tlačidlom myši na **ikonu na paneli úloh** sa otvorí krátko kontextová ponuka s týmito možnosťami:

- **Otvoriť používateľské rozhranie AVG** – kliknutím na túto položku sa otvorí [používateľské rozhranie AVG](#)
- **Kontroly** – kliknutím na túto položku sa otvára kontextová ponuka
- **Firewall** – kliknutím na túto možnosť sa otvára kontextová ponuka s možnosťami nastavenia súčasti [Firewall](#), ktorá umožňuje editovať základné parametre: [Stav súčasti Firewall](#) (Súčasť Firewall je zapnutá/Súčasť Firewall je vypnutá/Núdzový režim), [prepnutie režimu hrania](#) a [profily súčasti Firewall](#)
- **Otvoriť PC Analyzer** – kliknutím na túto možnosť sa spúšťa súčasť [PC Analyzer](#).
- **Spustené kontroly** – táto položka sa zobrazí len v prípade, keď na počítači práve beží kontrola. Tejto kontrole môžete potom nastaviť prioritu, alebo ju môžete zastaviť alebo pozastaviť. Ďalej sa tu nachádzajú tieto funkcie: *Nastaviť prioritu pre všetky kontroly*, *Pozastaviť všetky kontroly* a *Zastaviť všetky kontroly*.
- **Aktualizovať teraz** – spustí okamžitú [aktualizáciu](#)
- **Pomocník** – otvorí súbor pomocníka na úvodnej strane.

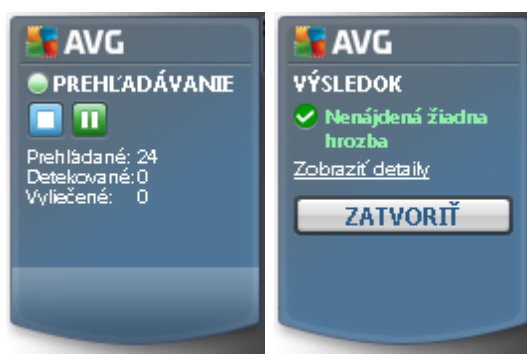
6.7. Mini-aplikácia AVG

Mini-aplikácia AVG sa nachádza na pracovnej ploche operačného systému Windows (*bočnom paneli systému Windows*). Túto aplikáciu podporujú len operačné systémy Windows Vista a Windows 7. **Mini-aplikácia AVG** umožňuje okamžitý prístup k najdôležitejším funkciám programu AVG Internet Security 2011, t. j. [prehľadávaniu](#) a [aktualizácii](#):

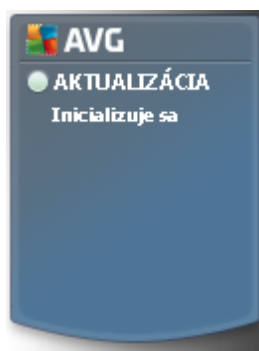


Mini-aplikácia AVG ponúka tieto funkcie s okamžitým prístupom:

- **Kontrolovať teraz** – kliknutím na odkaz **Kontrolovať teraz** sa priamo spustí [kontrola celého počítača](#). Priebeh kontroly môžete pozorovať v prepínajúcom sa používateľskom rozhraní mini-aplikácie. Stručný štatistický prehľad informuje o počte skontrolovaných objektov a detegovaných a vyliečených hrozieb. Počas kontroly môžete vždy pozastaviť  alebo zastaviť  kontrolu. Podrobné informácie súvisiace s výsledkami prehľadávania sa nachádzajú v štandardnom dialógovom okne [Prehľad výsledkov prehľadávania](#), ktoré sa otvára priamo v mini aplikácii výberom možnosti **Zobraziť podrobnosti** (príslušné výsledky prehľadávania budú uvedené pod položkou **Prehľadávanie z mini-aplikácie na bočnom paneli**).



- **Aktualizovať teraz** – kliknutím na odkaz **Aktualizovať teraz** sa AVG aktualizuje priamo v mini-aplikácii:



- **Odkaz na Twitter**  – otvorí nové rozhranie **mini-aplikácie AVG** s prehľadom najnovších informačných kanálov AVG zverejnených na stránkach Twitter. Kliknutím na odkaz **Zobraziť všetky informačné kanály služby Twitter súvisiace s AVG** otvorte nové okno internetového prehliadača s internetovými stránkami Twitter, konkrétne stránkou so správami súvisiacimi s AVG:



- **Odkaz na Facebook**  – otvorí internetový prehliadač s internetovými stránkami Facebook, konkrétne na stránke **komunity AVG**.
- **LinkedIn**  – táto možnosť je dostupná len v rámci sieťovej inštalácie (t.j. pod podmienkou, že ste si produkt AVG nainštalovali pomocou licencie pre jednu z edícií AVG Business Edition) a otvára internetový prehliadač na internetových stránkach **AVG SMB Community** v sociálnej sieti LinkedIn.
- **PC Analyzer**  – otvorí používateľské rozhranie súčasti [PC Analyzer](#).
- **Vyhľadávacie okienko** – zadajte kľúčové slovo na okamžité zobrazenie výsledkov vyhľadávania v novom otvorenom okne vo vašom predvolenom internetovom prehliadači.



7. Súčasti AVG

7.1. Anti-Virus

7.1.1. Princíp fungovania súčasti Anti-Virus

Kontrolné jadro antivírusového softvéru kontroluje všetky súbory a súborové aktivity (otváranie/zatváranie súborov atď.) z hľadiska prítomnosti známych vírusov. Každý detegovaný vírus sa zablokuje, aby nemohol vykonávať žiadnu činnosť, a potom sa vymaže, alebo sa premiestni do karantény. Väčšina antivírusových softvérov používa aj heuristickú kontrolu, ktorá kontroluje typické vlastnosti vírusov v súboroch, tzv. vírusové signatúry. To znamená, že antivírusový program dokáže detegovať nový, neznámy vírus, ak tento nový vírus obsahuje isté typické vlastnosti existujúcich vírusov.

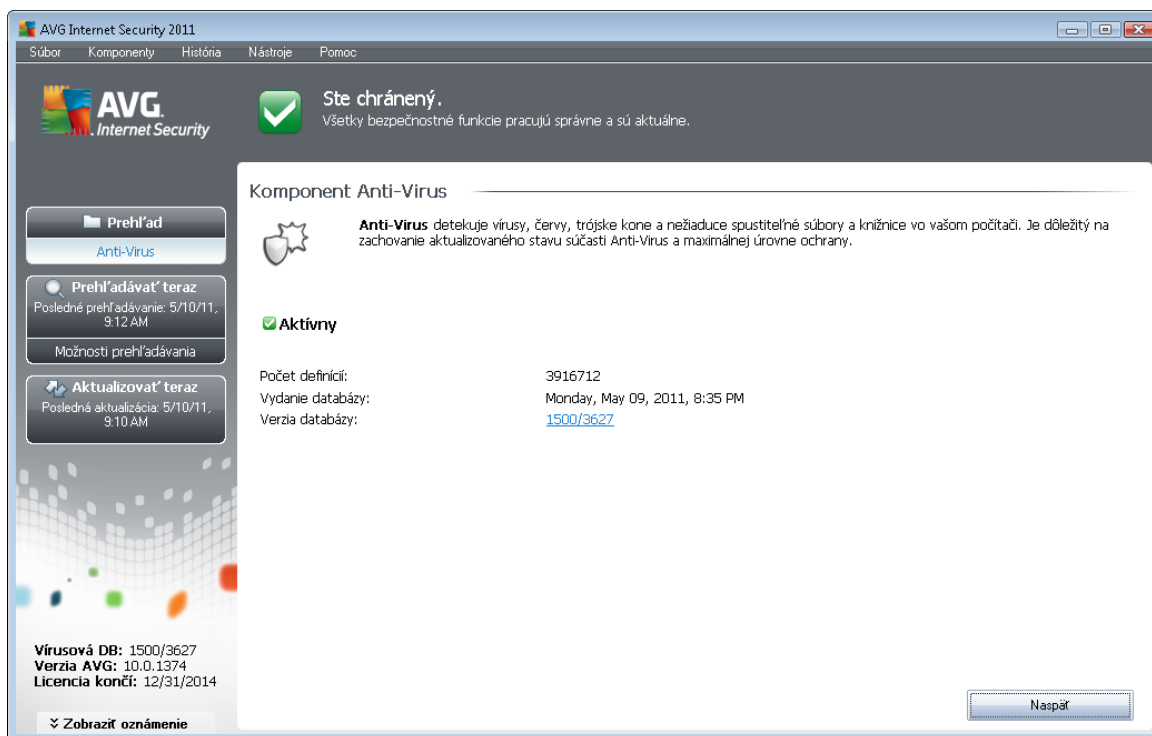
Dôležitou funkciou antivírusovej ochrany je, že neumožní spustiť na počítači žiaden známy vírus!

Zatiaľ čo pri použití len jednej technológie sa nemusí podariť detegovať alebo identifikovať vírus, **Anti-Virus** využíva naraz niekoľko technológií, aby sa garantovala ochrana počítača pred vírusmi:

- Kontrola – vyhľadávanie reťazcov znakov, ktoré sú charakteristické pre konkrétny vírus.
- Heuristická analýza – dynamická emulácia inštrukcií v kontrolovaných objektoch vo virtuálnom prostredí počítača.
- Generická detekcia – detekcia inštrukcií, ktoré sú charakteristické pre konkrétny vírus alebo skupinu vírusov.

AVG dokáže zároveň analyzovať a detegovať spustiteľné aplikácie alebo knižnice DLL, ktoré by mohli byť v počítači potenciálne nechcené. Tieto hrozby nazývame potenciálne nežiaduce programy (rôzne druhy spywaru, adwaru atď.). AVG ďalej kontroluje podozrivé záznamy v databáze Registry, dočasné internetové súbory a sledovacie súbory cookies a spracuje všetky potenciálne škodlivé položky rovnakým spôsobom ako každú inú infekciu.

7.1.2. Rozhranie súčasti Anti-Virus



Rozhranie súčasti **Anti-Virus** obsahuje niektoré základné informácie o funkcionalite, momentálnom stave (*Súčasť Anti-Virus je zapnutá*) a základné štatistické informácie o súčasti **Anti-Virus**:

- **Počet definícií** – číslo informujúce o počte vírusov definovaných v aktuálnej verzii vírusovej databázy.
- **Verzia databázy** – informuje o tom, kedy a v akom čase bola vírusová databáza aktualizovaná.
- **Verzia databázy** – informuje o čísle momentálne nainštalovanej verzii vírusovej databázy; toto číslo rastie s každou aktualizáciou vírusovej databázy.

V rozhraní tejto súčasti sa nachádza len jedno ovládacie tlačidlo (**Naspäť**); stlačením tohto tlačidla sa vrátite na základné [používateľské rozhranie AVG](#) (prehľad súčastí).

7.2. Anti-Spyware

7.2.1. Princíp fungovania súčasti Anti-Spyware

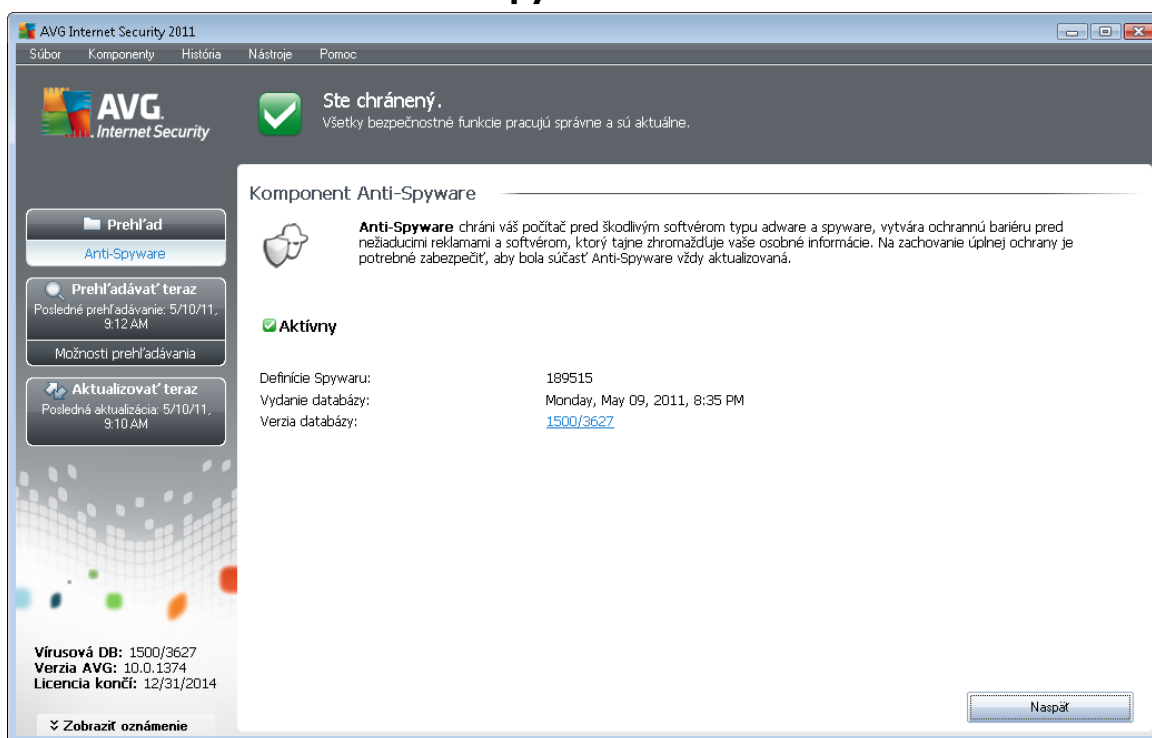
Základná definícia spywaru: Spyware je druh škodlivého softvéru, t. j. softvér, ktorý zhromažďuje informácie z počítača bez vedomia alebo súhlasu jeho používateľa. Niektoré aplikácie typu spyware môžu byť nainštalované aj zámerne a často zobrazujú reklamu, prekryvacie okná, alebo obsahujú rôzne druhy neprijemného softvéru.



Najčastejšie sa vyskytujúcim zdrojom infekcie sú v súčasnosti internetové stránky s potenciálne nebezpečným kódom. Škodlivý kód sa šíri aj inými metódami prenosu, napr. e-mailom alebo červami a vírusmi. Základná ochrana spočíva v používaní kontrolných programov bežiacich na pozadí (tzv. **Anti-Spyware**), ktoré fungujú ako rezidentný štít a kontrolujú aplikácie na pozadí, keď ich spúšťate.

Existuje aj potenciálne riziko, že sa škodlivý program dostal do vášho počítača pred nainštalovaním programu AVG, resp. že ste zabudli nainštalovať najnovšiu [databázu a programové aktualizácie](#) používaného programu **AVG Internet Security 2011**. Z tohto dôvodu vám AVG umožňuje skontrolovať celý počítač a vyhľadať škodlivé programy a spyware. Deteguje aj spiaci a neaktívny škodlivý softvér, t. j. taký, ktorý bol prevzatý do počítača, ale doposiaľ sa neaktivoval.

7.2.2. Rozhranie súčasti Anti-Spyware



Rozhranie súčasti **Anti-Spyware** obsahuje stručný prehľad funkcionality, informácie o momentálnom stave a niektoré štatistické informácie o súčasti **Anti-Spyware**:

- **Definície spywaru** – číslo informuje o počte vzoriek spywaru definovaných v najnovšej verzii databázy spywaru.
- **Verzia databázy** – informuje o tom, kedy a v akom čase bola databáza spywaru aktualizovaná.
- **Verzia databázy** – informuje o čísle najnovšej verzie databázy spywaru; toto číslo rastie s každou aktualizáciou vírusovej databázy.

V rozhraní tejto súčasti sa nachádza len jedno ovládacie tlačidlo (**Naspäť**); stlačením tohto tlačidla sa vrátite na základné [používateľské rozhranie AVG](#) (prehľad súčastí).

7.3. Anti-Spam

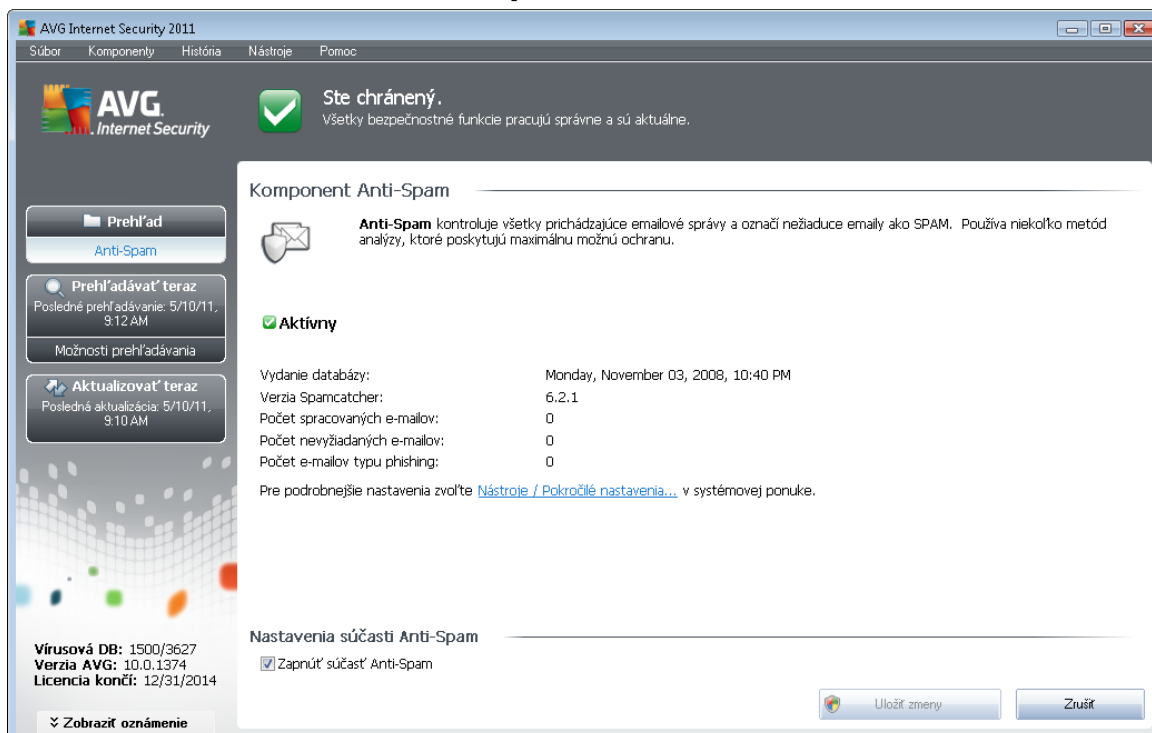
Spam označuje nevyžiadané e-mailové správy, väčšinou propagujúce výrobok alebo službu, ktoré sa hromadne rozosielať na veľký počet e-mailových adries a zaplňajú poštové schránky prijímateľov. Spam neoznačuje legítimne komerčné e-maily, s ktorých prijímaním zákazníci poskytli súhlas. Spam je nielen otravný, ale niekedy môže byť aj zdrojom podvodov, vírusov alebo môže obsahovať urážlivé informácie.

7.3.1. Princíp fungovania súčasti Anti-Spam

AVG Anti-Spam kontroluje všetky prichádzajúce e-mailové správy a označí nežiaduce e-maily ako spam. **AVG Anti-Spam** dokáže zmeniť predmet e-mailovej správy (ktorá bola označená ako spam) pridaním špeciálneho textového reťazca. Potom môžete jednoducho filtrovať e-mailové správy v poštovej aplikácii.

Súčasť AVG Anti-Spam používa niekoľko metód analýzy na spracovanie jednotlivých e-mailových správ a prináša najvyššiu možnú úroveň ochrany pred neželanými e-mailovými správami. **AVG Anti-Spam** používa pravidelne aktualizovanú databázu na detegovanie spamu. Rovnako môžete použiť [servery RBL](#) (verejné databázy e-mailových adries „známych odosielateľov spamu“) a ručne pridať e-mailové adresy do vlastného [zoznamu povolených](#) (nikdy neoznačiť ako spam) a [zoznamu blokovaných](#) (vždy označiť ako spam).

7.3.2. Rozhranie súčasti Anti-Spam



V dialógovom okne súčasti **Anti-Spam** sa nachádza krátky text, ktorý opisuje funkcionality súčasti, a obsahuje informácie o jej aktuálnom stave a tieto štatistické informácie:

- **Verzia databázy** – informuje o tom, kedy a v akom čase bola databáza spamu



aktualizovaná a zverejnená.

- **Verzia programu Spamcatcher** – informuje o čísle najnovšej verzie jadra súčasti Anti-Spam.
- **Počet spracovaných e-mailov** – informuje o tom, koľko e-mailových správ bolo prehľadaných od posledného spustenia jadra súčasti Anti-Spam.
- **Počet spamových e-mailov** – informuje o tom, koľko správ bolo označených ako spam medzi všetkými prehľadanými e-mailmi.
- **Počet e-mailov typu phishing** – informuje o tom, koľko správ bolo označených ako útok typu phishing medzi všetkými prehľadanými e-mailmi.

V dialógovom okne **Anti-Spam** sa ďalej nachádza odkaz na [nástroje/rozšírené nastavenia](#). Použite odkaz na otvorenie prostredia s rozšírenou konfiguráciou súčasti všetkých súčastí programu **AVG Internet Security 2011**.

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu AVG, ak na to nemáte skutočný dôvod. Zmenu nastavení by mali robiť len skúsení používatelia.

V rozhraní tejto súčasti sa nachádza len jedno ovládacie tlačidlo (**Naspäť**); stlačením tohto tlačidla sa vrátite na základné [používateľské rozhranie AVG](#) (prehľad súčastí).

7.4. Firewall

Firewall je systém, ktorý vynucuje politiku riadenia prístupu medzi dvomi alebo viacerými sieťami blokovaním resp. povolením prenosov. Firewall má skupinu pravidiel, ktoré chránia internú sieť pred útokmi zvonka (zvyčajne z internetu) a riadi komunikáciu na každom jednom sieťovom porte. Komunikácia sa vyhodnotí podľa definovaných pravidiel, a potom sa buď povolí alebo zakáže. Keď Firewall zistí pokus o preniknutie do systému, zablokuje tento pokus a nedovolí narušiteľovi vstúpiť do počítača.

Súčasť Firewall je nastavená tak, aby umožňovala alebo blokovala internú alebo externú komunikáciu (oboma smermi, dnu aj von) na definovaných portoch a pre definované softvérové aplikácie. Brána firewall sa môže nastaviť napríklad tak, aby umožňovala tok webových dát smerom dnu a von, len keď sa používa program Microsoft Explorer. Každý pokus o prenos webových dát iným prehliadačom sa zablokuje.

Firewall chráni informácie, ktoré vás môžu osobne identifikovať, pred odoslaním z vášho počítača bez vášho povolenia. Kontroluje spôsob, akým si váš počítač vymieňa dáta s ostatnými počítačmi na internete alebo v miestnej sieti. V rámci organizácie firewall zároveň chráni jednotlivé počítače pred útokmi pochádzajúcimi od interných používateľov iných počítačov v sieti.

Odporúčanie: Vo všeobecnosti sa neodporúča používať viac ako jednu bránu firewall na tom istom počítači. Nainštalovaním viacerých brán firewall sa nezvýši úroveň zabezpečenie počítača. Vzniká však vyššia pravdepodobnosť, že medzi týmito dvomi aplikáciami nastane konflikt. Preto vám odporúčame, aby ste používali len jednu bránu firewall na počítači a vypli všetky ostatné, aby sa eliminovalo riziko vzniku konfliktu a súvisiacich problémov.



7.4.1. Princíp fungovania súčasti Firewall

V AVG komponent **Firewall** riadi všetky prenosy na každom sieťovom porte vášho počítača. Na základe zadefinovaných pravidiel **Firewall** vyhodnocuje aplikácie, ktoré sa buď spúšťajú na vašom počítači (a chcú sa pripojiť k Internetu/lokálnej sieti) alebo aplikácie, ktoré sa približujú k vášmu počítaču zvonku a snažia sa na váš počítač pripojiť. Pri každej z týchto aplikácií **Firewall** potom buď povolí alebo zakáže komunikáciu na sieťových portoch. Ak je aplikácia neznáma (teda nemá žiadne zadefinované pravidlá **Firewallu**), **Firewall** sa vás štandardne spýta, či chcete blokovať alebo povoliť tento pokus o komunikáciu.

Poznámka: AVG Firewall nie je určený pre serverové platformy!

Čo dokáže AVG Firewall:

- Povoliť alebo blokovať komunikačné pokusy známych aplikácií automaticky alebo vás požiadať o potvrdenie
- Použiť úplné [profily](#) s vopred definovanými pravidlami, podľa vašich potrieb.
- [Prepnúť profily](#) automaticky, keď sa pripájate na rôzne siete alebo používate rôzne sieťové karty.

7.4.2. Profily súčasti Firewall

Firewall umožňuje definovať konkrétne bezpečnostné pravidlá podľa toho, či sa počítač nachádza v doméne, alebo či ide o samostatný počítač alebo dokonca notebook. Každá z týchto možností si vyžaduje inú úroveň ochrany a jednotlivé úrovne patria do príslušných profilov. Povedané v skratke, profil súčasti **Firewall** je špeciálna konfigurácia súčasti **Firewall** a program umožňuje použiť niekoľko takýchto vopred definovaných konfigurácií.

Definované profily

- **Povoliť všetky** – systémový profil súčasti **Firewall**, ktorý vopred nastavil výrobca, a ktorý je vždy prítomný. Keď je tento profil aktivovaný, potom je celá sieťová komunikácia povolená a neuplatňujú sa žiadne pravidlá bezpečnostnej politiky, rovnako ako keby bola ochrana **Firewall** vypnutá (t. j. *všetky aplikácie sú povolené, ale pakety sa stále kontrolujú – na úplné vypnutie filtrovania je potrebné vypnúť súčasť Firewall*). Tento systémový profil sa nedá kopírovať, vymazať a jeho nastavenia sa nedajú meniť.
- **Blokovať všetky** – systémový profil súčasti **Firewall**, ktorý vopred nastavil výrobca, a ktorý je vždy prítomný. Keď je tento profil aktivovaný, potom sa každá sieťová komunikácia zablokuje a počítač je nedostupný z vonkajších sietí a zároveň nemôže komunikovať smerom von. Tento systémový profil sa nedá kopírovať, vymazať a jeho nastavenia sa nedajú meniť.
- **Vlastné profily:**
 - o **Priamo pripojený na internet** – nastavenie vhodné pre bežné domáce stolové počítače pripojené priamo na internet, alebo notebooky pripájajúce sa na internet

mimo zabezpečenej podnikovej siete. Vyberte túto možnosť, ak sa pripájate z domu, alebo ste pripojený k malej podnikovej sieti bez centrálného riadenia. Túto možnosť vyberte aj v prípade, keď cestujete a pripájate sa s notebookom na rôznych neznámych a prípadne nezabezpečených miestach (*v internetových kaviarňach, na hotelovej izbe a pod.*). Vytvorí sa prísnejšie pravidlá, keďže sa predpokladá, že tieto počítače nepoužívajú žiadnu ďalšiu ochranu, a preto si vyžadujú maximálnu ochranu.

- o **Počítač v doméne** – nastavenie vhodné pre počítače v miestnej sieti, napr. škole alebo podnikovej sieti. Predpokladá sa, že sieť je chránená ďalšími prostriedkami, aby sa mohla použiť nižšia úroveň zabezpečenia ako v prípade samostatného počítača.
- o **Malá domáca alebo podniková sieť** – možnosť vhodná pre počítače v malej sieti, napr. domácnosti alebo malom podniku, zvyčajne ide len o niekoľko vzájomne pripojených počítačov bez „centrálného“ správcu.

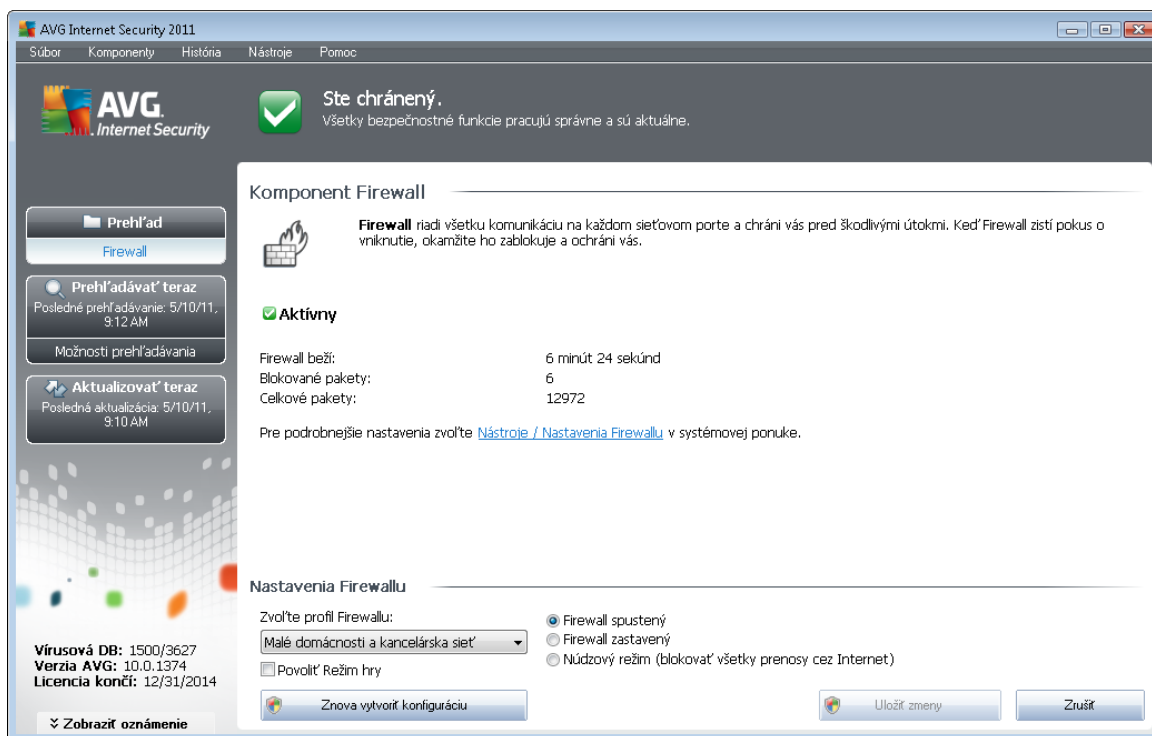
Prepínanie profilov

Funkcia Prepínanie profilov umožňuje súčasti [Firewall](#) automaticky prepnúť na definovaný profil pri použití konkrétnej sieťovej karty, alebo keď je počítač pripojený ku konkrétnemu typu siete. Ak nebol sieťovej oblasti doposiaľ pridelený žiaden profil, potom pri ďalšom pripojení k tejto oblasti otvorí súčasť [Firewall](#) dialógové okno, ktorým vás požiada, aby ste pridelili profil.

Dialógové okno [Profily oblastí a sieťových kariet](#) umožňuje prideliť profily rozhraniám všetkých miestnych sietí alebo oblastí a definovať ďalšie nastavenia. Zároveň umožňuje vypnúť túto funkciu, keď ju nechcete používať (*potom sa pri každom type pripojenia použije predvolený profil*).

Túto funkciu používajú zvyčajne používatelia, ktorí vlastnia notebook a používajú rôzne typy pripojenia. Ak vlastníte stolový počítač a používate len jeden typ pripojenia (*napr. káblové pripojenie na internet*), nemusíte si robiť starosti s prepínaním profilov, pretože ho zrejme nikdy nevyužijete.

7.4.3. Rozhranie súčasti Firewall



Rozhranie súčasti **Firewall** poskytuje niektoré základné informácie o jej funkcionalite, stave a stručný prehľad štatistických informácií o jej činnosti:

- **Súčasť Firewall je zapnutá** – čas, ktorý uplynul od spustenia súčasti Firewall.
- **Blokovane pakety** – počet blokovanych paketov z celkového počtu kontrolovaných paketov.
- **Celkové pakety** – počet všetkých paketov kontrolovaných v čase, keď bola súčasť Firewall zapnutá.

Nastavenia súčasti Firewall

- **Vybrať profil súčasti Firewall** – v rozbaľovacej ponuke vyberte jeden z uvedených profilov – vždy sú k dispozícii dva profily (*predvolené profily s názvom **Povolit' všetky** a **Blokovat' všetky***), ostatné profily sa pridali ručne pri zmene profilu v dialógovom okne [Profilu](#) v časti [Nastavenia súčasti Firewall](#).
- **Zapnúť režim hrania** – začiarňte toto okienko, aby v čase, keď sú otvorené aplikácie na celú obrazovku (*hier, prezentácií, filmov a pod.*), súčasť [Firewall](#) nezobrazovala dialógové okná s otázkou, či chcete povoliť alebo blokovat' komunikáciu neznámym aplikáciám. Ak sa neznáma aplikácia pokúsi komunikovať v sieti v danom čase, súčasť [Firewall](#) automaticky povolí alebo zablokuje tento pokus podľa nastavení aktuálneho profilu.
Poznámka: V režime hrania sa všetky naplánované úlohy (kontroly, aktualizácie) odložia

do zatvorenia aplikácie.

- **Stav súčasti Firewall:**

- o **Súčasť Firewall zapnutá** – vyberte túto možnosť, ak chcete povoliť komunikáciu tým aplikáciám, ktoré sú definované ako „povolené“ v skupine pravidiel definovaných vo vybranom profile súčasti [Firewall](#).
- o **Súčasť Firewall vypnutá** – táto možnosť úplne vypne [Firewall](#), všetky sieťové prenosy budú povolené ale nie kontrolované!
- o **Núdzový režim (blokovat' všetky prenosy na internete)** – vyberte túto možnosť, ak si želáte blokovat' prenosy na všetkých sieťových portoch; súčasť [Firewall](#) ostane zapnutá, ale všetky prenosy v sieti budú zastavené.

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu AVG, ak na to nemáte skutočný dôvod. Vykonávať zmeny nastavení sa odporúčajú len skúseným používateľom. Keď potrebujete zmeniť konfiguráciu súčasti Firewall, vyberte položku **Nástroje/Nastavenia súčasti Firewall** v hlavnej ponuke programu a zmeňte konfiguráciu súčasti Firewall v novo otvorenom dialógovom okne [Nastavenia súčasti Firewallu](#).

Ovládacie tlačidlá

- **Obnoviť konfiguráciu** – stlačením tohto tlačidla sa prepíše používaná konfigurácia súčasti **Firewall** a obnoví sa predvolená konfigurácia na základe automatickej detekcie.
- **Uložiť zmeny** – stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť** – stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

7.5. LinkScanner

7.5.1. Princíp fungovania súčasti LinkScanner

LinkScanner chráni pred narastajúcim počtom hrozieb typu „dnes je tu, zajtra je preč“ na internete. Tieto hrozby sa môžu ukrývať na internetových stránkach akéhokoľvek typu, od vládnych až po veľké, od známych značiek až po malé podniky, a len málokedy sa na týchto stránkach udržia viac ako 24 hodín. **LinkScanner** vás chráni tak, že analyzuje internetové stránky za všetkými odkazmi na internetovej stránke, ktorú pozeráte, a stará sa o to, aby boli bezpečné práve v momente, keď je to najviac dôležité – v momente, keď sa chystáte kliknúť na odkaz.

Technológia **LinkScanner** má dve funkcie, [Search-Shield](#) a [Surf-Shield](#):

- **Search Shield** používa zoznam internetových stránok (adres URL), o ktorých je známe, že sú nebezpečné. Ak bude vyhľadávať pomocou vyhľadávača Google, Yahoo! JP,



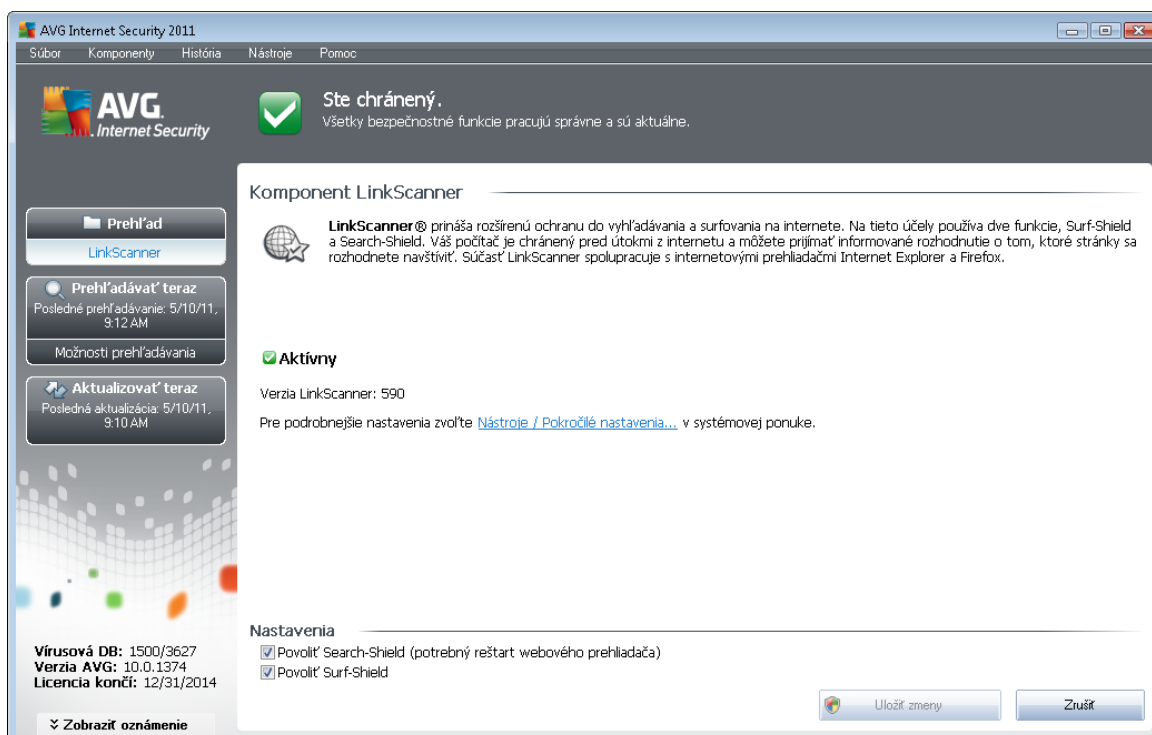
WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg alebo SlashDot, všetky výsledky vyhľadávania budú porovnávať s týmto zoznamom a zobrazí sa ikona verdiktu (vo výsledkoch vyhľadávania zobrazených vyhľadávačom Yahoo sa zobrazia len ikony verdiktu súvisiace so „zneužitými internetovými stránkami“).

- **Surf-Shield** kontroluje obsah navštívených internetových stránok bez ohľadu na ich internetovú adresu. Dokonca aj keď **Search Shield** nezachytí niektoré internetové stránky (napr. keď sa vytvoria nové škodlivé internetové stránky, alebo keď pôvodne čisté internetové stránky teraz obsahujú škodlivý kód), **Surf-Shield** ich zachytí a zablokuje v momente, keď sa ich pokúsite navštíviť.

Poznámka: Súčasť Link Scanner nie je určená pre serverové platformy!

7.5.2. Rozhranie súčasti LinkScanner

V rozhraní súčasti **LinkScanner** sa nachádza stručný opis funkcionality súčasti a informácie o jej aktuálnom stave. Ďalej sa v ňom nachádzajú informácie o čísle najnovšej verzie databázy súčasti **LinkScanner** (Verzia databázy Link Scanner).



Nastavenia súčasti LinkScanner

V spodnej časti dialógového okna môžete zmeniť niekoľko nastavení:

- **Zapnúť Search-Shield** (štandardne zapnuté): informačné ikony s odporúčaniami pre výsledky vyhľadávania zistené vyhľadávačom Google, Yahoo! JP, WebHledani, Yandex,



Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg alebo SlashDot: a vopred skontrolované.

- **Zapnúť [Surf-Shield](#)** (štandardne zapnuté) – používa sa na zapnutie ochrany (v reálnom čase) pred internetovými stránkami s nebezpečným obsahom pri ich otváraní. Pripojenie k známym škodlivým stránkam a ich nebezpečnému obsahu sa zablokuje pri otváraní v internetovom prehliadači (alebo inej aplikácii, ktorá používa protokol HTTP).

7.5.3. Search-Shield

Ak vyhľadáte na internete so zapnutou funkciou **Search-Shield**, všetky výsledky vyhľadávania v najrozšírenejších vyhľadávačoch (Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg a SlashDot) sú hodnotené z hľadiska nebezpečných a podozrivých odkazov. Kontrolou týchto odkazov a označením zlých odkazov vás upozorní súčasť [AVG Link Scanner](#) ešte predtým, než kliknete na nebezpečné resp. podozrivé odkazy, takže získate istotu, že navštevujete len bezpečné internetové stránky.

Počas analyzovania odkazu sa na stránke s výsledkami vyhľadávania vedľa odkazu zobrazí značka, ktorá informuje o prebiehajúcej kontrole odkazu. Po dokončení procesu hodnotenia sa zobrazí príslušná informačná ikona:

 Stránka odkazu je bezpečná (táto ikona sa nezobrazí pre bezpečné výsledky vyhľadávania zobrazené službou Yahoo! JP).

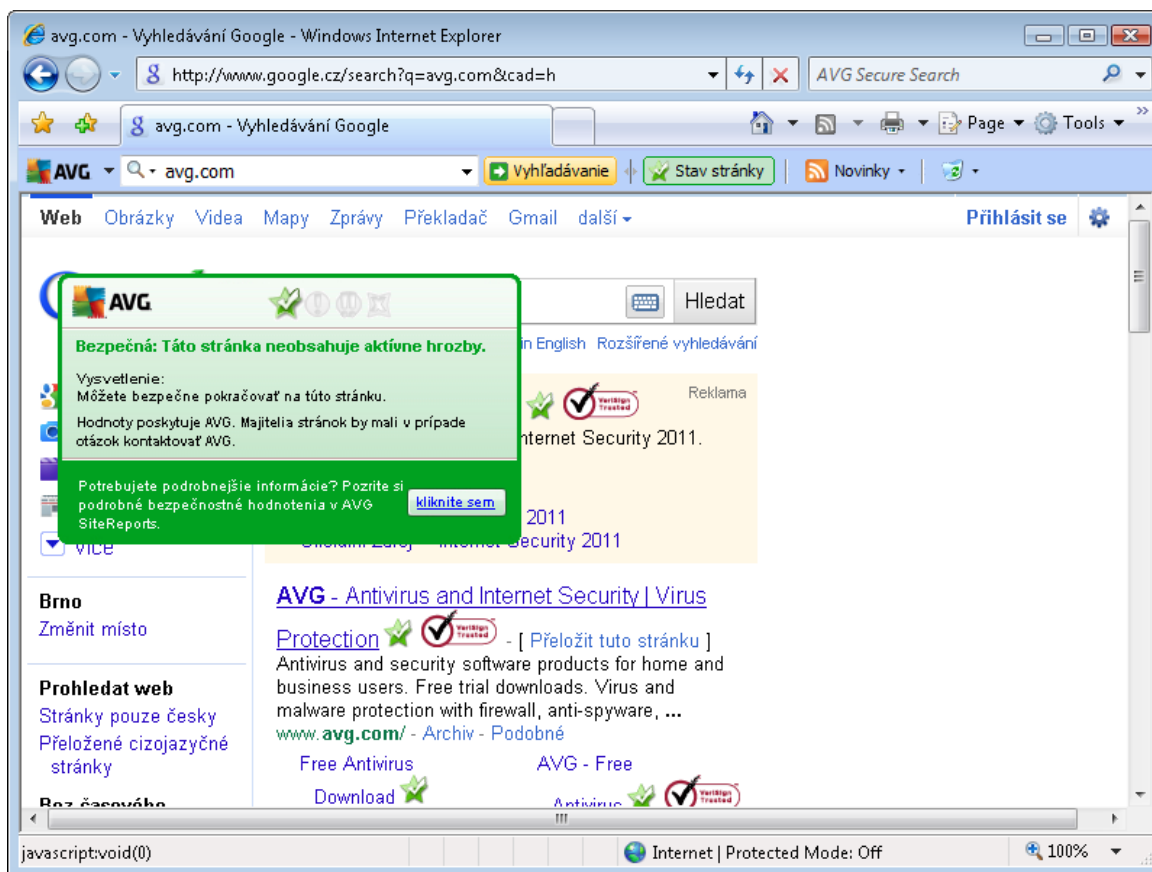
 Na stránke odkazu sa nenachádzajú hrozby, ale je do istej miery podozrivá (otázny pôvod alebo motív, a preto vám ju neodporúčame používať na internetové nakupovanie atď.).

 Stránka odkazu je buď bezpečná, ale zároveň sa na nej nachádzajú ďalšie odkazy na pozitívne nebezpečné stránky, alebo obsahuje podozrivý kód, hoci v tomto momente nepredstavuje žiadnu priamu hrozbu.

 Na stránke odkazu sa nachádzajú činné hrozby! Pre vašu vlastnú bezpečnosť vám nebude umožnené navštíviť túto stránku.

 Stránka odkazu nie je prístupná a nedala sa skontrolovať.

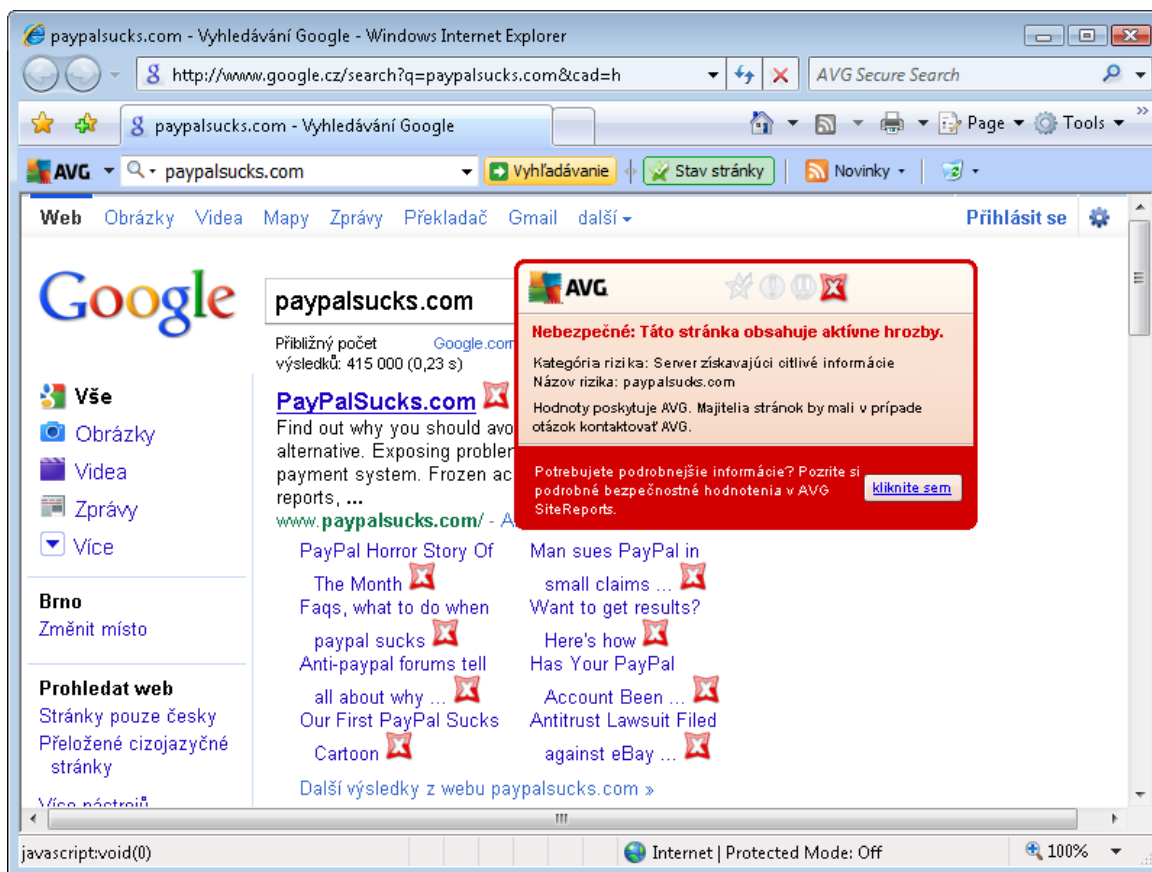
Nastavením kurzora nad jednotlivé ikony hodnotenia sa zobrazia podrobnosti o príslušnom odkaze. Informácie obsahujú ďalšie podrobnosti o hrozbe (ak sú dostupné):



7.5.4. Surf-Shield

Táto účinná ochrana zablokuje škodlivý kód každej webovej stránky, ktorú sa pokúšate otvoriť a zabráni jeho prevzatíu do počítača. Ak je táto funkcia zapnutá a kliknete na odkaz alebo zadáte adresu URL nebezpečných stránok, funkcia automaticky zablokuje otvorenie týchto webových stránok, aby vás chránila pred náhodným infikovaním. Je dôležité mať na pamäti, že nebezpečné webové stránky môžu infikovať váš počítač jednoducho tak, že navštívite príslušné stránky a z tohto dôvodu, keď sa pokúsíte otvoriť nebezpečné webové stránky so škodlivým kódom a inými závažnými hrozbami, súčasť **AVG Link Scanner** neumožní prehliadaču, aby tieto stránky zobrazil.

Ak narazíte na škodlivé webové stránky, **AVG Link Scanner** vás upozorní pomocou zobrazením podobnej obrazovky:



Otvorenie týchto webových stránok predstavuje vysoké riziko a neodporúča sa!

7.6. Rezidentný štít

7.6.1. Princíp fungovania súčasti Rezidentný štít

Súčasť **Rezidentný štít** zabezpečuje neustálu ochranu vášho počítača. Prehľadáva každý jeden otváraný, ukladajúci a kopírovaný súbor a chráni systémové oblasti počítača. Keď **Rezidentný štít** odhalí vírus v súbore, ktorý sa snažíte otvoriť, zastaví práve prebiehajúcu operáciu a nedovolí vírusu, aby sa aktivoval. Tento proces si normálne ani nevšimnete, pretože prebieha „na pozadí“ a budete informovaný len pri zistení hrozby a **Rezidentný štít** zároveň zablokuje aktivovanie hrozby a odstráni ju. **Rezidentný štít** sa načíta do pamäte počítača počas zavádzania systému.

Čo dokáže súčasť **Rezidentný štít**:

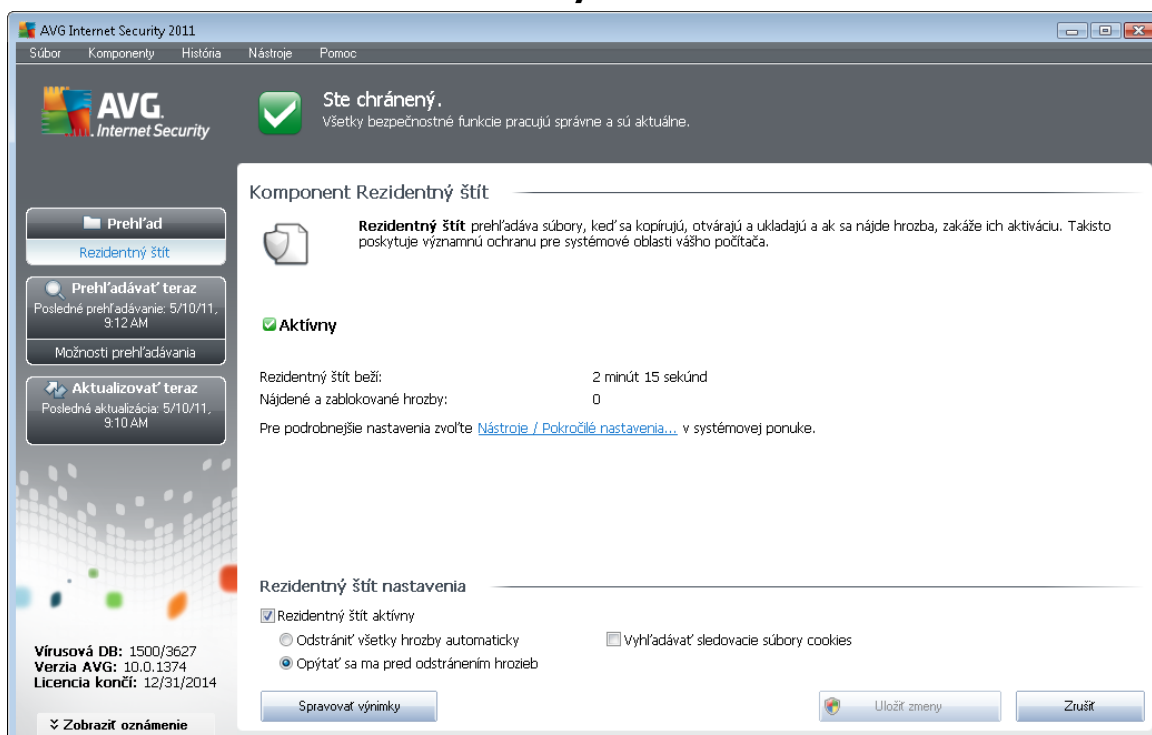
- Vyhľadať konkrétne typy možných hrozieb
- Prehľadávať vyberateľné médiá (*pripojiteľné pamäťové zariadenia a pod.*)
- Prehľadať súbory s konkrétnymi príponami alebo bez prípon



- Povolit' výnimky z prehľadávania – konkrétne súbory a priečinky, ktoré sa nebudú nikdy prehľadávať

Upozornenie: Súčasť Rezidentný štít sa načíta do pamäte počítača pri spustení systému a je dôležitá, aby zostala stále zapnutá!

7.6.2. Rozhranie súčasti Rezidentný štít



Okrem prehľadu funkcionality súčasti **Rezidentný štít** a informácií o jej stave sa v rozhraní súčasti **Rezidentný štít** nachádzajú aj niektoré štatistické informácie:

- **Doba spustenia súčasti Rezidentný štít** – informuje o dobe, ktorá uplynula od posledného spustenia súčasti.
- **Detegované a zablokované hrozby** – počet detegovaných infekcií, ktoré program neumožnil spustiť alebo otvoriť (v prípade potreby sa dá táto hodnota vynulovať; napr. na štatistické účely – Vynulovať hodnotu).

Nastavenia súčasti Rezidentný štít

V spodnej časti dialógového okna sa nachádza časť s názvom **Nastavenia súčasti Rezidentný štít**, ktorá umožňuje editovať niektoré základné nastavenia funkcionality súčasti (podrobná konfigurácia, rovnako ako pri všetkých ostatných súčastiach, sa otvára kliknutím na položku **Nástroje/Rozšírené nastavenia** v hlavnej ponuke programu).

Možnosť **Súčasť Rezidentný štít je zapnutá** sa používa na rýchle zapnutie a vypnutie rezidentnej



ochrany. Táto funkcia je štandardne zapnutá. Po zapnutí rezidentnej ochrany môžete ďalej rozhodnúť, ako sa majú spracovať (odstrániť) prípadné detegované infekcie:

- o buď automaticky (**Odstrániť všetky hrozby automaticky**),
- o alebo až po súhlase používateľa (**Opýtať sa pred odstránením hrozieb**).

Táto možnosť nemá žiaden vplyv na úroveň zabezpečenia a odzrkadľuje len vaše preferencie.

V oboch prípadoch môžete nastaviť, či chcete **odstrániť sledovacie súbory cookies automaticky**. V špecifických prípadoch môžete túto funkciu zapnúť na dosiahnutie maximálnej úrovne zabezpečenia, štandardne je však vypnutá. (Cookies sú textové pakety posielané serverom do internetového prehliadača a následne posielané nezmenené naspäť z prehliadača pri každom prístupnení príslušného servera. HTTP cookies sa používajú na autentifikáciu, sledovanie a zachovanie špecifických informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronického nákupného košíka).

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu programu AVG, ak na to nemáte skutočný dôvod. Zmeny nastavení odporúčame robiť len skúseným používateľom. Ak chcete zmeniť konfiguráciu programu AVG, vyberte položku **Nástroje/Rozšírené nastavenia** v hlavnej ponuke programu a zmeňte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).

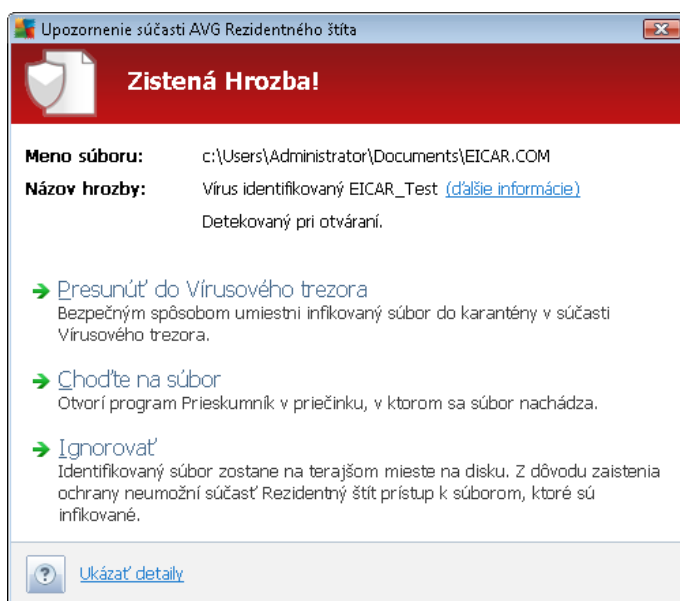
Ovládacie tlačidlá

V rozhraní súčasti **Rezidentný štít** sa nachádzajú tieto ovládacie tlačidlá:

- **Správa výnimiek** – otvorí dialógové okno [Rezidentný štít – Vylúčené položky](#), ktoré umožňuje definovať priečinky, ktoré sa majú vynechať z kontroly súčasťou [Rezidentný štít](#).
- **Uložiť zmeny** – stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť** – stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

7.6.3. Detekcia súčasti Rezidentný štít

Rezidentný štít kontroluje súbory pri kopírovaní, otváraní a ukladaní. Pri detegovaní vírusu alebo akéhokoľvek druhu hrozby vás program ihneď upozorní zobrazením tohto dialógového okna:



V tomto dialógovom okne sa nachádzajú informácie o súbore, ktorý bol detegovaný a označený ako infikovaný (*Názov súboru*), názve rozpoznanej infekcie (*Názov hrozby*) a odkaz na [Encyklopédiu vírusov](#) s podrobnými informáciami o detegovanej infekcii, ak je známa (*Ďalšie informácie*).

Ďalej musíte rozhodnúť, aké opatrenie sa má v tomto momente urobiť – máte k dispozícii tieto možnosti:

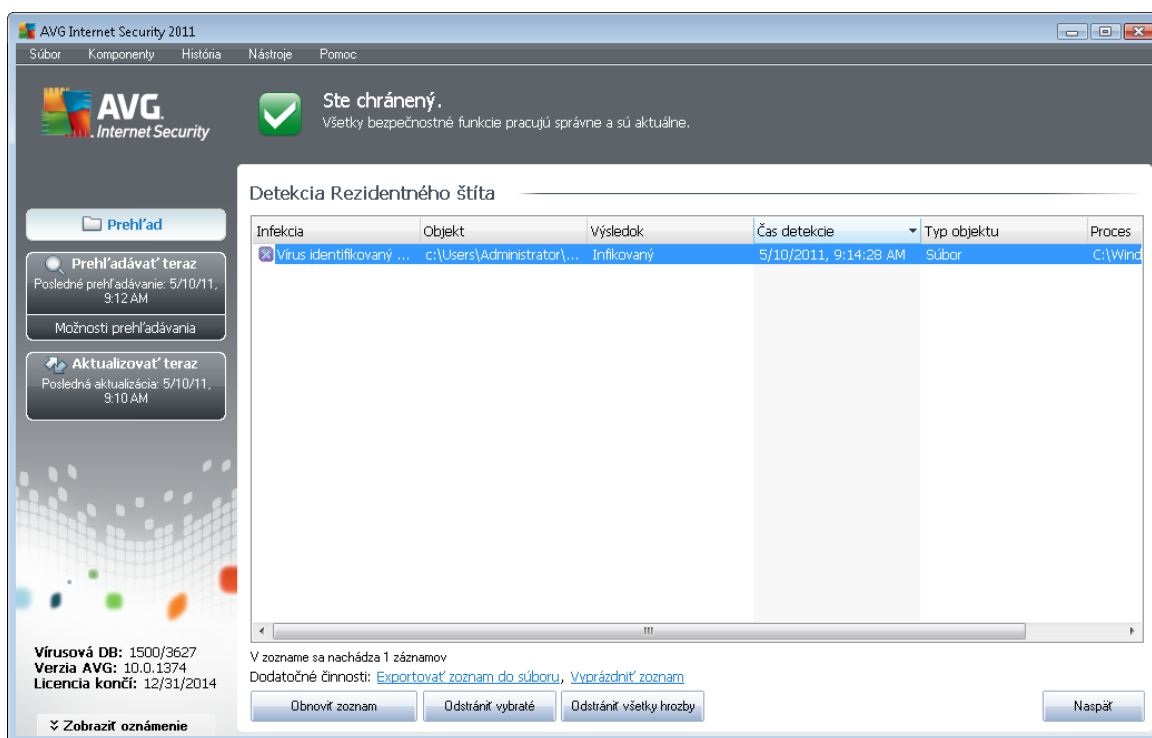
Upozorňujeme, že pri určitých podmienkach (aký typ súboru bol infikovaný a kde sa nachádza) nie sú vždy k dispozícii všetky možnosti.

- **Odstrániť hrozbu ako výkonný používateľ** – začiarknite toto okienko, ak predpokladáte, že nemáte postačujúce práva na odstránenie hrozby ako bežný užívateľ. Výkonný používateľia majú rozsiahle prístupové práva, a ak sa hrozba nachádza v určitom systémovom priečinku, potom na jej úspešné odstránenie budete zrejme musieť začiarknuť toto začiarkovacie okienko.
- **Vyliečiť** – toto tlačidlo sa zobrazí, len keď je možné detegovanú infekciu vyliečiť. Odstráni infekciu a obnoví pôvodný stav súboru. Ak je však samotný súbor vírus, použite túto funkciu na jeho vymazanie (t. j. odstránenie do [Vírusového trezora](#)).
- **Premiestniť do trezora** – vírus sa premiestni do [Vírusového trezora](#)
- **Ísť na súbor** – táto možnosť vás presmeruje na presné umiestnenie podozrivého objektu (otvorí nové okno programu Prieskumník).
- **Ignorovať** – odporúčame vám, aby ste túto možnosť NEPOUŽÍVALI, pokiaľ na to nemáte veľmi dobrý dôvod!

Poznámka: Môže sa stať, že veľkosť detegovaného objektu prekročí veľkosť voľného miesta vo Vírusovom trezore. V tom prípade sa zobrazí upozornenie informujúce o probléme v súvislosti s premiestňovaním infikovaného súboru do Vírusového trezora. Veľkosť Vírusového trezora však môžete zmeniť. Je definovaná ako nastavitelné percento skutočnej veľkosti vášho pevného disku. Na zväčšenie veľkosti Vírusového trezora otvorte dialógové okno [Vírusový trezor](#) v časti [Rozšírené nastavenia programu AVG](#) kliknutím na možnosť „Obmedziť veľkosť Vírusového trezora“.

V spodnej časti dialógového okna sa nachádza odkaz **Zobraziť podrobnosti** – kliknutím naň otvorte prekryvacie okno s podrobnými informáciami o procese, ktorý bol spustený v čase detegovania infekcie, a identifikáciou procesu.

Celý prehľad všetkých hrozieb detegovaných súčasťou [Rezidentný štít](#) sa nachádza v dialógovom okne **Detekcia súčasti Rezidentný štít**, ktoré sa otvára pomocou možnosti [História/Detekcia súčasti Rezidentný štít](#) v hlavnej ponuke programu:



Detekcia súčasti Rezidentný štít poskytuje prehľad objektov detegovaných súčasťou [Rezidentný štít](#), vyhodnotených ako nebezpečné a buď vyliečených alebo premiestnených do [Vírusového trezora](#). Pre každý detegovaný objekt sú k dispozícii tieto informácie:

- **Infekcia** – opis (prípadne aj názov) detegovaného objektu.
- **Objekt** – umiestnenie objektu.
- **Výsledok** – akcia urobená na detegovanom objekte.
- **Čas detekcie** – dátum a čas detegovania objektu.



- **Typ objektu** – typ detegovaného objektu.
- **Proces** – aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detegovať.

V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detegovaných objektov. Ďalej môžete exportovať celý zoznam detegovaných objektov do súboru (**Exportovať zoznam do súboru**) a vymazať všetky záznamy o detegovaných objektoch (**Vyprázdniť zoznam**). Tlačidlo **Obnoviť zoznam** aktualizuje zoznam hrozieb detegovaných súčasťou **Rezidentný štít**. Tlačidlo **Naspäť** otvorí hlavné [používateľské rozhranie programu AVG](#) (prehľad súčastí).

7.7. Family Safety

AVG Family Safety pomáha chrániť vaše deti pred nevhodnými internetovými stránkami, multimédiami a výsledkami vyhľadávania online a hlási vám ich aktivitu online. Môžete nastaviť vhodnú úroveň ochrany pre každé vaše dieťa a monitorovať deti individuálne pomocou jedinečných prihlasovacích údajov.

Súčasť je zapnutá, len ak je produkt **AVG Family Safety** nainštalovaný na počítači. Ak nemáte nainštalovaný produkt **AVG Family Safety**, kliknite na príslušnú ikonu v používateľskom rozhraní produktu **AVG Internet Security 2011** na otvorenie internetových stránok, kde nájdete všetky potrebné informácie.

7.8. AVG LiveKive

AVG LiveKive automaticky zálohuje všetky vaše súbory, fotografie a hudbu na jednom bezpečnom mieste a umožňuje vám zdieľať tieto dáta s rodinou a priateľmi a získať k nim prístup z akéhokoľvek zariadenia s pripojením na internet, vrátane telefónov iPhone a zariadení s operačným systémom Android.

Súčasť je zapnutá, len ak je produkt **AVG LiveKive** nainštalovaný v počítači. Ak nemáte nainštalovaný produkt **AVG LiveKive**, kliknutím na príslušnú ikonu v používateľskom rozhraní produktu **AVG Internet Security 2011** otvorte internetové stránky, na ktorých nájdete všetky potrebné informácie.

7.9. E-mail Scanner

Jeden z najbežnejších zdrojov vírusov a trójskych košov je email. Ohrozenia typu phishing a spam ďalej zvyšujú riziko emailu. Bezplatné e-mailové účty sú náchylnejšie na prijímanie takýchto škodlivých e-mailov (*pretože málokedy využívajú technológiu na ochranu pred spamom*) a domáci používatelia sa v pomerne veľkej miere spoliehajú na tieto e-mailové schránky. Domáci používatelia, ktorí surfujú po neznámych stránkach a do online formulárov vyplňajú osobné údaje (*napr. e-mailové adresy*), sú vo zvýšenej miere vystavení útoku cez e-mail. Spoločnosti obyčajne využívajú hromadné emailové účty a používajú antispamové filtre, atď., aby toto riziko znížili.



7.9.1. Princíp fungovania súčasti E-mail Scanner

Personal E-mail Scanner automaticky kontroluje prichádzajúce a odchádzajúce e-maily. Môže sa používať s poštovými aplikáciami, ktoré nemajú vlastný zásuvný modul v programe AVG (zároveň sa môže používať aj na kontrolu e-mailových správ v poštových aplikáciách, s ktorými AVG spolupracuje pomocou špeciálneho zásuvného modulu – napr. Microsoft Outlook a The Bat). Primárne je určený pre poštové aplikácie ako sú Outlook Express, Mozilla, Incredimail atď.

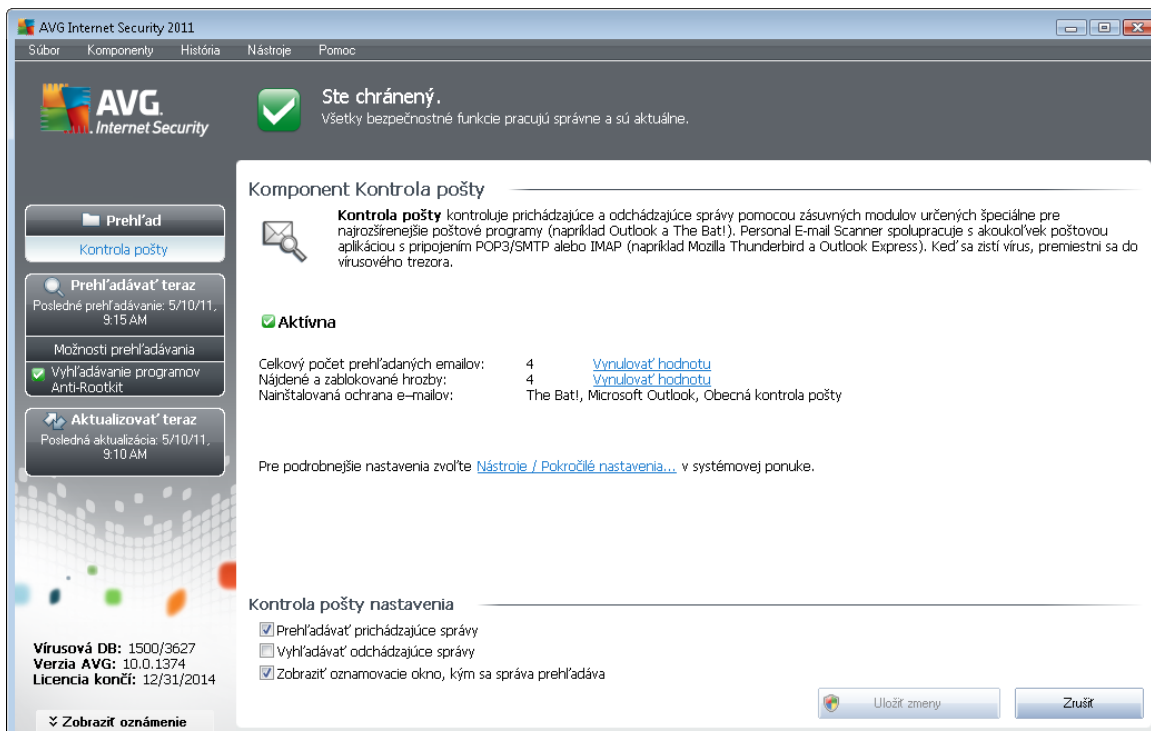
Počas [inštalácie programu AVG](#) sa vytvoria automatické servery na kontrolu e-mailov: jeden na kontrolu prichádzajúcich e-mailov a druhý na kontrolu odchádzajúcich e-mailov. Pomocou týchto dvoch serverov sa e-maily automaticky kontrolujú na portoch 110 a 25 (štandardné porty pre posielanie a prijímanie e-mailov).

E-mail Scanner pôsobí ako rozhranie medzi poštovou aplikáciou a poštovými servermi na internete.

- **Prichádzajúca pošta:** Počas prijímania správy zo servera testuje súčasť **E-mail Scanner** správu z hľadiska prítomnosti vírusov, odstráni infikované prílohy a pridá certifikáciu. Zistené vírusy sa ihneď uložia do karantény vo [vírusovom trezore](#). Správa sa potom pošle do poštovej aplikácie.
- **Odchádzajúca pošta:** Správa sa pošle z poštovej aplikácie do súčasti E-mail Scanner, ktorá otestuje samotnú správu a jej prílohy z hľadiska výskytu vírusov, a potom ju pošle na server SMTP (kontrola odchádzajúcich e-mailov je štandardne vypnutá a môže sa nastaviť ručne).

Poznámka: Súčasť AVG E-mail Scanner nie je určená pre serverové platformy!

7.9.2. Rozhranie súčasti E-mail Scanner





V dialógovom okne súčasti **E-mail Scanner** sa nachádza stručný text s opisom funkcionality súčasti, informáciami o jej aktuálnom stave a týmito štatistickými informáciami:

- **Celkový počet prehľadaných e-mailov** – koľko e-mailových správ sa prehľadalo od posledného spustenia súčasti **E-mail Scanner** (v prípade potreby môžete túto hodnotu vynulovať, napr. na štatistické účely – Vynulovať hodnotu).
- **Nájdené a zablokované hrozby** – informuje o počte infekcií detegovaných v e-mailových správach od posledného spustenia súčasti **E-mail Scanner**.
- **Nainštalovaná ochrana e-mailov** – informácie o konkrétnom zásuvnom module na ochranu e-mailov v predvolenej nainštalovanej poštovej aplikácii.

Nastavenia súčasti E-mail Scanner

V spodnej časti tohto dialógového okna sa nachádza časť s názvom **Nastavenia súčasti E-mail Scanner**, kde môžete zmeniť niektoré základné funkcie súčasti:

- **Prehľadávať prichádzajúce správy** – začiarknite túto možnosť, ak sa má kontrolovať prítomnosť vírusov vo všetkých e-mailoch doručených do vašej e-mailovej schránky. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nemenili!
- **Prehľadávať odchádzajúce správy** – začiarknite túto možnosť, ak sa má zisťovať prítomnosť vírusov vo všetkých e-mailoch poslaných z vašej e-mailovej schránky. Možnosť je štandardne vypnutá.
- **Zobraziť oznamovacie okno počas prehľadávania e-mailov** – začiarknite túto možnosť, ak chcete byť informovaný otvorením oznamovacieho dialógového okna nad ikonou AVG na paneli úloh počas prehľadávania pošty súčasťou **E-mail Scanner**. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nemenili!

Rozšírená konfigurácia súčasti **E-mail Scanner** sa otvára výberom položky **Nástroje/Rozšírené nastavenia** v ponuke programu; odporúča sa však, aby rozšírenú konfiguráciu používali len skúsení používatelia!

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu AVG, ak na to nemáte skutočný dôvod. Zmeny nastavení odporúčame robiť len skúseným používateľom. Ak chcete zmeniť konfiguráciu programu AVG, vyberte položku **Nástroje/Rozšírené nastavenia** v hlavnej ponuke programu a zmeňte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).

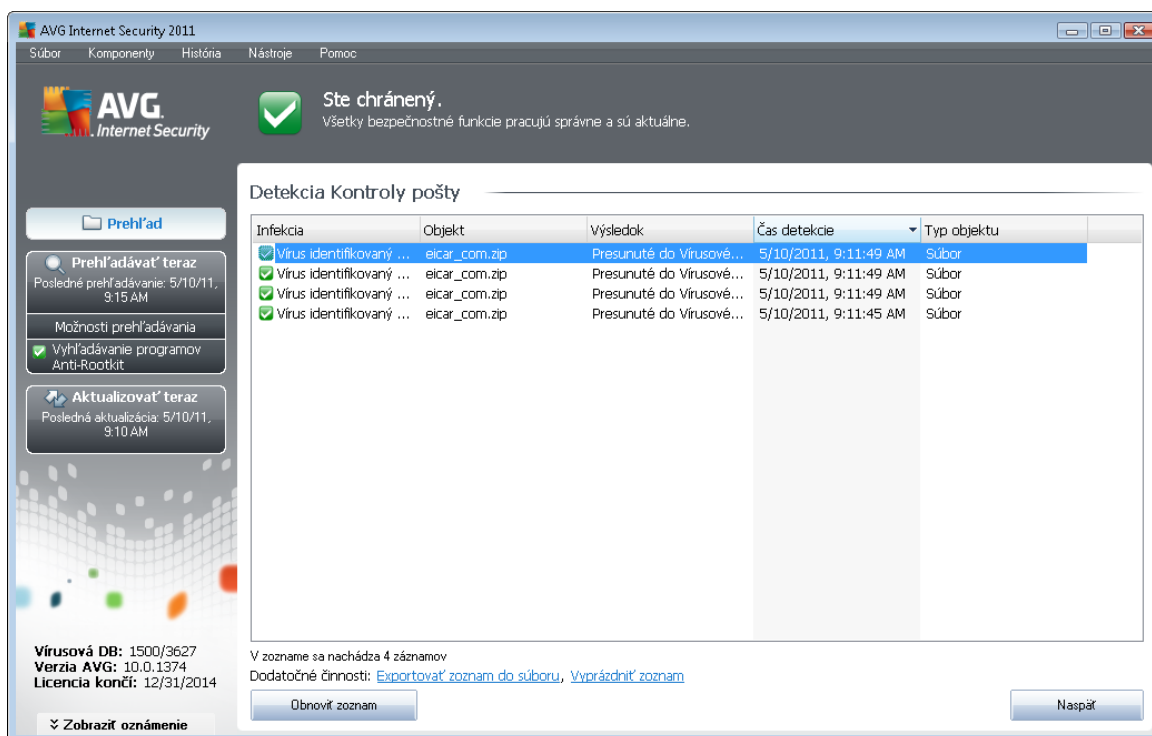
Ovládacie tlačidlá

V rozhraní súčasti **E-mail Scanner** sa nachádzajú tieto ovládacie tlačidlá:

- **Uložiť zmeny** – stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť** – stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (

prehľad súčastí)

7.9.3. Detekcia súčasti E-mail Scanner



V dialógovom okne **Detekcia súčasti E-mail Scanner** (otvára sa pomocou možnosti *História/ Detekcia súčasti E-mail Scanner*) sa zobrazí zoznam všetkých hrozieb detegovaných súčastou **E-mail Scanner**. Pre každý detegovaný objekt sú k dispozícii tieto informácie:

- **Infekcia** – opis (prípadne aj názov) detegovaného objektu.
- **Objekt** – umiestnenie objektu.
- **Výsledok** – akcia urobená na detegovanom objekte.
- **Čas detegovania** – dátum a čas detegovania podozrivého objektu.
- **Typ objektu** – typ detegovaného objektu.

V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detegovaných objektov. Ďalej môžete exportovať celý zoznam detegovaných objektov do súboru (**Exportovať zoznam do súboru**) a vymazať všetky záznamy o detegovaných objektoch (**Vyprázdniť zoznam**).

Ovládacie tlačidlá

V rozhraní **Detekcia súčasti E-mail Scanner** sa nachádzajú tieto tlačidlá:



- **Obnoviť zoznam** – aktualizuje zoznam detegovaných hrozieb.
- **Naspäť** – vráti naspäť na predchádzajúce dialógové okno

7.10. Update Manager

7.10.1. Princíp fungovania súčasti Update Manager

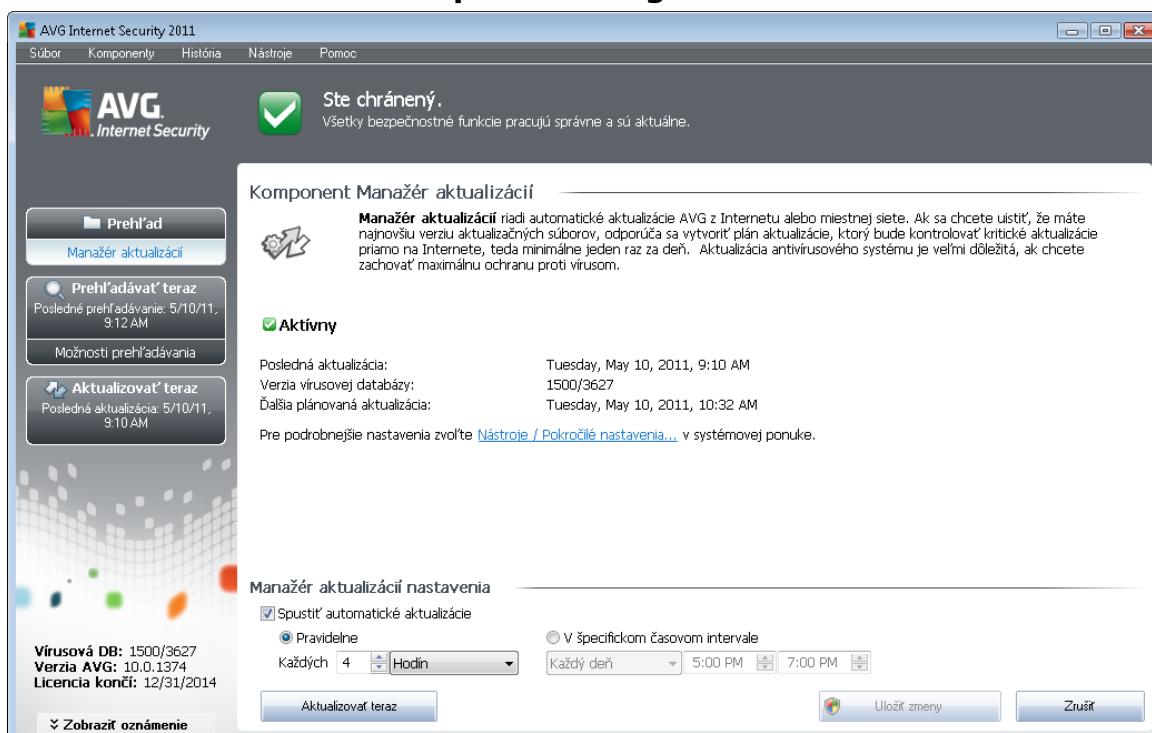
Žiaden bezpečnostný softvér nedokáže zaručiť skutočnú ochranu pred rôznymi typmi hrozieb, ak sa pravidelne neaktualizuje! Autori vírusov stále hľadajú nové trhliny, ktoré by mohli využiť, či už v softvéri alebo v operačných systémoch. Nové vírusy, nový malware a nové útoky hackerov sa objavujú denne. Z tohto dôvodu dodávateľia softvéru neustále vydávajú aktualizácie a bezpečnostné záplaty na opravu všetkých odhalených bezpečnostných dier.

Pravidelná aktualizácia programu AVG je nevyhnutná!

Update Manager uľahčuje správu pravidelných aktualizácií. Súčasť umožňuje naplánovať automatické prevzatie aktualizáčnych súborov buď z internetu alebo lokálnej siete. Dôležité aktualizácie vírusových definícií by sa mali robiť denne, ak to je možné. Menej urgentné programové aktualizácie sa môžu robiť raz za týždeň.

Poznámka: Venujte pozornosť kapitole [Aktualizácie programu AVG](#), v ktorej sa nachádzajú ďalšie informácie o typoch a úrovniach aktualizácie!

7.10.2. Rozhranie súčasti Update Manager





V rozhraní súčasti **Update Manager** sa nachádzajú informácie o funkcionalite súčasti a jej momentálnom stave a súvisiace štatistické informácie:

- **Posledná aktualizácia** – informuje o dátume a čase poslednej aktualizácie databázy.
- **Verzia vírusovej databázy** – uvádza číslo momentálne nainštalovanej verzie vírusovej databázy a toto číslo narastá s každou aktualizáciou vírusovej databázy.
- **Ďalšia naplánovaná aktualizácia** – informuje o dátume a čase ďalšej aktualizácie databázy.

Nastavenia súčasti Update Manager

V spodnej časti tohto dialógového okna sa nachádza časť s názvom **Nastavenia súčasti Update Manager**, ktorá umožňuje urobiť zmeny pravidiel spustenia procesu aktualizácie. Umožňuje nastaviť, aby sa aktualizčné súbory preberali automaticky (**Spustiť automatické aktualizácie**), alebo len na požiadanie. Štandardne je možnosť **Spúšťať automatické aktualizácie** zapnutá a odporúčame vám, aby ste toto nastavenie nemenili! Pravidelné preberanie najnovších aktualizčných súborov je rozhodujúce na správne fungovanie každého bezpečnostného softvéru!

Ďalej môžete nastaviť, kedy sa má aktualizácia spúšťať:

- o **Pravidelne** – nastavte časový interval.
- o **V nastavenom časovom intervale** – nastavte presný čas dňa, kedy sa má aktualizácia spustiť.

Štandardne je aktualizácia nastavená na každé 4 hodiny. Odporúčame vám, aby ste toto nastavenie nemenili, ak na to nemáte vážny dôvod!

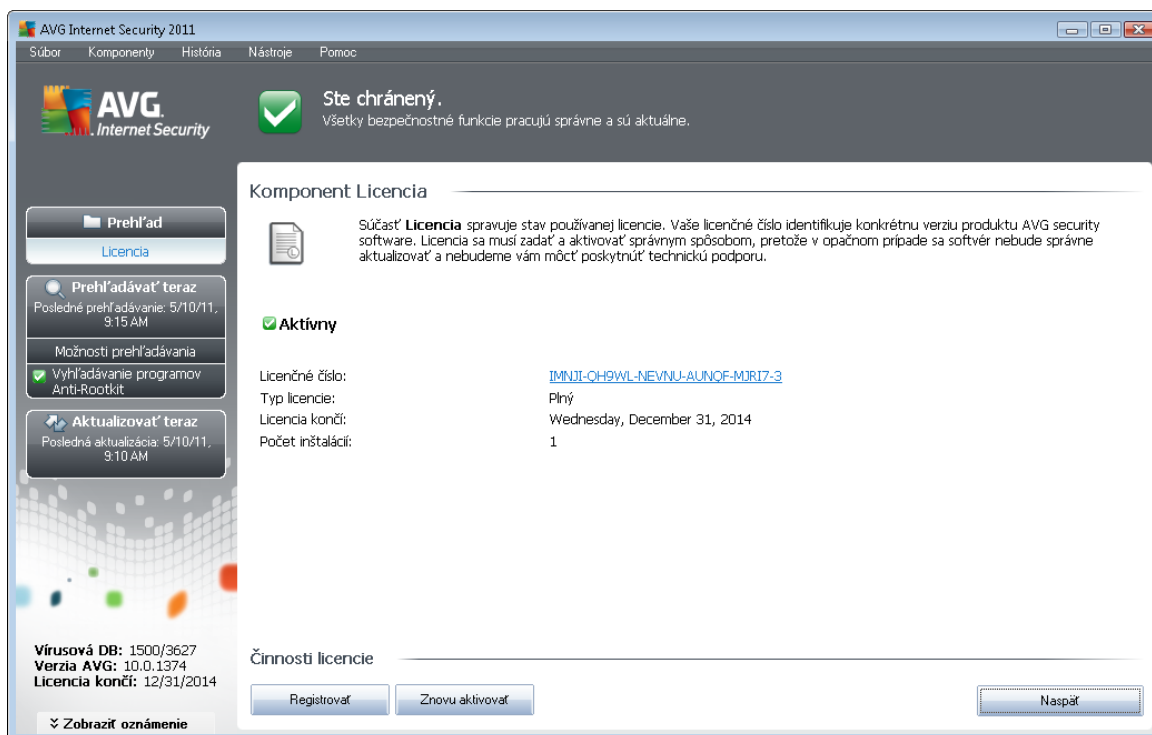
Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu programu AVG, ak na to nemáte skutočný dôvod. Zmeny nastavení odporúčame robiť len skúseným používateľom. Ak chcete zmeniť konfiguráciu programu AVG, vyberte položku **Nástroje/Rozšírené nastavenia** v hlavnej ponuke programu a zmeňte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).

Ovládacie tlačidlá

V rozhraní súčasti **Update Manager** sa nachádzajú tieto ovládacie tlačidlá:

- **Aktualizovať teraz** – spustí [okamžitú aktualizáciu](#) na požiadanie.
- **Uložiť zmeny** – stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť** – stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

7.11. Licencia



V rozhraní súčasti **Licencia** sa nachádza stručný prehľad funkcionality súčasti, informácie o jej aktuálnom stave a tieto štatistické informácie:

- **Licenčné číslo** – skrátená podoba licenčného čísla (z bezpečnostných dôvodov sú posledné štyri znaky vynechané). Licenčné číslo sa musí zadať úplne presne tak, ako je uvedené. Preto vám odporúčame, aby ste použili funkciu „kopírovať“ a prilepiť pri každej manipulácii s licenčným číslom.
- **Typ licencie** – informuje o type nainštalovaného produktu.
- **Platnosť licencie vyprší** – tento dátum informuje o dobe platnosti vašej licencie. Ak chcete aj naďalej používať **AVG Internet Security 2011** aj po tomto dátume, musíte si obnoviť licenciu. Obnovenie licencie môžete urobiť online na [internetových stránkach AVG](http://www.avg.com).
- **Počet inštalácií** – na koľko počítačov sa môže produkt **AVG Internet Security 2011** inštalovať.

Ovládacie tlačidlá

- **Registrovať** – program sa pripojí k registračnej stránke na internetových stránkach AVG (<http://www.avg.com>). Vyplňte vaše registračné údaje; nárok na bezplatnú technickú podporu získajú len tí zákazníci, ktorí si svoj produkt AVG zaregistrujú.
- **Znova aktivovať** – otvorí dialógové okno **Aktivácia produktu AVG** s údajmi, ktoré ste zadali v dialógovom okne [Prispôbiť AVG](#) v [processe inštalácie](#). Toto dialógové okno sa

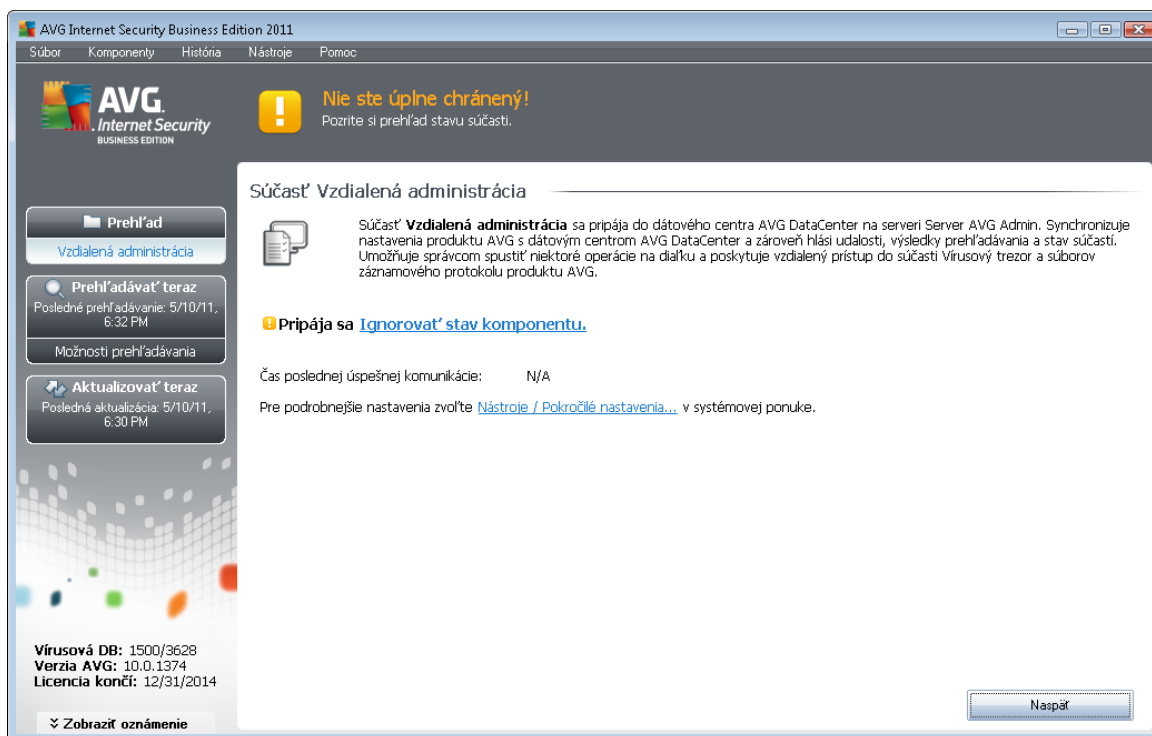


používa na vloženie licenčného čísla, buď pri nahradení predajného čísla (čísla, s ktorým ste nainštalovali AVG) alebo starého licenčného čísla (napr. pri upgradovaní na nový produkt AVG).

Poznámka: Ak používate skúšobnú verziu produktu **AVG Internet Security 2011**, tlačidlá sa zobrazia v podobe **Kúpiť teraz** a **Aktivovať** a umožnia vám ihneď zakúpiť úplnú verziu programu. Ak ste produkt **AVG Internet Security 2011** nainštalovali pomocou predajného čísla, potom sa tlačidlá zobrazia v podobe **Registrovať** a **Aktivovať**.

- **Naspäť** – stlačením tohto tlačidla sa vrátite na hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

7.12. Remote Administration



Súčasť **Remote Administration** sa zobrazí v používateľskom rozhraní produktu **AVG Internet Security 2011** len v tom prípade, ak máte nainštalovaný produkt Business Edition (pozri súčasť [Licencia](#)). V dialógovom okne **Remote Administration** sa nachádzajú informácie o tom, či je súčasť zapnutá a pripojená k serveru. Všetky nastavenia súčasti **Remote Administration** sa robia v ponuke **Rozšírené nastavenia/Remote Administration**.

Podrobný opis možností a funkcionality súčasti v systéme AVG Remote Administration sa nachádza v príslušnej dokumentácii vyhradenej špeciálne tejto téme. Túto dokumentáciu si môžete prevziať na [internetových stránkach AVG](#) (www.avg.com) v časti **Centrum podpory/Na prevzatíe/Dokumentácia**.

Ovládacie tlačidlá

- **Naspäť** – stlačením tohto tlačidla sa vrátite na hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

7.13. Webový štít

7.13.1. Princíp fungovania súčasti Webový štít

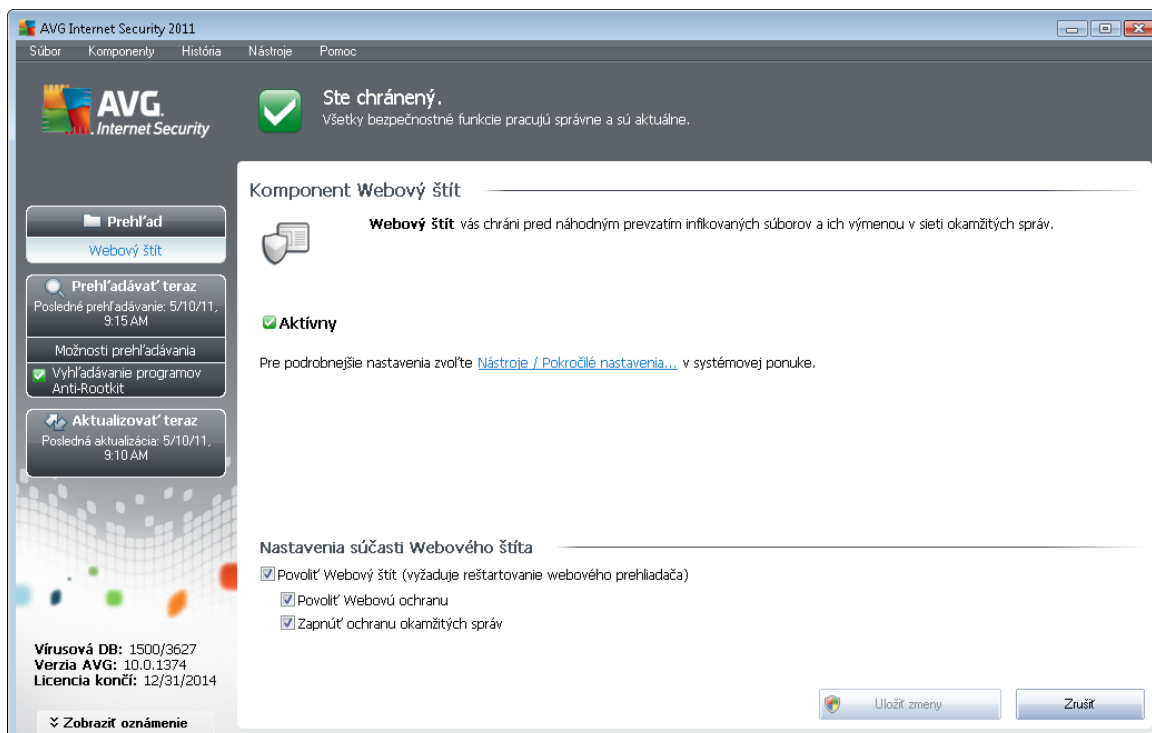
Webový štít je druh rezidentnej ochrany, ktorá pracuje v reálnom čase; prehľadáva obsah navštívených internetových stránok (a súborov, ktoré sa na nich môžu nachádzať) ešte predtým, než sa zobrazia v internetovom prehliadači alebo prevezmú do počítača.

Webový štít zistí prítomnosť nebezpečného kódu JavaScript na stránke, ktorú sa práve chystáte navštíviť, a neumožní stránku zobrazit'. Zároveň rozpozná škodlivý softvér, ktorý sa nachádza na tejto stránke, a ihneď zastaví jeho preberanie, aby sa nikdy nedostal do počítača.

Poznámka: Súčasť AVG Webový štít nie je určená pre serverové platformy!

7.13.2. Rozhranie súčasti Webový štít

V rozhraní súčasti **Webový štít** sa nachádzajú informácie o správaní tohto typu ochrany. Ďalej sa tam nachádzajú informácie o aktuálnom stave súčasti. V spodnej časti dialógového okna sa potom nachádzajú základné funkcie na editovanie funkcionality tejto súčasti:



Nastavenia súčasti Webový štít



V prvom rade môžete okamžite zapnúť alebo vypnúť **Webový štít** začiarknutím položky **Zapnúť Webový štít**. Táto možnosť je štandardne povolená a súčasť **Webový štít** je zapnutá. Ak však nemáte dobrý dôvod meniť tieto nastavenia, odporúčame vám, aby ste nechali súčasť zapnutú. Ak je táto položka začiarknutá a súčasť **Webový štít** je spustená, potom sa aktivujú ďalšie dve možnosti konfigurácie:

- **Zapnúť Webovú ochranu** – keď je táto funkcia zapnutá, potom bude súčasť **Webový štít** kontrolovať obsah internetových stránok.
- **Zapnúť ochranu okamžitých správ** – začiarknite toto okienko, ak si želáte, aby súčasť **Webový štít** kontrolovala, či sa v komunikácii pomocou okamžitých správ (napr. ICQ, MSN Messenger...) nenachádzajú vírusy.

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu programu AVG, ak na to nemáte skutočný dôvod. Zmeny nastavení odporúčame robiť len skúseným používateľom. Ak chcete zmeniť konfiguráciu programu AVG, vyberte položku **Nástroje/Rozšírené nastavenia** v hlavnej ponuke programu a zmeňte konfiguráciu v novo otvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).

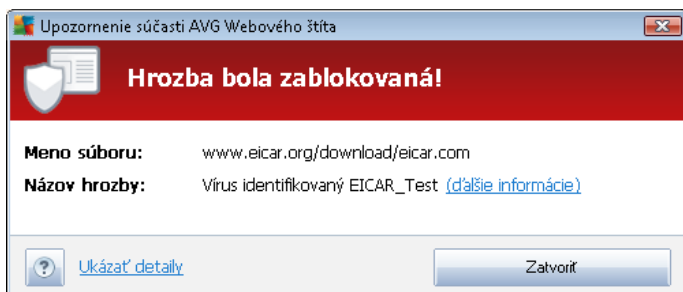
Ovládacie tlačidlá

V rozhraní súčasti **Webový štít** sa nachádzajú tieto ovládacie tlačidlá:

- **Uložiť zmeny** – stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť** – stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí).

7.13.3. Detekcia súčasti Webový štít

Webový štít prehľadáva obsah navštívených internetových stránok a súborov, ktoré sa na nich môžu nachádzať, ešte predtým, než sa zobrazia v internetovom prehliadači alebo prevezmú do počítača. Pri detegovaní hrozby vás program ihneď upozorní otvorením tohto dialógového okna:

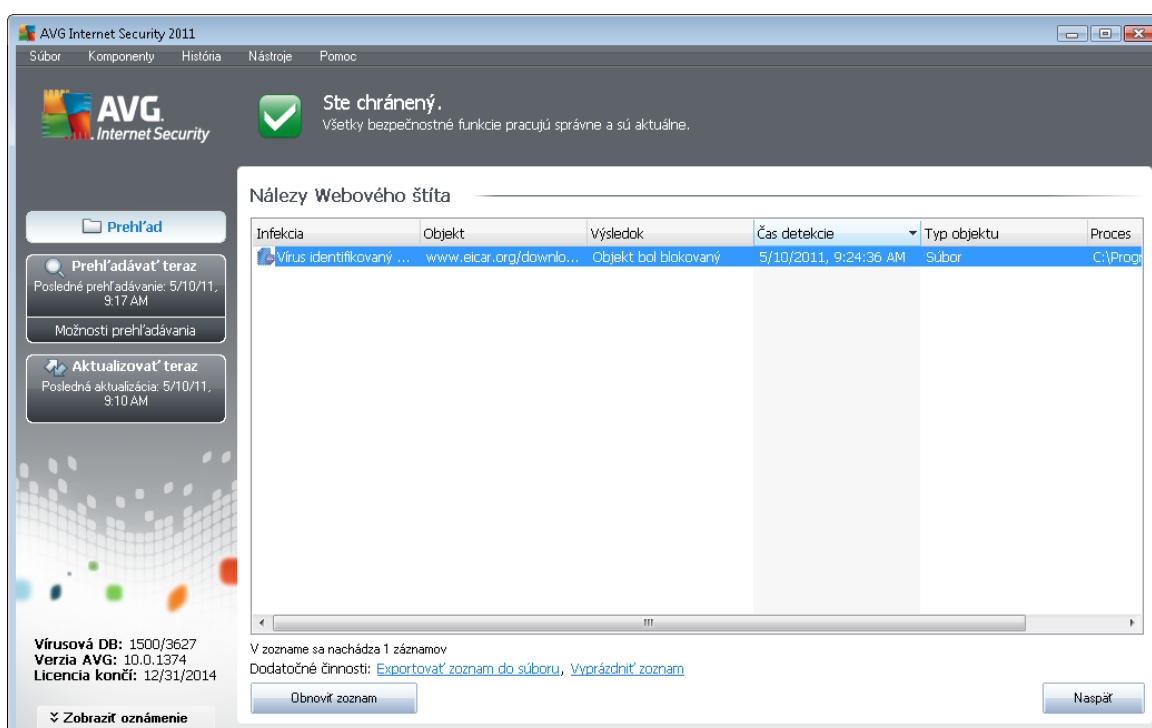


V tomto dialógovom okne sa nachádzajú informácie o súbore, ktorý bol detegovaný a označený ako infikovaný (**Názov súboru**), názve rozpoznanej infekcie (**Názov hrozby**) a odkaz na [Encyklopédiu vírusov](#) s podrobnými informáciami o detegovanej infekcii, ak je známa (**Ďalšie informácie**). V tomto dialógovom okne sa nachádzajú tieto tlačidlá:



- **Zobrazit' podrobnosti** – kliknutím na tlačidlo **Zobrazit' podrobnosti** otvorte nové prekrývacie okno s informáciami o procese, ktorý bol spustený v čase detegovania infekcie, a identifikáciou procesu.
- **Zatvorit'** – kliknutím na toto tlačidlo zatvorte dialógové okno s upozornením.

Podozrivá internetová stránka sa neotvorí a detegovaná hrozba sa zaznamená v zozname **nálezov súčasti Webový štít** – tento prehľad detegovaných hrozieb sa otvára v hlavnej ponuke [História/ Nálezy súčasti Webový štít](#).



Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Infekcia** – opis (prípadne aj názov) detegovaného objektu.
- **Objekt** – zdroj objektu (internetová stránka).
- **Výsledok** – akcia urobená na detegovanom objekte.
- **Čas detegovania** – dátum a čas detegovania a zablokovania hrozby.
- **Typ objektu** – typ detegovaného objektu.
- **Proces** – aká akcia sa vykonala na zavolanie potenciálne nebezpečného objektu, aby sa dal detegovať.

V spodnej časti dialógového okna pod zoznamom sa nachádzajú informácie o celkovom počte detegovaných objektov. Ďalej môžete exportovať celý zoznam detegovaných objektov do súboru (**Exportovať zoznam do súboru**) a vymazať všetky záznamy o detegovaných objektoch (



Vyprázdniť zoznam). Tlačidlo **Obnoviť zoznam** aktualizuje zoznam nálezov detegovaných súčasťou **Webový štít**. Tlačidlo **Naspäť** otvorí hlavné [používateľské rozhranie programu AVG](#) (*prehľad súčastí*).

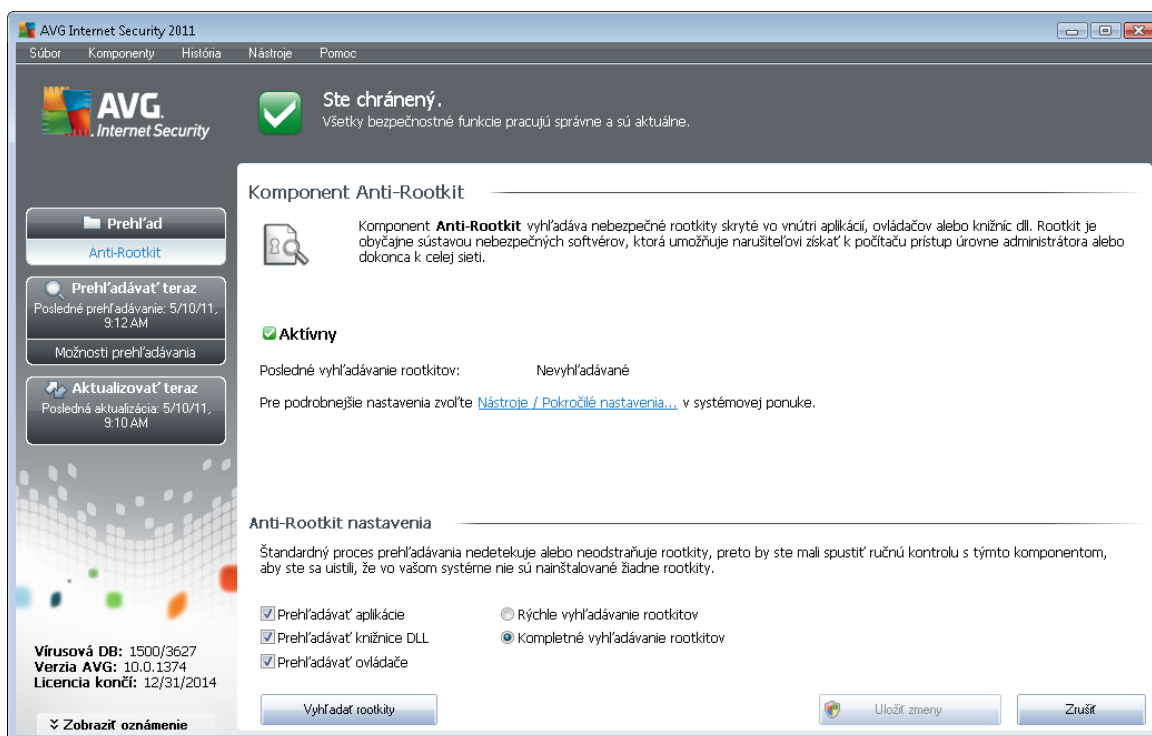
7.14. Anti-Rootkit

Rootkit je program, ktorý sa používa na prevzatie základnej kontroly nad počítačovým systémom bez súhlasu vlastníka počítača a jeho právoplatných správcov. Prístup k hardvéru sa väčšinou nepožaduje, pretože účelom rootkitu je zmocniť sa kontroly nad operačným systémom spusteným na hardvéri. Rootkity zvyčajne maskujú svoju prítomnosť v systéme rozvratnou činnosťou, alebo vyhýbaním sa štandardným bezpečnostným mechanizmom operačného systému. Často ide aj o trójske kone, ktoré klamlivo presvedčia používateľov, že sa môžu bezpečne spustiť na počítači. Medzi metódy používané na dosiahnutie tohto cieľa patria utajenie spustených procesov pred sledovacími programami, alebo skrývanie súborov alebo systémových dát pred operačným systémom.

7.14.1. Princíp fungovania súčasti Anti-Rootkit

AVG Anti-Rootkit je špeciálny nástroj, ktorý deteguje a účinne odstraňuje nebezpečné rootkity, t. j. programy a technológie, ktoré dokážu zamaskovať prítomnosť škodlivého softvéru vo vašom počítači. **AVG Anti-Rootkit** dokáže zistiť prítomnosť rootkitov pomocou vopred definovanej skupiny pravidiel. Upozorňujeme, že program zistí prítomnosť všetkých rootkitov (*nielen infikovaných*). Ak **AVG Anti-Rootkit** nájde rootkit, nemusí to nevyhnutne znamenať, že tento rootkit je infikovaný. Rootkity sa niekedy používajú ako ovládače, alebo tvoria súčasť dobrých aplikácií.

7.14.2. Rozhranie súčasti Anti-Rootkit





Používateľské rozhranie súčasti **Anti-Rootkit** stručne opisuje funkcionality súčasti, informuje o momentálnom stave súčasti a zároveň poslednom čase, kedy bol spustený test súčastou **Anti-Rootkit (posledné vyhľadávanie rootkitov)**. V dialógovom okne **Anti-Rootkit** sa ďalej nachádza odkaz na [nástroje/rozšírené nastavenia](#). Použite odkaz na otvorenie prostredia s rozšírenou konfiguráciou súčasti **Anti-Rootkit**.

Poznámka: Dodávateľ softvéru nastavil všetky súčasti AVG tak, aby fungovali optimálnym spôsobom. Nemeňte konfiguráciu AVG, ak na to nemáte skutočný dôvod. Zmenu nastavení by mali robiť len skúsení používatelia.

Nastavenia súčasti Anti-Rootkit

V spodnej časti tohto dialógového okna sa nachádza časť **Nastavenia súčasti Anti-Rootkit**, v ktorej môžete nastaviť niektoré základné funkcie na zisťovanie prítomnosti rootkitov. Najskôr začiarknutím príslušných okienok definujte objekty, ktoré sa majú prehľadávať:

- **Prehľadávať aplikácie**
- **Prehľadávať knižnice DLL**
- **Prehľadávať ovládače**

Ďalej môžete vybrať režim vyhľadávania rootkitov:

- **Rýchle vyhľadávanie rootkitov** – prehľadáva všetky spustené procesy, zavedené ovládače a systémový priečinok (zvyčajne c:\Windows).
- **Úplné vyhľadávanie rootkitov** – prehľadáva všetky spustené procesy, zavedené ovládače, systémový priečinok (zvyčajne c:\Windows), plus všetky disky počítača (vrátane pamäťových médií, nie však disketové jednotky/jednotky CD-ROM).

Ovládacie tlačidlá

- **Vyhľadávať rootkity** – keďže vyhľadávanie rootkitov netvorí integrálnu súčasť [prehľadávania celého počítača](#), vyhľadávanie rootkitov môžete spustiť priamo v rozhraní súčasti **Anti-Rootkit** pomocou tohto tlačidla.
- **Uložiť zmeny** – stlačením tohto tlačidla sa uložia všetky zmeny urobené v tomto rozhraní a otvorí sa základné [používateľské rozhranie AVG](#) (prehľad súčastí).
- **Zrušiť** – stlačením tohto tlačidla sa znova otvorí základné [používateľské rozhranie AVG](#) (prehľad súčastí) bez uloženia urobených zmien.

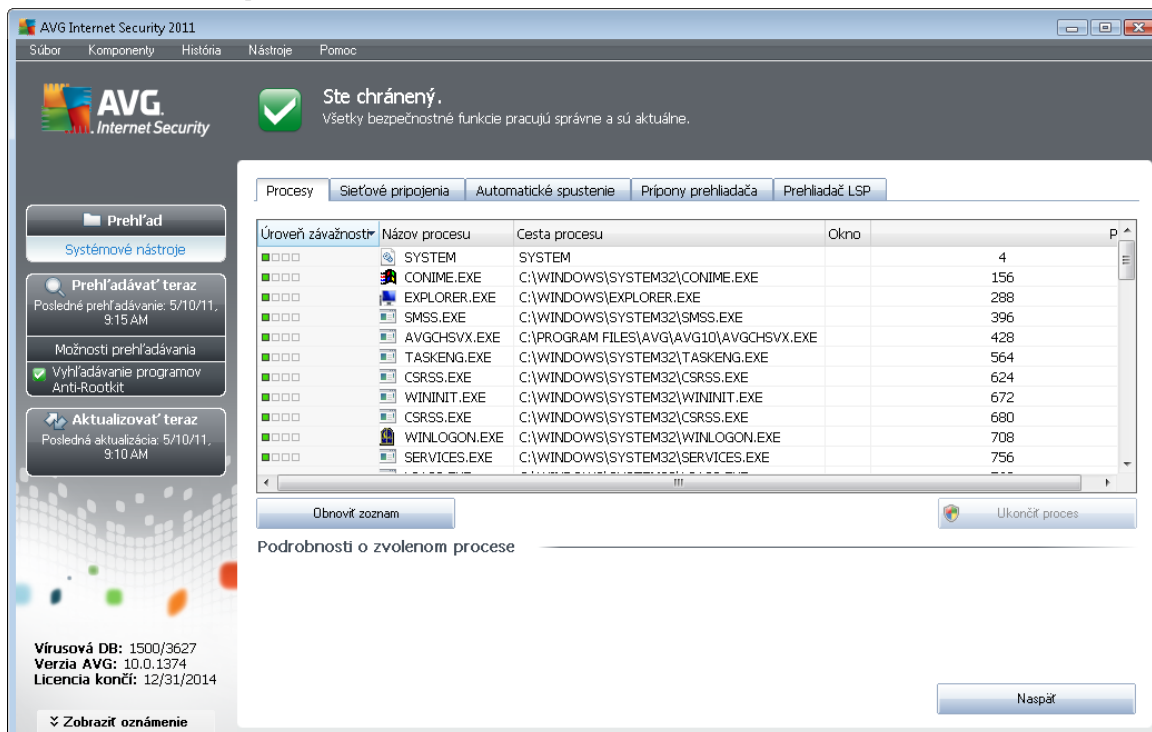
7.15. System Tools

System Tools sú nástroje poskytujúce podrobný prehľad o prostredí produktu **AVG Internet Security 2011** a operačnom systéme. V tejto súčasti sa nachádza prehľad týchto objektov:

- [Procesy](#) – zoznam procesov (t. j. *spustených aplikácií*), ktoré sú momentálne činné v počítači.
- [Sieťové pripojenia](#) – zoznam momentálne činných pripojení.
- [Automatické spustenie](#) – zoznam aplikácií, ktoré sa spúšťajú pri spustení systému Windows.
- [Rozšírenia prehliadača](#) – zoznam zásuvných modulov (t. j. *aplikácií*), ktoré sú nainštalované v internetovom prehliadači.
- [Prehliadač LSP](#) – zoznam ovládačov LSP (Layered Service Provider).

Jednotlivé prehľady sa dajú aj editovať; toto však odporúčame robiť len veľmi skúseným používateľom!

7.15.1. Procesy



V dialógovom okne **Procesy** sa nachádza zoznam procesov (*teda spustených aplikácií*), ktoré sú momentálne činné v počítači. Zoznam je rozdelený na niekoľko stĺpcov.

- **Úroveň závažnosti** – grafické znázornenie závažnosti príslušného procesu na stupnici so štyrmi úrovňami od najmenej významnej (■ ■ ■ ■) až po kritickú (■ ■ ■ ■).

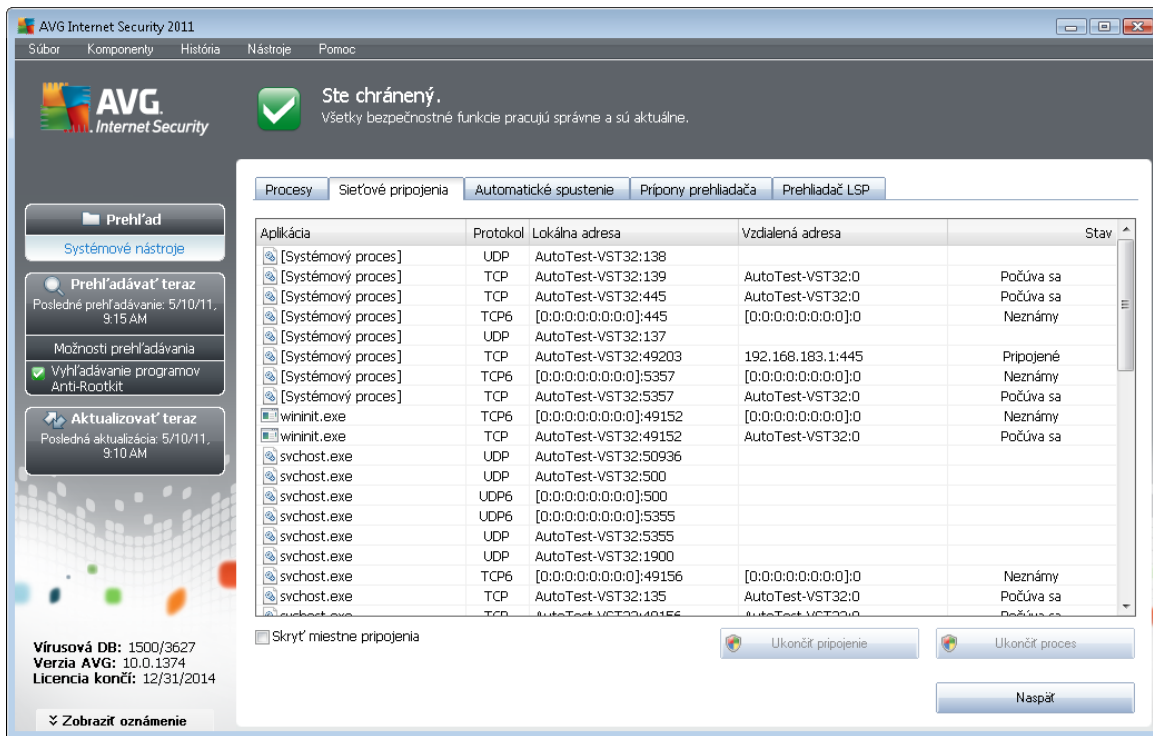
- **Názov procesu** – názov spusteného procesu
- **Cesta k procesu** – fyzická cesta k spustenému procesu.
- **Okno** – ak existuje, uvádza názov aplikácie Windows
- **PID** – identifikačné číslo procesu je jedinečný interný identifikátor procesu operačného systému Windows.

Ovládacie tlačidlá

V rozhraní súčasti **System Tools** sa nachádzajú tieto ovládacie tlačidlá:

- **Obnoviť** – aktualizuje zoznam procesov podľa momentálneho stavu.
- **Ukončiť proces** – môžete vybrať jednu alebo niekoľko aplikácií, a potom ich ukončiť stlačením tohto tlačidla. **Odporúčame vám, aby ste neukončili žiadnu aplikáciu, ak si nie ste stopercentne istý, že predstavuje skutočnú hrozbu!**
- **Naspäť** – vráti naspäť na predvolené [používateľské rozhranie AVG](#) (prehľad súčastí).

7.15.2. Sieťové pripojenia



AVG Internet Security 2011

Súbory Komponenty História Nástroje Pomoc

AVG Internet Security

Ste chránený. Všetky bezpečnostné funkcie pracujú správne a sú aktuálne.

Prehľad
Systémové nástroje

Prehľadovať teraz
Posledné prehľadávanie: 5/10/11, 9:15 AM

Možnosti prehľadávania
Vyhľadanie programov Anti-Rootkit

Aktualizovať teraz
Posledná aktualizácia: 5/10/11, 9:10 AM

Vírusová DB: 1500/3627
Verzia AVG: 10.0.1374
Licencia končí: 12/31/2014

Zobrazíť oznámenie

Sieťové pripojenia

Aplikácia	Protokol	Lokálna adresa	Vzdialená adresa	Stav
[Systémový proces]	UDP	AutoTest-VST32:138	AutoTest-VST32:0	Počúva sa
[Systémový proces]	TCP	AutoTest-VST32:139	AutoTest-VST32:0	Počúva sa
[Systémový proces]	TCP	AutoTest-VST32:445	AutoTest-VST32:0	Počúva sa
[Systémový proces]	TCP6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	Neznámy
[Systémový proces]	UDP	AutoTest-VST32:137	AutoTest-VST32:0	Počúva sa
[Systémový proces]	TCP	AutoTest-VST32:49203	192.168.183.1:445	Pripojené
[Systémový proces]	TCP6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	Neznámy
[Systémový proces]	TCP	AutoTest-VST32:5357	AutoTest-VST32:0	Počúva sa
wininit.exe	TCP6	[0:0:0:0:0:0:0:0]:49152	[0:0:0:0:0:0:0:0]:0	Neznámy
wininit.exe	TCP	AutoTest-VST32:49152	AutoTest-VST32:0	Počúva sa
svchost.exe	UDP	AutoTest-VST32:50936	AutoTest-VST32:0	Počúva sa
svchost.exe	UDP	AutoTest-VST32:500	AutoTest-VST32:0	Počúva sa
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:500	[0:0:0:0:0:0:0:0]:0	Neznámy
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:5355	[0:0:0:0:0:0:0:0]:0	Neznámy
svchost.exe	UDP	AutoTest-VST32:5355	AutoTest-VST32:0	Počúva sa
svchost.exe	UDP	AutoTest-VST32:1900	AutoTest-VST32:0	Počúva sa
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49156	[0:0:0:0:0:0:0:0]:0	Neznámy
svchost.exe	TCP	AutoTest-VST32:135	AutoTest-VST32:0	Počúva sa
svchost.exe	TCP	AutoTest-VST32:49156	AutoTest-VST32:0	Počúva sa

☐ Skryť miestne pripojenia

Ukončiť pripojenie Ukončiť proces

Naspäť

V dialógovom okne **Sieťové pripojenia** sa nachádza zoznam momentálne vytvorených pripojení. Zoznam je rozdelený na tieto stĺpce:



- **Aplikácia** – názov aplikácie súvisiacej s pripojením (okrem operačných systémov Windows 2000, v ktorých tieto informácie nie sú k dispozícii)
- **Protokol** – typ prenosového protokolu použitého na vytvorenie pripojenia:
 - o TCP – protokol, ktorý sa používa spolu s internetovým protokolom (IP) na prenos informácií na internete.
 - o UDP – alternatíva protokolu TCP.
- **Lokálna adresa** – adresa IP lokálneho počítača a číslo použitého portu.
- **Vzdialená adresa** – adresa IP vzdialeného počítača a číslo portu, na ktorom je vytvorené pripojenie. Podľa možností sa vyhľadá aj hostiteľský názov vzdialeného počítača.
- **Stav** – informuje o najpravdepodobnejšom momentálnom stave (*Pripojené, Server sa musí odpojiť, Počúva, Aktívne zatvorenie dokončené, Pasívne zatvorenie, Aktívne zatvorenie*)

Ak chcete zobraziť len externé pripojenia, začiarknite začiarkovacie okienko **Skryť miestne pripojenia** v spodnej časti dialógového okna pod zoznamom.

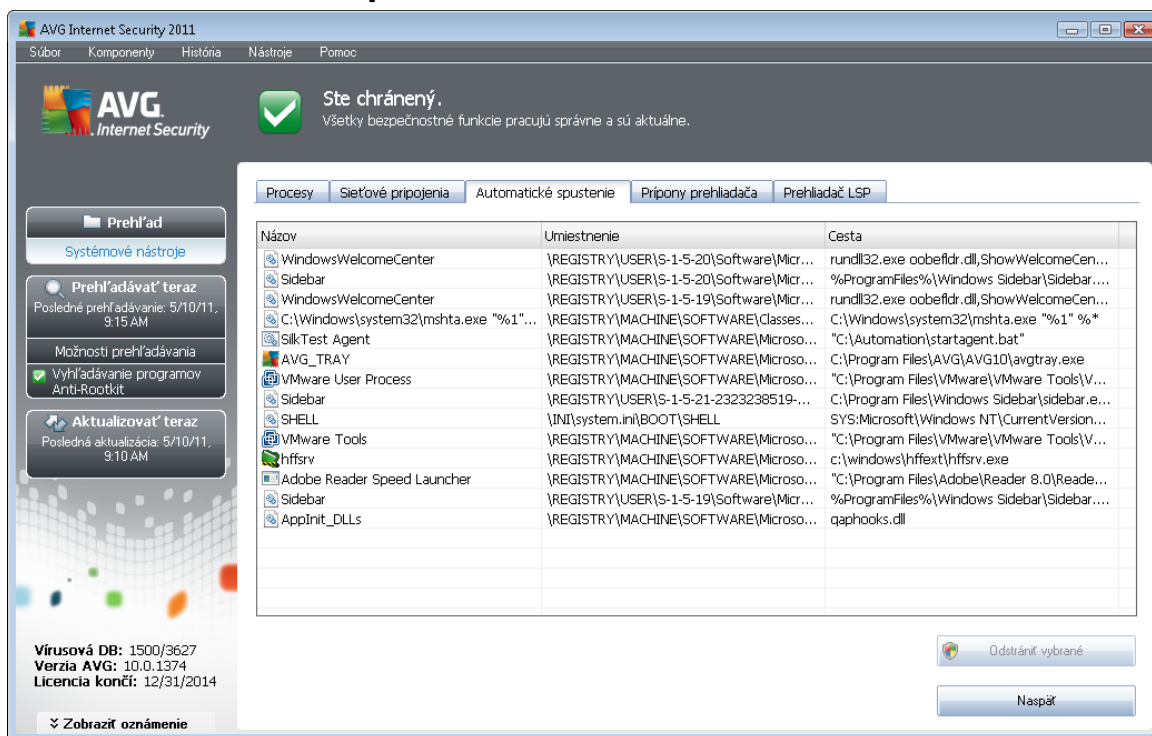
Ovládacie tlačidlá

Zobrazené sú tieto ovládacie tlačidlá:

- **Ukončiť pripojenie** – zatvorí jedno alebo viac pripojení vybraných v zozname.
- **Ukončiť proces** – zatvorí jednu alebo viac aplikácií súvisiacich s pripojeniami vybranými v zozname.
- **Naspäť** – otvorí hlavné [používateľské rozhranie programu AVG](#) (prehľad súčastí).

Niekedy vám program umožní ukončiť len tie aplikácie, ktoré sú práve pripojené. Odporúčame vám, aby ste neukončovali žiadne pripojenia, ak si nie ste stopercentne istý, že predstavujú skutočnú hrozbu!

7.15.3. Automatické spúšťanie

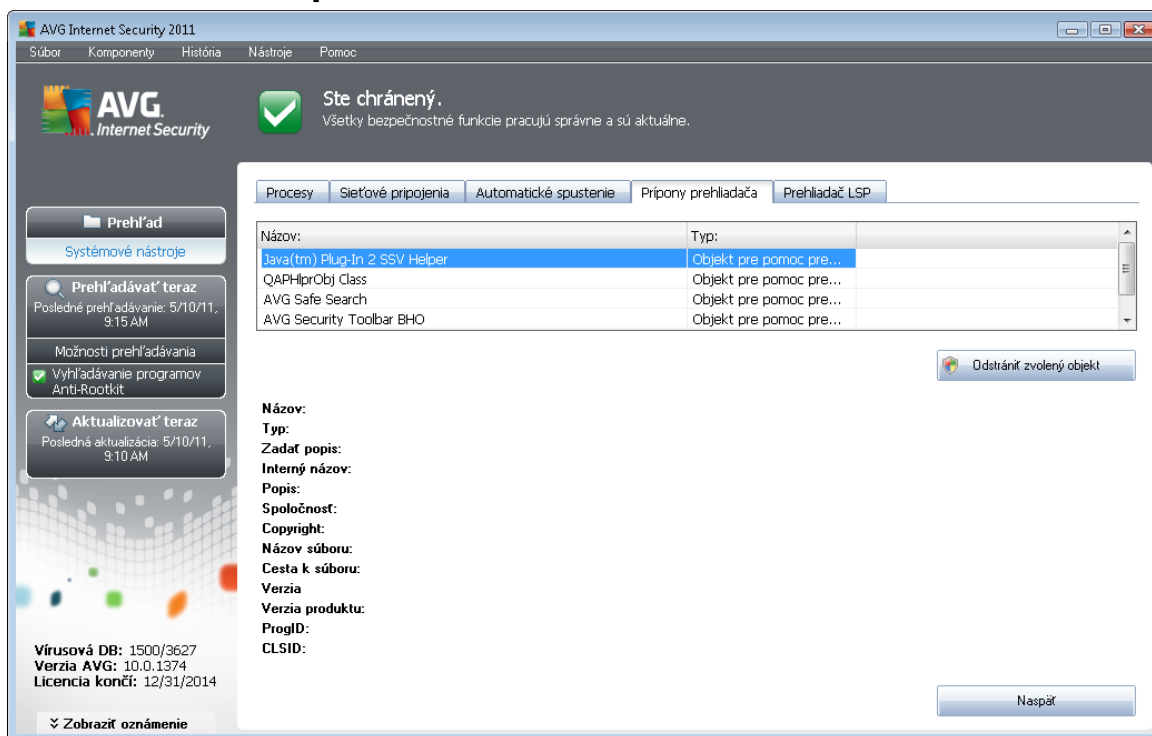


Dialógové okno **Automatické spustenie** zobrazuje zoznam aplikácií, ktoré sa spúšťajú pri spustení systému Windows. Často sa do spúšťacieho registra samovoľne pridá niekoľko aplikácií malware.

Môžete vymazať jednu alebo viac položiek tak, že ich zvolíte a stlačíte tlačidlo **Vymazať zvolenú(é) položku(y)**. Tlačidlo **Naspäť** otvorí hlavné [používateľské rozhranie programu AVG](#) (prehľad súčastí).

Odporúčame vám nevymazať žiadne aplikácie zo zoznamu, ak si nie ste stopercentne istý, že predstavujú skutočnú hrozbu!

7.15.4. Rozšírenia prehliadača



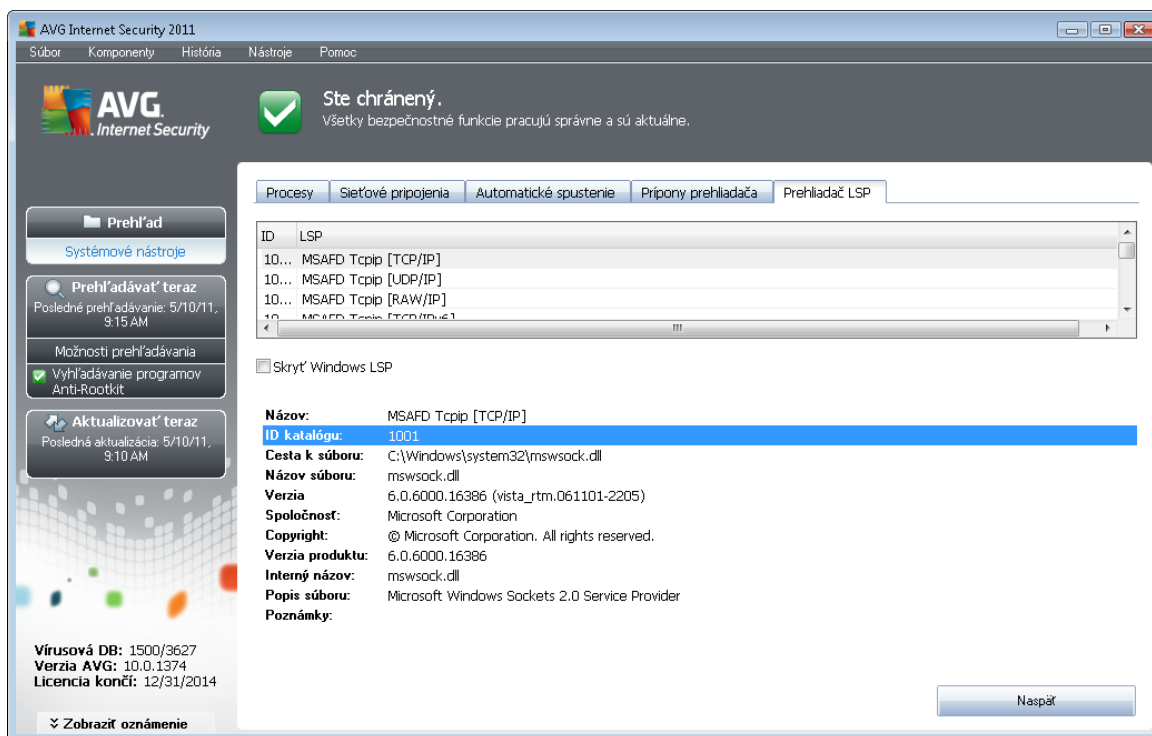
V dialógovom okne **Rozšírenia prehliadača** sa nachádza zoznam zásuvných modulov (t. j. aplikácií), ktoré sú nainštalované vo vašom internetovom prehliadači. V tomto zozname sa môžu nachádzať bežné aplikačné zásuvné moduly a rovnako aj potenciálne škodlivé programy. Po kliknutí na objekt v zozname sa v spodnej časti dialógového okna zobrazia podrobné informácie o vybranom zásuvnom module.

Ovládacie tlačidlá

Na karte **Rozšírenia prehliadača** sa nachádzajú tieto ovládacie tlačidlá:

- **Odstrániť vybraný objekt** – odstráni zásuvný modul, ktorý je momentálne zvýraznený v zozname. **Odporúčame vám, aby ste nevymazali žiadne zásuvné moduly zo zoznamu, ak nie ste stopercentne presvedčení, že predstavujú skutočnú hrozbu!**
- **Naspäť** – vráti naspäť na predvolené [používateľské rozhranie AVG](#) (prehľad súčastí).

7.15.5. Prehliadač LSP



V dialógovom okne **Prehliadač LSP** sa nachádza zoznam ovládačov LSP (Layered Service Provider).

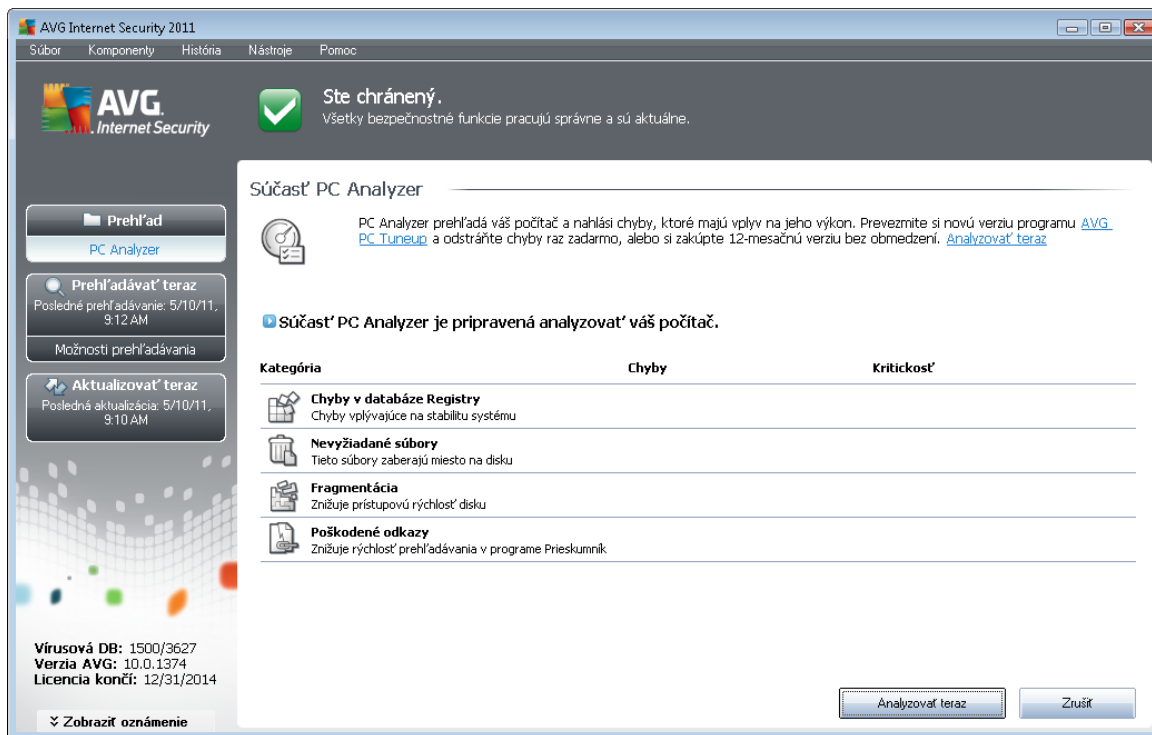
LSP (Layered Service Provider) je systémový ovládač, ktorý sa používa so sieťovými službami operačného systému Windows. Má prístup ku všetkým dátam, ktoré vstupujú do a vystupujú z počítača, a zároveň ich dokáže meniť. Niektoré LSP sú potrebné na to, aby umožnili systému Windows pripojiť sa k iným počítačom, vrátane pripojenia na internet. Niektoré škodlivé aplikácie sa však môžu tiež inštalovať ako LSP, a tak získať prístup ku všetkým dátam, ktoré váš počítač prenáša. Preto by vám tieto informácie mohli pomôcť pri kontrole všetkých možných hrozieb súvisiacich s LSP.

Za určitých okolností je možné opraviť poškodený ovládač LSP (napríklad, keď sa súbor odstráni, ale záznamy databázy Registry zostali nedotknuté). Keď sa zistí prítomnosť opraviteľného ovládača LSP, zobrazí sa nové tlačidlo, ktoré umožní problém odstrániť.

Ak chcete vložiť LSP operačného systému Windows do zoznamu, zrušte začiarknutie začiarkovacieho okienka **Skryť LSP operačného systému Windows**. Tlačidlo **Naspäť** otvorí hlavné [používateľské rozhranie programu AVG](#) (prehľad súčastí).

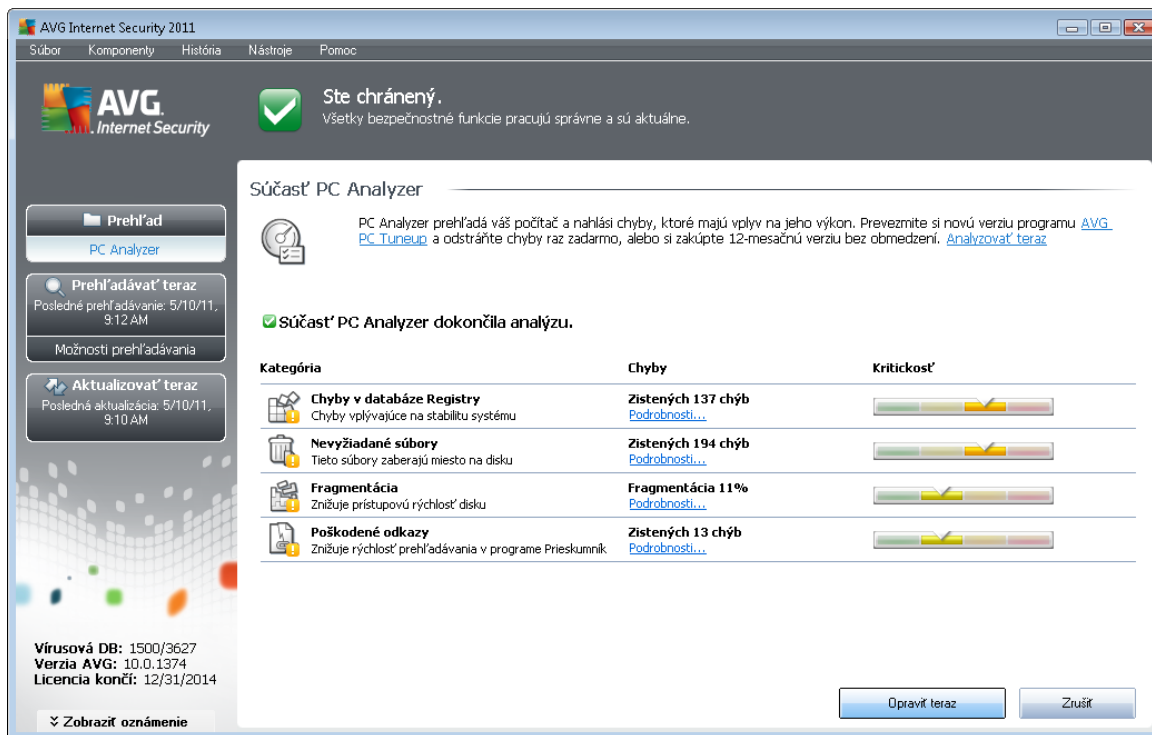
7.16. PC Analyzer

Súčasť **PC Analyzer** dokáže vyhľadať systémové problémy vášho počítača a zobrazí prehľad toho, čo môže zhoršovať celkový výkon počítača. V používateľskom rozhraní súčasti sa nachádza tabuľka rozdelená na štyri riadky podľa príslušných kategórií: chyby databázy Registry, nežiaduce súbory a poškodené odkazy:



- **Chyby databázy Registry** informuje o počte chýb v databáze Registry operačného systému Windows. Keďže na opravenie databázy Registry sú potrebné vedomosti na pomerne vysokej úrovni, neodporúčame vám, aby ste sa ju pokúšali opraviť vlastnými silami.
- **Nevyžiadané súbory** informuje o počte súborov, bez ktorých sa s veľkou pravdepodobnosťou zaobídete. Zvyčajne ide o mnohé typy dočasných súborov a súbory v Koši.
- **Fragmentácia** vypočíta podiel pevného disku, ktorý je fragmentovaný, t. j. používal sa dlhú dobu a väčšina súborov je teraz porozhadzovaná na rôznych miestach na fyzickom disku. Na odstránenie tohto problému môžete použiť nástroj na defragmentáciu.
- **Poškodené odkazy** informuje o odkazoch, ktoré už nie sú funkčné, vedú na neexistujúce miesta atď.

Na spustenie analýzy počítača stlačte tlačidlo **Analyzovať teraz**. Potom si budete môcť pozrieť priebeh analýzy a výsledky priamo v tabuľke:



Prehľad výsledkov informuje o počte detegovaných systémových problémov (**Chyby**), ktoré sú rozdelené podľa príslušnej testovanej kategórie. Výsledky analýzy sa zobrazia aj v grafickej podobe na osi v stĺpci **Závažnosť**.

Ovládacie tlačidlá

- **Analyzovať teraz** (zobrazí sa pred spustením analýzy) – stlačením tohto tlačidla sa ihneď spustí analýza počítača.
- **Opraviť teraz** (zobrazí sa po dokončení analýzy) – stlačením tohto tlačidla sa otvoria internetové stránky AVG (<http://www.avg.com/>) na stránke s podrobnými a najnovšími informáciami o súčasti **PC Analyzer**.
- **Zrušiť** – stlačením tohto tlačidla sa zastaví spustená analýza, resp. po dokončení analýzy sa otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí).

7.17. ID Protection

AVG Identity Protection je produkt na ochranu pred škodlivým softvérom, ktorý zabraňuje zlodejom identít ukradnúť vaše heslá, informácie o bankových účtoch, čísla kreditných kariet a iné cenné osobné digitálne dáta pomocou akéhokoľvek druhu škodlivého softvéru (*malware*), ktorý útočí na váš počítač. Zabezpečuje, aby všetky programy bežiacie na počítači fungovali správne. **AVG Identity Protection** zaznamenáva a blokuje podozrivé správanie a chráni počítač pred každým novým malwarom.

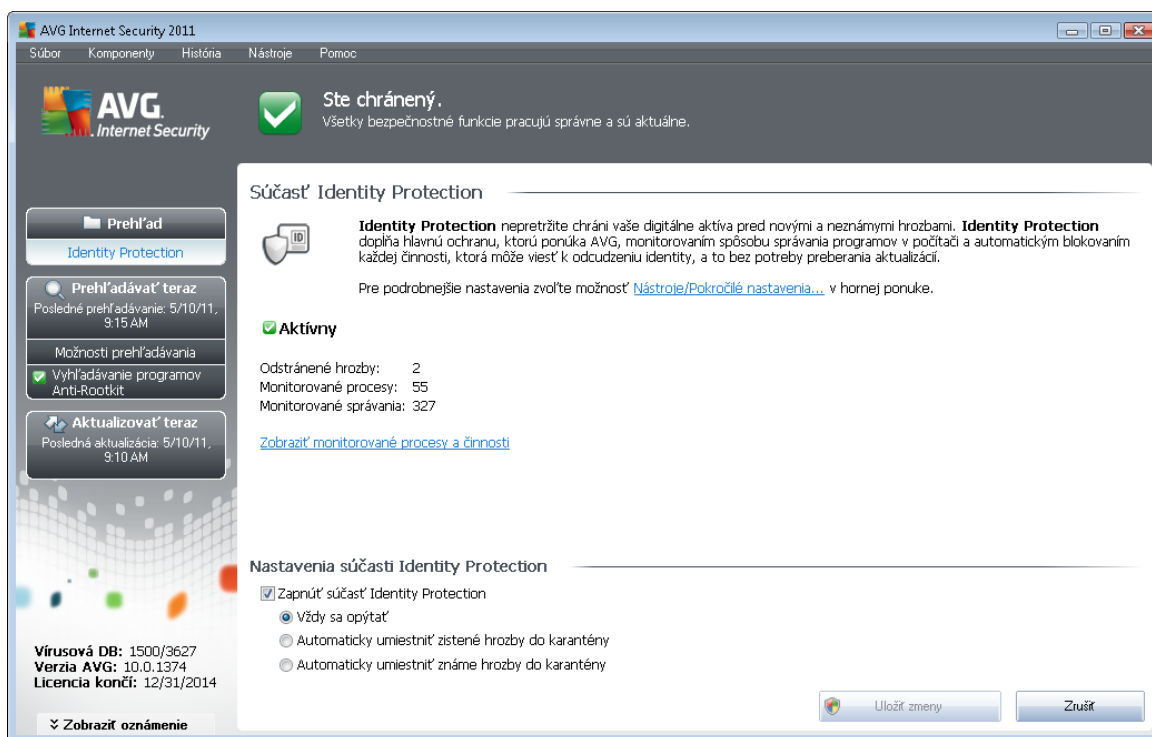


7.17.1. Princípy fungovania súčasti ID Protection

AVG Identity Protection je súčasť na ochranu pred malwarom, ktorá chráni pred všetkými druhmi malwaru (*spywarom, softvérovými robotmi, odcudzením identity...*) používaním technológií monitorovania správania a poskytuje okamžitú ochranu pred novými vírusmi. Škodlivý softvér sa stáva stále viac sofistikovanejší a objavuje sa v podobe normálnych programov, ktoré dokážu otvoriť počítač vzdialenému útočníkovi a umožnia mu odcudziť identitu, pričom aplikácia **AVG Identity Protection** vás chráni pred týmto novým spustiteľným škodlivým softvérom. Predstavuje doplnkovú ochranu k programu **AVG Anti-Virus**, ktorá chráni pred súborovými a známymi vírusmi pomocou mechanizmu signatúr a prehľadávania.

Odporúčame vám nainštalovať program [AVG Anti-Virus](#) aj súčasť **AVG Identity Protection na získanie úplnej ochrany počítača.**

7.17.2. Rozhranie súčasti ID Protection



V rozhraní súčasti **Identity Protection** sa nachádza stručný prehľad základnej funkcionality súčasti, jej stavu a niektoré štatistické informácie:

- **Odstránený škodlivý softvér** – informuje o počte odstránených aplikácií, ktoré boli označené ako škodlivý softvér.
- **Monitorované procesy** – počet momentálne spustených aplikácií monitorovaných súčastou IDP.
- **Monitorované správanie** – počet konkrétnych činností spustených v rámci monitorovaných aplikácií.



Nižšie sa nachádza odkaz [Zobraziť monitorované procesy a činnosti](#), ktorý otvára používateľské rozhranie súčasti [System Tools](#) s podrobným prehľadom všetkých monitorovaných procesov.

Nastavenia súčasti Identity Protection

V spodnej časti tohto dialógového okna sa nachádza časť s názvom **Nastavenia súčasti Identity Protection**, ktorá umožňuje zmeniť niektoré základné funkcie súčasti:

- **Súčasť Identity Protection je zapnutá** (štandardne zapnuté) – začiarknutím sa aktivuje súčasť IDP a otvoria sa ďalšie možnosti editovania.

V niektorých prípadoch môže súčasť **Identity Protection** hlásiť, že je niektorý legitímny súbor podozrivý alebo nebezpečný. Keďže **Identity Protection** deteguje hrozby na základe ich správania, toto sa zvyčajne vyskytne v prípade, keď sa niektorý program pokúsi monitorovať kľúčové procesy, nainštalovať iné programy, alebo keď sa do počítača nainštaluje nový ovládač. Preto vyberte jednu z týchto možností, ktoré definujú správanie súčasti **Identity Protection** v prípade detegovania podozrivej činnosti:

- o **Vždy sa opýtať** – keď sa aplikácia označí ako škodlivá, potom sa vás program opýta, či ju chcete blokovať (*táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nemenili, ak na to nemáte skutočný dôvod*).
- o **Automaticky umiestniť detegované hrozby do karantény** – všetky aplikácie označené ako škodlivé sa budú automaticky blokovať.
- o **Automaticky umiestniť známe hrozby do karantény** – blokovať sa budú len aplikácie, ktoré sa so stopercentnou istotou detegujú ako škodlivé.

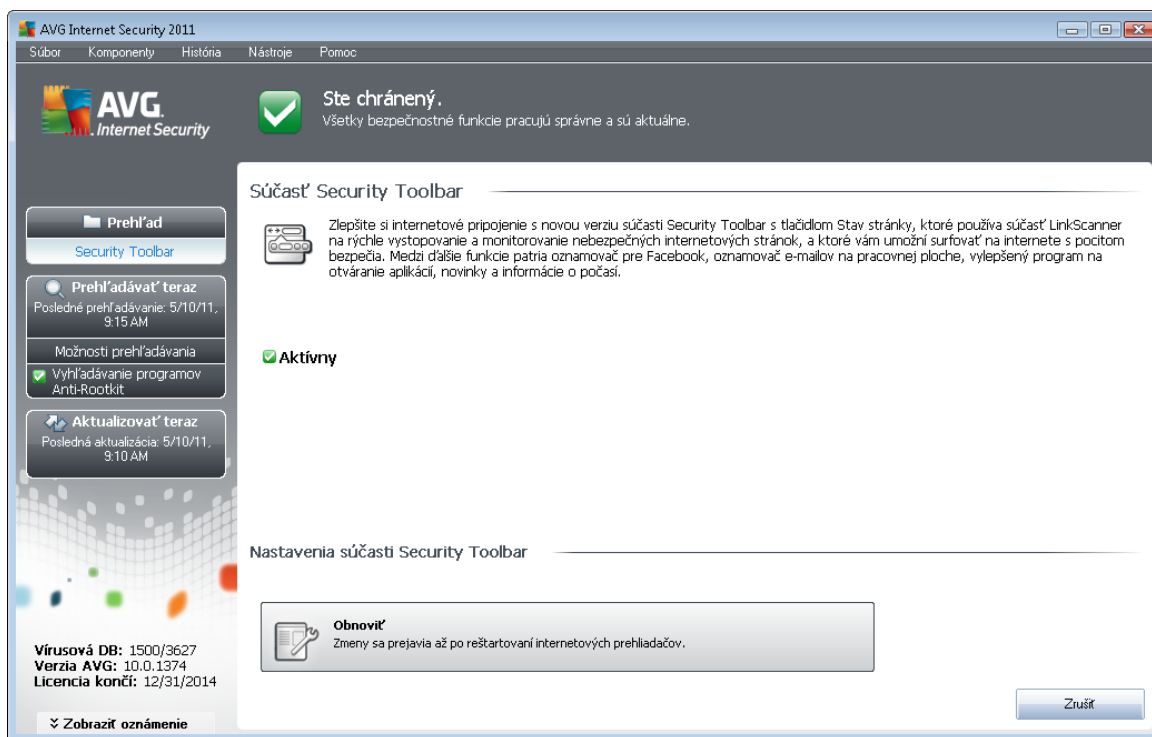
Ovládacie tlačidlá

V rozhraní **Identity Protection** sa nachádzajú tieto ovládacie tlačidlá:

- **Uložiť zmeny** – stlačením tohto tlačidla sa uložia a použijú všetky zmeny urobené v tomto dialógovom okne.
- **Zrušiť** – stlačením tohto tlačidla sa znova otvorí hlavné [používateľské rozhranie AVG](#) (prehľad súčastí)

7.18. Security Toolbar

Security Toolbar je doplnkový panel nástrojov pre internetový prehliadač, ktorý rozširuje ochranu AVG a pridáva rôzne funkcie a nástroje, ktoré sú potom k dispozícii na dosah ruky počas surfovania na internete. Súčasť **Security Toolbar** momentálne spolupracuje s internetovými prehliadačmi Internet Explorer (verzia 6.0 alebo novšia) a Mozilla Firefox (verzia 3.0 alebo novšia):



Všetky nastavenia súčasti **Security Toolbar** sú dostupné priamo v súčasti [Security Toolbar](#) v internetovom prehliadači.



8. AVG Security Toolbar

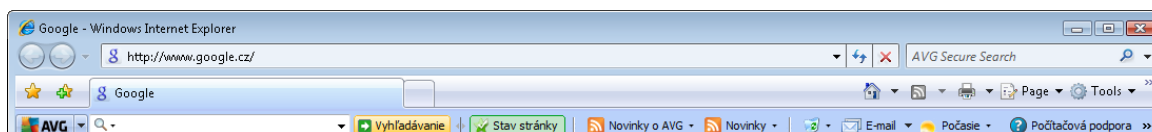
AVG Security Toolbar je nový nástroj, ktorý spolupracuje so súčasťou [LinkScanner](#). **AVG Security Toolbar** sa používa na ovládanie funkcií súčasti [LinkScanner](#) a nastavenie jej správania.

Ak sa rozhodnete nainštalovať súčasť Toolbar počas inštalácie programu **AVG Internet Security 2011**, potom sa automaticky pridá do internetového prehliadača (*Internet Explorer 6.0 alebo novšieho a Mozilla Firefox 3.0. alebo novšieho*). Iné internetové prehliadače nie sú momentálne podporované.

Poznámka: Ak používate nejaký iný internetový prehliadač (napr. Avant Browser), môžete sa stretnúť s neočakávaným správaním.

8.1. Rozhranie súčasti AVG Security Toolbar

Súčasť **AVG Security Toolbar** spolupracuje s programami **MS Internet Explorer** (verzia 6.0 alebo novšia) a **Mozilla Firefox** (verzia 3.0 alebo novšia). Keď sa rozhodnete nainštalovať súčasť **AVG Security Toolbar** (počas [procesu inštalácie produktu AVG](#) sa vás program opýta, či si želáte súčasť nainštalovať), potom sa súčasť nachádza v internetovom prehliadači hneď pod riadkom s adresou:



Súčasť **AVG Security Toolbar** tvoria tieto časti:

8.1.1. Tlačidlo s logom AVG

Toto tlačidlo umožňuje prístup ku všeobecným položkám panela nástrojov. Kliknite na tlačidlo s logom; otvoria sa [internetové stránky AVG](#). Po kliknutí na kurzor vedľa ikony AVG sa otvoria tieto možnosti:

- **Informácie o súčasti Toolbar** – odkaz na domovskú stránku súčasti **AVG Security Toolbar** s podrobnými informáciami o ochrane poskytovanej súčasťou Toolbar.
- **Spustiť AVG** – otvorí .
- **Informácie o AVG** – otvorí kontextovú ponuku s týmito odkazmi, ktoré vedú k dôležitým bezpečnostným informáciám súvisiacim s produktom **AVG Internet Security 2011**:
 - o *O hrozbách* – otvorí [internetové stránky AVG](#) na stránke s najdôležitejšími informáciami o najväčších hrozbách, odporúčaniami na odstránenie vírusov, informáciami o aktualizáciách AVG, prístupom k [vírusovej databáze](#) a ďalšími súvisiacimi informáciami.
 - o *Novinky od AVG* – otvorí internetovú stránku s najnovšími tlačovými správami súvisiacimi s produktmi a spoločnosťou AVG.

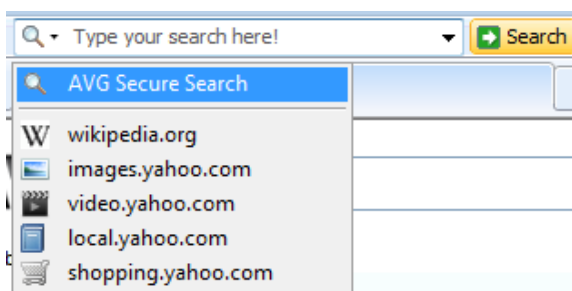


- o *Momentálna úroveň hrozieb* – otvorí internetovú stránku vírusového laboratória s grafickým zobrazením momentálnej úrovne hrozieb na internete.
- o *AVG Threat Labs* – otvorí internetové stránky [AVG Site Reports](#), na ktorých môžete vyhľadať hrozby podľa názvu a získate podrobné informácie o každej z ich.
- **Možnosti** – otvorí dialógové okno konfigurácie, ktoré vám umožní prispôbiť nastavenia súčasti **AVG Security Toolbar** vašim potrebám (pozri ďalšiu kapitolu [Možnosti súčasti AVG Security Toolbar](#)).
- **Vymazať históriu** – umožňuje vymazať celú históriu súčasti **AVG Security Toolbar**, resp. individuálne vymazať históriu hľadania, históriu internetového prehliadača, históriu prevzatých súborov a súbory cookies.
- **Aktualizovať** – vyhľadá nové aktualizácie súčasti **AVG Security Toolbar**
- **Pomocník** – umožňuje otvoriť súbor pomocníka, kontaktovať [technickú podporu AVG](#), poslať súvisiacu spätnú väzbu, alebo zobraziť informácie o momentálnej verzii súčasti Toolbar.

8.1.2. Vyhľadávacie okienko AVG Secure Search (powered by Google) powered

Okienko **AVG Secure Search (powered by Google)** umožňuje jednoducho a bezpečne vyhľadávať na internete pomocou vyhľadávača AVG Secure Search (powered by Google). Zadáte slovo alebo výraz do vyhľadávacieho okienka a stlačením tlačidla **Vyhľadávať** alebo klávesu **Enter** spustíte vyhľadávanie priamo na serveri AVG Secure Search (powered by Google), bez ohľadu na práve otvorenú stránku. Vo vyhľadávacom okienku sa zobrazí aj vaša história hľadania. Vyhľadávania urobené pomocou vyhľadávacieho okienka sa analyzujú pomocou ochrany [Search-Shield](#).

Alternatívne môžete vo vyhľadávacom okienku používať službu Wikipedia alebo iný konkrétny vyhľadávač – pozri obrázok:



8.1.3. Stav stránky

Priamo v súčasti Toolbar zobrazí toto tlačidlo hodnotenie práve zobrazenej internetovej stránky v závislosti od kritérií súčasti [Surf-Shield](#):

-  – stránka odkazu je bezpečná.
-  – stránka je do určitej miery podozrivá.

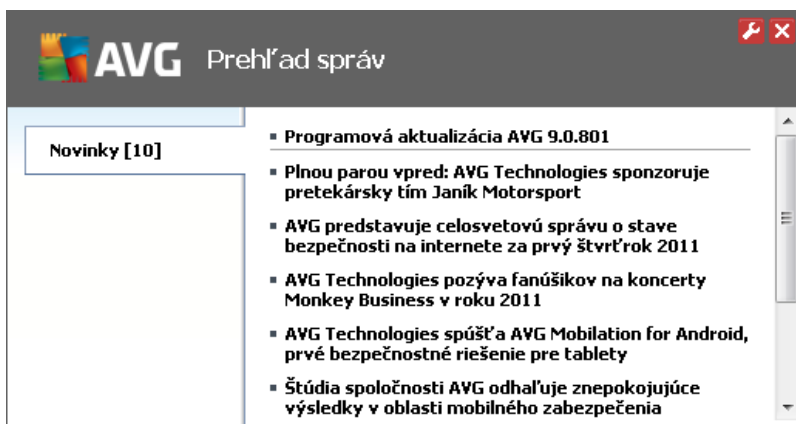


-  – na stránke sa nachádzajú odkazy na pozitívne nebezpečné stránky.
-  – na stránke odkazu sa nachádzajú činné hrozby! Pre vašu vlastnú bezpečnosť vám nebude umožnené navštíviť túto stránku.
-  – stránka nie je prístupná a nedá sa prehľadať.

Kliknutím na tlačidlo otvorte informačný panel s podrobnými informáciami o konkrétnej internetovej stránke.

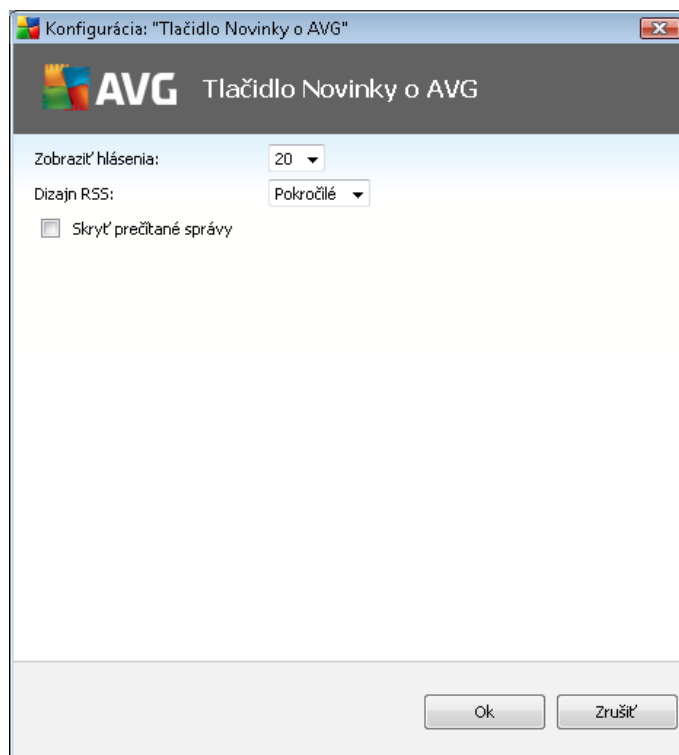
8.1.4. Novinky od AVG

Priamo na paneli **AVG Security Toolbar** sa týmto tlačidlom otvára prehľad najnovších **hlavných správ**, ktoré súvisia s AVG, či už ide o správy z tlače alebo podnikové komuniké pre tlač:



V pravom hornom rohu sa nachádzajú dve červené ovládacie tlačidlá:

-  – tlačidlo otvára dialógové okno editovania, ktoré sa používa na definovanie parametrov tlačidla **Novinky od AVG** zobrazeného na paneli **AVG Security Toolbar**:

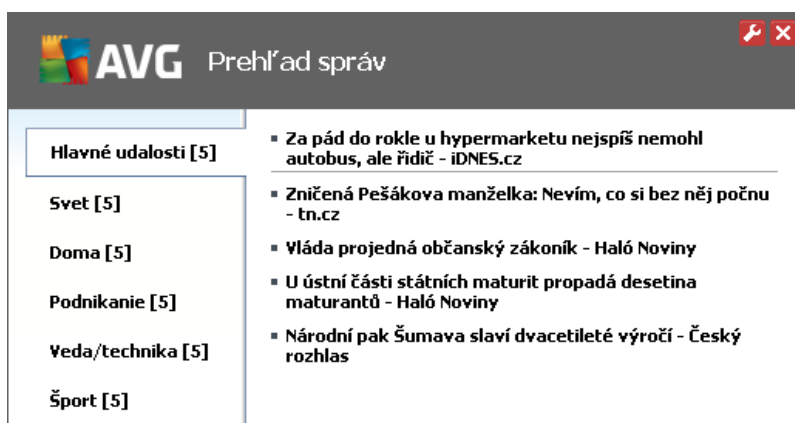


- o **Zobraziť správy** – nastavte požadovaný počet správ, ktoré sa vždy zobrazia.
- o **Dizajn RSS** – vyberte buď rozšírený alebo základný režim momentálneho zobrazenia prehľadu správ (*štandardne je nastavený rozšírený režim – pozri obrázok vyššie*).
- o **Skryť prečítané správy** – označte túto položku, aby sa už nezobrazovali prečítané správy a mohli sa doručovať nové správy.

-  – kliknutím na toto tlačidlo zatvorte momentálne zobrazený prehľad správ.

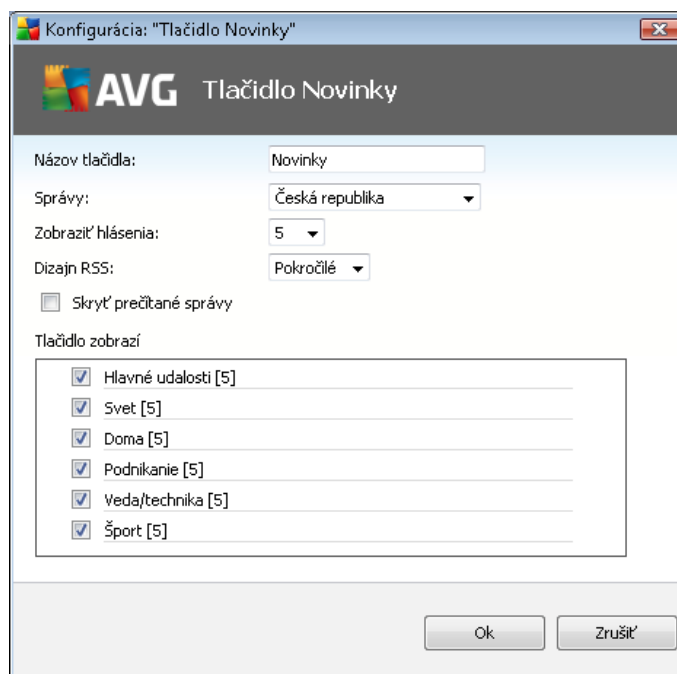
8.1.5. Správy

Podobne priamo na paneli **AVG Security Toolbar** sa týmto tlačidlom otvára prehľad najnovších správ z vybraných médií, ktoré sú rozdelené na niekoľko častí:



V pravom hornom rohu sa nachádzajú dve červené ovládacie tlačidlá:

-  – tlačidlo otvára dialógové okno editovania, ktoré sa používa na definovanie parametrov tlačidla **Správy** na paneli **AVG Security Toolbar**:



o **Názov tlačidla** – môžete zmeniť názov tlačidla tak, ako sa zobrazí na paneli **AVG Security Toolbar**

o **Edícia správ** – v zozname vyberte krajinu na zobrazenie správ z vybraného regiónu.

o **Zobraziť správy** – nastavte požadovaný počet správ, ktoré sa vždy zobrazia.

o **Dizajn RSS** – vyberte buď základný alebo rozšírený režim na zobrazenie požadovaného prehľadu



správ (štandardne je nastavený rozšírený režim, pozri obrázok vyššie).

- o **Skryt' prečítané správy** – začiarňte túto položku, aby sa v prehľade správ nezobrazovali prečítané správy a nahradili sa novými titulkami.
- o **Tlačidlo zobrazí** – v tomto poli môžete nastaviť typ správ, ktoré sa zobrazia v prehľade správ na paneli **AVG Security Toolbar**.
 - – kliknutím na toto tlačidlo zatvorte momentálne zobrazený prehľad správ.

8.1.6. Vymazanie histórie

Toto tlačidlo sa používa na vymazanie histórie prehliadača rovnako ako v prípade funkcie **Logo AVG** -> **Vymazať históriu**.

8.1.7. Upozornenie na nové e-maily

Tlačidlo **Upozornenie na nové e-maily** sa používa na zapnutie funkcie na informovanie o novo prijatých e-mailových správach priamo v rozhraní súčasti **AVG Security Toolbar**. Tlačidlo otvorí nižšie znázornené dialógové okno editácie, v ktorom môžete definovať parametre e-mailového účtu a pravidiel pre zobrazenie e-mailov. Postupujte podľa pokynov v dialógovom okne:

- **Typ účtu** – vyberte typ protokolu, ktorý používa váš e-mailový účet. Môžete vybrať niektorú z týchto alternatív. *Gmail*, *POP3*, alebo vyberte názov servera v rozbaľovacej ponuke pod položkou *Iné* (v súčasnosti môžete použiť túto možnosť so službami *Yahoo!* *JP Mail* alebo *Hotmail*). Ak máte pochybnosti o tom, aký typ poštového servera používa váš účet, pokúste sa zistiť túto informáciu u vášho poskytovateľa e-mailových služieb alebo poskytovateľa internetového pripojenia.

- **Prihlasovacie meno** – v spodnej časti zadajte presný tvar vašej e-mailovej adresy a príslušné heslo. Nechajte možnosť *Automatické prihlásenie* začiarknutú, aby ste nemuseli znova vyplňať tieto údaje.
- **Otestovať konto** – toto tlačidlo sa používa na overenie zadaných údajov.
- **Vynulovať nastavenia** – rýchlo odstráni e-mailovú adresu zadanú vyššie.
- **Kontrolovať nové e-maily každých ... minút** – nastavte časový interval, ktorý sa použije na kontrolu nových e-mailových správ (v rozsahu 5 až 120 minút), a či chcete byť informovaný o prijatí novej správy a akým spôsobom.
- **Povolit' upozorňovanie na nové e-maily** – zrušte označenie tohto začiarkovacieho okienka na vypnutie vizuálnych oznámení o prijatí nových e-mailových správ.
 - o **Prehrať zvuk pri prijatí nových e-mailov** – zrušte označenie tohto začiarkovacieho okienka na vypnutie zvukových oznámení o prijatí nových e-mailových správ.
 - o **Zatvoriť okno s oznámením po 5 sekundách** – označte toto začiarkovacie okienko na automatické zatvorenie okna s vizuálnym oznámením o prijatí nových e-mailových správ po 5 sekundách.

8.1.8. Informácie o počasi

Tlačidlo **Počasie** zobrazí informácie o momentálnej teplote (*aktualizuje sa každé 3 – 6 hodín*) vo vami vybranej destinácii priamo v rozhraní panela **AVG Security Toolbar**. Kliknutím na tlačidlo otvorte nový informačný panel s podrobným prehľadom počasia:



Ostrava, CZ
[[zmeniť miesto](#)]

 **14° C**

Rýchlosť vetra: 3.22 km/h
Východ slnka: 05:10
Západ slnka: 20:17

 UTO Vys.: 22 °C Níz.: 9 °C	 STR Vys.: 21 °C Níz.: 9 °C
--	--

Aktualizované 05/10/2011 08:47:44 **YAHOO! NEWS** [Celá predpoveď >](#)

Nižšie uvádzame možnosti editácie:

- **Zmeniť miesto** – kliknutím na text **Zmeniť miesto** sa otvorí nové dialógové okno s názvom **Hľadať miesto**. Do textového poľa zadajte názov požadovaného miesta a potvrdte ho kliknutím na tlačidlo **Hľadať**. Potom v zozname všetkých miest s rovnakým názvom



vyberte destináciu, ktorú hľadáte. Nakoniec sa zobrazí informačný panel s informáciami o počasí vo vybranom mieste.

- **Prevodník stupňov Fahrenheita/Celzia** – v pravom hornom rohu informačného panela môžete prepnúť jednotky Fahrenheita a Celzia pre stupnicu. Na základe nastavenia sa na vybranej stupnici zobrazia aj informácie o teplote.
- **Úplná predpoveď** – ak máte záujem o podrobnú predpoveď, použite odkaz **Úplná predpoveď** na otvorenie špecializovaných internetových stránok s informáciami o počasí.

8.1.9. Facebook

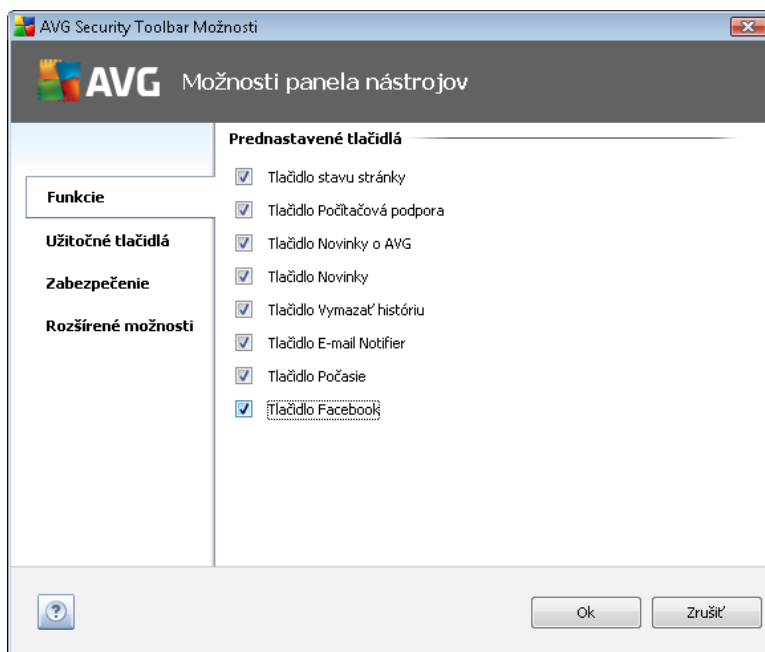
Tlačidlo **Facebook** sa používa na pripojenie k sociálnej sieti [Facebook](#) priamo z panela **AVG Security Toolbar**. Kliknutím na tlačidlo zobrazíte úvodné prihlásenie. Ďalším kliknutím otvorte dialógové okno **Prihlásenie na Facebook**. Zadáajte prístupové údaje a stlačte tlačidlo **Pripojiť**. Ak nemáte ešte vytvorený účet na [Facebooku](#), môžete si ho vytvoriť priamo pomocou odkazu **Registrovať sa na Facebooku**.

Po dokončení procesu registrácie na [Facebooku](#) sa zobrazí výzva na povolenie aplikácie **AVG Social Extension**. Táto aplikačná funkcionality je dôležitá pre súčasť Toolbar – pripojenie na [Facebook](#), a preto vám odporúčame, aby ste ju zapli. Potom sa vytvorí pripojenie k [Facebooku](#) a tlačidlo **Facebook** na paneli **AVG Security Toolbar** ponúkne štandardné možnosti ponuky [Facebooku](#).

8.2. Možnosti panela AVG Security Toolbar

Všetky konfiguračné parametre panela **AVG Security Toolbar** sa sprístupňujú priamo na paneli **AVG Security Toolbar**. Editačné rozhranie sa otvára pomocou položky v ponuke panela nástrojov **AVG/Možnosti** v novom dialógovom okne s názvom **Možnosti panela nástrojov**, ktoré je rozdelené na tri časti:

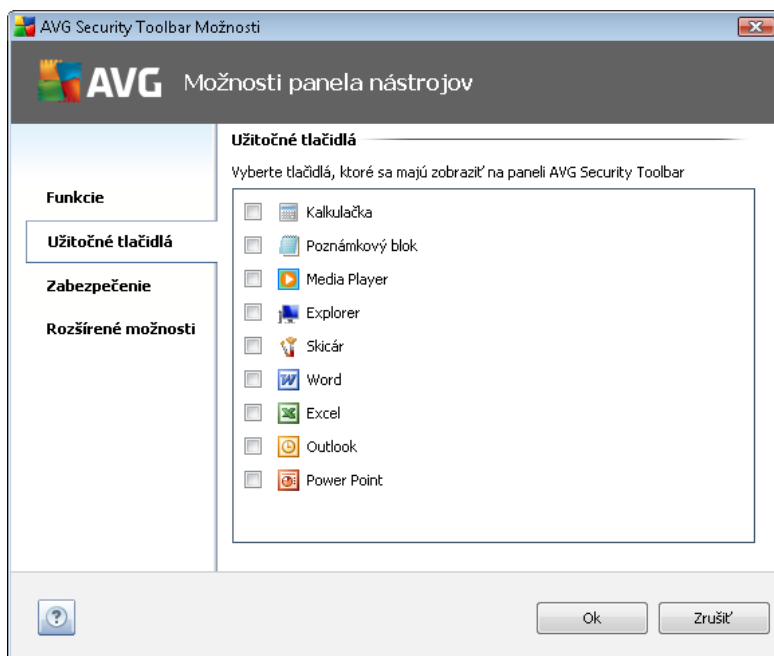
8.2.1. Karta Všeobecné



Táto karta umožňuje nastaviť, ktoré ovládacie tlačidlá sa zobrazia resp. skryjú na paneli **AVG Security Toolbar**. Označte ľubovoľnú možnosť podľa toho, ktoré tlačidlá chcete zobrazit'. Ďalej sa nachádza prehľad funkcionality jednotlivých tlačidiel na paneli Toolbar:

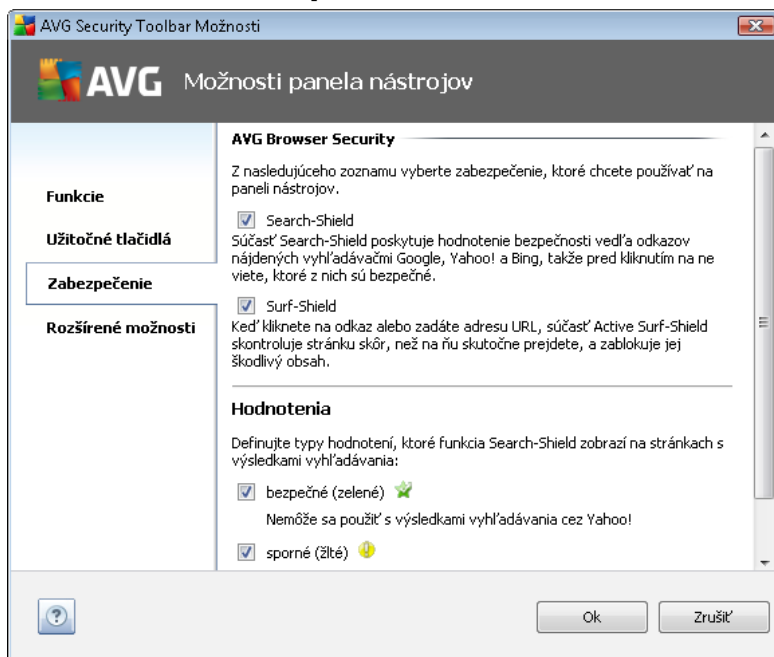
- **Tlačidlo Stav stránky** – tlačidlo umožňuje zobrazit' informácie o stave zabezpečenia práve otvorenej stránky na paneli **AVG Security Toolbar**
- **Tlačidlo Novinky od AVG** – otvorí internetovú stránku s najnovšími tlačovými správami súvisiacimi s produktmi a spoločnosťou AVG.
- **Tlačidlo Správy** – otvorí štruktúrovaný prehľad aktuálnych správ z dennej tlače.
- **Tlačidlo Vymazať históriu** – toto tlačidlo sa používa na vymazanie celej histórie resp. histórie hľadania, histórie prehliadača, histórie prevzatých súborov a súborov cookies priamo na paneli AVG Security Toolbar.
- **Tlačidlo Upozornenie na nové e-maily** – tlačidlo umožňuje zobrazit' novo prijaté e-mailové správy v rozhraní súčasť **AVG Security Toolbar**.
- **Tlačidlo Počasie** – zobrazí informácie o stave počasia na vybranom mieste.
- **Tlačidlo Facebook** – používa sa na pripojenie k sociálnej sieti [Facebook](https://www.facebook.com).

8.2.2. Karta Užitočné tlačidlá



Karta **Užitočné tlačidlá** umožňuje zvoliť aplikácie v zozname a zobrazit' ich ikonu v rozhraní panela nástrojov. Ikona sa potom používa ako skratka umožňujúca ihneď spustiť príslušnú aplikáciu.

8.2.3. Karta Zabezpečenie



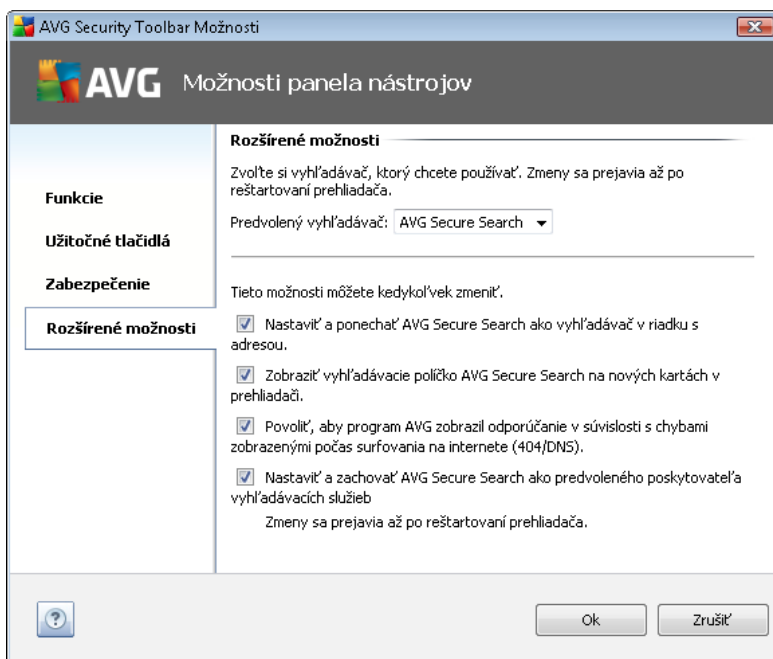
Karta **Zabezpečenie** je rozdelená na dve časti, **AVG Browser Security** a **Hodnotenia**, kde môžete označením konkrétnych začiarkovacích políčok pridať panelu **AVG Security Toolbar** funkcionality,

ktorú chcete používať:

- **Browser Security:** Pomocou tejto položky sa zapínajú a vypínajú služby [AVG Search-Shield](#) a [Surf-Shield](#).
- **Hodnotenia:** Zvoľte grafické symboly používané na hodnotenie výsledkov prehľadávania súčasťou [Search-Shield](#), ktoré chcete používať:
 - o  stránka je bezpečná
 - o  stránka je do istej miery podozrivá
 - o  na stránke sa nachádzajú odkazy na pozitívne nebezpečné stránky
 - o  na stránke sa nachádzajú aktívne hrozby
 - o  stránka nie je prístupná a nemožno ju skontrolovať

Označením príslušnej možnosti potvrdíte, že chcete byť informovaný o tejto konkrétnej úrovni hrozby. Zobrazenie červenej značky pridelené stránkam obsahujúcim aktívne a nebezpečné hrozby však nie je možné vypnúť. **Znova vám odporúčame ponechať predvolenú konfiguráciu nastavenú výrobcom programu, ak nemáte skutočný dôvod meniť ju.**

8.2.4. Karta Rozšírené možnosti



Na karte **Rozšírené možnosti** najskôr nastavte, ktorý vyhľadávač chcete používať ako predvolený. Na výber máte tieto možnosti: *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*,



Yandex a Yahoo! JP. Po zmene predvoleného vyhľadávača reštartujte prehľadávač, aby sa zmena prejavila.

Karta ďalej umožňuje zapnúť resp. vypnúť ďalšie nastavenia súvisiace so súčasťou **AVG Security Toolbar** (uvedená legenda sa týka predvolených nastavení vyhľadávača AVG Secure Search (powered by Google)):

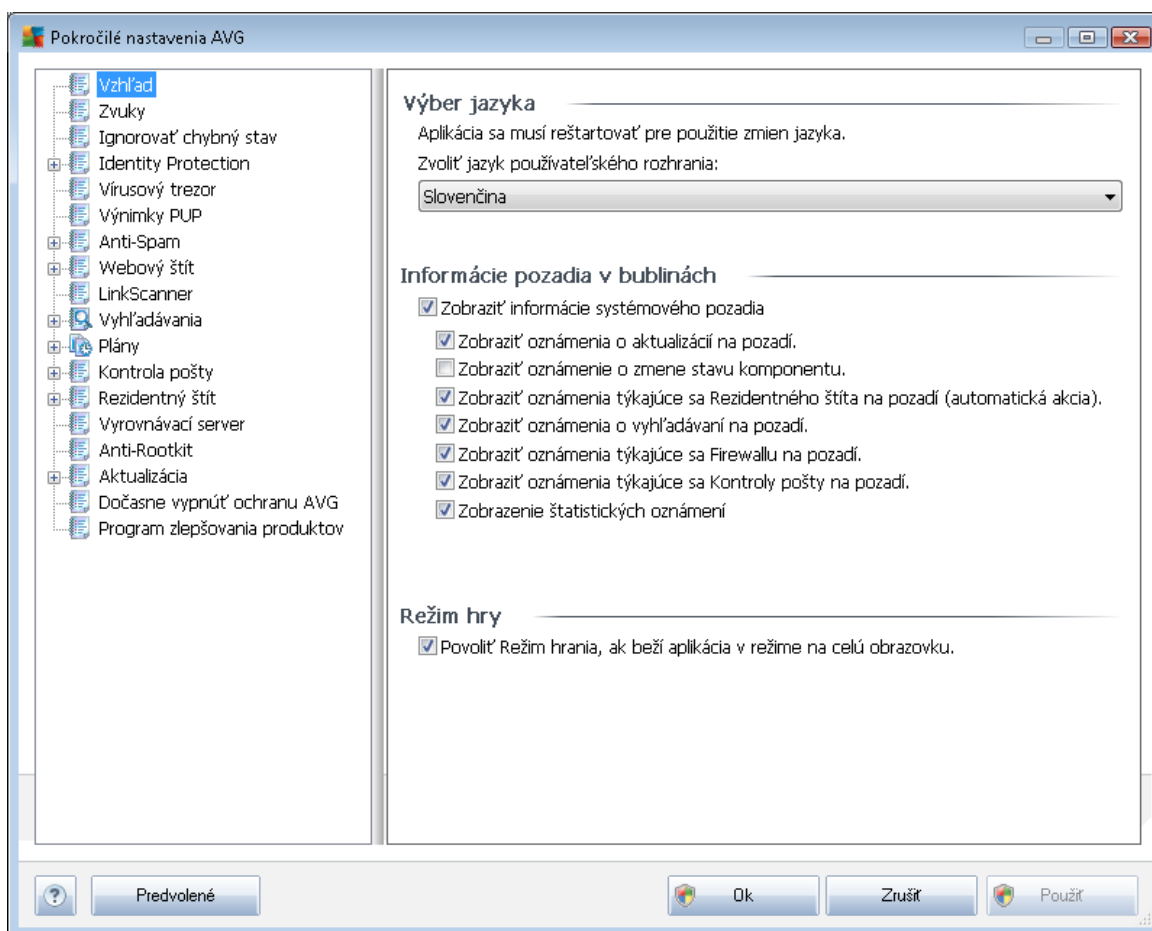
- **Nastaviť a ponechať AVG Secure Search (powered by Google) ako predvolený vyhľadávač pre riadok s adresou** – ak je toto okienko začiarknuté, funkcia umožňuje zadať hľadaný výraz priamo do riadka s adresou v internetovom prehliadači a služba Google sa automaticky použije na vyhľadanie príslušných internetových stránok.
- **Umožniť programu AVG zobrazit' odporúčania pri zobrazení chyby navigácie v prehliadači (404/DNS)** – ak počas vyhľadávania na internete narazíte na neexistujúcu stránku, alebo stránku, ktorá sa nedá zobrazit' (chyba 404), program automaticky otvorí internetovú stránku, ktorá vám umožní urobiť výber v prehľade alternatívnych stránok súvisiacich s hľadanou problematikou.
- **Nastaviť a ponechať AVG Secure Search (powered by Google) ako predvolený internetový vyhľadávač** – Google je predvolený internetový vyhľadávač pre internetové vyhľadávania urobené pomocou súčasti **AVG Security Toolbar** a zapnutím tejto funkcie sa zároveň stane predvoleným internetovým vyhľadávačom vo vašom internetovom prehliadači.

9. Rozšírené nastavenia programu AVG

Dialógové okno s rozšírenou konfiguráciou produktu **AVG Internet Security 2011** otvorí nové okno s názvom **Rozšírené nastavenia programu AVG**. Toto okno je rozdelené na dve časti: v ľavej časti sa nachádza stromová štruktúra, ktorá sa používa na navigovanie k možnostiam konfigurácie programu. Zvolením súčasti, ktorej konfiguráciu chcete zmeniť (*alebo jej konkrétnu časť*), otvorte dialógové okno editovania v pravej časti okna.

9.1. Vzhľad

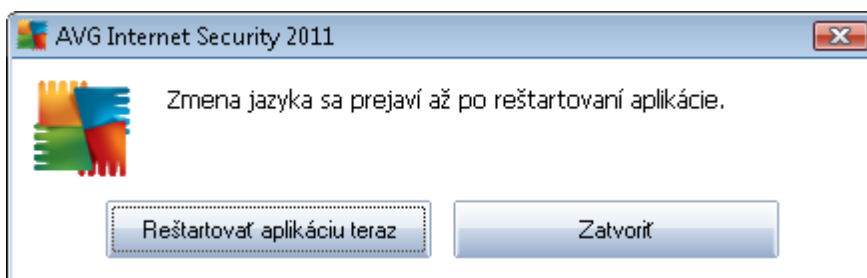
Prvá položka štruktúrovanej ponuky, **Vzhľad**, súvisí so všeobecnými nastaveniami [používateľského rozhrania AVG](#) a používa sa na nastavenie zopár základných možností správy aplikácie:



Výber jazyka

Časť **Výber jazyka** sa používa na nastavenie požadovaného jazyka pomocou rozbaľovacej ponuky; jazyk sa potom použije pre celé [používateľské rozhranie AVG](#). V rozbaľovacej ponuke sa nachádzajú len tie jazyky, ktoré ste už nainštalovali počas [procesu inštalácie](#) (pozri kapitolu [Vlastné možnosti](#)) plus angličtina (*tá sa inštaluje štandardne*). Aby sa zmena jazyka prejavila, je potrebné reštartovať používateľské rozhranie; postupujte podľa týchto pokynov.

- Vyberte požadovaný jazyk aplikácie a potvrdte výber stlačením tlačidla **Použiť** (v pravom spodnom rohu).
- Potvrdte stlačením tlačidla **OK**.
- Otvorí sa nové dialógové okno, ktoré informuje, že na zmenu jazyka používateľského rozhrania AVG je potrebné reštartovať aplikáciu:



Informačné bubliny na paneli úloh

Táto časť umožňuje zrušiť zobrazovanie informačných bublín na paneli úloh, ktoré informujú o stave aplikácie. Zobrazovanie informačných bublín je štandardne zapnuté a odporúčame vám, aby ste toto nastavenie nemenili! Informačné bubliny zvyčajne informujú o zmene stavu niektorých súčastí AVG a mali by ste im venovať pozornosť!

Ak sa však z nejakého dôvodu rozhodnete, že nechcete, aby sa tieto informácie zobrazovali, alebo chcete, aby sa zobrazovali len niektoré informácie (súvisiace s konkrétnou súčastou AVG), môžete definovať a zadať vlastné preferencie začiar knutím resp. zrušením začiar knutia týchto možností:

- **Zobrazit' oznámenia na paneli úloh** – táto položka je štandardne začiar knutá (zapnutá) a oznámenia sa zobrazujú. Zrušte začiar knutie tejto položky, aby ste úplne vypnúť zobrazovanie všetkých oznámení. Po zapnutí môžete ďalej vybrať konkrétne oznámenia, ktoré sa majú zobrazovať:
 - o **Zobrazit' oznámenia o aktualizácii** na paneli úloh – nastavte, či sa majú zobrazovať informácie súvisiace so spustením procesu aktualizácie programu AVG, jeho priebehom a dokončením.
 - o **Zobrazit' oznámenia o zmene stavu súčasti** – nastavte, či sa majú zobrazovať informácie súvisiace s činnosťou alebo nečinnosťou súčasti, prípadne či sa majú zobrazovať informácie o možnom probléme. Pri oznamovaní chybového stavu súčasti táto možnosť zodpovedá informačnej funkcii [ikony na paneli úloh](#) (zmena farby), ktorá informuje o probléme jednotlivých súčastí AVG.
 - o **Zobrazit' oznámenia súvisiace so súčastou Rezidentný štít na paneli úloh (automatická akcia)** – nastavte, či sa majú alebo nemajú zobrazovať informácie súvisiace s procesmi ukladania, kopírovania a otvárania súborov (táto funkcia sa dá nastaviť, len keď je zapnutá možnosť [Liečiť automaticky](#) v súčasti Rezidentný štít).
 - o **Zobrazit' oznámenia o kontrole** na paneli úloh – nastavte, či sa majú zobrazovať



informácie pri automatickom spustení naplánovanej kontroly, o jeho priebehu a výsledkoch.

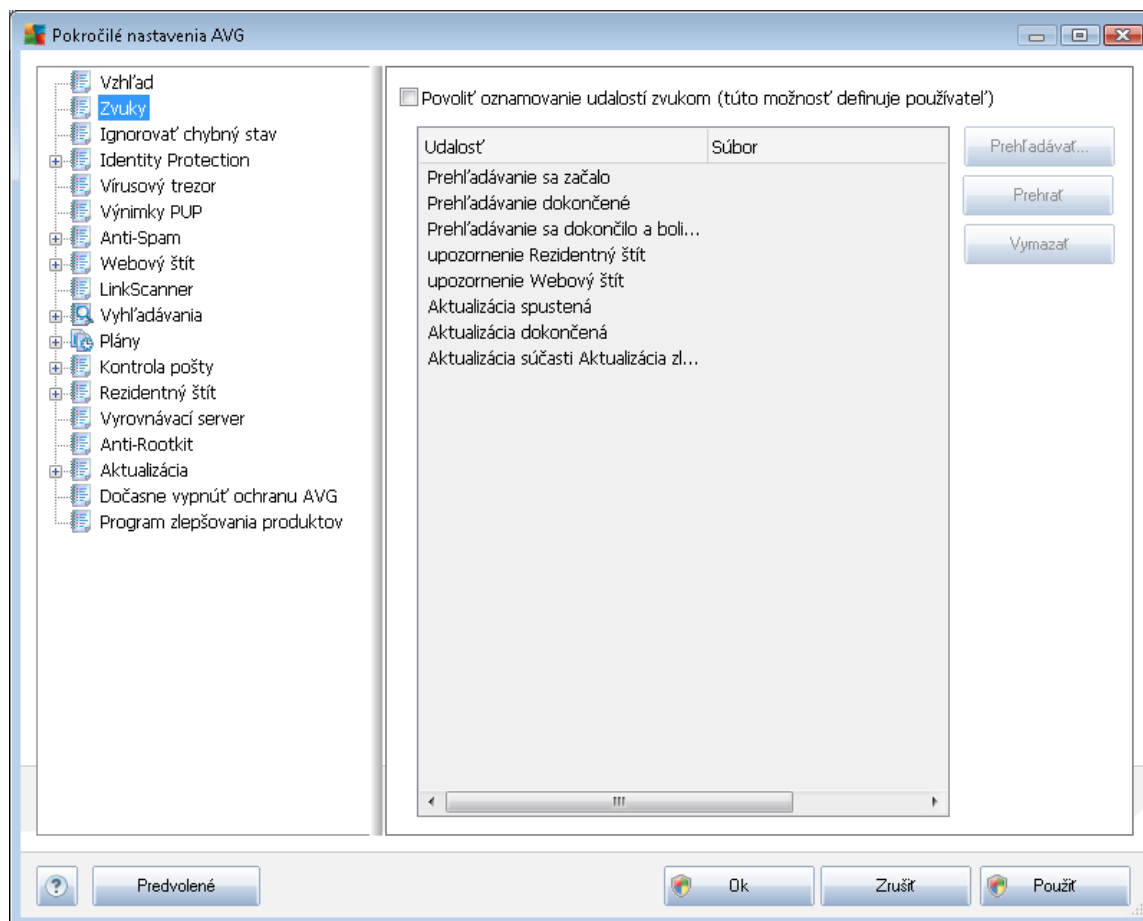
- o **Zobraziť oznámenia súvisiace so súčasťou Firewall na paneli úloh** – nastavte, či sa majú zobrazovať informácie súvisiace so stavom a procesmi súčasti Firewall, ako sú upozornenia o zapnutí alebo vypnutí súčasti, prípadne blokovanie prenosov atď.
- o **Zobraziť oznámenia súvisiace so súčasťou E-mail Scanner na paneli úloh** – nastavte, či sa majú zobrazovať informácie vždy po kontrole prichádzajúcich a odchádzajúcich e-mailových správ.
- o **Zobraziť štatistické oznámenia** – nechajte okienko začiarknuté, ak sa majú zobrazovať pravidelné štatistické prehľadové oznámenia na paneli úloh.

Režim hrania

Táto funkcia programu AVG sa používa v súvislosti s aplikáciami spustenými na celú obrazovku, ktorých spustenie by sa mohlo narušiť (*aplikácia by sa minimalizovala, alebo by sa porušila grafika*) zobrazením informačnej bubliny programu AVG (*ktorá sa zobrazí napr. pri spustení naplánovanej kontroly*). Ak sa chcete vyhnúť podobným situáciám, nechajte začiarkovacie okienko možnosti **Zapnúť režim hrania, keď je spustená aplikácia v režime na celú obrazovku** začiarknuté (*predvolené nastavenie*).

9.2. Zvuky

Dialógové okno **Zvuky** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych činnostiach programu AVG. Ak chcete túto funkciu zapnúť, označte možnosť **Povolit' oznamovanie udalostí zvukom** (štandardne vypnuté), ktorá aktivuje zoznam činností programu AVG:

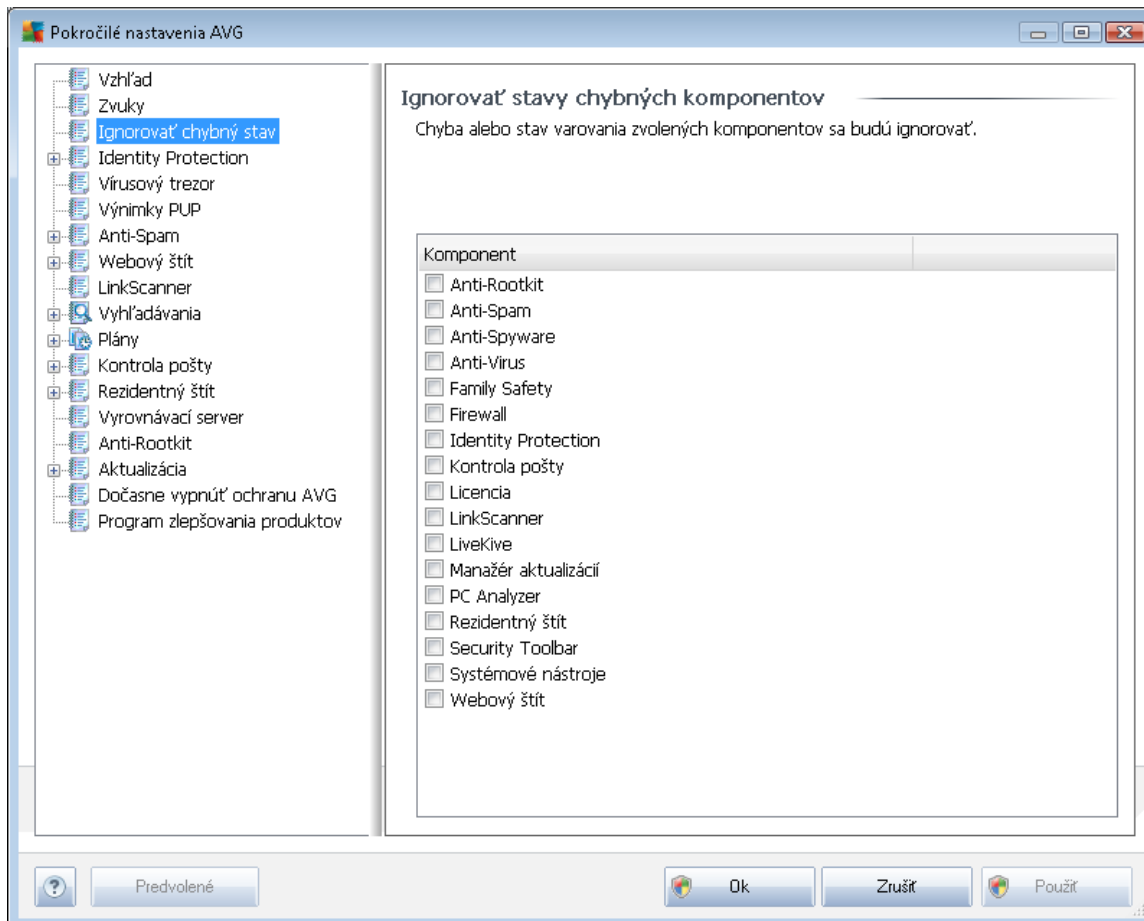


Potom zvolíte požadovanú udalosť v zozname a na disku vyhľadajte (tlačidlo **Prehľadávať**) vhodný zvuk, ktorý chcete pridelit' tejto udalosti. Ak si chcete vypočut' zvolený zvuk, zvýraznite udalosť v zozname a stlačte tlačidlo **Prehrať**. Na odstránenie zvuku prideleného konkrétnej udalosti použite tlačidlo **Vymazať**.

Poznámka: Použiť sa môžu len zvuky vo formáte *.wav.

9.3. Ignorovanie chybového stavu

Dialógové okno **Ignorovať chybový stav súčastí** umožňuje označiť tie súčasti, o ktorých nechcete byť informovaný:



Štandardne sa v tomto zozname nenachádza žiadna súčasť. To znamená, že ak sa niektorá súčasť dostane do chybového stavu, budete o tom ihneď informovaný pomocou:

- **Ikony na paneli úloh** – keď všetky časti aplikácie AVG fungujú správne, potom má ikona štyri farby; keď sa však vyskytne chyba, ikona bude mať žltý výkričník.
- Textového opisu existujúceho problému v časti **Informácie o stave zabezpečenia** v hlavnom okne programu AVG.

Môže sa vyskytnúť situácia, keď bude potrebné z nejakého dôvodu súčasť dočasne vypnúť (*neodporúčame vám však, aby ste to robili; podľa možností nechajte všetky súčasti stále zapnuté a nemeňte predvolenú konfiguráciu*). V tom prípade ikona na paneli úloh automaticky oznámi chybový stav súčasti. V tomto konkrétnom prípade však nemôžeme hovoriť o skutočnej chybe, pretože ste ju vyvolali úmyselne a ste si vedomý potenciálneho rizika. Zároveň, keď je ikona zobrazená sivou farbou, nemôže vlastne oznámiť žiadne ďalšie prípadné chyby, ktoré by sa mohli vyskytnúť.

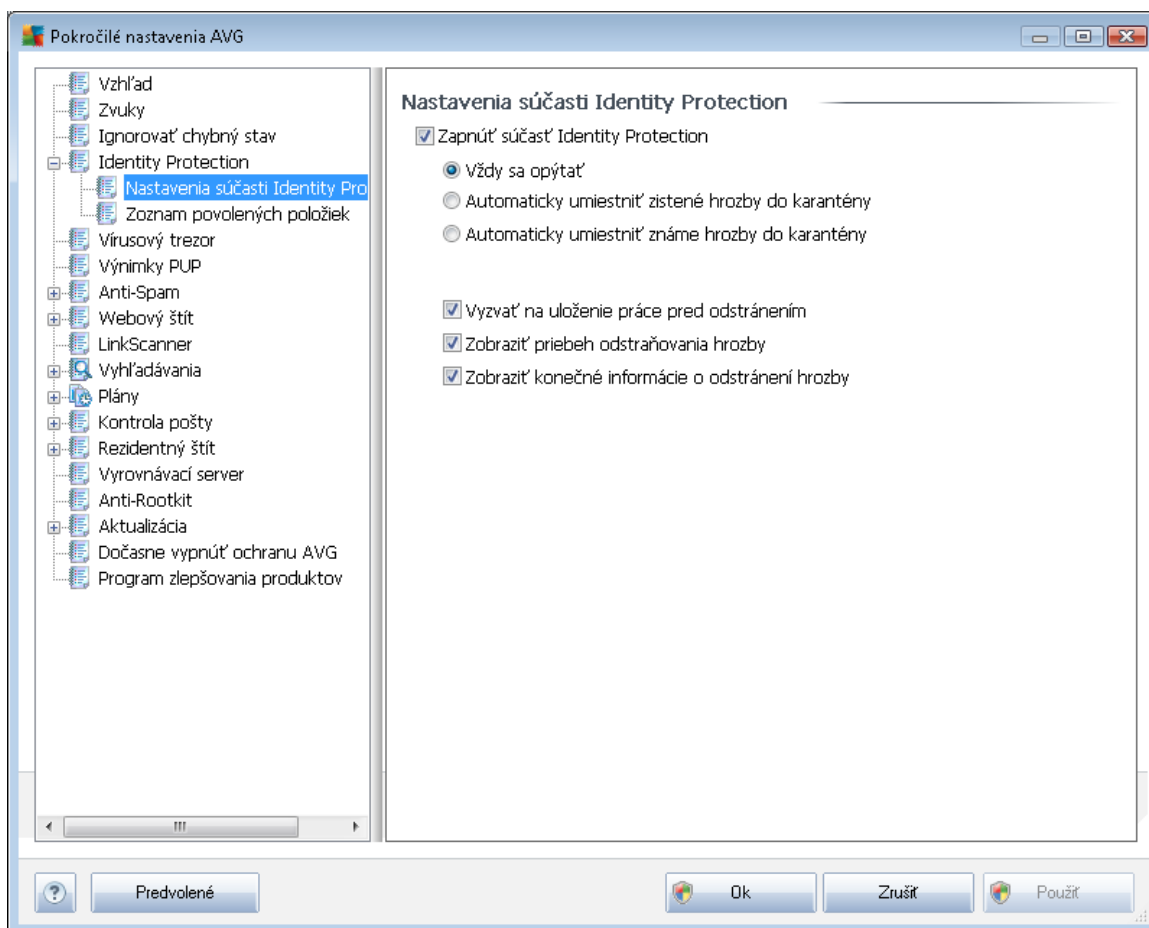


V tejto situácii môžete vo vyššie uvedenom dialógovom okne vybrať súčasti, o ktorých prípadnom chybovom stav (alebo vypnutí) si neželáte byť informovaný. Tá istá možnosť **Ignorovať chybový stav** sa môže použiť pre konkrétne súčasti aj priamo v [prehľade súčastí v hlavnom okne programu AVG](#).

9.4. Identity Protection

9.4.1. Nastavenia súčasti Identity Protection

Dialógové okno [Nastavenia súčasti Identity Protection](#) sa používa na zapnutie a vypnutie dvoch základných funkcií súčasti [Identity Protection](#):



Súčasť Identity Protection je zapnutá (štandardne zapnuté) – zrušením začiaroknutia sa vypne súčasť [Identity Protection](#).

Odporúčame vám, aby ste to urobili len v prípade, keď je to naozaj nevyhnutné!

Keď je súčasť [Identity Protection](#) zapnutá, môžete nastaviť, čo sa má urobiť pri detegovaní hrozby:

- **Vždy sa opýtať** (štandardne zapnuté) – pri detegovaní hrozby sa vás program opýta, či sa

má hrozba premiestniť do karantény, aby nedošlo k neželanému odstráneniu aplikácií, ktoré chcete používať.

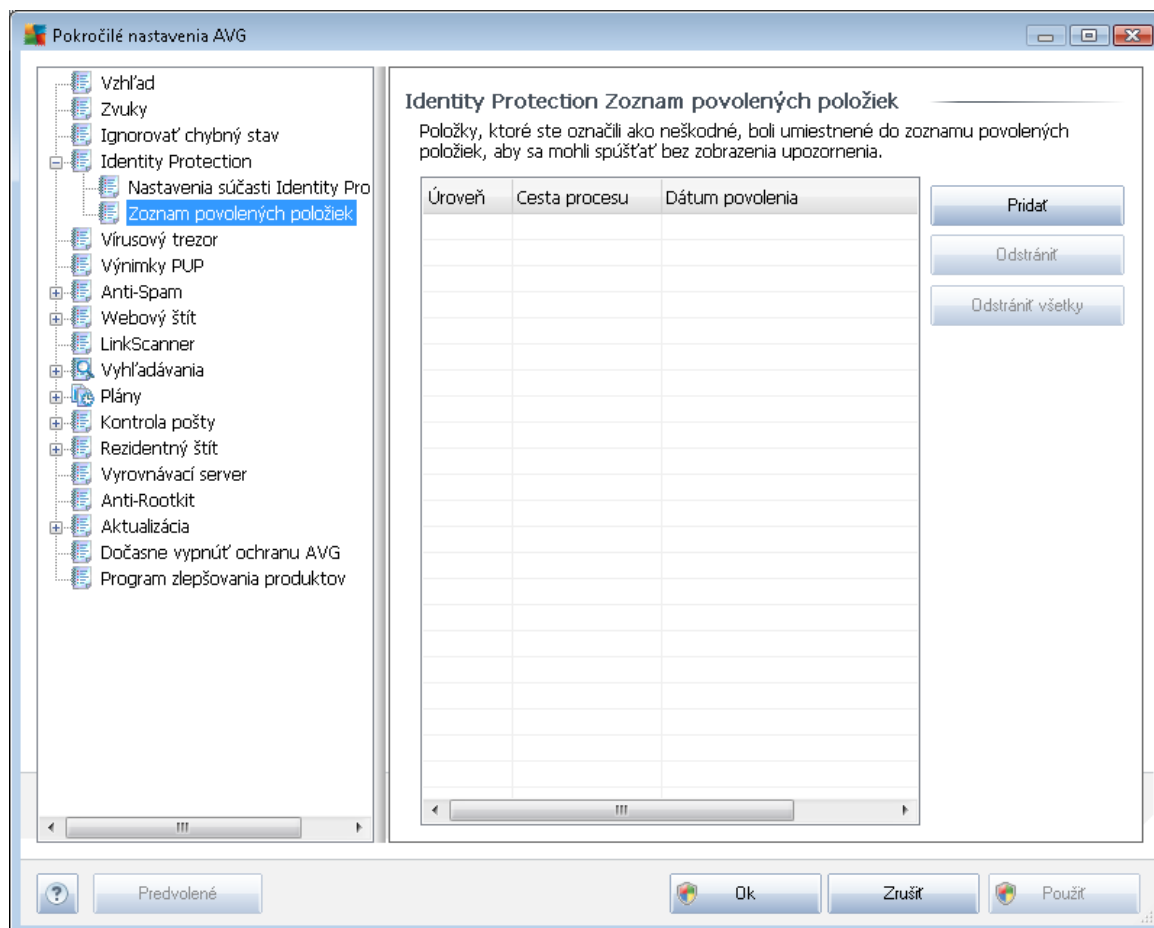
- **Automaticky umiestniť zistené hrozby do karantény** – začiaroknite toto začiarokovacie okienko, ak sa majú všetky potenciálne detegované hrozby ihneď premiestniť na bezpečné miesta vo [Vírusovom trezore AVG](#). Keď zachováte predvolené nastavenia, potom sa vás program opýta pri detegovaní hrozby, či sa má táto hrozba premiestniť do karantény, aby nedošlo k odstráneniu aplikácií, ktoré chcete používať.
- **Automaticky umiestniť známe hrozby do karantény** – nechajte toto začiarokovacie okienko začiaroknuté, ak sa majú všetky aplikácie detegované ako potenciálne škodlivé automaticky a ihneď premiestniť do [Vírusového trezora AVG](#).

Ďalej môžete nastaviť konkrétne položky a zapnúť ďalšie funkcie súčasti [Identity Protection](#):

- **Vyzvať na uloženie práce pred odstránením** (štandardne zapnuté) – nechajte toto začiarokovacie okienko začiaroknuté, ak chcete, aby sa pred premiestnením aplikácie detegovanej ako potenciálne škodlivá do karantény zobrazilo upozornenie. Ak práve pracujete s aplikáciou, projekt by sa mohol stratiť, a preto by ste ho mali najskôr uložiť. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nemenili.
- **Zobraziť priebeh odstraňovania škodlivého softvéru** (štandardne zapnuté) – keď je táto funkcia zapnutá, potom sa po detegovaní potenciálneho škodlivého softvéru otvorí nové dialógové okno s priebehom premiestňovania škodlivého softvéru do karantény.
- **Zobraziť konečné informácie o odstránení škodlivého softvéru** (štandardne zapnuté) – keď je táto funkcia zapnutá, potom súčasť **Identity Protection** zobrazí podrobné informácie o každom objekte premiestnenom do karantény (úroveň závažnosti, umiestnenie atď.).

9.4.2. Zoznam povolených

Keď máte otvorené dialógové okno **Nastavenia súčasti Identity Protection** a rozhodnete sa nechať položku **Automaticky umiestniť detegované hrozby do karantény** nezačiarknutú, potom sa vás pri každom detegovaní potenciálneho škodlivého softvéru program opýta, či ho chcete odstrániť. Ak potom označíte túto podozrivú aplikáciu (*rozpoznanú na základe jej správania*) za bezpečnú a potvrdíte, že sa má ponechať v počítači, aplikácia sa pridá do tzv. **zoznamu povolených v súčasti Identity Protection** a program ju už nebude označovať za potenciálne nebezpečnú:



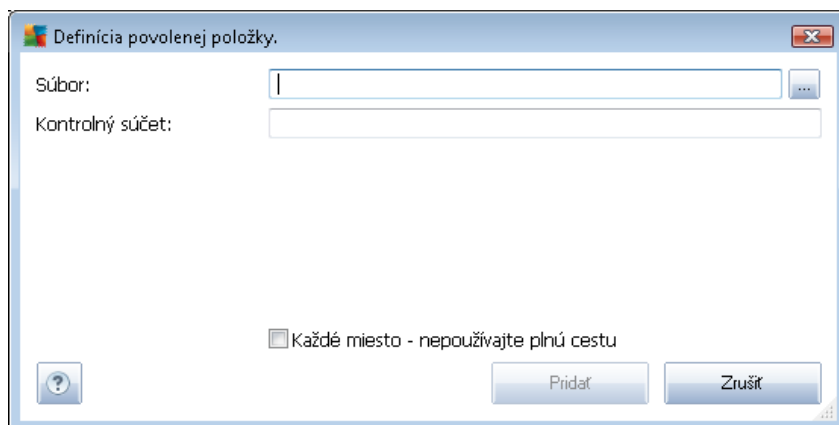
V **zozname povolených v Identity Protection** sa nachádzajú tieto informácie o každej aplikácii:

- **Úroveň** – grafické označenie závažnosti príslušného procesu na stupnici so štyrmi úrovňami od najmenej významnej (■□□□) až po kritickú (■ ■ ■ ■).
- **Cesta procesu** – cesta k umiestneniu spustiteľného súboru aplikácie (*procesu*).
- **Dátum povolenia** – dátum, keby bola aplikácia ručne označená za bezpečnú.

Ovládacie tlačidlá

V dialógovom okne **Zoznam povolených v Identity Protection** sa nachádzajú tieto ovládacie tlačidlá:

- **Pridať** – stlačením tohto tlačidla sa nová aplikácia pridá do zoznamu povolených. Otvorí sa toto prekrývacie okno:



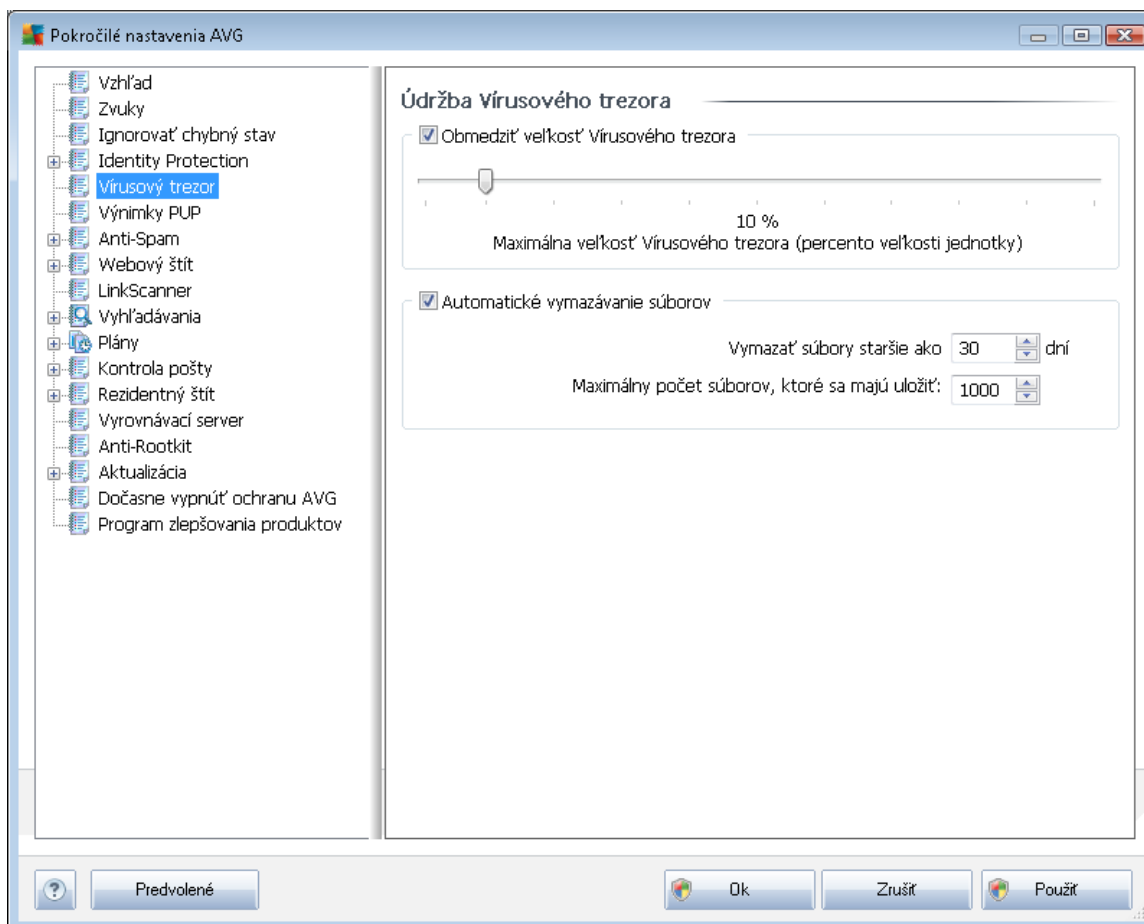
o **Súbor** – zadajte úplnú cestu k súboru (*aplikácii*), ktorý chcete označiť ako výnimku.

o **Kontrolný súčet** – uvádza jedinečnú „signatúru“ vybraného súboru. Tento kontrolný súčet je automaticky generovaný reťazec znakov, ktorý umožňuje programu AVG jasne odlíšiť vybraný súbor od ostatných súborov. Kontrolný súčet sa vygeneruje a zobrazí po úspešnom pridaní súboru.

o **Každé umiestnenie – nepoužívať úplnú cestu** – ak chcete definovať tento súbor ako výnimku len pre konkrétne umiestnenie, nechajte toto okienko nezačiarknuté.

- **Odstrániť** – stlačením tohto tlačidla sa vybraná aplikácia odstráni zo zoznamu.
- **Odstrániť všetky** – stlačením tohto tlačidla sa odstránia všetky uvedené aplikácie.

9.5. Vírusový trezor



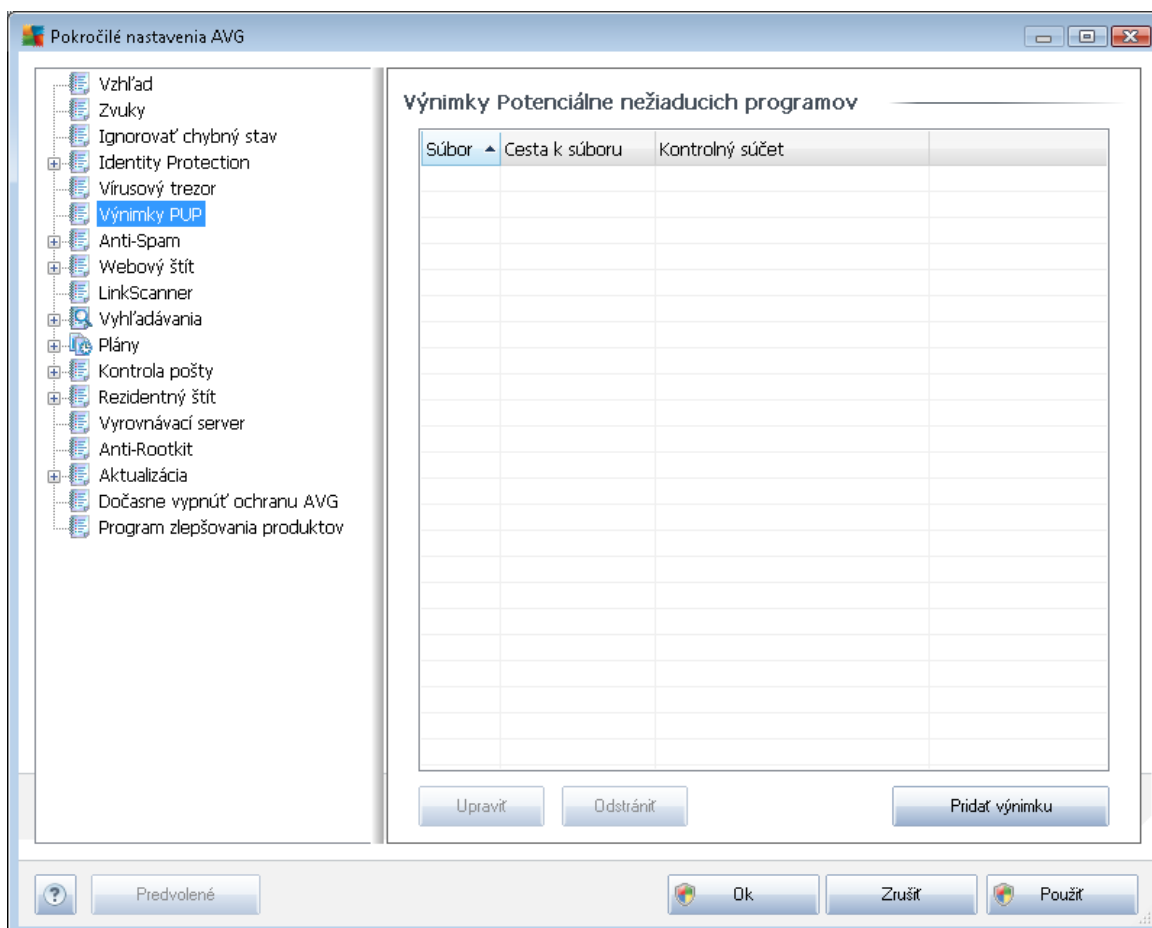
Dialógové okno **Zachovanie Vírusového trezora** vám umožňuje zdefinovať niekoľko parametrov ohľadom administrácie objektov uložených vo [Vírusovom trezore](#):

- **Obmedziť veľkosť vírusového trezora** - použijete posúvač na nastavenie maximálnej veľkosti [vírusového trezora](#). Táto veľkosť sa uvádza úmerne v porovnaní s veľkosťou vášho lokálneho disku.
- **Automatické vymazávanie súborov** - v tejto časti môžete zdefinovať maximálnu dĺžku času, počas ktorého by mali byť objekty uložené vo [Vírusovom trezore](#) (**Vymazať súbory staršie ako ... dní**) a maximálny počet súborov, ktoré budú uložené vo [Vírusovom trezore](#) (**Maximálny počet uložených súborov**)

9.6. Výnimky z PNP

AVG Internet Security 2011 dokáže analyzovať a detegovať spustiteľné aplikácie a knižnice DLL, ktoré by mohli predstavovať potenciálne nechcené položky v systéme. V niektorých prípadoch môže používateľ chcieť, aby niektoré nežiaduce programy zostali v počítači (*programy, ktoré boli nainštalované zámerne*). Programy, najmä bezplatné programy, obsahujú adware. AVG dokáže identifikovať tento adware a hlásiť ho ako **potenciálne nežiaduci program**. Ak chcete ponechať

tento program v počítači, nastavte ho ako výnimku z potenciálne nežiaducich programov.



V dialógovom okne **Výnimky z potenciálne nežiaducich programov** sa nachádza zoznam už definovaných a momentálne platných výnimiek z potenciálne nežiaducich programov. Môžete editovať zoznam, vymazať existujúce položky, alebo pridať nové výnimky. V zozname sa nachádzajú tieto informácie o každej jednej výnimke:

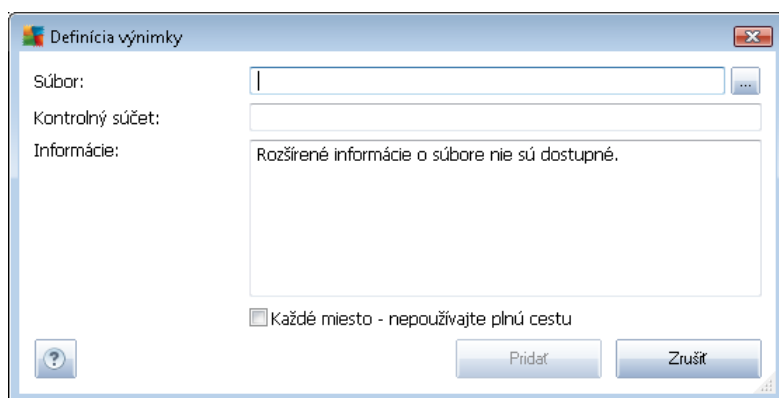
- **Súbor** – uvádza názov príslušnej aplikácie.
- **Cesta k súboru** – uvádza cestu k umiestneniu aplikácie.
- **Kontrolný súčet** – uvádza jedinečnú „signatúru“ vybraného súboru. Tento kontrolný súčet je automaticky generovaný reťazec znakov, ktorý umožňuje programu AVG jasne odlíšiť vybraný súbor od ostatných súborov. Kontrolný súčet sa vygeneruje a zobrazí po úspešnom pridaní súboru.

Ovládacie tlačidlá

- **Editovať** – otvorí dialógové okno editovania (je rovnaké ako dialógové okno definovania novej výnimky, pozri ďalej v texte) už definovanej výnimky, v ktorom môžete zmeniť

parametre výnimky.

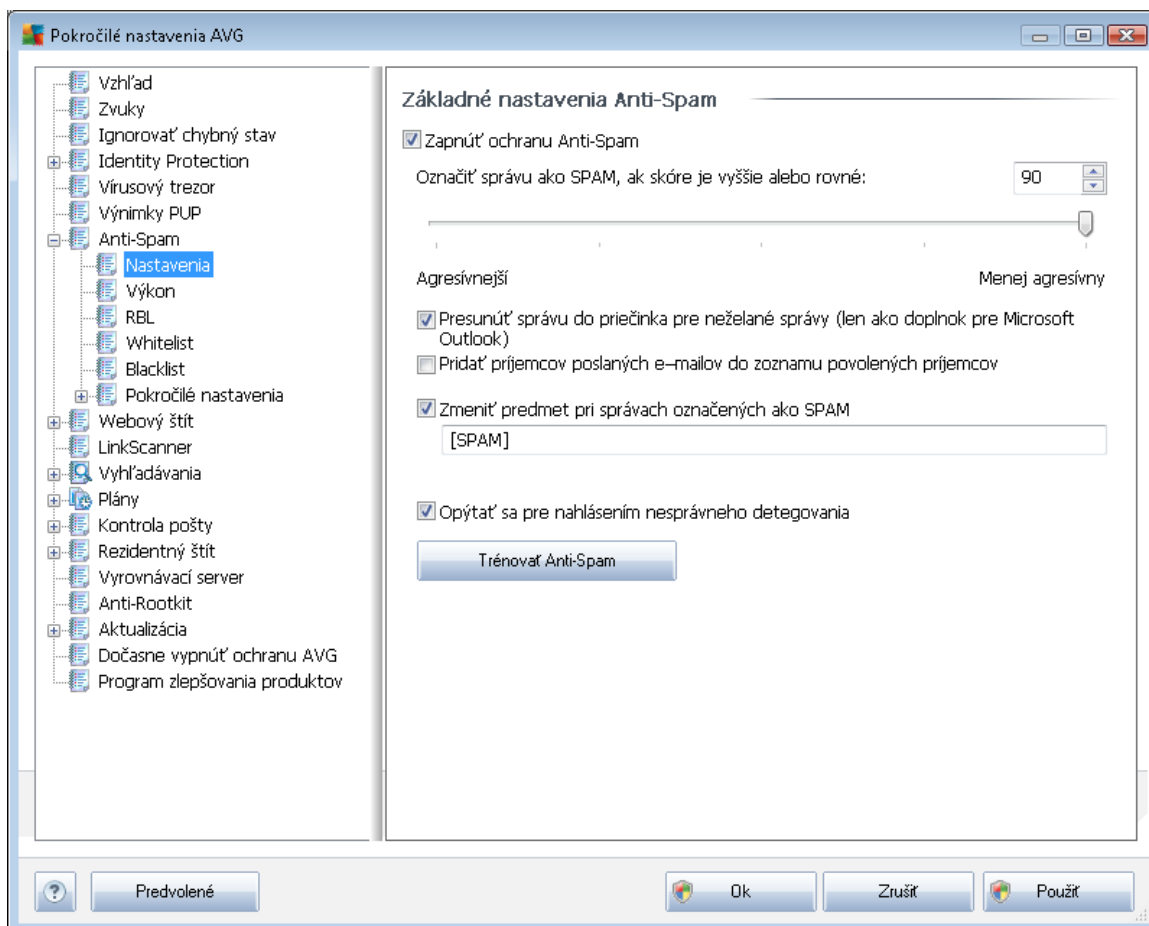
- **Odstrániť** – vymaže vybranú položku zo zoznamu výnimiek.
- **Pridať výnimku** – otvorí dialógové okno editovania, ktoré umožňuje definovať parametre novej výnimky, ktorá sa má vytvoriť:



- o **Súbor** – zadajte úplnú cestu k súboru, ktorý chcete označiť ako výnimku.
- o **Kontrolný súčet** – zobrazí jedinečnú „signatúru“ vybraného súboru. Tento kontrolný súčet je automaticky generovaný reťazec znakov, ktorý umožňuje programu AVG jasne odlíšiť vybraný súbor od ostatných súborov. Kontrolný súčet sa vygeneruje a zobrazí po úspešnom pridaní súboru.
- o **Informácie o súbore** – zobrazí všetky dostupné doplňujúce informácie o súbore (informácie o licencií, verzii atď.).
- o **Každé miesto – nepoužívajte úplnú cestu** – ak chcete definovať tento súbor ako výnimku len pre špecifické umiestnenie, nechajte toto okienko nezačiarknuté. Keď je toto začiarkovacie okienko začiarknuté, potom je príslušný súbor definovaný ako výnimka bez ohľadu na umiestnenie (aj napriek tomu však musíte uviesť úplnú cestu k príslušnému súboru; súbor sa potom použije ako typický príklad situácie, keď sa v počítači vyskytujú dva súbory s rovnakým názvom).

9.7. Anti-Spam

9.7.1. Nastavenia



V dialógovom okne **Základné nastavenia súčasti Anti-Spam** môžete začiarknutím alebo zrušením začiarknutia okienka **Zapnúť ochranu Anti-Spam** zapnúť resp. vypnúť kontrolu e-mailovej komunikácie súčasťou Anti-Spam. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod.

Ďalej môžete nastaviť viac alebo menej agresívne hodnotenie skóre. Filter súčasti **Anti-Spam** prideli každej správe skóre (t. j. v akej miere sa obsah správy podobá SPAMU) na základe niekoľkých dynamických metód kontroly. Hodnotu funkcie **Označiť správu ako spam, keď je skóre vyššie ako** môžete nastaviť buď zadáním hodnoty, alebo posunutím posúvača smerom doľava alebo doprava (nastavené hodnoty môžu byť v rozsahu 50 – 90).

Odporúčame vám, aby ste nastavili prahovú hodnotu v pásme 50 – 90, prípade ak máte naozaj pochybnosti ohľadne nastavenia, potom nastavte hodnotu 90. Toto je základný prehľad prahovej hodnoty skóre:

- **Hodnota 80 – 90** – e-mailové správy, ktoré sú s veľkou pravdepodobnosťou [spam](#), sa budú filtrovať. Niektoré správy, ktoré nie sú spam, sa môžu filtrovať nesprávne.
- **Hodnota 60 – 79** – považuje sa za pomerne agresívne nastavenie. E-mailové správy, ktoré môžu predstavovať [spam](#), sa budú filtrovať. Môžu sa zachytiť aj správy, ktoré nie sú spam.



- **Hodnota 50 – 59** – veľmi agresívne nastavenie. E-mailové správy, ktoré nie sú spam, sa celkom pravdepodobne zachytia ako [spamové](#) správy. Neodporúčame vám používať toto nastavenie na normálne účely.

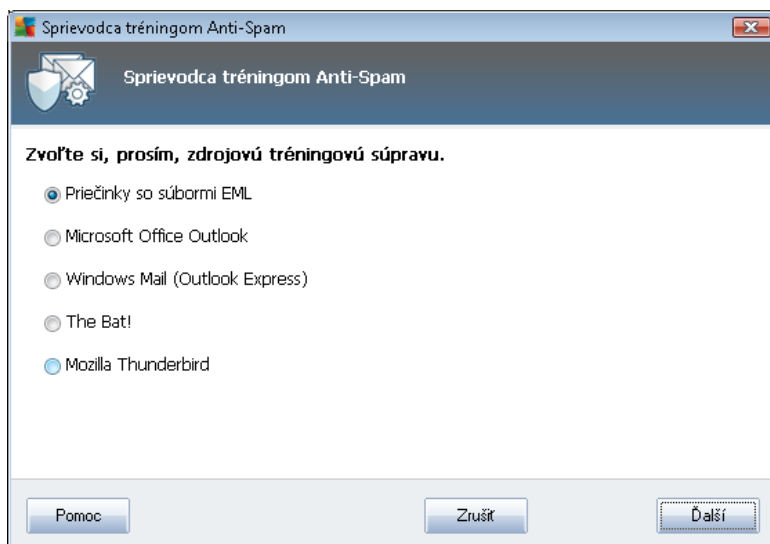
V dialógovom okne **Základné nastavenia súčasti Anti-Spam** môžete ďalej definovať, ako sa bude zaobchádzať s detegovaným [spamom](#):

- **Premiestniť správu do priechinka pre spam** – začiarknite toto okienko, ak sa má každý detegovaný spam automaticky premiestniť do konkrétneho priechinka pre spam v poštovej aplikácii.
- **Pridať príjemcov poslaných e-mailov do [zoznamu povolených](#)** – začiarknite toto okienko, ak sa majú všetci príjemcovia poslaných e-mailov považovať za dôveryhodných, a aby bolo možné doručovať všetky e-mailové správy prichádzajúce z ich e-mailových schránok.
- **Zmeniť predmet správ označených ako SPAM** – začiarknite toto okienko, ak sa majú všetky správy označené ako [spam](#) označiť špecifickým slovom alebo znakom v riadku s predmetom e-mailu; požadovaný text sa vkladá do zapnutého textového poľa.
- **Opýtať sa pred hlásením nesprávnej detekcie** – pod podmienkou, že ste počas [procesu inštalácie](#) súhlasili s účasťou v [programe zlepšovania produktov](#). V tom prípade ste povolili hlásenie detegovaných hrozieb do AVG. Hlásenie sa robí automaticky. Keď však začiarknete toto okienko, potom sa vás pred nahlásením detegovaného spamu do AVG program opýta, či sa má správa naozaj klasifikovať ako spam.

Ovládacie tlačidlá

Tlačidlo Trénovať Anti-Spam otvorí [sprievodcu trénovaním súčasti Anti-Spam](#). Informácie o tomto sprievodcovi sa nachádzajú v [ďalšej kapitole](#).

Prvé dialógové okno **Sprievodcu trénovaním Anti-Spamu** vás požiada, aby ste zvolili zdroj emailových správ, ktoré chcete použiť na trénovanie. Obyčajne budete chcieť použiť buď emaily, ktoré boli nesprávne označené ako SPAM alebo spamové správy, ktoré neboli rozpoznané.



Môžete si zvoliť z nasledujúcich možností:

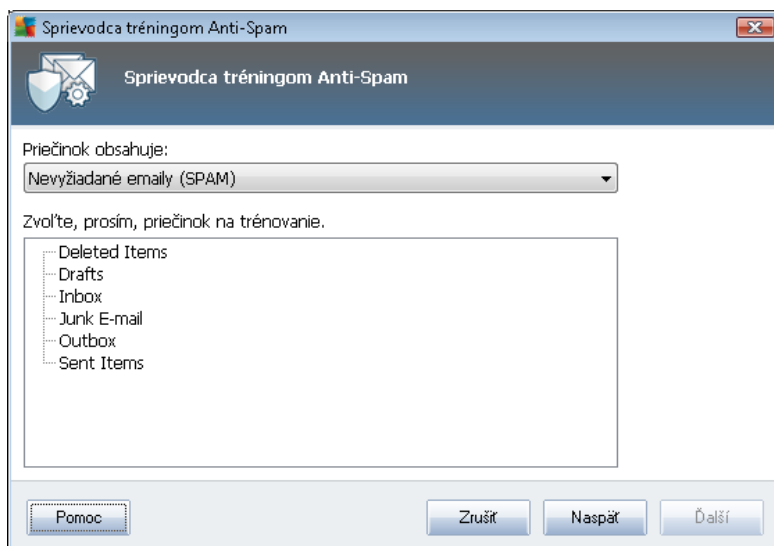
- **Konkrétna poštová aplikácia** – ak používate niektorú z uvedených poštových aplikácií (*MS Outlook, Outlook Express, The Bat!*), stačí, ak vyberiete príslušnú možnosť.
- **Priečinkov so súbormi EML** - ak používate iný e-mailový program, najskôr si uložte správy do samostatného priečinka (*vo formáte eml*), alebo si zapamätajte umiestnenie priečinkov so správami, ktoré používa poštový klient. Potom zvolte **Priečinkov so súbormi EML**, ktorý vám umožní lokalizovať želaný priečinkov v ďalšom kroku

Pre rýchlejší a jednoduchší proces trénovania je dobré triediť emaily v priečinkoch vopred, takže priečinkov, ktorý použijete na trénovanie, bude obsahovať len tréningové správy (či už chcené alebo nechcené). Nie je to však potrebné, keďže budete môcť filtrovať emaily neskôr.

Zvoľte vhodnú možnosť a kliknite na tlačidlo **Ďalej** pre pokračovanie sprievodcu.

Dialógové okno, ktoré sa otvorí v tomto kroku, závisí od výberu, ktorý ste urobili v predchádzajúcom kroku.

Priečinky so súbormi EML



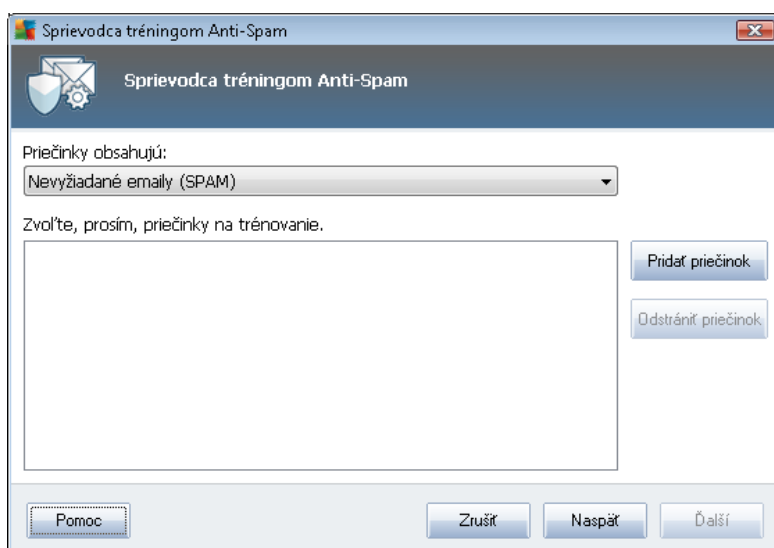
V tomto dialógovom okne vyberte priečinok so správami, ktorý chcete použiť na tréningovanie. Stlačením tlačidla **Pridať priečinok** vyhľadajte priečinok so súbormi .eml (uloženými e-mailovými správami). Vybraný priečinok sa potom zobrazí v dialógovom okne.

V rozbaľovacej ponuke **Priečinky obsahujú** nastavte jednu z dvoch možností – či sa vo vybranom priečinku nachádzajú želané správy (HAM) alebo nevyžiadané správy (SPAM). V ďalšom kroku budete môcť správy filtrovať, takže priečinok nemusí obsahovať len tréningové e-maily. Kliknutím na tlačidlo **Odstrániť priečinok** zároveň môžete odstrániť neželané vybrané priečinky zo zoznamu.

Nakoniec kliknutím na tlačidlo **Ďalšie** prejdite na [možnosti filtrovania správ](#).

Výber poštovej aplikácie

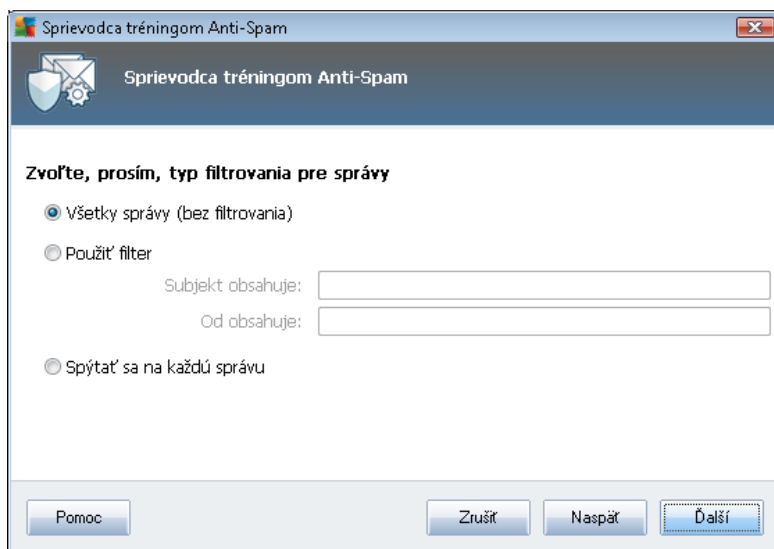
Po potvrdení jednej z možností sa otvorí nové dialógové okno.



Poznámka: Ak používate program Microsoft Office Outlook, program vás požiada, aby ste vybrali najskôr profil MS Office Outlook.

V rozbaľovacej ponuke **Priečinky obsahujú** nastavte jednu z dvoch možností – či sa vo vybranom priečinku nachádzajú želané správy (**HAM**) alebo nevyžiadané správy (**SPAM**). V ďalšom kroku budete môcť správy filtrovať, takže priečinok nemusí obsahovať len tréningové e-maily. Navigačná štruktúra vybranej poštovej aplikácie je už zobrazená v hlavnej časti dialógového okna. Vyhľadajte želaný priečinok v navigačnej štruktúre a zvýraznite ho myšou.

Nakoniec kliknutím na tlačidlo **Ďalšie** prejdite na [možnosti filtrovania správ](#).



Toto dialógové okno sa používa na nastavenie filtrovania e-mailových správ.

Ak ste presvedčení, že zvolený priečinok obsahuje len správy, ktoré chcete použiť na účely školenia, zvoľte možnosť **Všetky správy (bez filtrovania)**.

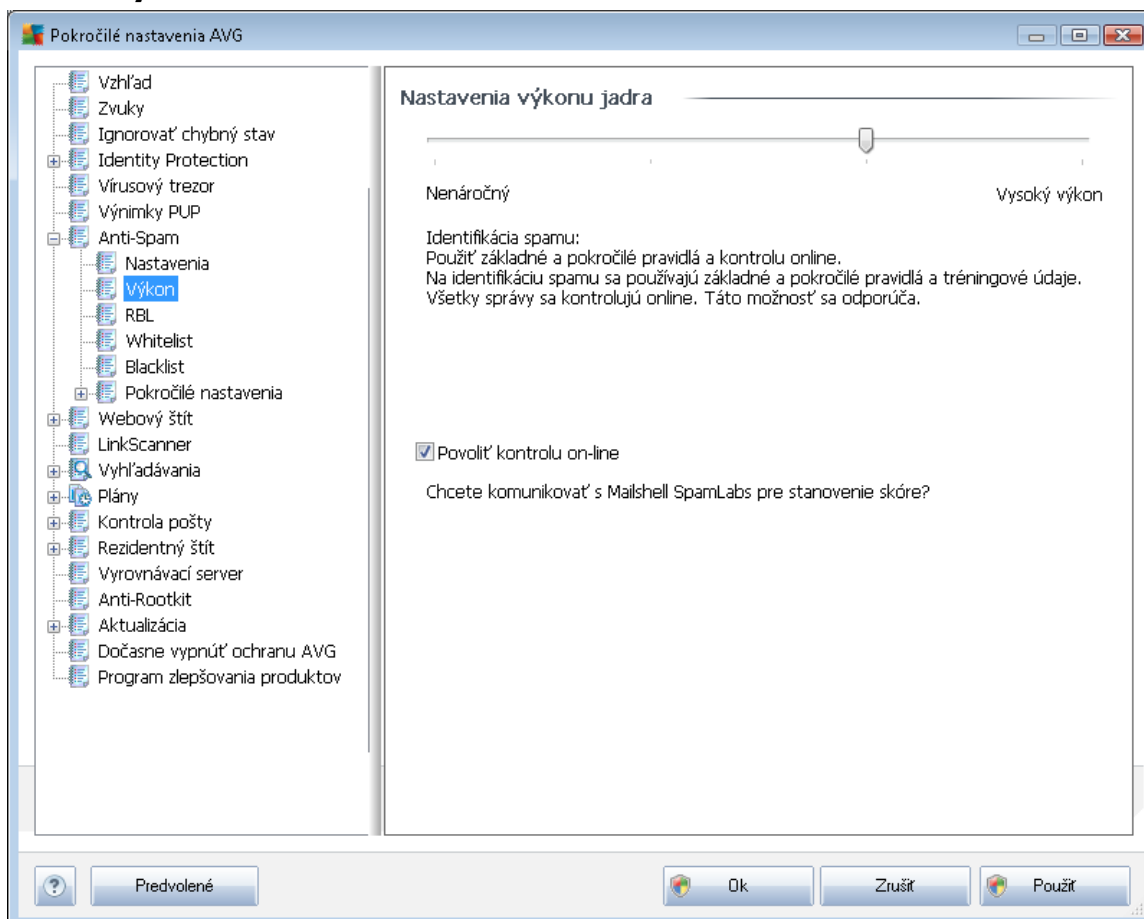
Ak si nie ste istý správami v priečinku a chcete, aby sa vás sprievodca spýtal na každú správu (tak, aby ste mohli určiť, či sa má použiť na tréning alebo nie), zvoľte možnosť **Spýtať sa na každú správu**.

Pre podrobnejšie filtrovanie zvoľte možnosť **Použiť filter**. Môžete doplniť slovo (názov), časť slova alebo vetu, ktorá sa má vyhľadať v predmete emailu a/alebo v poli odosielateľa. Všetky správy, ktoré presne súhlasia so zadanými kritériami, sa použijú na tréning, bez ďalšieho dotazovania.

Upozornenie! Keď vyplníte obidve textové polia, použijú sa aj adresy, ktoré súhlasia len s jednou z dvoch uvedených podmienok!

Po zvolení príslušnej možnosti kliknite na tlačidlo **Ďalej**. Nasledujúce dialógové okno bude len informatívne, hovorí vám, že sprievodca je pripravený na spracovanie správ. Pre spustenie tréningu znovu kliknite na tlačidlo **Ďalej**. Trénovanie sa potom začne podľa predtým zvolených podmienok.

9.7.2. Výkon



V dialógovom okne **Nastavenia výkonu jadra** (otvára sa pomocou položky **Výkon** v ponuke na ľavej strane) sa nachádzajú nastavenia výkonu súčasti **Anti-Spam**. Posunutím posúvača smerom doľava resp. doprava nastavíte úroveň výkonu procesu kontroly, od režimu **Malé využitie pamäte** po režim **Vysoký výkon**.

- **Malé využitie pamäte** – počas procesu kontroly sa nepoužijú žiadne pravidlá na identifikovanie [spamu](#). Na identifikáciu sa použijú len tréningové údaje. Tento režim vám neodporúčame používať na bežné účely. Používajte ho len vtedy, keď má počítač veľmi slabý hardvér.
- **Vysoký výkon** – v tomto režime sa využíva veľké množstvo pamäte. Počas procesu kontroly na zisťovanie prítomnosti [spamu](#) sa použijú tieto funkcie: pravidlá a vyrovnávacia pamäť databázy [spamu](#), základné a rozšírené pravidlá, adresy IP rozosielateľov spamu a databázy rozosielateľov spamu.

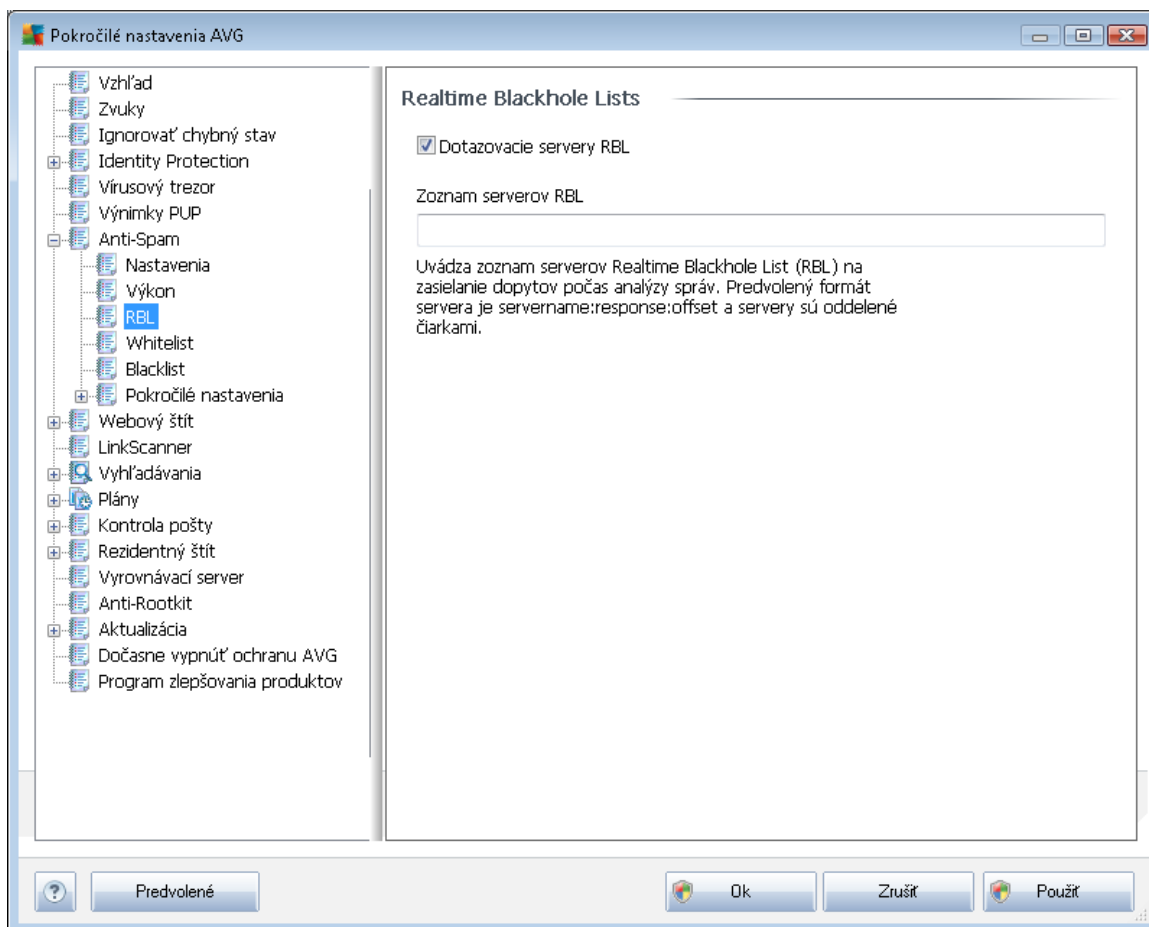
Položka **Zapnúť online kontrolu** je štandardne zapnutá. Používa sa na presnejšie detegovanie [spamu](#) pomocou komunikácie so servermi [Mailshell](#), t. j. kontrolované dáta sa porovnávajú s online databázami [Mailshell](#).

Odporúčame vám, aby ste zachovali predvolené nastavenia a zmenili ich len v prípade, keď

na to máte vážny dôvod. Zmeny konfigurácie odporúčame robiť len skúseným používateľom!

9.7.3. RBL

Položka **RBL** otvorí dialógové okno úprav s názvom **Zoznamy čiernych dier v reálnom čase**:



Toto dialógové okno umožňuje zapnúť/vypnúť funkciu **Pýtať sa na servery RBL**.

RBL (*Realtime Blackhole List*) server je DNS server s obsiahlou databázou známych odosielateľov spamov. Keď je táto funkcia zapnutá, všetky emailové správy sa preveria a porovnajú s databázou serveru RBL, či sú označené ako [spam](#) a či sú identické s niektorou položkou databázy. Databázy serverov RBL obsahujú najnovšie aktuálne hlavičky spamov, aby mohli poskytnúť tú najlepšiu a najpresnejšiu detekciu [spamov](#). Táto funkcia je zvlášť užitočná pre používateľov, ktorí dostávajú veľké množstvo spamov, ktoré normálne zariadenie [Anti-Spam](#) nedetekuje.

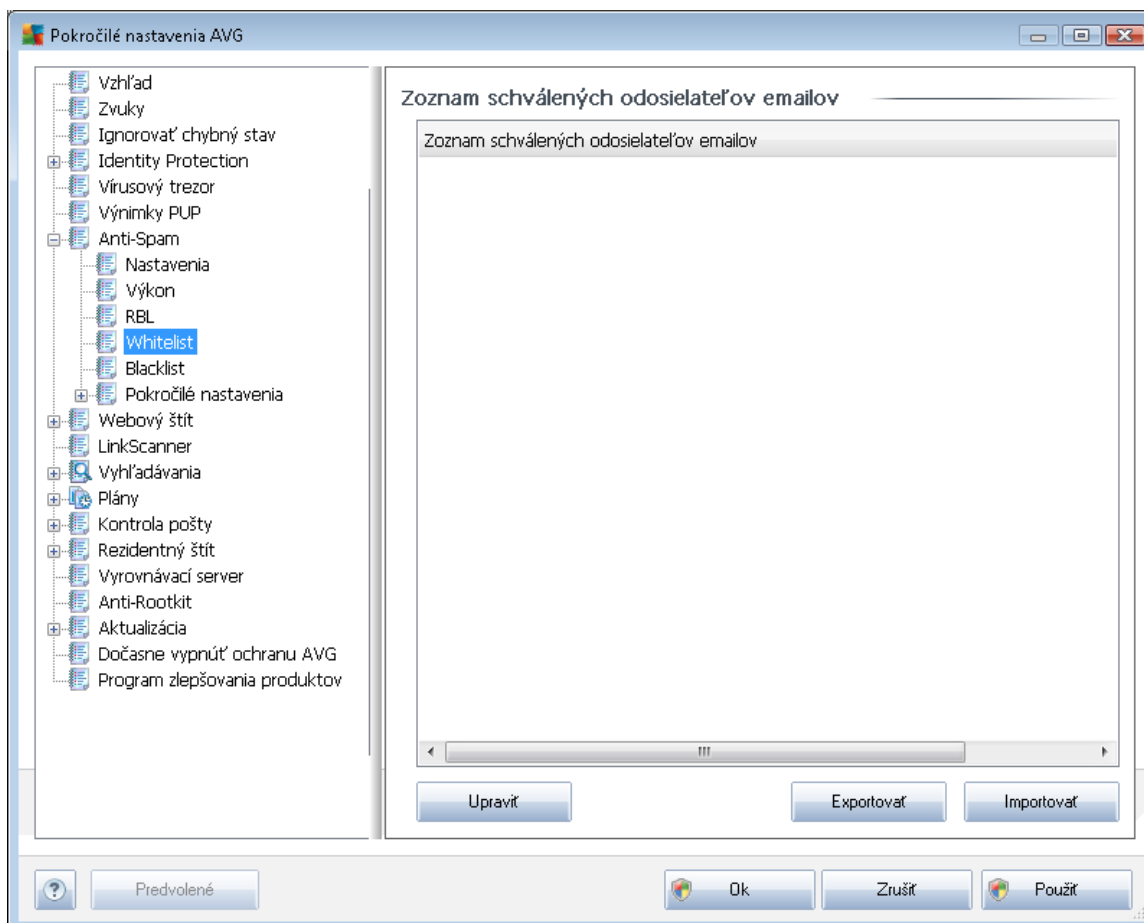
Zoznam serverov RBL vám umožňuje zadať špecifické umiestnenia serverov RBL.

Poznámka: Zapnutím tejto funkcie sa môže spomaliť proces prijímania emailových správ u niektorých systémov a konfigurácií, pretože každá správa sa musí preveriť a porovnať s databázou serveru RBL.

Na server sa neposielajú žiadne osobné údaje!

9.7.4. Zoznam povolených

Položka **Zoznam povolených odosielateľov** otvorí dialógové okno s názvom **Zoznam schválených odosielateľov e-mailov** s globálnym zoznamom povolených e-mailových adries odosielateľov a názvov domén, ktorých správy nebudú nikdy označené ako [spam](#).



V rozhraní úprav môžete zostaviť zoznam odosielateľov, od ktorých nikdy neočakávate nevyžiadané správy ([spam](#)). Zároveň môžete vytvoriť zoznam úplných názvov domén (e.g. *avg.com*), o ktorých viete, že nevytvárajú spamové správy.

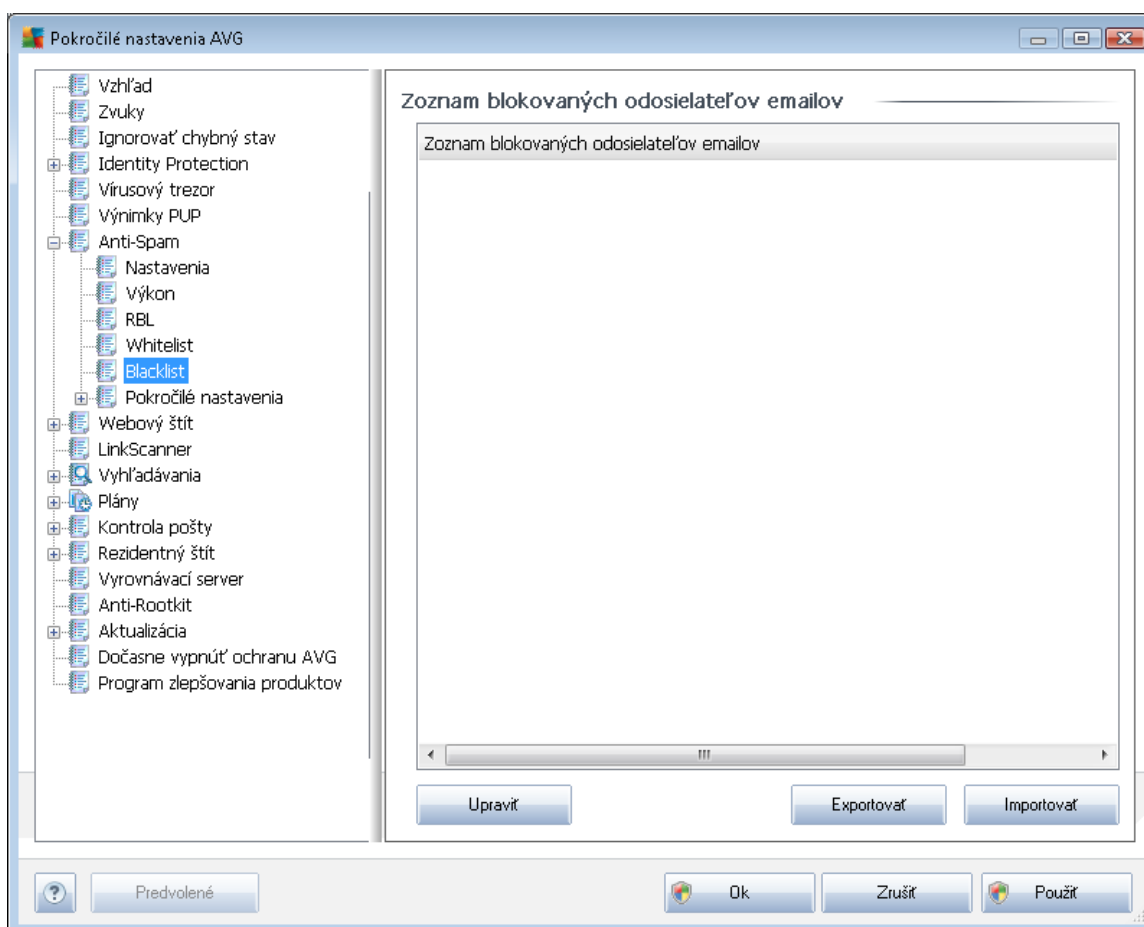
Keď máte zostavený takýto zoznam odosielateľov a/alebo názvov domén, môžete ich zadať niektorou z nasledujúcich metód: priamym zadaním každej emailovej adresy alebo importovaním celého zoznamu adries naraz. Sú dostupné nasledovné ovládacie tlačidlá:

- **Editovať** - po stlačení tohto tlačidla sa otvorí dialógové okno, do ktorého môžete ručne zadať zoznam adries (*môžete použiť aj metódu kopírovať a prilepiť*). Do každého riadka vložte vždy jednu položku (*odosielateľa, názov domény*).
- **Exportovať** - ak sa z nejakého dôvodu rozhodnete exportovať záznamy, môžete tak urobiť stlačením tohto tlačidla. Všetky súbory sa uložia do jednoduchého textového súboru.
- **Importovať** – ak už máte pripravený textový súbor s emailovými adresami / názvami

domén, môžete ho len importovať pomocou tohto tlačidla. Súbor môže obsahovať len jednu položku (*adresu, názov domény*) v každom riadku.

9.7.5. Zoznam blokových

Položka **Blacklist** otvorí dialógové okno s celkovým zoznamom blokových emailových adries odosielateľov a názvov domén, ktorých správy sa vždy označia ako [spam](#).



V rozhraní úprav môžete zostaviť zoznam odosielateľov, od ktorých očakávate nevyžiadané správy ([spam](#)). Zároveň môžete vytvoriť zoznam úplných názvov domén (*napr. spamingovaspolocnost.sk*), od ktorých očakávate, alebo ste dostali spam. Všetky emaily z uvedených adries/domén budú identifikované ako SPAM.

Keď máte zostavený takýto zoznam odosielateľov a/alebo názvov domén, môžete ich zadať niektorou z nasledujúcich metód: priamym zadaním každej emailovej adresy alebo importovaním celého zoznamu adries naraz. Sú dostupné nasledovné ovládacie tlačidlá:

- **Editovať** - po stlačení tohto tlačidla sa otvorí dialógové okno, do ktorého môžete ručne zadať zoznam adries (*môžete použiť aj metódu kopírovať a prilepiť*). Do každého riadka vložte vždy jednu položku (*odosielateľa, názov domény*).
- **Exportovať** - ak sa z nejakého dôvodu rozhodnete exportovať záznamy, môžete tak urobiť



stlačením tohto tlačidla. Všetky súbory sa uložia do jednoduchého textového súboru.

- **Importovať** – ak už máte pripravený textový súbor s emailovými adresami / názvami domén, môžete ho len importovať pomocou tohto tlačidla.

9.7.6. Rozšírené nastavenia

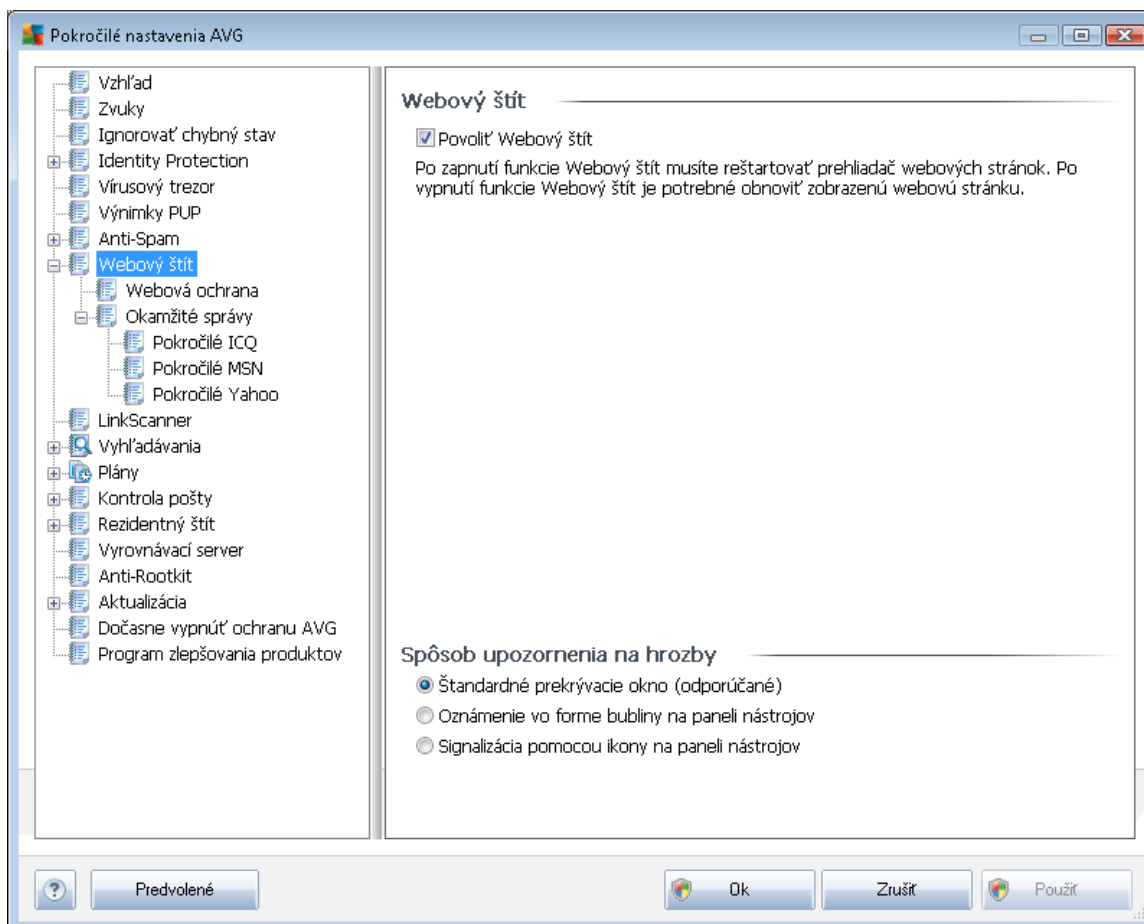
Vo vetve Rozšírené nastavenia sa nachádzajú široké možnosti nastavenia súčasti Anti-Spam. Tieto nastavenia sú určené pre skúsených používateľov, zvyčajne správcov siete, ktorí potrebujú veľmi podrobne nastaviť konfiguráciu antispamovej ochrany na dosiahnutie najlepšej možnej ochrany poštových serverov. Z tohto dôvodu nie je dostupná žiadna ďalšia pomoc pre jednotlivé dialógové okná, ale v používateľskom rozhraní sa nachádza stručný opis každej príslušnej možnosti.

Dôrazne vám odporúčame, aby ste nemenili žiadne nastavenia, ak nie ste dokonale oboznámený s rozšírenými nastaveniami programu Spamcatcher (MailShell Inc.). Každá nevhodná zmena môže mať za následok zníženie výkonu alebo nesprávne fungovanie aplikácie.

Ak sa aj napriek tomu rozhodnete zmeniť konfiguráciu súčasti [Anti-Spam](#) na veľmi podrobnej úrovni, postupujte podľa pokynov uvedených priamo v používateľskom rozhraní. V každom dialógovom okne sa bežne nachádza jedna konkrétna funkcia, ktorú môžete upraviť – jej opis sa vždy nachádza v samotnom dialógovom okne:

- **Vyrovňavacia pamäť** – odtlačok, názov domény, LegitRepute.
- **Trénovanie** – maximálny počet slov, prahová hodnota automatického tréningu, váhy.
- **Filtrovanie** – zoznam jazykov, zoznam krajín, povolené adresy IP, blokované adresy IP, blokované krajiny, blokované súbory znakov, nežiaduci odosielatelia.
- **RBL** – servery RBL, viacnásobné detegovanie, prahová hodnota, časový limit, maximálny počet adries IP.
- **Internetové pripojenie** – časový limit, server proxy, autentifikácia servera proxy.

9.8. Webový štít



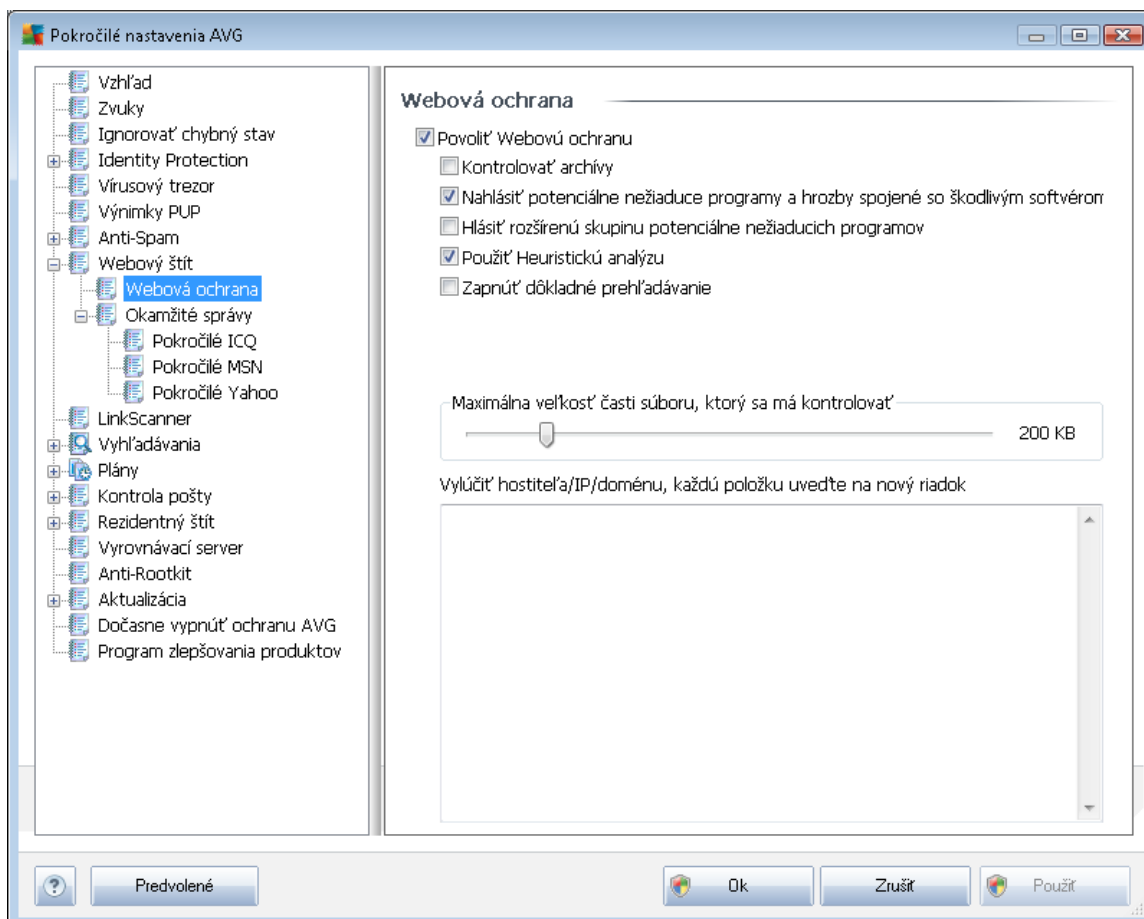
Dialógové okno **Webový štít** umožňuje zapnúť a vypnúť celú súčasť **Webový štít** pomocou možnosti **Zapnúť Webový štít** (štandardne zapnuté). Ak chcete prispôsobiť ďalšie rozšírené nastavenia tejto súčasti, prejdite na ďalšie dialógové okná uvedené v stromovej štruktúre:

- [Webová ochrana](#)
- [Okamžité správy](#)

Spôsob upozornenia na hrozby

V spodnej časti dialógového okna nastavte, akým spôsobom vás má program informovať o potenciálnej detegovanej hrozbe: pomocou štandardného prekryvacieho okna, oznámenia v bubline na paneli úloh alebo informačnej ikony na paneli úloh.

9.8.1. Webová ochrana



Dialógové okno **Webová ochrana** umožňuje editovať konfiguráciu súčasti z hľadiska prehľadávania obsahu internetových stránok. Rozhranie editácie umožňuje nastaviť tieto základné možnosti:

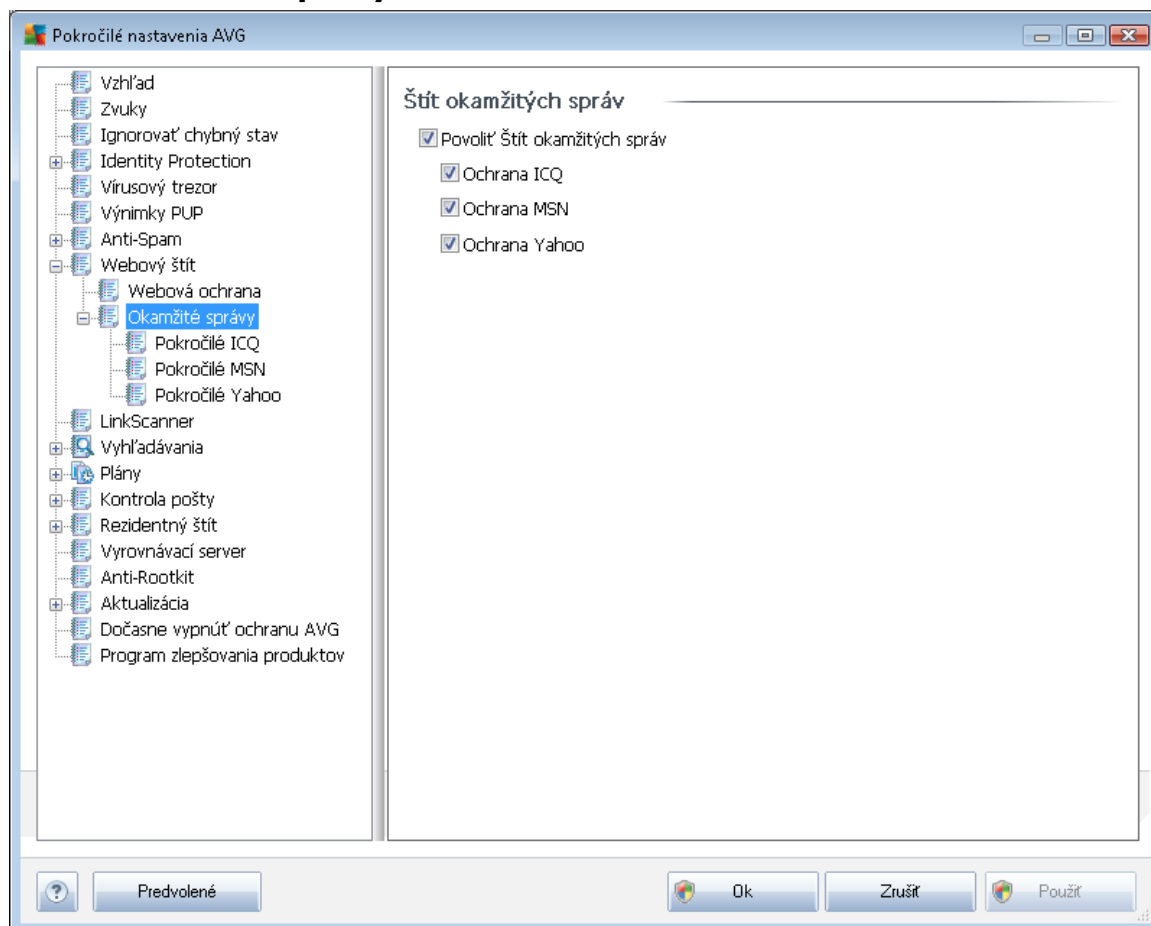
- **Zapnúť webovú ochranu** – keď je táto funkcia zapnutá, potom bude súčasť [Webový štít](#) prehľadávať obsah internetových stránok. Keď je táto možnosť zapnutá (štandardne), môžete ďalej zapnúť alebo vypnúť tieto položky:
 - o **Kontrolovať archívy** – (štandardne vypnuté): prehľadávať obsah archívov, ktoré sa môžu nachádzať na otvorenej internetovej stránke.
 - o **Hlásiť potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté) – začiarňte túto možnosť, ak chcete zapnúť súčasť [Anti-Spyware](#) a vyhľadávať spyware a vírusy. [Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne.](#) Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
 - o **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** – (štandardne vypnuté): začiarňte toto okienko, ak sa má detegovať rozšírená skupina [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu,



ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovat' dobré programy, a preto je táto funkcia štandardne vypnutá.

- o **Používať heuristickú analýzu** (štandardne zapnuté): prehľadať obsah zobrazenej stránky pomocou metódy [heuristickej analýzy](#) (dynamickej emulácie inštrukcií prehľadávaného objektu vo virtuálnom počítačovom prostredí).
- o **Zapnúť dôkladné prehľadávanie** (štandardne vypnuté) – v určitých situáciách (napr. pri podozrení na infikovanie počítača) môžete začiarknutím tohto okienka zapnúť algoritmus najdôkladnejšieho prehľadávania, ktorý prehľadá aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.
- o **Maximálna čiastková veľkosť prehľadávaného súboru** – ak sa priložené súbory nachádzajú na otvorenej stránke, potom sa ich obsah môže zároveň skontrolovať ešte predtým, než sa súbory prevezmú do počítača. Prehľadávanie veľkých súborov však chvíľu trvá a preberanie z internetovej stránky sa môže výrazne spomaliť. Pomocou posúvača môžete nastaviť maximálnu veľkosť súboru, ktorá sa má prehľadať súčasťou [Webový štít](#). Aj keď je prevzatý súbor väčší než nastavená hodnota, a z tohto dôvodu ho súčasť Webový štít neprehľadá, je váš počítač stále chránený: ak je súbor infikovaný, súčasť [Rezidentný štít](#) ho ihneď deteguje.
- o **Vylúčiť hostiteľa/adresu IP/doménu** – do textového poľa zadajte presný názov servera (hostiteľa, adresu IP, adresu IP s maskou alebo adresu URL) alebo doménu, ktorú nemá súčasť [Webový štít](#) prehľadávať. Preto vylúčte len hostiteľa, o ktorom ste absolútne presvedčený, že by nikdy neposlal nebezpečné dáta.

9.8.2. Okamžité správy

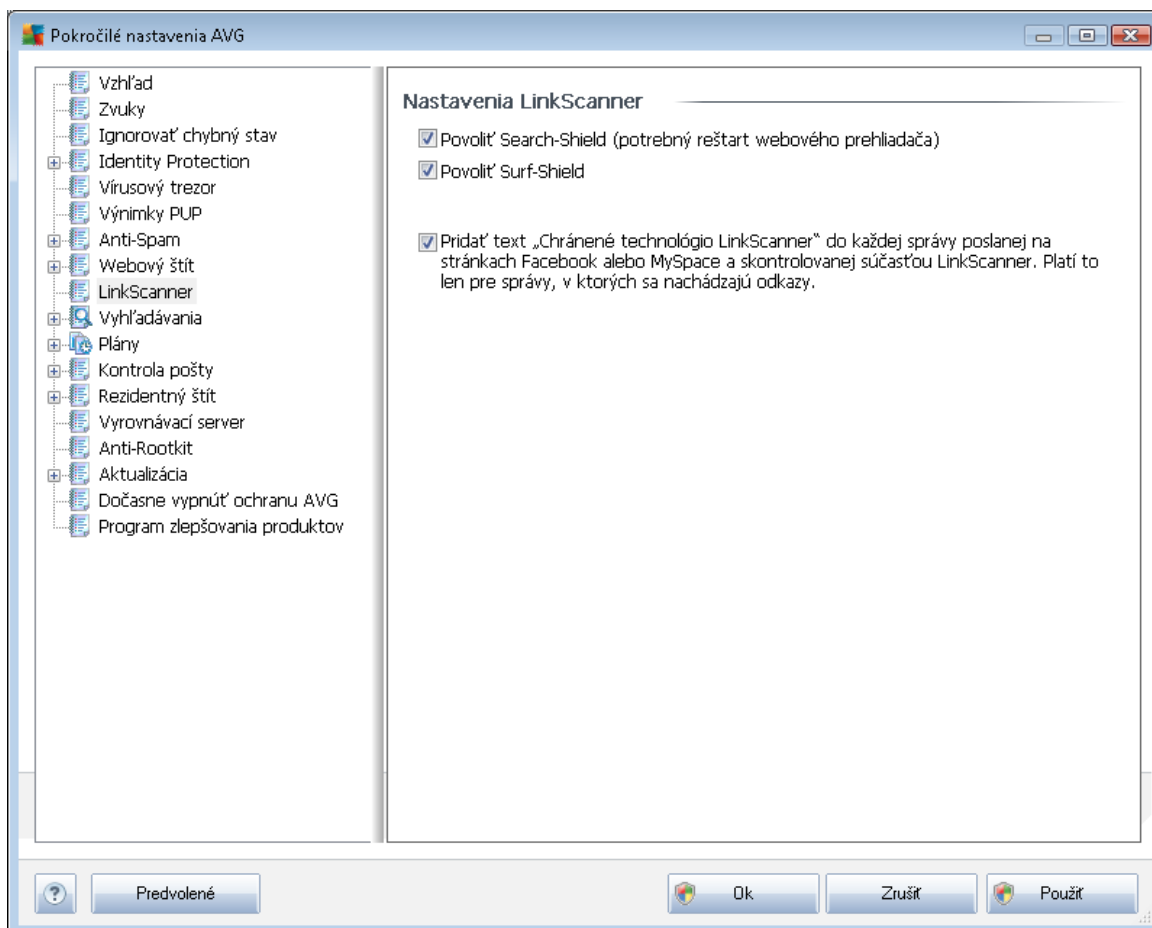


Dialógové okno **Štít okamžitých správ** umožňuje editovať nastavenia súčasti **Webový štít**, ktoré súvisia s prehľadávaním okamžitých správ. Aplikácia v súčasnosti podporuje nasledujúce tri programy pre okamžité správy: **ICQ**, **MSN** a **Yahoo** – označte príslušnú položku pre každý z týchto programov, ak chcete, aby súčasť **Webový štít** kontrolovala, či online komunikácia neobsahuje vírusy.

Ak chcete ďalej definovať povolených/blokovaných používateľov, otvorte príslušné dialógové okno (**Rozšírené ICQ**, **Rozšírené MSN**, **Pokročilé Yahoo**) a upravte jeho nastavenia a definujte **zoznam povolených používateľov** (zoznam používateľov, ktorí s vami budú môcť komunikovať) a **zoznam blokovaných používateľov** (používateľov, ktorí budú blokovaní).

9.9. LinkScanner

Dialógové okno **Nastavenia súčasti LinkScanner** umožňuje zapnúť a vypnúť základné funkcie súčasti **LinkScanner**:



- **Zapnúť Search-Shield** (štandardne zapnuté): informačné ikony s odporúčaniami pre výsledky vyhľadávania vo vyhľadávačoch Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg a SlashDot a vopred skontrolované.
- **Zapnúť Surf-Shield** (štandardne zapnuté) – používa sa na zapnutie ochrany (v reálnom čase) pred internetovými stránkami s nebezpečným obsahom pri ich otvorení. Pripojenie k známym škodlivým stránkam a ich nebezpečnému obsahu sa zablokuje pri otváraní v internetovom prehliadači (alebo inej aplikácii, ktorá používa protokol HTTP).
- **Pridať text „Chránené technológie AVG LinkScanner“** – začiarknutím tohto okienka potvrdíte, že si želáte pridať certifikáciu súčasti **LinkScanner** do všetkých správ s činnými hypertextovými odkazmi, ktoré boli poslané zo sociálnych sietí Facebook a MySpace.

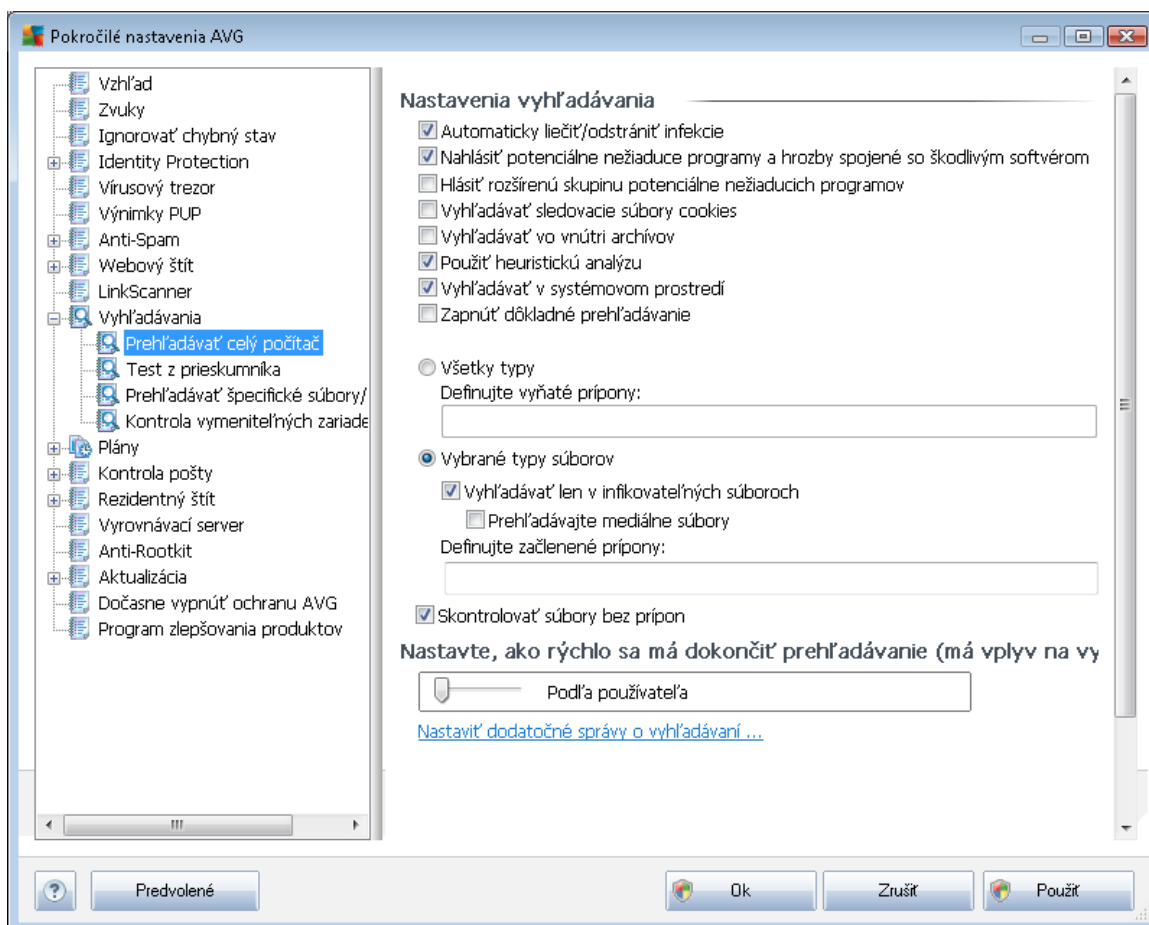
9.10. Kontroly

Rozšírené nastavenia prehľadávania sú rozdelené na štyri kategórie podľa konkrétnych typov prehľadávania definovaných dodávateľom softvéru:

- [Prehľadávanie celého počítača](#) – štandardné preddefinované prehľadávanie celého počítača.
- [Prehľadávanie programom na správu súborov](#) – špeciálne prehľadávanie vybraného objektu priamo v prostredí programu Prieskumník.
- [Prehľadávať konkrétne súbory alebo priečinky](#) – štandardné preddefinované prehľadávanie vybraných oblastí počítača.
- [Prehľadávanie vymeniteľných zariadení](#) – špeciálne prehľadávanie vymeniteľných zariadení pripojených k počítaču.

9.10.1. Kontrola celého počítača

Funkcia **Kontrola celého počítača** umožňuje editovať parametre jednej z kontrol vopred definovaných výrobcom softvéru – [Kontrola celého počítača](#):



Nastavenia kontroly

V časti **Nastavenia kontroly** sa nachádza zoznam parametrov kontroly, ktoré sa dajú voliteľne zapnúť resp. vypnúť:

- **Automaticky liečiť/odstrániť infekciu** (štandardne zapnuté) – ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Hlásiť potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté) – začiarknite toto okienko, ak chcete zapnúť súčasť [Anti-Spyware](#) a kontrolovať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – začiarknite toto okienko, ak sa má detegovať rozšírená skupina [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovать dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrolovať sledovacie súbory cookies** (štandardne vypnuté) – tento parameter súčasti [Anti-Spyware](#) zapína funkciu na detegovanie súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Kontrolovať vo vnútri archívov** (štandardne vypnuté) – tento parameter určuje, že sa majú počas kontroly overiť všetky súbory uložené vo vnútri archívov, napr. ZIP, RAR...
- **Používať heuristiku** (štandardne zapnuté) – heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jednou z metód, ktoré sa použijú na detegovanie vírusov počas kontroly.
- **Kontrolovať systémové prostredie** (štandardne zapnuté) – počas kontroly sa overujú systémové oblasti počítača.
- **Zapnúť dôkladnú kontrolu** (štandardne vypnuté) – v určitých situáciách (*napr. pri podozrení na infikovanie počítača*) môžete začiarknutím tohto okienka zapnúť algoritmus najdôkladnejšej kontroly, ktorá overí aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.

Ďalej rozhodnite, či chcete kontrolovať:

- **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu čiarkou oddelených (*uložením sa čiarky zmenia na bodkočiarky*) prípon súborov, ktoré sa nemajú kontrolovať.

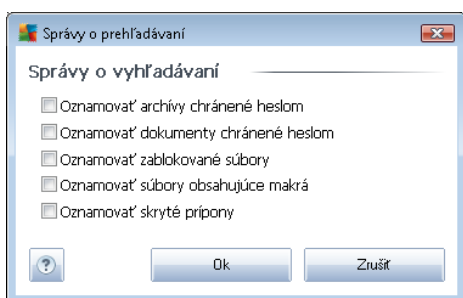
- **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio súborov* – *ak necháte toto okienko nezačiarknuté, potom sa čas kontroly skrúti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete nastaviť (podľa prípony), ktoré súbory sa majú kontrolovať vždy.
- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

Nastaviť rýchlosť dokončenia kontroly

V časti **Nastaviť rýchlosť dokončenia kontroly** môžete ďalej nastaviť požadovanú rýchlosť kontroly v závislosti od využívania počítačových zdrojov. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „*podľa používateľa*“. Ak chcete, aby kontrola prebiehala rýchlejšie, bude trvať kratšie, ale výrazne sa zvýši využitie systémových zdrojov a spomalia sa ostatné činnosti počítača (*táto možnosť sa môže použiť, keď je počítač zapnutý, ale nikto na ňom momentálne nepracuje*). Na druhej strane môžete znížiť využívanie počítačových zdrojov predĺžením doby trvania kontroly.

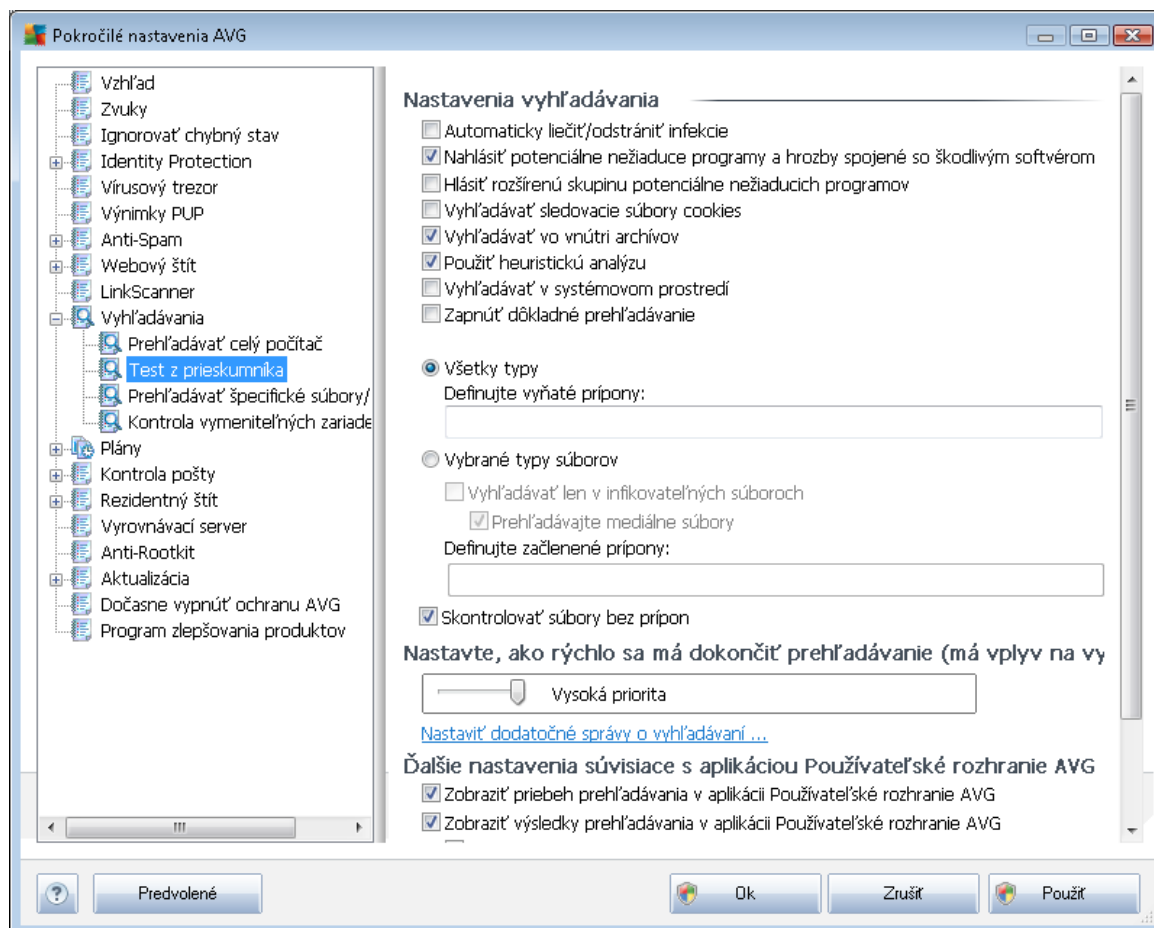
Vytvoriť ďalšie správy o kontrole...

Kliknutím na odkaz **Vytvoriť ďalšie správy o kontrole...** otvorte samostatné dialógové okno s názvom **Správy o kontrole**, v ktorom môžete začiaroknutím konkrétnych položiek definovať, aké nálezy sa majú hlásiť:



9.10.2. Kontrola zo správcu súborov

Rovnako ako predchádzajúca funkcia [Prehľadávanie celého počítača](#), aj táto funkcia s názvom **Prehľadávanie v programe na správu súborov** ponúka niekoľko možností na editovanie prehľadávania preddefinovaného dodávateľom softvéru. V tomto prípade súvisí konfigurácia s [prehľadávaním konkrétnych objektov spustených v prostredí programu Prieskumník](#) (*shell extension*), pozri kapitolu [Prehľadávanie v programe Prieskumník](#):



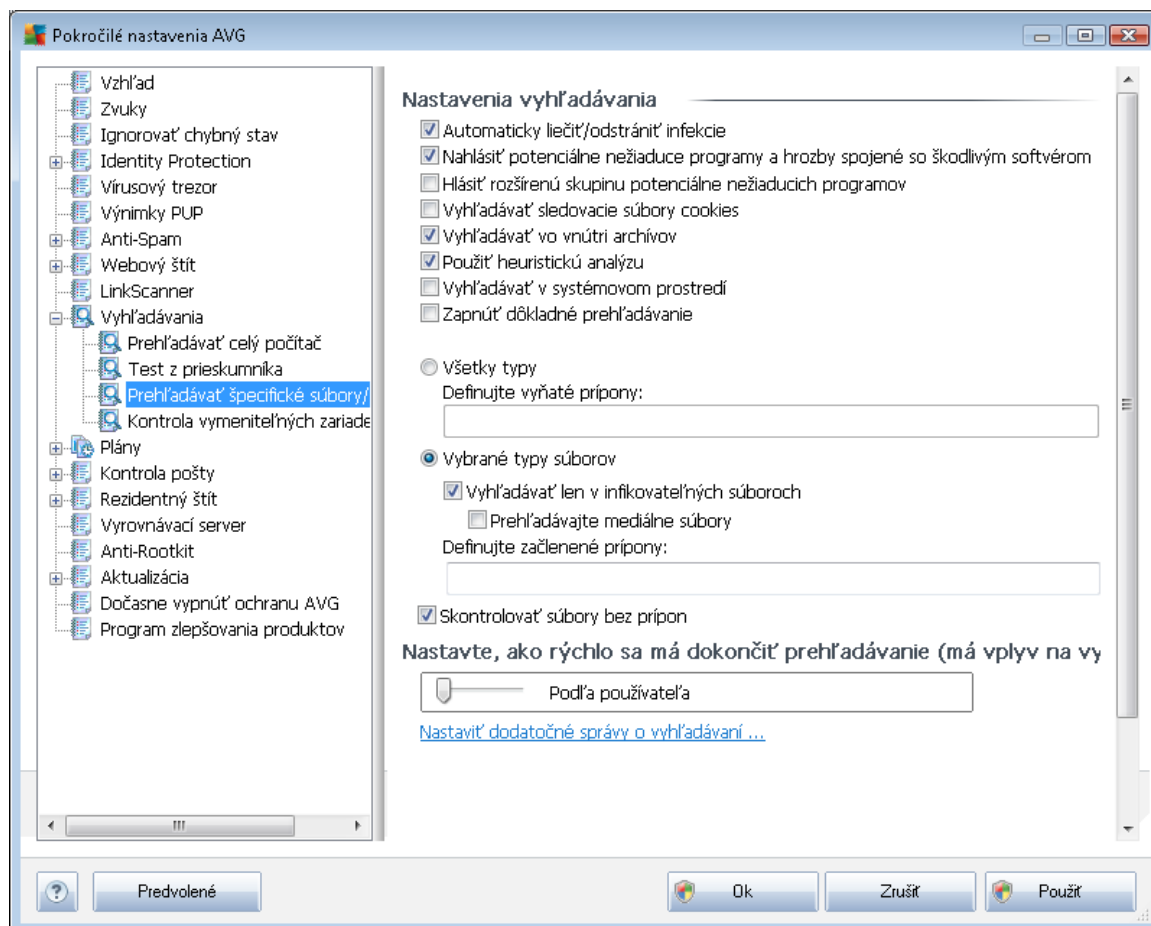
Zoznam parametrov je identický s parametrami použitelnými pre [prehľadavanie celého počítača](#). Predvolené nastavenia sa však líšia (napríklad Prehľadavanie celého počítača štandardne nekontroluje archívy, ale prehľadáva systémové prostredie, zatiaľ čo Prehľadavanie programom na správu súborov má presne opačné nastavenia).

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Prehľadávania/Prehľadavanie celého počítača](#).

V porovnaní s dialógovým oknom [Prehľadavanie celého počítača](#) sa v dialógovom okne **Prehľadavanie v programe na správu súborov** nachádza aj časť s názvom **Ďalšie nastavenia súvisiace s používateľským rozhraním AVG**, ktorá umožňuje nastaviť, či majú byť výsledky prehľadávania a priebeh prehľadávania prístupné v používateľskom rozhraní AVG. Zároveň umožňuje nastaviť, aby sa výsledky prehľadávania zobrazili len v prípade, keď sa počas prehľadávania deteguje infekcia.

9.10.3. Kontrola špecifických súborov alebo priečinkov

Rozhranie editácie na **prehľadavanie konkrétnych súborov alebo priečinkov** je rovnaké ako dialógové okno editácie s názvom [Prehľadávať celý počítač](#). Všetky možnosti konfigurácie sú rovnaké, predvolené nastavenia sú však prísnejšie pri [prehľadávaní celého počítača](#):

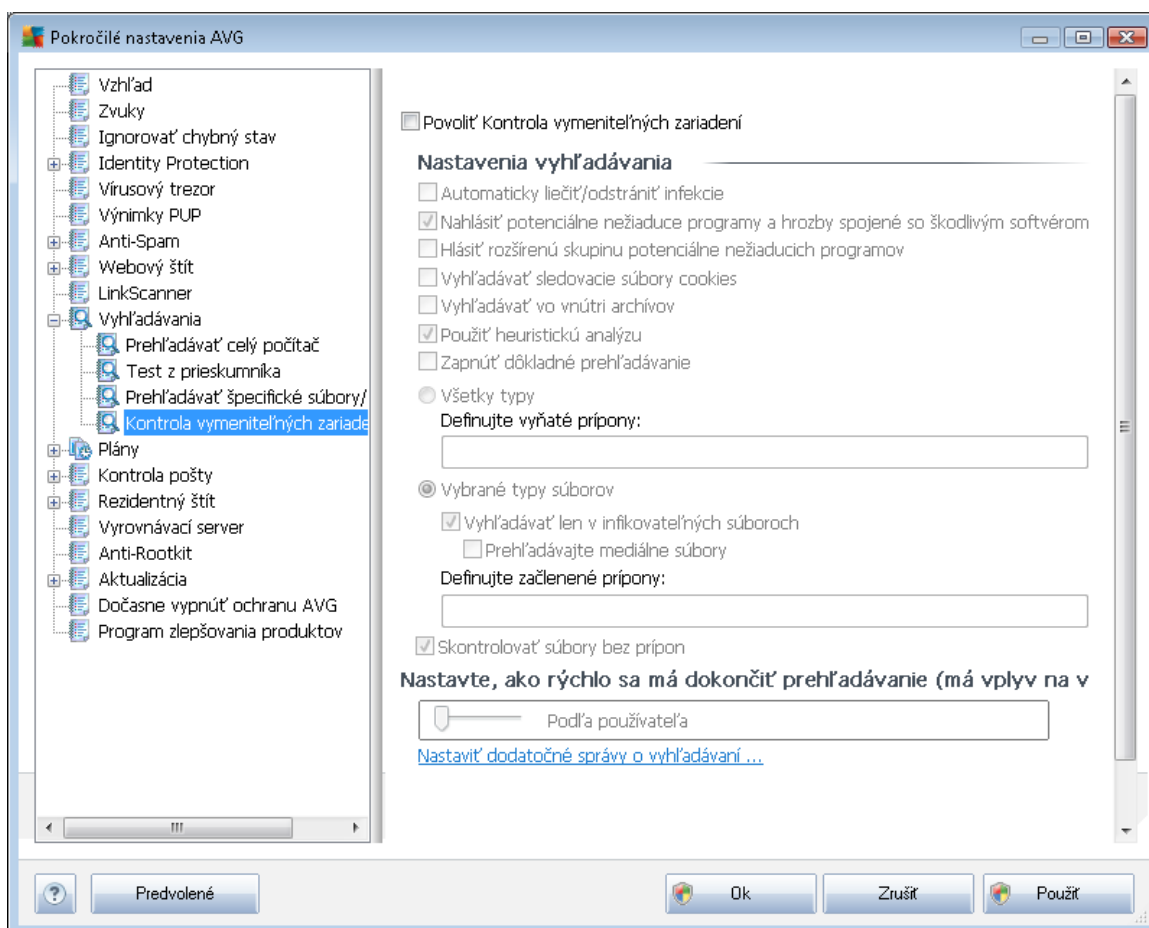


Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vzťahujú len na oblasti vybrané na prehľadávanie v dialógovom okne [Prehľadávať konkrétne súbory alebo priečinky!](#)

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Prehľadávania/Prehľadávať celý počítač.](#)

9.10.4. Kontrola vymeniteľných zariadení

Rozhranie editácie *prehľadávania vymeniteľný zariadení* sa veľmi podobá dialógovému oknu editácie *prehľadávania celého počítača*:



Prehľadanie vymeniteľných zariadení sa spustí automaticky po pripojení vymeniteľného zariadenia k počítaču. Toto prehľadanie je štandardne vypnuté. Prehľadanie vymeniteľných zariadení je však veľmi dôležité z hľadiska potenciálnych hrozieb, pretože tieto predstavujú zdroj infekcie. Ak chcete, aby bolo toto prehľadanie pripravené a spustilo sa automaticky, keď je to potrebné, začiarknite možnosť **Zapnúť prehľadanie vymeniteľných zariadení**.

Poznámka: Informácie o konkrétnych parametroch sa nachádzajú v kapitole [Rozšírené nastavenia AVG/Prehľadania/Prehľadanie celého počítača](#).

9.11. Plány

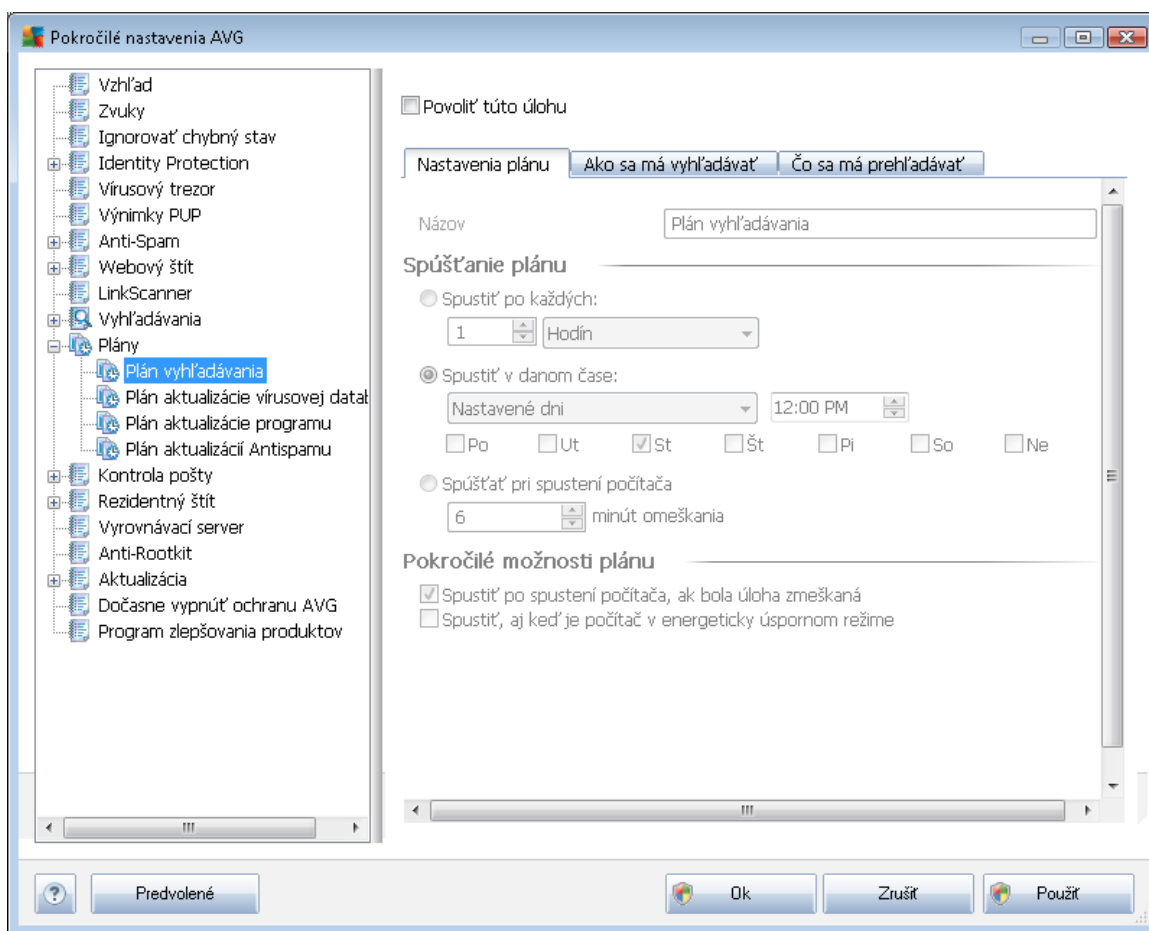
V časti **Plány** môžete upraviť predvolené nastavenia pre:

- [Naplánované prehľadanie](#)
- [Plán aktualizácie vírusovej databázy](#)

- [Plán aktualizácie programu](#)
- [Plán aktualizácie súčasti Anti-Spamu](#)

9.11.1. Plánovaná kontrola

Parametre naplánovanej kontroly je možné editovať (alebo nastaviť novú kontrolu) na troch kartách. Na každej karte najskôr začiarknutím resp. zrušením začiarknutia položky **Povoliť túto úlohu** dočasne vypnete naplánovaný test a znova ho zapnete, keď je potrebný:



Potom v textovom poli s názvom **Názov** (pole je neaktívne pre všetky predvolené plány) sa nachádza názov, ktorý tomuto jedinečnému plánu prideliť dodávateľ programu. Pre novo pridané plány (nový plán sa pridá kliknutím pravým tlačidlom myši nad položkou **Naplánované prehľadávanie** v ľavej navigačnej štruktúre) môžete definovať vlastný názov a v tom prípade bude textové pole editovateľné a budete môcť zmeniť jeho obsah. Pokúste sa použiť stručné, opisné a výstižné názvy pre prehľadávanie, aby sa dali neskôr ľahšie navzájom odlíšiť.

Príklad: Nie je vhodné nazvať prehľadávanie „Nové prehľadávanie“ alebo „Moje vyhľadávanie“, pretože tieto názvy nesúvisia s tým, čo prehľadávanie vlastne kontroluje. Na druhej strane, príkladom dobrého opisného názvu je „Prehľadávanie systémových oblastí“ a pod. Takisto nie je



potrebné zadať do názvu prehľadávania, či ide o prehľadávanie celého počítača alebo prehľadávanie vybraných súborov alebo priečinkov, pretože vaše vlastné prehľadávania budú vždy predstavovať špeciálnu verziu [prehľadávania vybraných súborov alebo priečinkov](#).

Toto dialógové umožňuje ďalej definovať tieto parametre prehľadávania:

Spúšťanie naplánovaných úloh

Tu môžete nastaviť časové intervaly spúšťania novo naplánovaného prehľadávania. Čas spúšťania sa definuje ako opakované spúšťanie prehľadávania po uplynutí určitého času (**Spustiť každých...**), definovaním presného dátumu a času (**Spúšťať v konkrétnom časovom intervale...**), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie prehľadávania (**Činnosť pri spustení počítača**).

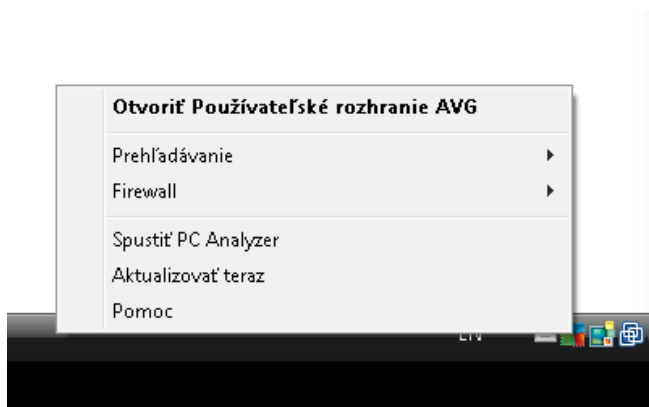
Rozšírené možnosti plánu

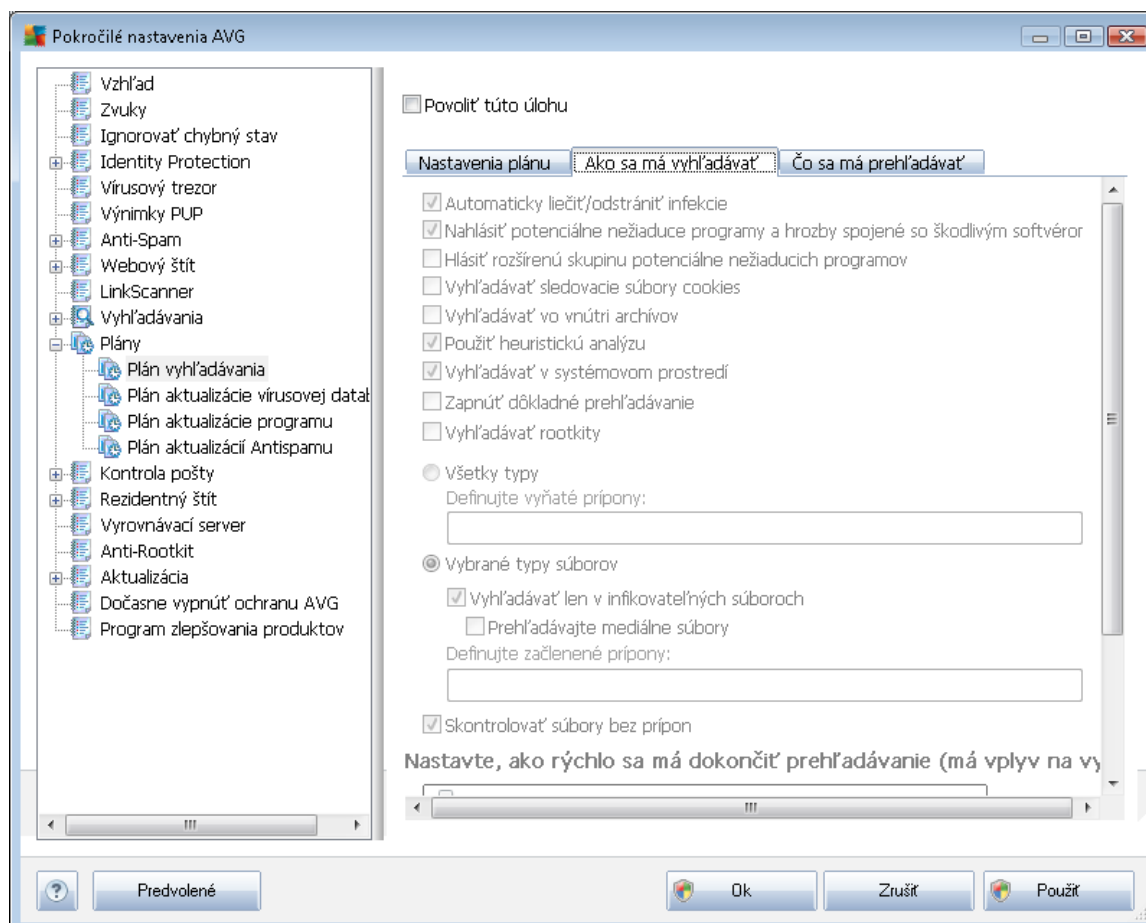
Táto časť sa používa na definovanie podmienok, pri ktorých sa má resp. nemá spustiť prehľadávanie, keď je počítač v úspornom režime alebo úplne vypnutý.

Keď sa spustí naplánované prehľadávanie v nastavenom čase, budete o tejto skutočnosti informovaný pomocou prekryvacieho okna, ktoré sa otvorí nad [ikonou AVG na paneli úloh](#):



Potom sa zobrazí nová [ikona AVG na paneli úloh](#) (farebná s blikajúcim svetlom), ktorá informuje o tom, že prebieha naplánované prehľadávanie. Kliknutím pravým tlačidlom myši na ikone AVG prebiehajúceho prehľadávania otvoríte kontextovú ponuku, ktorá vám umožní pozastaviť alebo dokonca zastaviť prebiehajúce prehľadávania a zároveň zmeniť prioritu práve spusteného prehľadávania:





Na karte **Ako kontrolovať** sa nachádza zoznam parametrov kontroly, ktoré sa dajú zapnúť resp. vypnúť. Štandardne je väčšina parametrov zapnutá a príslušná funkcia sa použije počas kontroly. Ak nemáte vážny dôvod meniť tieto nastavenia, potom vám odporúčame, aby ste zachovali preddefinovanú konfiguráciu:

- **Automaticky liečiť/odstrániť infekcie** (štandardne zapnuté): ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Hlásiť potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté): začiarknite toto okienko, ak chcete zapnúť súčasť [Anti-Spyware](#) a kontrolovať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté): začiarknite toto okienko, ak sa má detegovať rozšírená skupina [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje zabezpečenie

vášho počítača, ale môže blokovať dobré programy, a preto je táto funkcia štandardne vypnutá.

- **Kontrolovať sledovacie súbory cookies** (štandardne vypnuté): Tento parameter súčasti [Anti-Spyware](#) zapína funkciu na detegovanie súborov cookies počas kontroly; (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, akými sú napr. preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Kontrolovať v archívoch** (štandardne vypnuté): tento parameter určuje, že sa majú počas kontroly overovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR...
- **Používať heuristiku** (štandardne zapnuté): heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jedna z metód, ktoré sa použijú na detegovanie vírusov počas kontroly.
- **Kontrolovať systémové prostredie** (štandardne zapnuté): počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnúť dôkladnú kontrolu** (štandardne vypnuté) – v určitých situáciách (*napr. pri podozrení na infikovanie počítača*) môžete začiatkom tohto okienka zapnúť algoritmus najdôkladnejšej kontroly, ktorý kontroluje aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Kontrolovať rootkity** (štandardne vypnuté): začiatkom toto okienko, ak chcete zahrnúť detegovanie rootkitov do kontroly celého počítača. Funkcia na detegovanie rootkitov sa nachádza aj samostatne v súčasti [Anti-Rootkit](#).

Ďalej rozhodnite, či chcete kontrolovať:

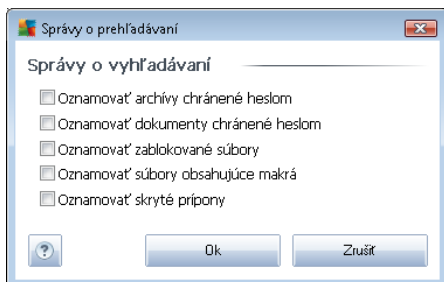
- **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu čiarkou oddelených (*uložením sa čiarky zmenia na bodkočiarky*) prípon súborov, ktoré sa nemajú kontrolovať.
- **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto okienko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete nastaviť (podľa prípony), ktoré súbory sa majú kontrolovať vždy.
- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

Nastaviť rýchlosť dokončenia kontroly

V časti **Nastaviť rýchlosť dokončenia kontroly** môžete ďalej nastaviť požadovanú rýchlosť kontroly v závislosti od využívania počítačových zdrojov. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „podľa používateľa“. Ak chcete, aby kontrola prebiehala rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie počítačových zdrojov a spomalí sa ostatné činnosti v počítači (*táto funkcia sa používa, keď je počítač zapnutý, ale nikto na ňom v danom momente nepracuje*). Na druhej strane môžete znížiť využívanie počítačových zdrojov predĺžením doby trvania kontroly.

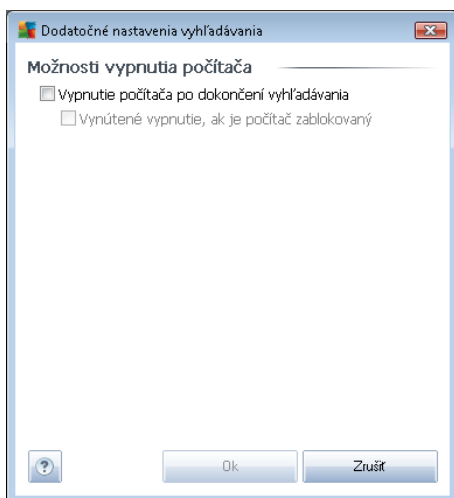
Vytvoriť ďalšie správy o kontrole

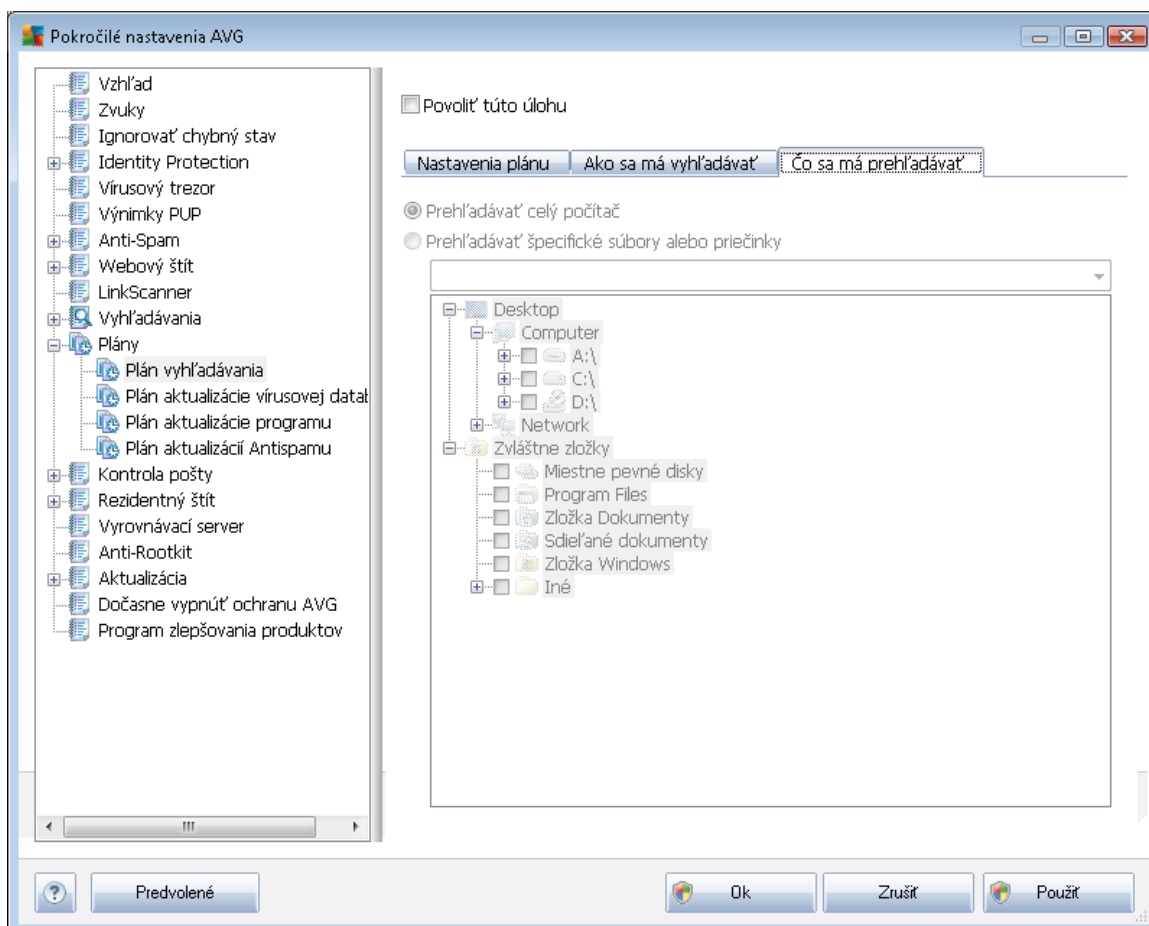
Kliknutím na odkaz **Vytvoriť ďalšie správy o kontrole...** otvorte samostatné dialógové okno s názvom **Správy o kontrole**, v ktorom môžete začiatkom konkrétnych položiek definovať, ktoré nálezy sa majú hlásiť:



Ďalšie nastavenia kontroly

Kliknutím na možnosť **Ďalšie nastavenia kontroly...** otvorte nové dialógové okno **Možnosti vypnutia počítača**, ktoré vám umožní nastaviť, či sa má počítač automaticky vypnúť po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútené vypnutie počítača, keď je zamknutý**).

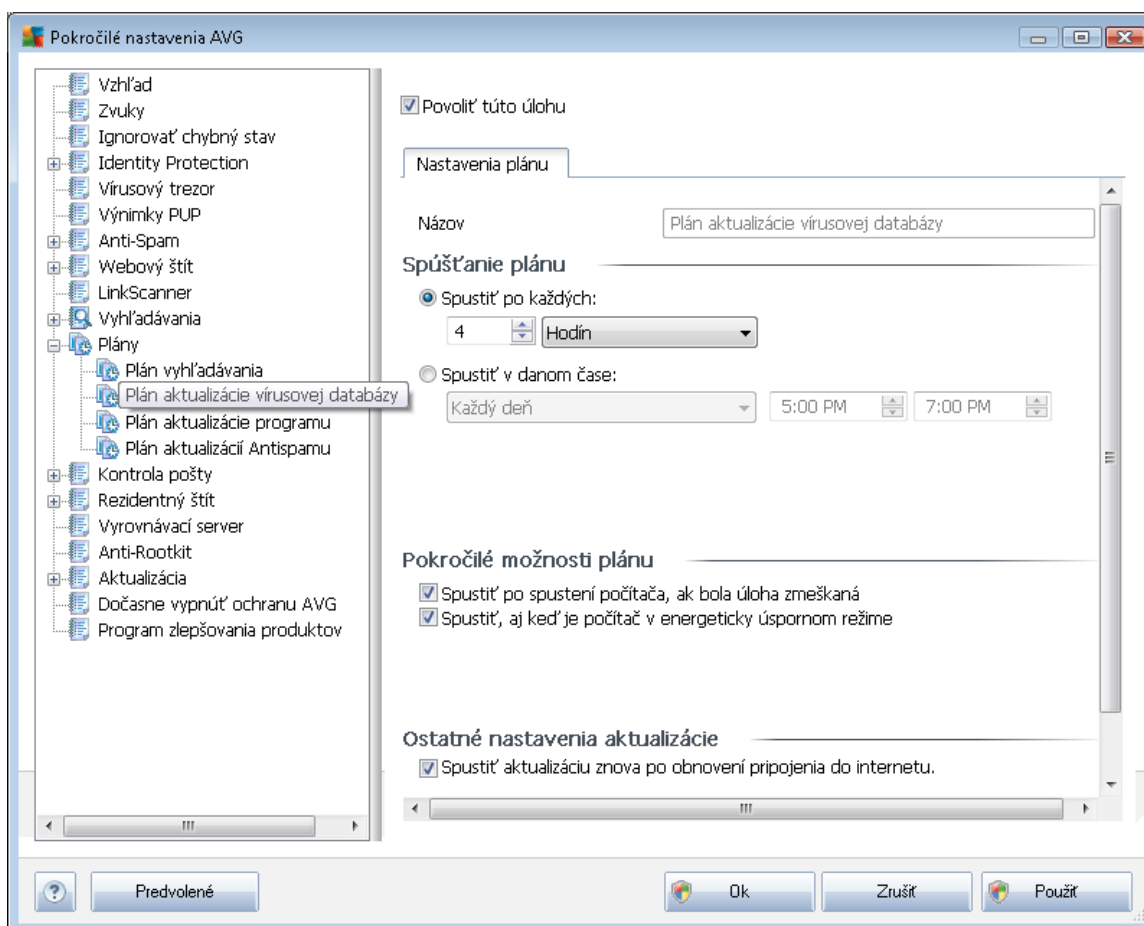




Karta **Čo sa má prehľadávať** umožňuje nastaviť, či chcete naplánovať [prehľadávanie celého počítača](#) alebo [prehľadávanie konkrétnych súborov alebo priečinkov](#). V prípade, že zvolíte prehľadávanie špecifických súborov alebo priečinkov, v spodnej časti tohto dialógového okna sa aktivuje zobrazená stromová štruktúra a môžete uviesť priečinky, ktoré sa majú prehľadávať.

9.11.2. Plán aktualizácie vírusovej databázy

Ak je to **naozaj potrebné**, zrušením začiarknutia okienka **Povolit' túto úlohu** môžete dočasne vypnúť naplánovanú aktualizáciu databázy vírusov a neskôr ju znova zapnúť:



Základný plán aktualizácie databázy vírusov je nastavený v súčasti [Update Manager](#). Toto dialógové okno umožňuje nastaviť niektoré podrobné parametre plánu aktualizácie databázy. V textovom poli **Názov** (pole je neaktívne pre všetky predvolené plány) sa nachádza názov, ktorý tomuto konkrétnemu plánu pridelil výrobca programu.

Spúšťanie naplánovaných úloh

V tejto časti nastavte časové intervaly pre spúšťanie novo naplánovanej aktualizácie databázy vírusov. Časovanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (**Spustiť po každých...**) alebo nastavením presného dátumu a času (**Spúšťať v konkrétnom čase...**).

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, za ktorých sa má/nemá spustiť aktualizácia databázy vírusov, keď je počítač v úspornom režime alebo úplne vypnutý.

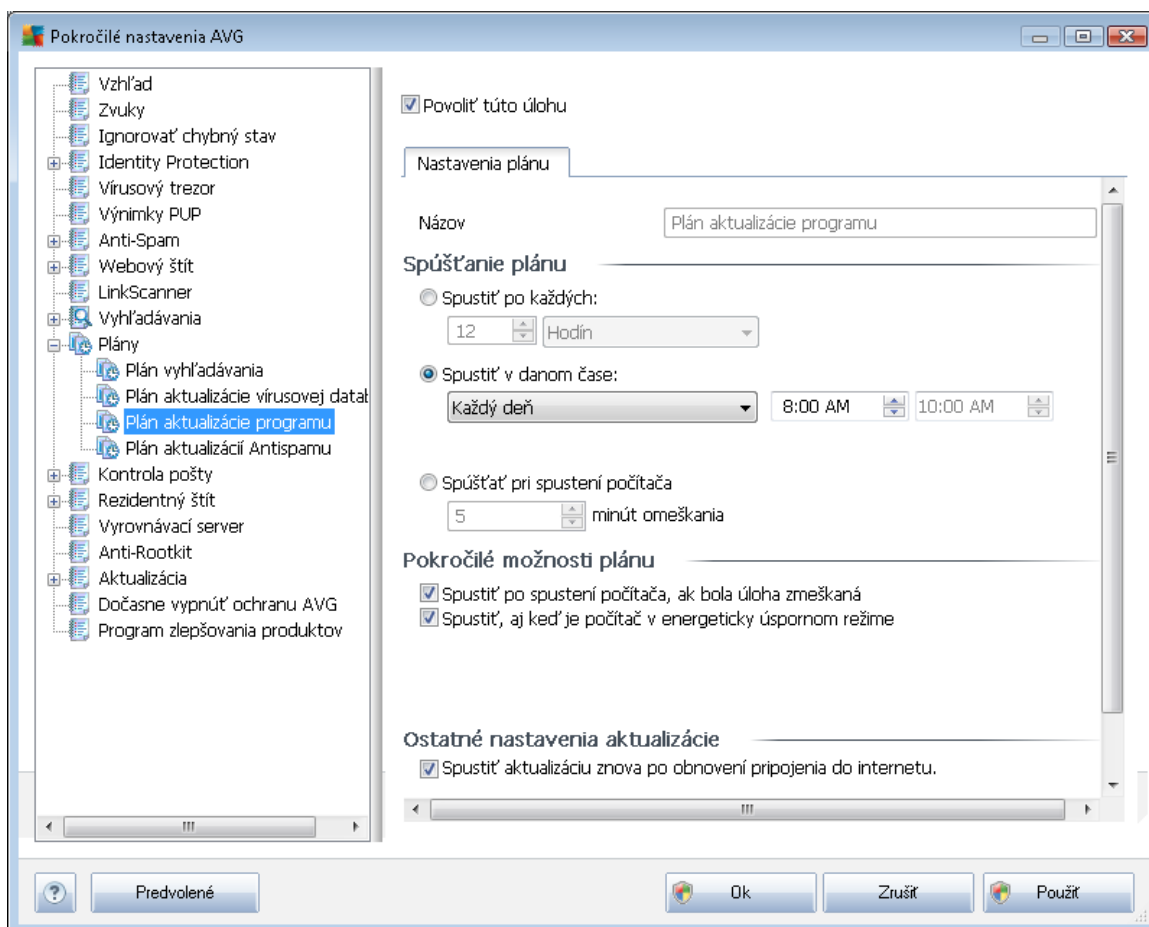
Ďalšie nastavenia aktualizácie

Nakoniec označte možnosť **Spustiť aktualizáciu znova hneď po obnovení internetového pripojenia**, ak sa má v prípade výpadku internetového pripojenia obnoviť proces aktualizácie hneď po jeho obnovení.

Po spustení naplánovanej aktualizácie vo vami nastavenom čase sa zobrazí informácia o tejto skutočnosti v prekryvacom okne nad [ikonou AVG na paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne [Rozšírené nastavenia/Vzhľad](#)).

9.11.3. Plán aktualizácie programu

Ak je to **naozaj potrebné**, zrušením začiarknutia okienka **Povolit túto úlohu** môžete dočasne vypnúť naplánovanú aktualizáciu programu a neskôr ju znova zapnúť:



V textovom poli s názvom **Názov** (pole je neaktívne pre všetky predvolené plány) sa nachádza názov, ktorý tomuto jedinečnému plánu pridelil výrobca programu.



Spúšťanie naplánovaných úloh

Tu zadajte časové intervaly pre spustenie novo naplánovanej aktualizácie programu. Načasovanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (**Spustiť po každých...**), definovaním presného dátumu a času (**Spúšťať v konkrétnom čase...**), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie aktualizácie (**Činnosť pri spustení počítača**).

Rozšírené možnosti plánu

Táto časť sa používa na definovanie podmienok, za akých sa má/nemá spustiť aktualizácia programu, ak je počítač v úspornom režime alebo úplne vypnutý.

Ďalšie nastavenia aktualizácie

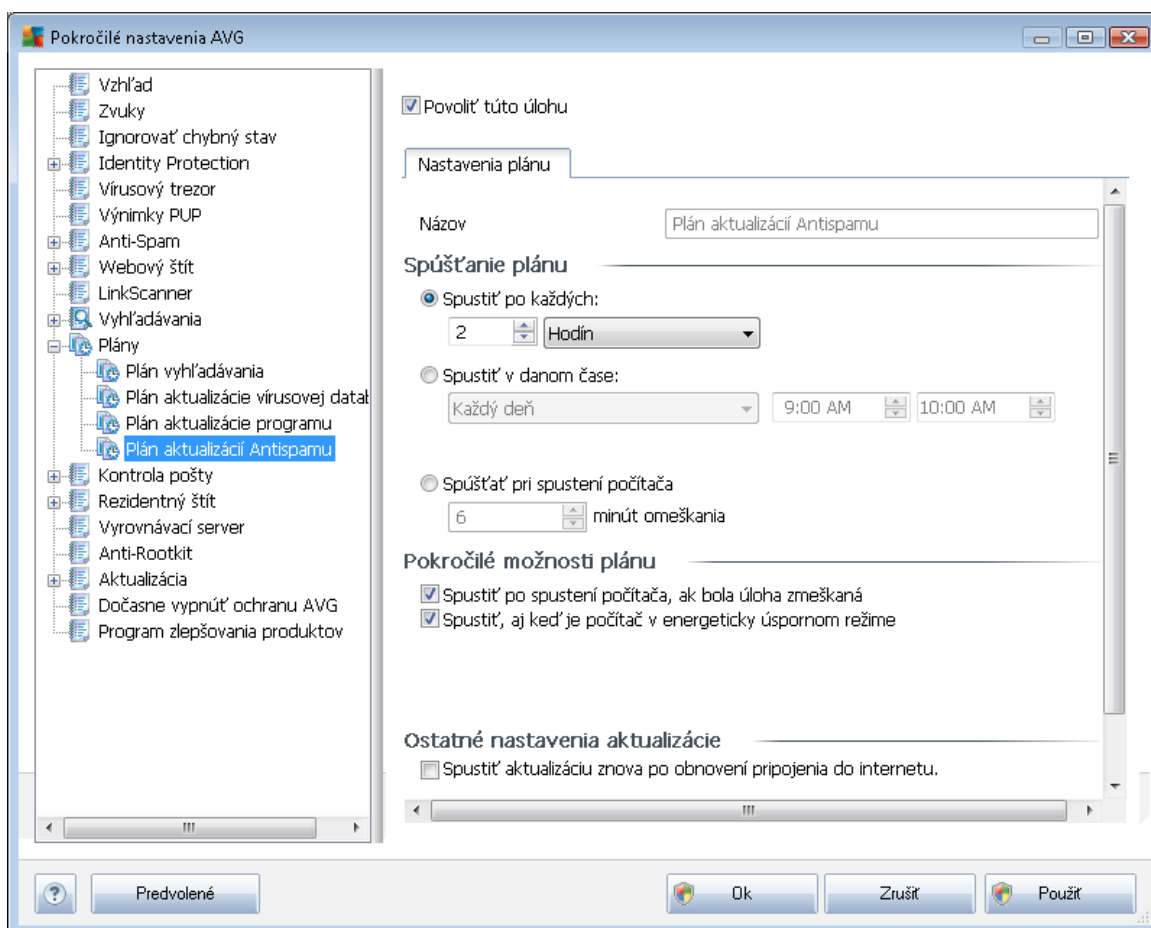
Označte možnosť **Spustiť aktualizáciu znova ihneď po obnovení internetového pripojenia**, ak sa má v prípade výpadku internetového pripojenia obnoviť proces aktualizácie ihneď po jeho obnovení.

Po spustení naplánovanej aktualizácie vo vami nastavenom čase sa zobrazí informácia o tejto skutočnosti v prekrývacom okne nad [ikonou AVG na paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógom okne [Rozšírené nastavenia/Vzhľad](#)).

Poznámka: Ak sa čas naplánovanej aktualizácie programu náhodou prekrýva s naplánovaným prehľadávaním, proces aktualizácie má vyššiu prioritu a prehľadávanie sa preruší.

9.11.4. Plán aktualizácie súčasti Anti-Spam

Ak je to **naozaj potrebné**, zrušením začiarknutia okienka **Povolit' túto úlohu** môžete dočasne vypnúť naplánovanú aktualizáciu súčasti **Anti-Spam** a neskôr ju znova zapnúť:



Základné naplánované aktualizácie súčasti **Anti-Spam** sú nastavené v súčasti **Update Manager**. Toto dialógové okno sa používa na nastavenie niektorých podrobných parametrov plánu aktualizácie. V textovom poli **Názov** (pole je neaktívne pre všetky predvolené plány) sa nachádza názov, ktorý tomuto konkrétnemu plánu prideliť dodávateľ programu.

Spúšťanie naplánovaných úloh

Tu definujete časové intervaly pre novo naplánované spúšťanie aktualizácie súčasti **Anti-Spam**. Načasovanie sa nastavuje buď ako opakované spúšťanie aktualizácie súčasti **Anti-Spam** po uplynutí určitej doby (**Spustiť každých...**), nastavením presného dátumu a času (**Spustiť v konkrétnom čase...**), alebo definovaním udalosti, s ktorou sa bude spájať spustenie aktualizácie (**Akcia pri spustení počítača**).

Rozšírené možnosti plánu



Táto časť sa používa na definovanie podmienok, pri ktorých sa má/nemá spustiť aktualizácia súčasti [Anti-Spam](#), keď je počítač v úspornom režime alebo úplne vypnutý.

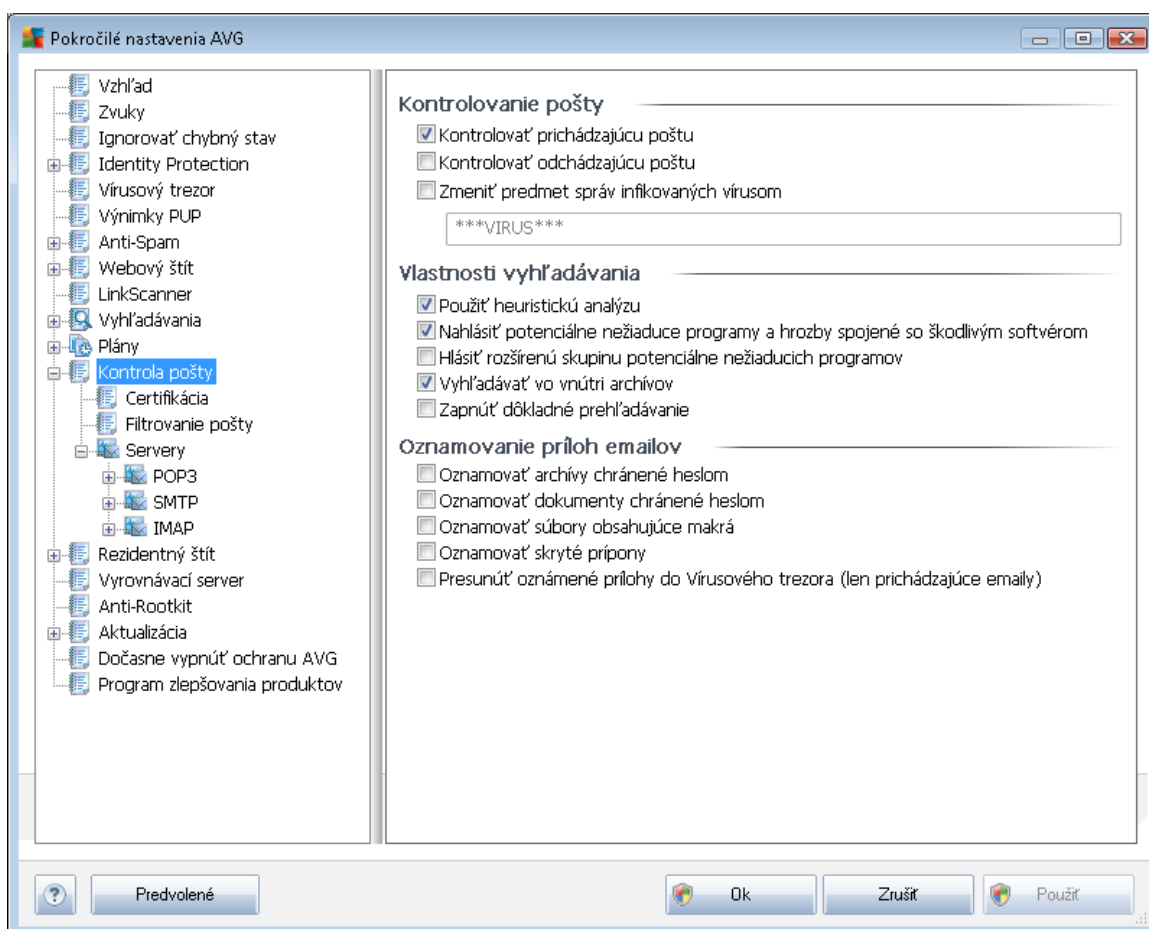
Ďalšie nastavenia aktualizácie

Označte možnosť **Znova spustiť aktualizáciu hneď po obnovení internetového pripojenia**, ak sa má v prípade výpadku internetového pripojenia obnoviť proces aktualizácie súčasti [Anti-Spam](#) hneď po pripojení.

Po spustení naplánovaného prehľadávania vo vami nastavenom čase sa zobrazí informácia o tejto skutočnosti v prekryvacom okne nad [ikonou AVG na paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógovom okne [Rozšírené nastavenia/Vzhľad](#)).

9.12. E-mail Scanner

Dialógové okno **E-mail Scanner** je rozdelené na tri časti:



Kontrola pošty



Táto časť umožňuje definovať tieto základné nastavenia pre prichádzajúce a/alebo odchádzajúce e-mailové správy:

- **Kontrolovať prichádzajúce e-mail** (štandardne zapnuté) – začiarknutím zapnete resp. vypnete funkciu na prehľadávanie všetkých e-mailových správ doručených do vašej poštovej aplikácie.
- **Kontrolovať odchádzajúce e-mail** (štandardne vypnuté) – začiarknutím zapnete resp. vypnete funkciu na prehľadávanie všetkých e-mailov poslaných z vašej poštovej aplikácie.
- **Zmeniť predmet správ infikovaných vírusom** (štandardne vypnuté) – ak chcete byť informovaný o detegovaní infekcie v prehľadanej e-mailovej správe, začiarknite túto položku a do textového poľa zadajte požadovaný text. Tento text sa potom pridá do poľa „Predmet“ každej detegovanej e-mailovej správy na účely jednoduchšej identifikácie a filtrovania. Predvolená hodnota je ***VIRUS*** a odporúčame vám, aby ste ju nemenili.

Vlastnosti prehľadávania

Táto časť sa používa na nastavenie spôsobu, akým sa budú e-mailové správy prehľadávať:

- **Použiť heuristiku** (štandardne zapnuté) – začiarknite túto možnosť, ak chcete používať [metódu heuristického detegovania](#) pri prehľadávaní e-mailových správ. Keď je táto možnosť zapnutá, môžete filtrovať prílohy e-mailov nielen podľa prípony, ale aj podľa samotného obsahu prílohy. Filtrovanie sa nastavuje v dialógovom okne [Filtrovanie pošty](#).
- **Hlásit potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté) – začiarknite toto okienko, ak chcete zapnúť súčasť [Anti-Spyware](#) a vyhľadávať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásit rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – začiarknite toto okienko, ak sa má detegovať rozšírená skupina [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Prehľadávať vo vnútri archívov** (štandardne zapnuté) – začiarknite toto okienko, ak sa má prehľadávať obsah archívov priložených k e-mailovým správam.
- **Zapnúť dôkladné prehľadávanie** (štandardne vypnuté) – v určitých situáciách (napr. pri podozrení na infikovanie počítača vírusom alebo zneužitím) môžete začiarknutím tohto okienka zapnúť algoritmus najdôkladnejšieho prehľadávania, ktorý prehľadá aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.

Hlásenie príloh e-mailov

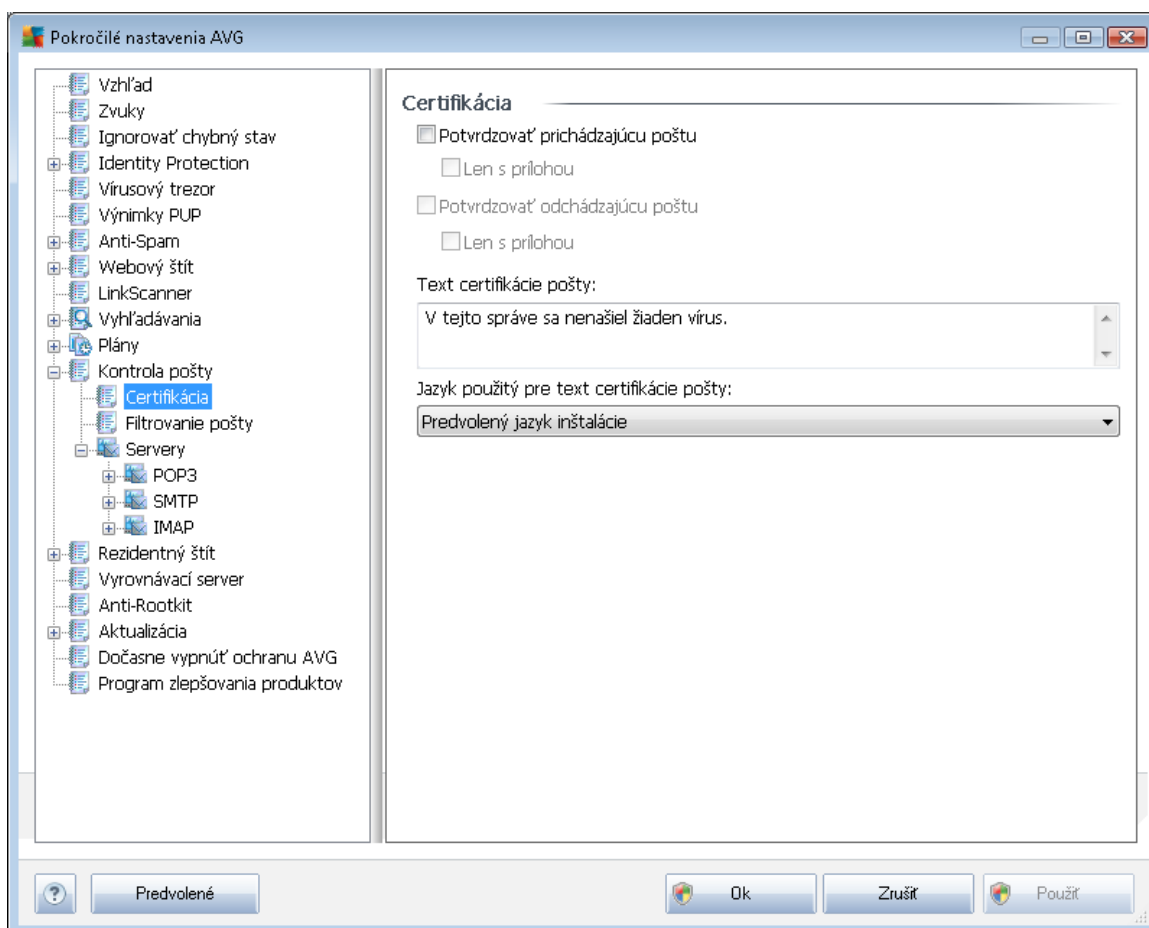


Táto časť umožňuje nastaviť ďalšie správy o súboroch, ktoré môžu byť potenciálne nebezpečné alebo podozrivé. Nezobrazí sa žiadne dialógové okno s upozornením, len sa pridá text certifikácie na koniec e-mailovej správy a všetky takéto správy sa uvedú v dialógovom okne [Detekcia súčasti E-mail Scanner](#):

- **Hlásiť archívy chránené heslom** – archivačné súbory (*ZIP, RAR atď.*) chránené heslom sa nedajú prehľadávať z hľadiska prítomnosti vírusov; začiarknite toto okienko, ak sa majú hlásiť tieto archívy ako potenciálne nebezpečné.
- **Hlásiť dokumenty chránené heslom** – dokumenty chránené heslom sa nedajú prehľadávať z hľadiska prítomnosti vírusov; začiarknite toto okienko, ak sa majú hlásiť tieto dokumenty ako potenciálne nebezpečné.
- **Hlásiť súbory obsahujúce makrá** – makro je vopred definovaný sled krokov, ktoré zjednodušujú konkrétne úlohy používateľovi (*makrá sa bežne používajú v programe MS Word*). Makro, ako také, môže obsahovať potenciálne nebezpečné inštrukcie, a preto je vhodné začiarknuť toto okienko, aby sa súbory s makrami hlásili ako podozrivé.
- **Hlásiť skryté prípony** – skrytá prípona môže spôsobiť, že sa bude podozrivý spustiteľný súbor „niečo.txt.exe“ javiť ako neškodný jednoduchý textový súbor „niečo.txt“. Začiarknite toto okienko, ak majú byť hlásené ako potenciálne nebezpečné.
- **Premiestniť hlásené prílohy do Vírusového trezora** – nastavte, či si želáte byť informovaný e-mailom o archívoch chránených heslom, dokumentoch chránených heslom, súboroch s makrami alebo súboroch so skrytou príponou, ktoré boli detegované ako príloha prehľadávanej e-mailovej správy. Ak sa má táto správa zobraziť počas prehľadávania, potom nastavte, či sa má detegovaný infikovaný objekt premiestniť do [Vírusového trezora](#).

9.12.1. Certifikácia

Dialógové okno **Certifikácia** umožňuje definovať text a jazyk certifikácie pre prichádzajúce aj odchádzajúce e-mailové správy:



Text certifikácie pozostáva z dvoch častí – používateľskej a systémovej – pozri príklad nižšie: prvý riadok je používateľská časť, zvyšok sa generuje automaticky:

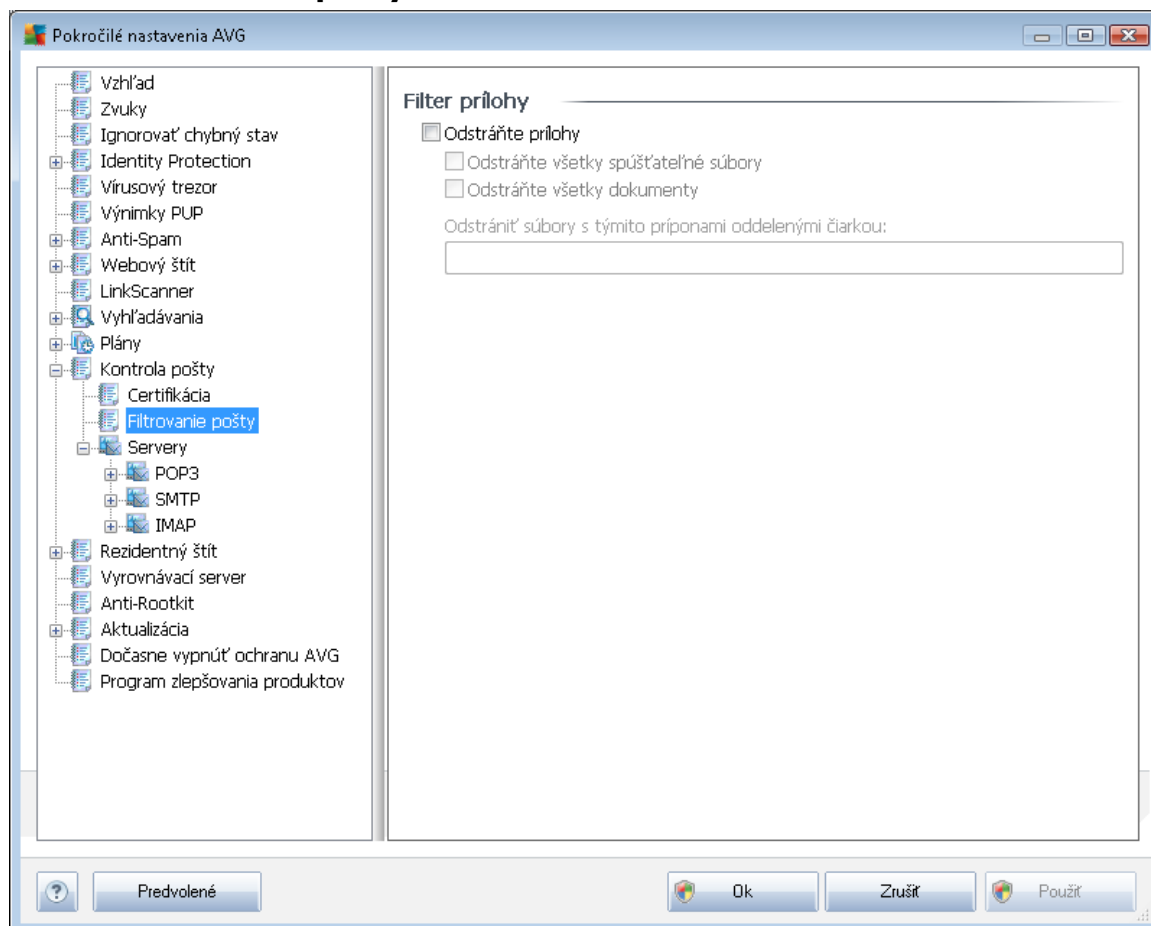
V tejto správe sa nenašiel žiaden vírus.

Skontrolované programom AVG.

Verzia: x.y.zz/vírusová databáza: xx.y.z – dátum vydania: 12/9/2010

Ak sa rozhodnete používať certifikáciu buď pre prichádzajúce alebo odchádzajúce e-mailové správy, potom ďalej v tomto dialógovom okne môžete zadať presné znenie používateľskej časti textu certifikácie (**Text certifikácie e-mailov**) a vybrať jazyk, ktorý sa bude používať na automatické generovanie systémovej časti certifikácie (**Jazyk použitý pre text certifikácie pošty**).

9.12.2. Filtrovanie pošty

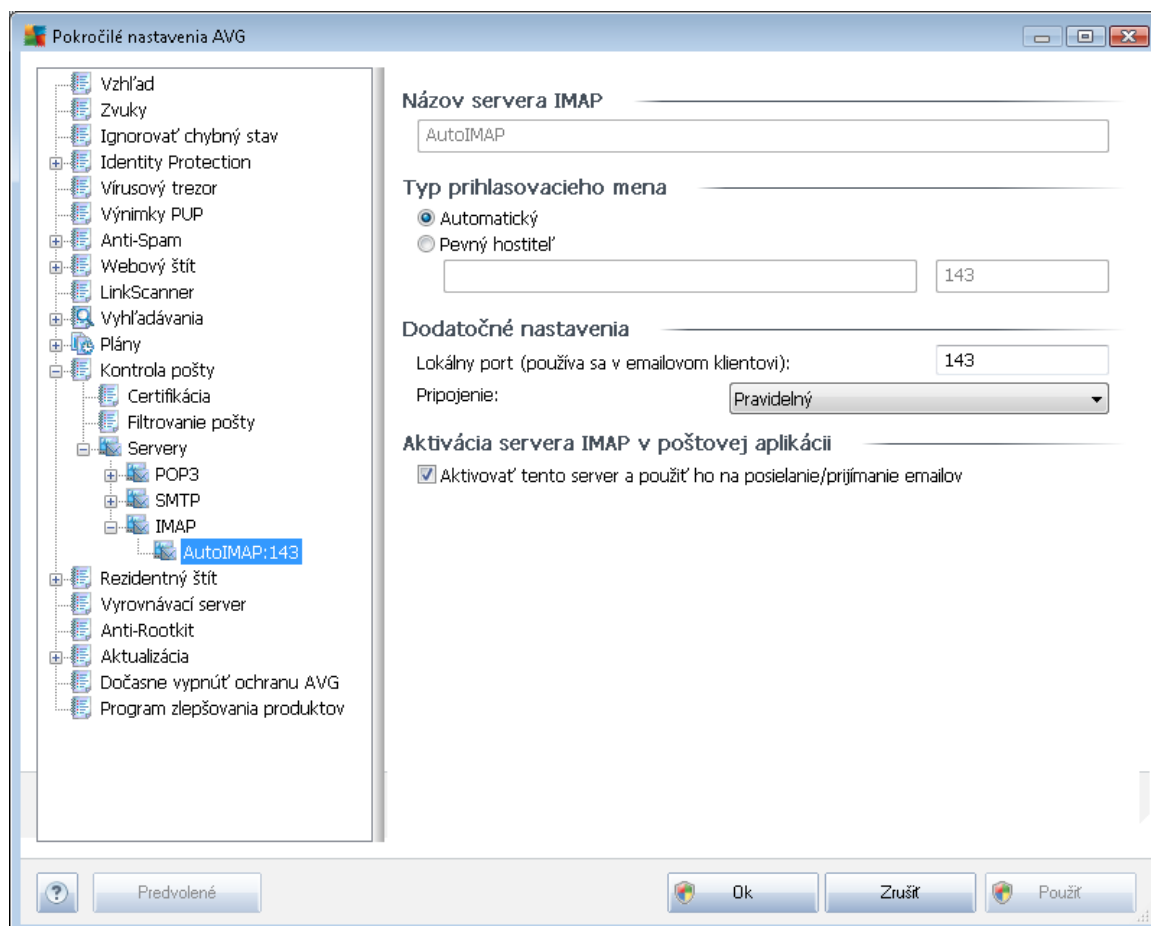


Dialógové okno **Filter príloh** umožňuje nastaviť parametre kontroly príloh e-mailových správ. Štandardne je možnosť **Odstrániť prílohy** vypnutá. Keď ju zapnete, potom sa všetky prílohy e-mailových správ detegované ako infekcie alebo potenciálne nebezpečné programy automaticky odstraňujú. Ak chcete definovať konkrétne typy príloh, ktoré sa majú odstrániť, vyberte príslušnú možnosť:

- **Odstrániť všetky spustiteľné súbory** – vymažú sa všetky súbory s príponou exe.
- **Odstrániť všetky dokumenty** – vymažú sa všetky súbory s príponami doc, docx, xls a xlsx.
- **Odstrániť súbory s týmito príponami oddelenými čiarkou** – odstraňujú sa všetky súbory s uvedenými príponami.

9.12.3. Servery

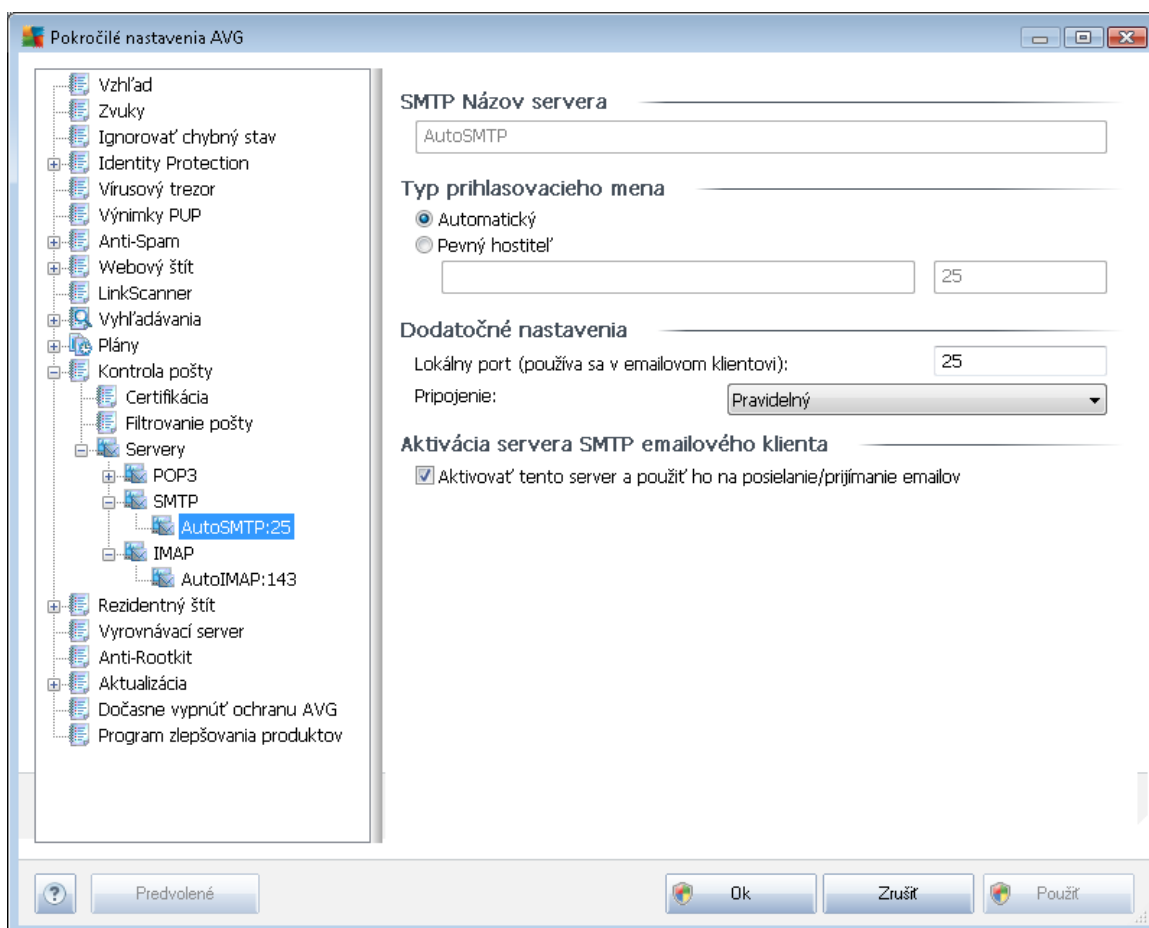
V časti **Servery** môžete zmeniť parametre pre servery komponentu **Kontrola pošty**, alebo nastaviť nový server stlačením tlačidla **Pridať nový server**.



Toto dialógové okno (otvára sa v ponuke **Servery/POP3**) umožňuje nastaviť nový server súčasti **E-mail Scanner** pomocou protokolu POP3 pre prichádzajúcu poštu:

- **Názov servera POP3** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie servera POP3 kliknite pravým tlačidlom myši na položku POP3 v ľavej navigačnej ponuke). Pre automaticky vytvorený server „AutoPOP3“ je toto pole vypnuté.
- **Typ prihlasovacieho mena** – určíte spôsob stanovenia poštového servera pre prichádzajúcu poštu:
 - o **Automaticky** – prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie.
 - o **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Prihlasovacie meno zostane nezmenené. Ako názov môžete použiť názov domény (napríklad *pop.acme.com*) alebo adresu IP (napríklad *123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera a použite dvojbodku ako oddeľovací znak (napríklad *pop.acme.com:8200*). Štandardný port pre komunikáciu POP3 je 110.

- **Ďalšie nastavenia** – používa sa na definovanie podrobnejších parametrov.
 - o **Lokálny port** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z vašej poštovej aplikácie. Potom musíte v poštovej aplikácii nastaviť tento port ako port pre komunikáciu POP3.
 - o **Pripojenie** – táto rozbaľovacia ponuka sa používa na nastavenie typu pripojenia, ktoré sa má použiť (*bežné/SSL/SSL predvolené*). Ak nastavíte pripojenie SSL, potom sa budú posielané dáta šifrovať a žiadna tretia strana ich nebude môcť vystopovať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- **Aktivovanie servera POP3 v poštovej aplikácii** – začiarinknutím alebo zrušením začiarinknutia tejto položky sa aktivuje resp. deaktivuje uvedený server POP3.

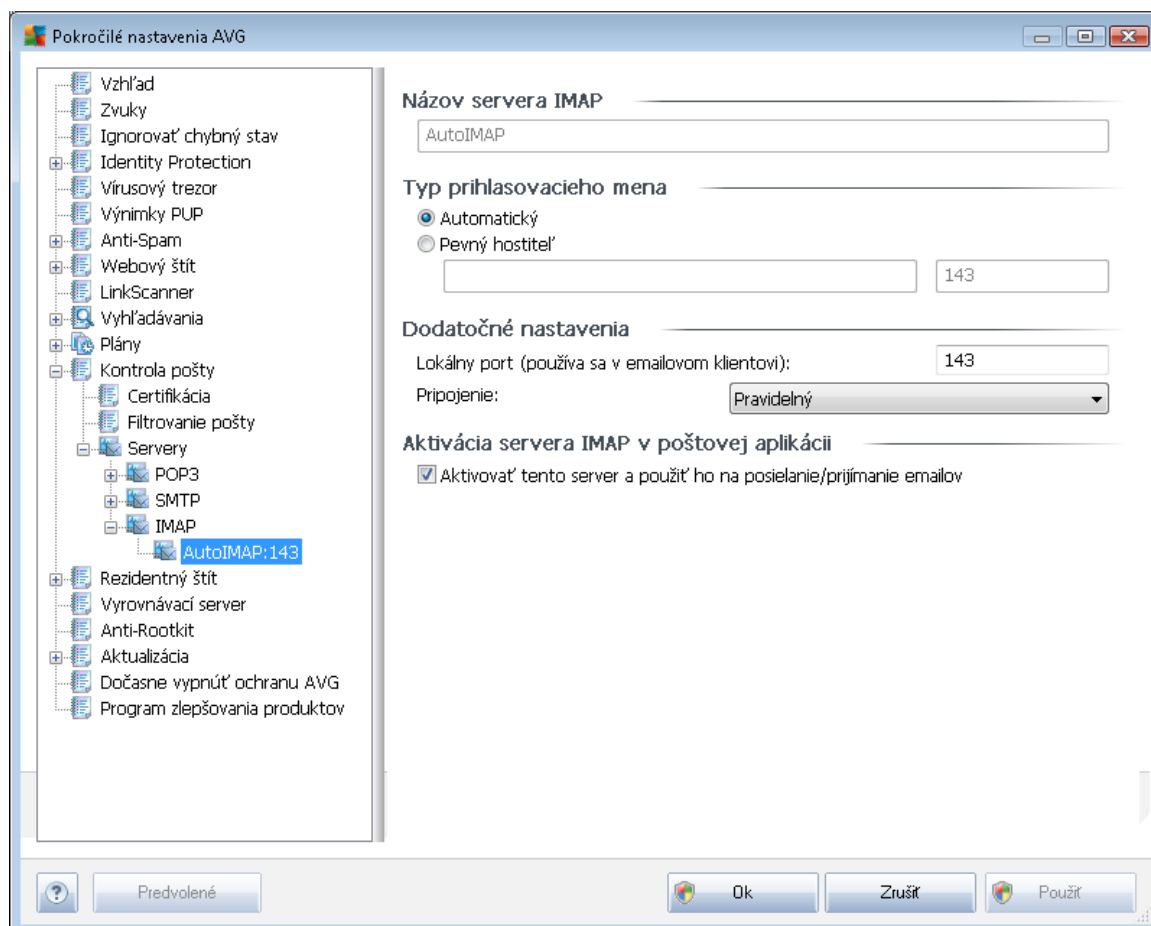


Toto dialógové okno (otvára sa v ponuke **Servery/SMTP**) umožňuje nastaviť nový server **E-mail Scanner** pomocou protokolu SMTP pre odchádzajúcu poštu:

- **Názov servera SMTP** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie servera SMTP kliknite pravým tlačidlom myši na položku SMTP v ľavej navigačnej ponuke)

). Pre automaticky vytvorený server „AutoSMTP“ je toto pole vypnuté.

- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre prichádzajúcu poštu:
 - o **Automaticky** – prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie.
 - o **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadaťte adresu alebo názov vášho poštového servera. Ako názov môžete použiť názov domény (napríklad *smtp.acme.com*) alebo adresu IP (napríklad *123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera. Ako oddeľovací znak použijete dvojbodku (napríklad *smtp.acme.com:8200*). Štandardný port komunikácie SMTP je 25.
- **Ďalšie nastavenia** – používa sa na definovanie podrobnejších parametrov.
 - o **Lokálny port** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z vašej poštovej aplikácie. Potom musíte v poštovej aplikácii nastaviť tento port ako port pre komunikáciu SMTP.
 - o **Pripojenie** – táto rozbaľovacia ponuka sa používa na nastavenie typu pripojenia, ktorý sa má použiť (bežné/SSL/SSL predvolené). Ak nastavíte pripojenie SSL, potom sa budú posielať dáta šifrovať a žiadna tretia strana ich nebude môcť vystopovať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- **Aktivovanie servera SMTP v poštovej aplikácii** – začiatkom alebo zrušením začiatku tohto okienka sa aktivuje resp. deaktivuje uvedený server SMTP.



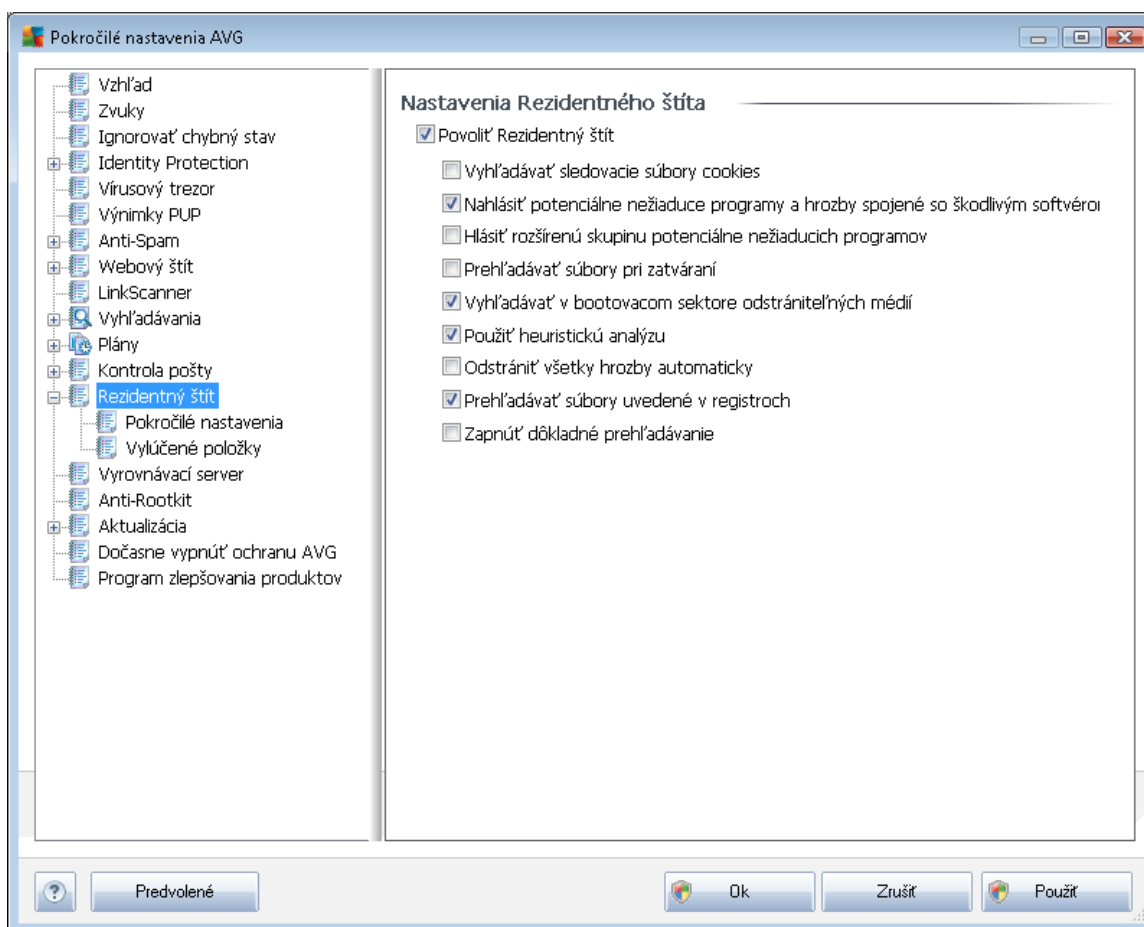
Toto dialógové okno (otvára sa pomocou ponuky **Servery/IMAP**) umožňuje nastaviť nový server typu **E-mail Scanner** pomocou protokolu IMAP pre odchádzajúcu poštu:

- **Názov servera IMAP** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie servera IMAP kliknite pravým tlačidlom myši na položku IMAP v ľavej navigačnej ponuke). Pre automaticky vytvorený server „AutoIMAP“ je toto pole vypnuté.
- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre prichádzajúcu poštu:
 - o **Automaticky** – prihlásenie sa uskutoční automaticky podľa nastavení poštovej aplikácie.
 - o **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov vášho poštového servera. Ako názov môžete použiť názov domény (napríklad *smtp.acme.com*) alebo adresu IP (napríklad *123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera použitím dvojbodky ako oddeľovací znak (napríklad *smtp.acme.com:8200*). Štandardný port pre komunikáciu IMAP je 143.

- **Ďalšie nastavenia** – používa sa na definovanie podrobnejších parametrov.
 - o **Lokálny port** – určuje port, na ktorom sa očakáva komunikácia prichádzajúca z vašej poštovej aplikácie. Potom musíte nastaviť tento port v poštovej aplikácii ako port komunikácie IMAP.
 - o **Pripojenie** – táto rozbaľovacia ponuka sa používa na nastavenie druhu pripojenia, ktoré sa má použiť (*bežné/SSL/SSL predvolené*). Ak nastavíte pripojenie SSL, potom sa budú posielané dáta šifrovať a žiadna tretia strana ich nebude môcť vystopovať ani monitorovať. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- **Aktivovanie servera IMAP v poštovej aplikácii** – začiarknutím alebo zrušením začiarknutia tohto okienka sa aktivuje resp. deaktivuje uvedený server IMAP.

9.13. Rezidentný štít

Súčasť **Rezidentný štít** zabezpečuje živú ochranu súborov a priečinkov pred vírusmi, spywarom a iným škodlivým softvérom.



Dialógové okno **Nastavenia súčasti Rezidentný štít** umožňuje kompletne zapnúť alebo vypnúť ochranu zabezpečovanú súčasťou **Rezidentný štít** začiarknutím/zrušením začiarknutia položky

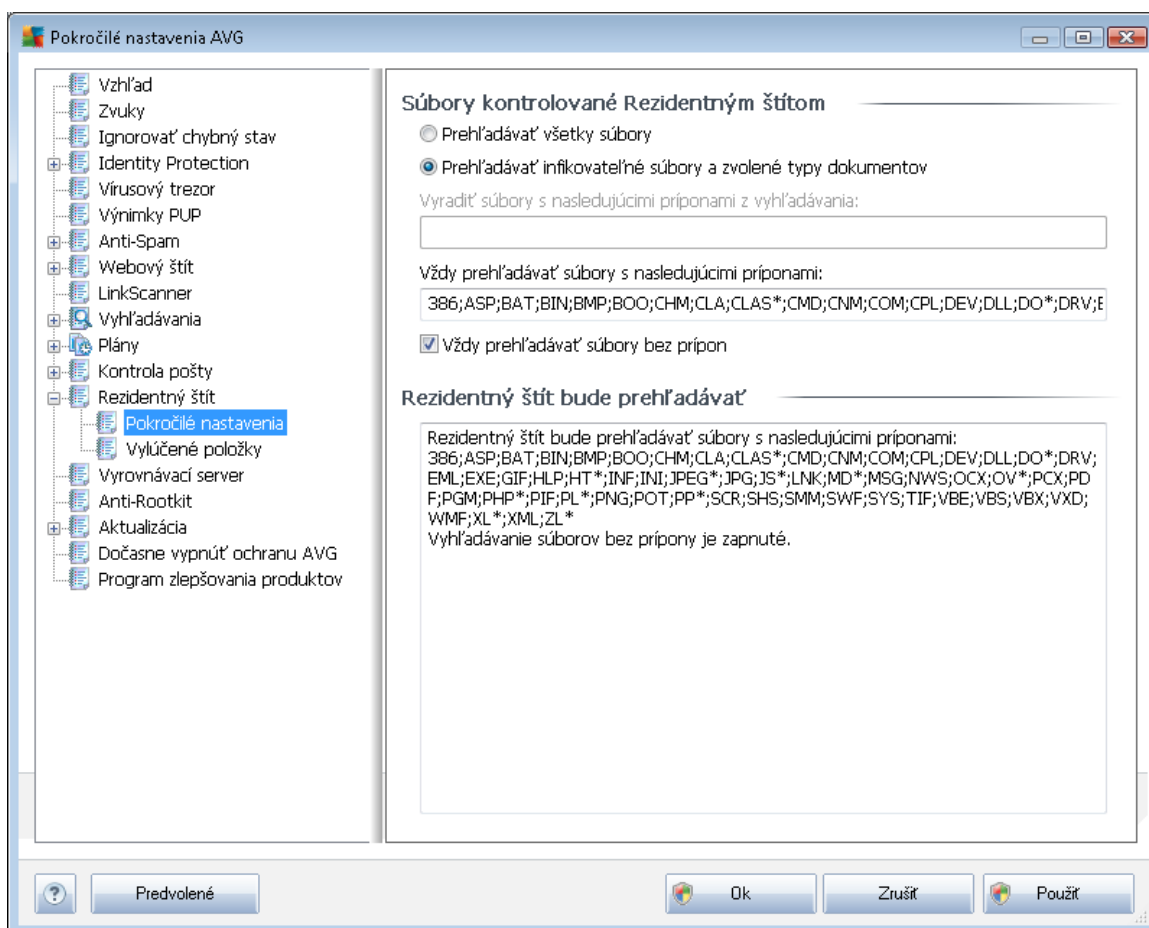


Zapnúť Rezidentný štít (táto funkcia je štandardne zapnutá). Okrem toho môžete nastaviť, ktoré funkcie súčasti **Rezidentný štít** sa majú zapnúť:

- **Vyhľadávať sledovacie súbory cookies** (štandardne vypnuté) – tento parameter určuje, že sa majú počas prehľadávania detegovať aj súbory cookies. (*HTTP cookies sa používajú na autentifikáciu, sledovanie a uchovanie konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov.*)
- **Hlásit' potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté) – začiar knite túto možnosť, ak chcete zapnúť súčasť **Anti-Spyware** a vyhľadávať spyware a vírusy. Spyware predstavuje pochybnú kategóriu škodlivého softvéru: aj keď v bežných prípadoch predstavuje bezpečnostné riziko, niektoré tieto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásit' rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – začiar knite toto okienko, ak sa má detegovať rozšírená skupina spywaru: programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovat' dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Prehľadávať súbory pri zatvorení** (štandardne vypnuté) – prehľadávanie pri zatvorení zabezpečí, že AVG prehľadá činné objekty (napr. aplikácie, dokumenty...), keď sa otvárajú alebo zatvárajú; táto funkcia pomáha chrániť počítač pred niektorými druhmi sofistikovaných vírusov.
- **Prehľadávať zavádzací sektor vyberateľných médií** (štandardne zapnuté)
- **Použiť heuristiku** (štandardne zapnuté) – na detegovanie sa použije heuristická analýza (*dynamická emulácia inštrukcií prehľadávaného objektu v prostredí virtuálneho počítača*).
- **Odstrániť všetky hrozby automaticky** (predvolené nastavenie – vypnuté) – každá detegovaná infekcia bude automaticky vyliečená, ak je dostupná liečba, a všetky nevyliečiteľné infekcie budú odstránené.
- **Prehľadávať súbory uvedené v databáze Registry** (štandardne zapnuté) – tento parameter určuje, že AVG bude prehľadávať všetky spustiteľné súbory pridané do databázy Registry na spúšťanie pri štarte počítača, aby sa známa infekcia nemohla spustiť pri ďalšom spustení počítača.
- **Zapnúť dôkladné prehľadávanie** (štandardne vypnuté) – v určitých situáciách (napr. v stave mimoriadnej núdze) môžete začiar knutím tohto okienka zapnúť algoritmus najdôkladnejšieho prehľadávania, ktorý skontroluje všetky možné nebezpečné objekty do hĺbky. Upozorňujeme však, že tento spôsob je náročný na čas.

9.13.1. Rozšírené nastavenia

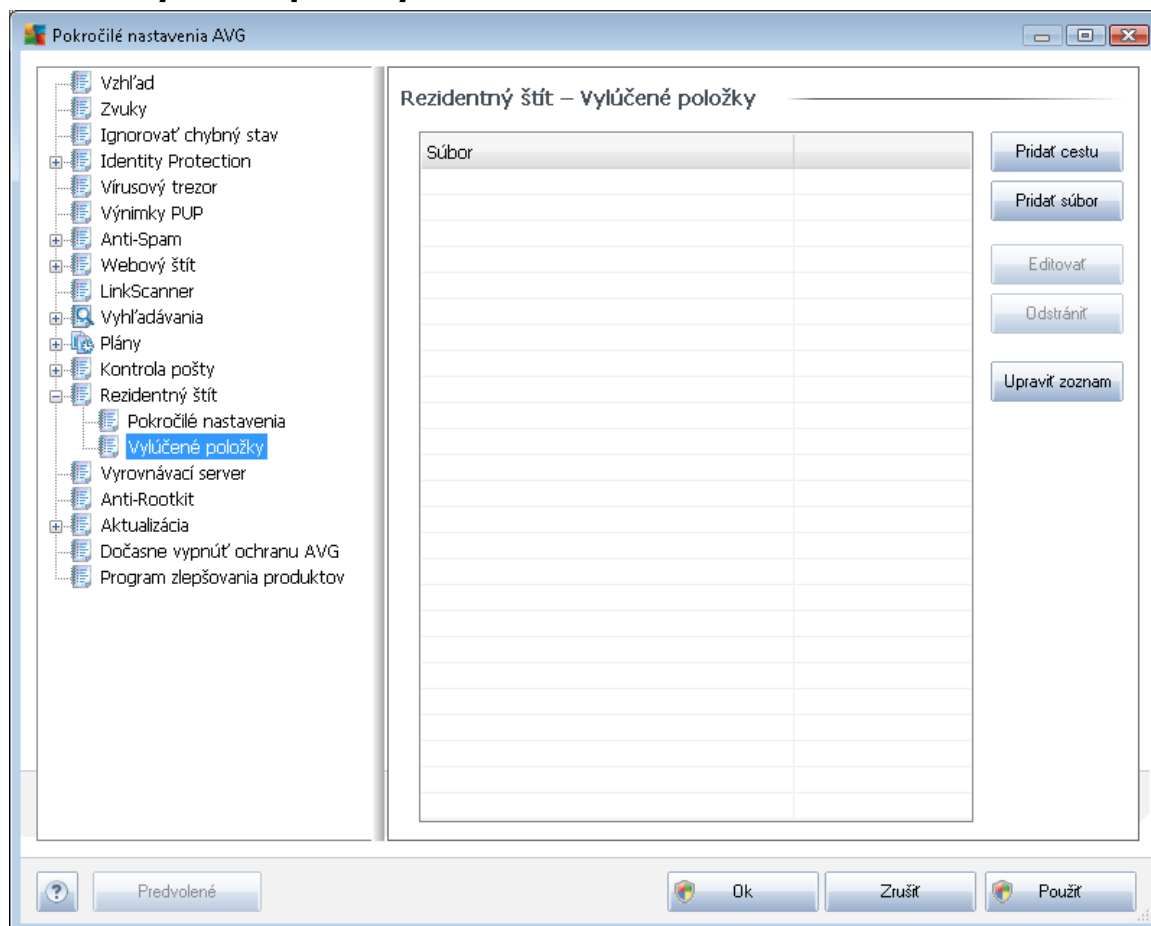
V dialógovom okne **Súbory prehľadané súčasťou Rezidentný štít** môžete nastaviť, ktoré súbory sa budú prehľadávať (podľa konkrétnych prípon):



Nastavte, či sa majú prehľadávať všetky súbory alebo len indikovateľné súbory. V druhom prípade môžete ďalej zadať zoznam prípon, ktoré definujú súbory, ktoré sa majú vylúčiť z prehľadávania, a tiež zoznam prípon súborov, ktoré definujú súbory, ktoré sa budú prehľadávať za každých okolností.

V časti nižšie s názvom **Rezidentný štít bude prehľadávať** sa nachádza prehľad momentálnych nastavení s podrobným prehľadom toho, čo bude súčasť **Rezidentný štít** skutočne prehľadávať.

9.13.2. Vylúčené položky



Dialógové okno **Rezidentný štít – Vylúčené položky** umožňuje definovať súbory a/alebo priečinky, ktoré sa vylúčia z prehľadávania súčasťou **Rezidentný štít**.

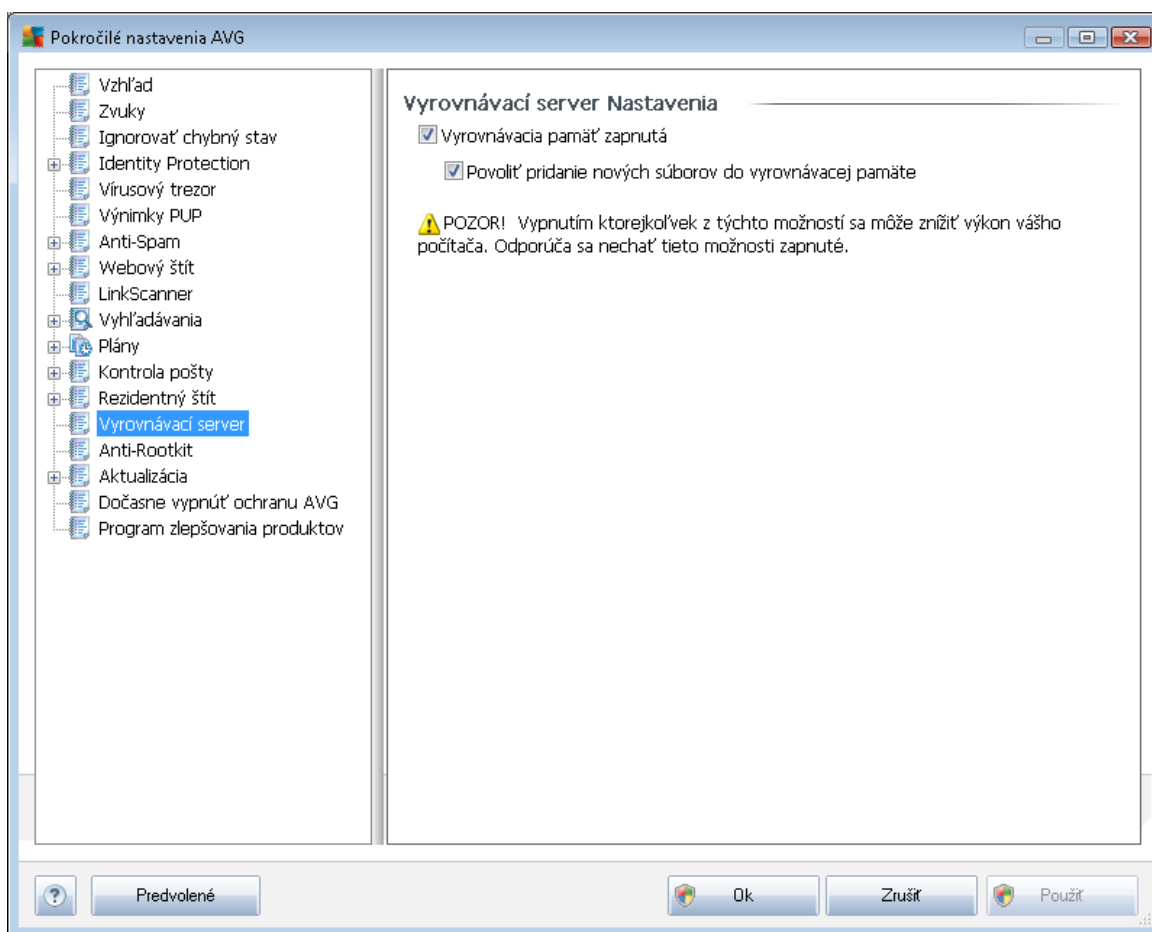
Odporúčame vám, aby ste nevylúčili žiadne položky, ak to nie je naozaj nevyhnutné!

V tomto dialógovom okne sa nachádzajú tieto ovládacie tlačidlá:

- **Pridať cestu** – uvedte adresáre, ktoré sa majú vylúčiť z prehľadávania, tak, že ich postupne vyberiete v navigačnej štruktúre lokálneho disku.
- **Pridať súbor** – uvedte súbory, ktoré sa majú vylúčiť z prehľadávania, tak, že ich postupne vyberiete v navigačnej štruktúre lokálneho disku.
- **Editovať položku** – umožňuje editovať zadanú cestu k vybranému súboru alebo priečinku.
- **Odstrániť položku** – umožňuje vymazať cestu k vybranej položke zo zoznamu.

9.14. Vyrovnávací server

Vyrovnávací server je proces, ktorý sa používa na skrátenie doby prehľadávania (*prehľadávania na požiadanie, naplánovaného prehľadávania celého počítača, prehľadávania súčasťou [Rezidentný štít](#)*). Zhromažďuje a uchováva informácie o dôveryhodných súboroch (*systémových súboroch s digitálnym podpisom a pod.*): Tieto súbory sa potom považujú za bezpečné a počas prehľadávania sa vynechajú.

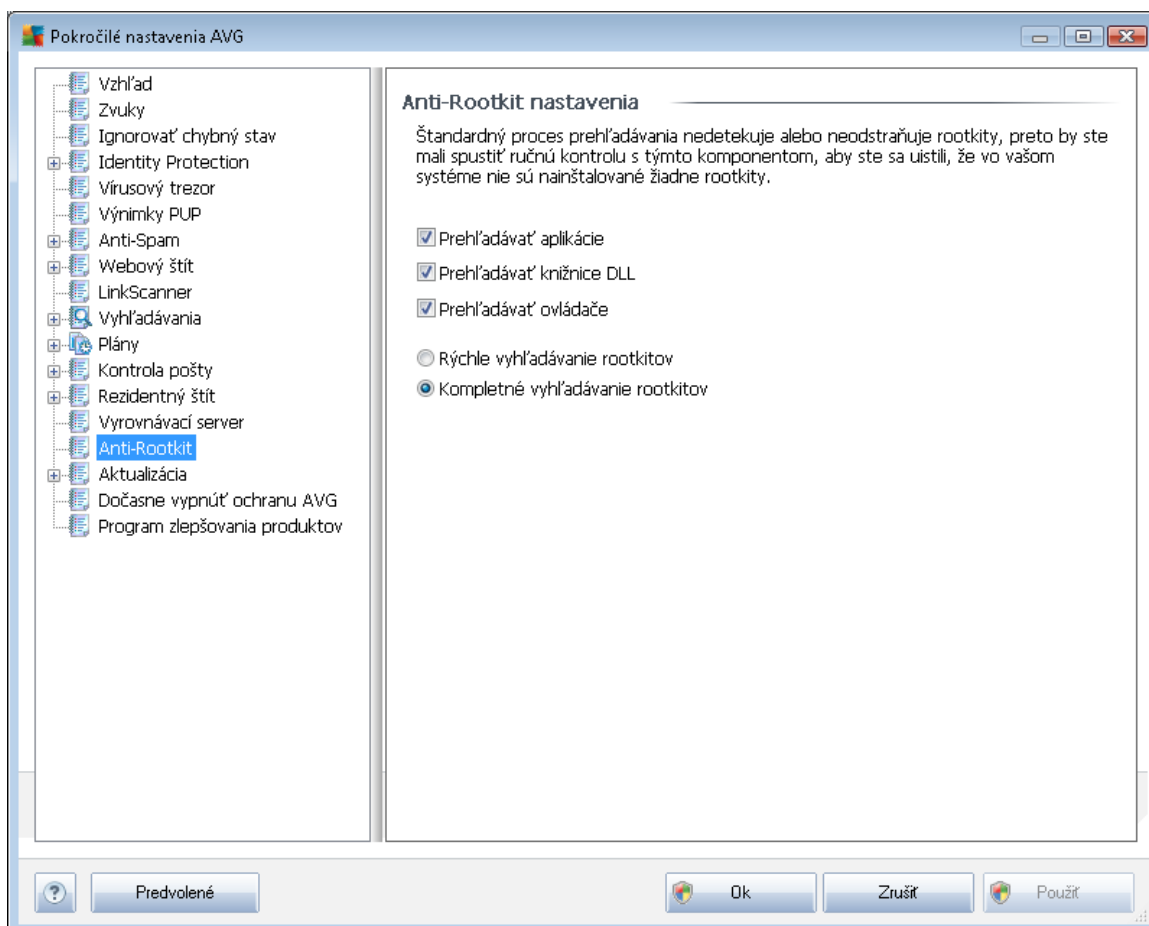


Dialógové okno s nastaveniami ponúka na výber z dvoch možností:

- **Vyrovnávací pamäť zapnutá** (štandardne zapnuté): Zrušením označenia tohto políčka sa vypne **vyrovnávací server** a vyprázdni sa vyrovnávací pamäť. Upozorňujeme, že týmto sa môže spomaliť prehľadávanie a znížiť celkový výkon počítača, pretože každý jeden používaný súbor sa najskôr skontroluje z hľadiska prítomnosti vírusov a spywaru.
- **Povolit' pridanie nových súborov do vyrovnávacej pamäte** (štandardne zapnuté): Zrušením označenia tohto políčka sa vypne pridávanie ďalších súborov do vyrovnávacej pamäte. Všetky súbory vo vyrovnávacej pamäti sa zachovávajú a budú sa používať do úplného vypnutia funkcie vyrovnávacej pamäte, resp. do ďalšieho aktualizovania vírusovej databázy.

9.15. Anti-Rootkit

Toto dialógové okno sa používa na zmenu konfigurácie súčasti [Anti-Rootkit](#):



Editovanie všetkých funkcií súčasti [Anti-Rootkit](#), tak ako sú uvedené v tomto dialógovom okne, je možné robiť aj priamo v [rozhraní súčasti Anti-Rootkit](#).

Začiarknutím príslušných políčok definujete objekty, ktoré sa majú prehľadávať:

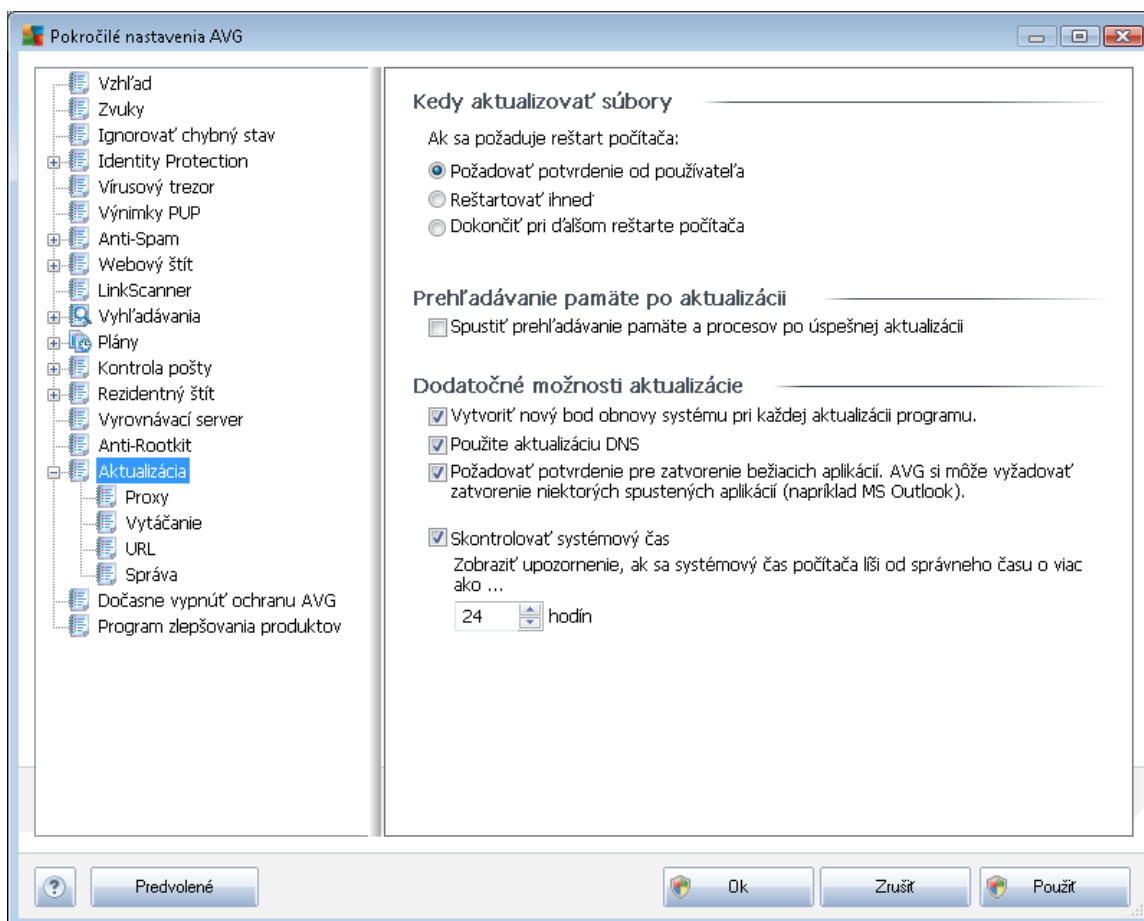
- **Prehľadávať aplikácie**
- **Prehľadávať knižnice DLL**
- **Prehľadávať ovládače**

Ďalej môžete vybrať režim vyhľadávania rootkitov:

- **Rýchle vyhľadávanie rootkitov** – prehľadáva všetky spustené procesy, zavedené ovládače a systémový priečinok (zvyčajne c:\Windows).
- **Úplné vyhľadávanie rootkitov** – Prehľadáva všetky spustené procesy, zavedené ovládače,

systémový priečinok (obyčajne c:\Windows), plus všetky miestne disky (vrátane pamäťových médií, nie však disketové jednotky/jednotky CD-ROM).

9.16. Aktualizácia



Položka **Aktualizácia** v navigačnej štruktúre otvorí nové dialógové okno, ktoré umožňuje nastaviť všeobecné parametre súvisiace s [aktualizáciou produktu AVG](#):

Kedy aktualizovať súbory

V tejto časti môžete vybrať jednu z troch alternatívnych možností, ktorá bude použitá v prípade, ak si aktualizácia vyžiada reštartovanie počítača. Dokončenie aktualizácie môžete naplánovať na ďalšie reštartovanie počítača, alebo môžete ihneď reštartovať počítač:

- **Požiadat' o potvrdenie používateľa** (predvolené) – budete požiadaný, aby ste potvrdili reštartovanie počítača, ktoré je potrebné na dokončenie [procesu aktualizácie](#)
- **Reštartovať ihneď** – počítač sa automaticky reštartuje ihneď po dokončení [procesu aktualizácie](#) a nepožiadá vás o udelenie súhlasu.



- **Dokončiť pri ďalšom reštartovaní počítača** – dokončenie [aktualizácie](#) bude odložené na ďalšie reštartovanie počítača. Odporúčame vám, aby ste túto možnosť zapli len v prípade, ak sa počítač reštartuje pravidelne, najmenej raz za deň!

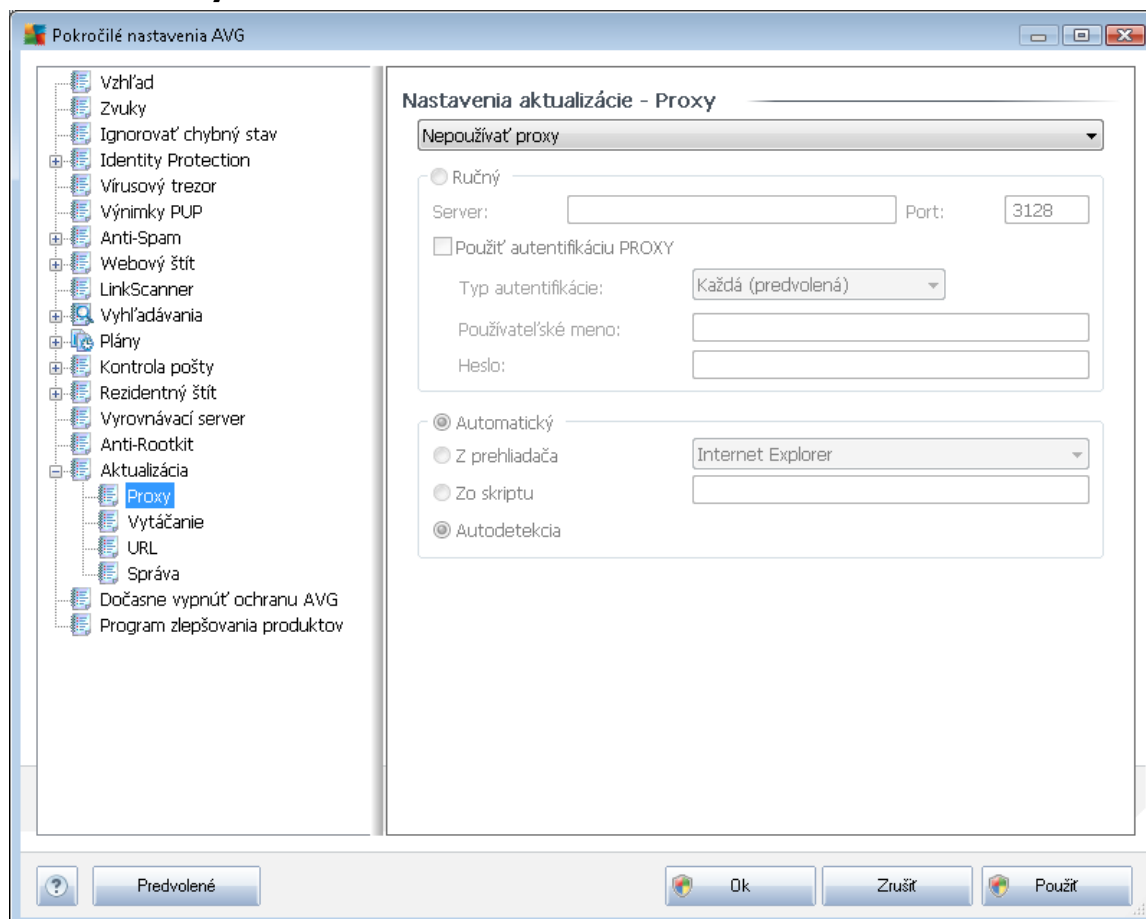
Kontrola pamäte po aktualizácii

Začiarknite toto začiarkovacie okienko, ak sa má nová kontrola pamäte spustiť po každej úspešnej aktualizácii. Najnovšia prevzatá aktualizácia môže obsahovať nové definície vírusov, ktoré sa môžu ihneď použiť pri kontrole.

Ďalšie možnosti aktualizácie

- **Vytvoriť nový bod obnovenia systému počas každej aktualizácie programu** – pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovenia systému. Ak proces aktualizácie zlyhá a operačný systém spadne, potom vám tento bod obnovenia umožní obnoviť stav operačného systému s pôvodnou konfiguráciou. Táto funkcia sa otvára v ponuke Štart/Všetky programy/Príslušenstvo/Systémové nástroje/Obnovenie systému. Zmeny týchto nastavení však odporúčame robiť len skúseným používateľom! Nechajte toto začiarkovacie okienko začiarknuté, ak chcete používať túto funkcionálnosť.
- **Používať aktualizáciu DNS** (štandardne zapnuté) – ak je toto začiarkovacie okienko označené, po spustení aktualizácie program **AVG Internet Security 2011** vyhľadá informácie o najnovšej verzii vírusovej databázy a najnovšej verzii programu na serveri DNS. Až potom sa prevezmú a nainštalujú najmenšie nevyhnutne potrebné aktualizčné súbory. Týmto spôsobom sa minimalizuje celkový objem prevzatých dát a zrýchli proces aktualizácie.
- **Funkcia Požadovať súhlas so zatvorením spustených aplikácií** (štandardne zapnuté) sa postará o to, aby sa žiadna spustená aplikácia nezatvorila bez vášho súhlasu, keď to je potrebné na dokončenie procesu aktualizácie.
- **Skontrolovať systémový čas** – začiarknite toto okienko, ak chcete byť informovaný v prípade, keď sa systémový čas líši od skutočného času o viac ako je nastavený počet hodín.

9.16.1. Proxy



Server proxy je samostatný server alebo služba spustená na počítači, ktorá zaručuje bezpečnejšie pripojenie do internetu. Podľa definovaných pravidiel siete potom môžete pristupovať na internet buď priamo alebo cez server proxy, pričom súčasne môžete použiť aj obidve možnosti. Potom v prvej položke dialógového okna **Nastavenia aktualizácie – Proxy** musíte nastaviť v ponuke, či chcete:

- **Použiť proxy**
- **Nepoužívať server proxy:** Predvolené nastavenie.
- **Pokúsiť sa pripojiť pomocou servera proxy a ak sa to nepodarí, pripojiť priamo**

Ak si zvolíte niektorú z možností používajúcich server proxy, budete musieť zadať ďalšie údaje. Nastavenia servera sa nastavujú buď ručne alebo automaticky.

Ručná konfigurácia

Ak sa rozhodnete pre ručnú konfiguráciu (začiarknite možnosť **Ručná** na aktivovanie príslušnej časti dialógového okna), musíte nastaviť nasledujúce parametre:



- **Server:** Zadáte adresu IP servera alebo názov servera.
- **Port:** Zadáte číslo portu, ktorý umožňuje prístup na internet (*štandardne je toto číslo nastavené na hodnotu 3128, ale môžete nastaviť inú hodnotu; ak máte pochybnosti, kontaktujte správcu siete*).

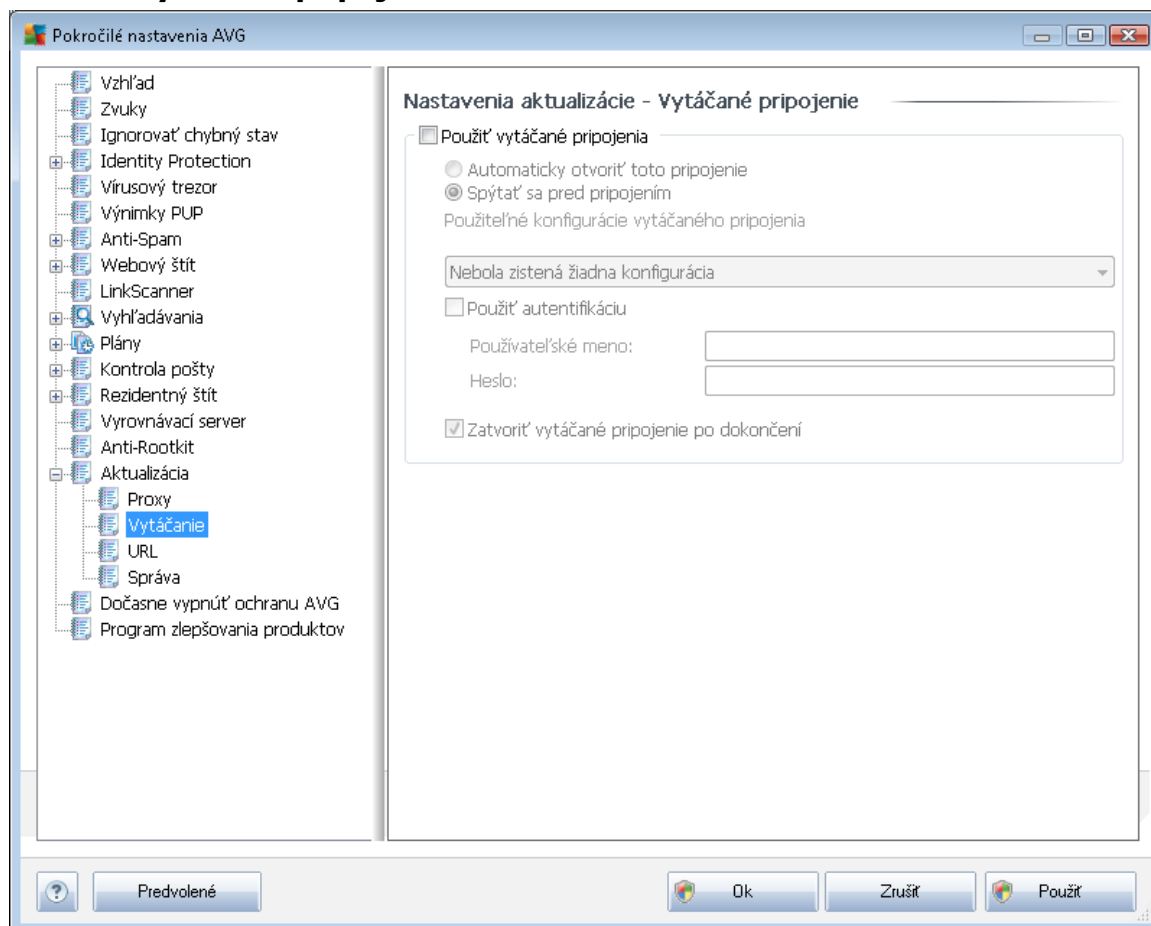
Server proxy môže mať tiež nastavené špeciálne pravidlá pre každého používateľa. Ak je server proxy nastavený týmto spôsobom, začiarknite možnosť **Použiť autentifikáciu PROXY** na overenie, či sú vaše používateľské meno a heslo platné na vytvorenie pripojenia na internet cez server proxy.

Automatická konfigurácia

Ak sa rozhodnete pre automatickú konfiguráciu (začiarknite možnosť **Automatická** na aktivovanie príslušnej časti dialógového okna), nastavte, odkiaľ sa má prevziať konfigurácia servera proxy:

- **Z prehliadača:** Konfigurácia sa načíta z predvoleného internetového prehliadača.
- **Zo skriptu:** Konfigurácia sa načíta z prevzatého skriptu pomocou funkcie, ktorá vráti adresu servera proxy.
- **Automatické zistenie:** Konfigurácia sa zistí automaticky priamo zo servera proxy.

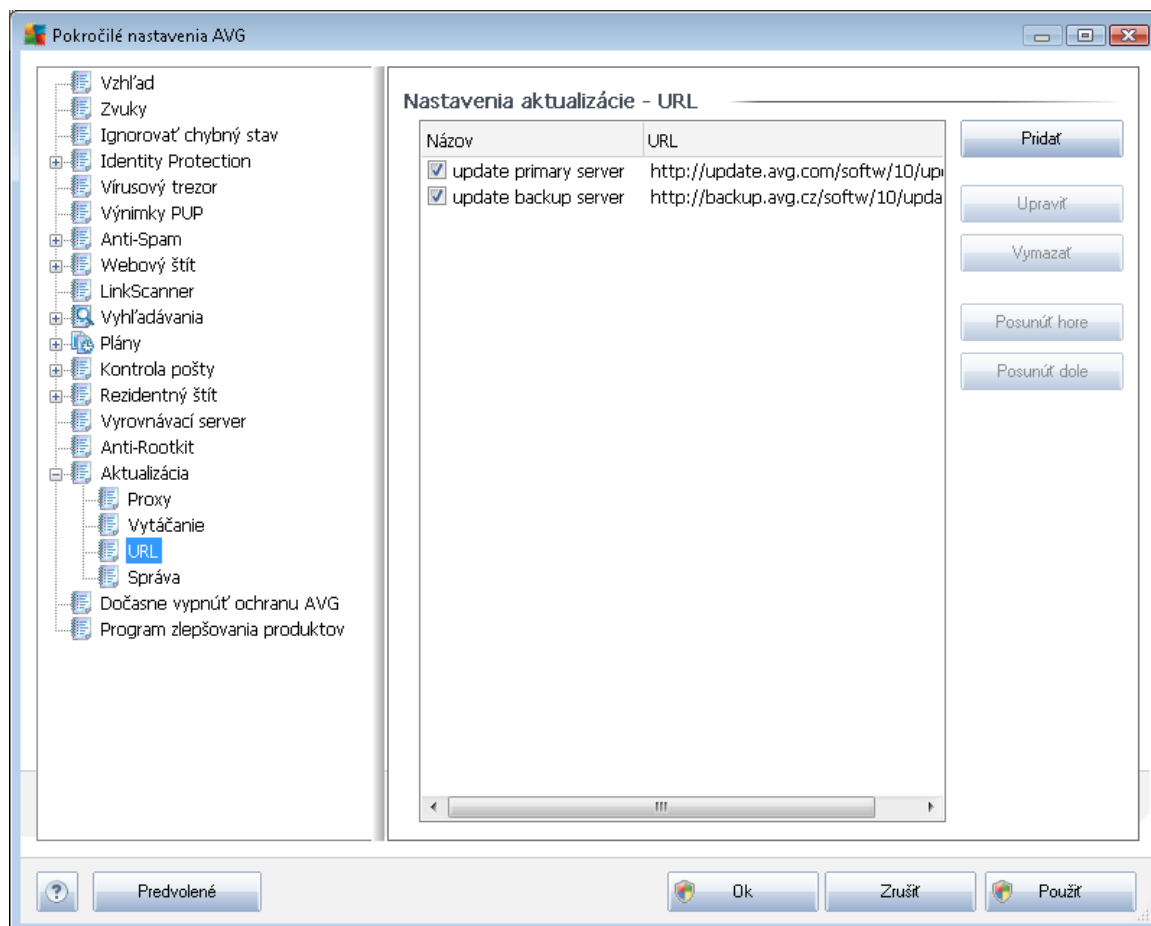
9.16.2. Vytáčané pripojenie



Všetky parametre voliteľne zadané v dialógovom okne **Nastavenia aktualizácie - Vytáčané pripojenie** sa vzťahujú na vytáčané pripojenie k Internetu. Polia v tomto dialógovom okne nebudú aktívne, kým neoznačíte možnosť **Použiť vytáčané pripojenie**, potom sa polia aktivujú.

Zadajte, či sa chcete pripojiť k Internetu automaticky (**Automaticky otvoriť toto pripojenie**) alebo chcete každý krát potvrdiť toto pripojenie ručne (**Spýtať sa pred pripojením**). Pri automatickom pripojení by ste mali ďalej zvoliť, či sa má pripojenie zatvoriť po skončení aktualizácie (**Zatvoriť vytáčané pripojenie po dokončení**).

9.16.3. Adresa URL

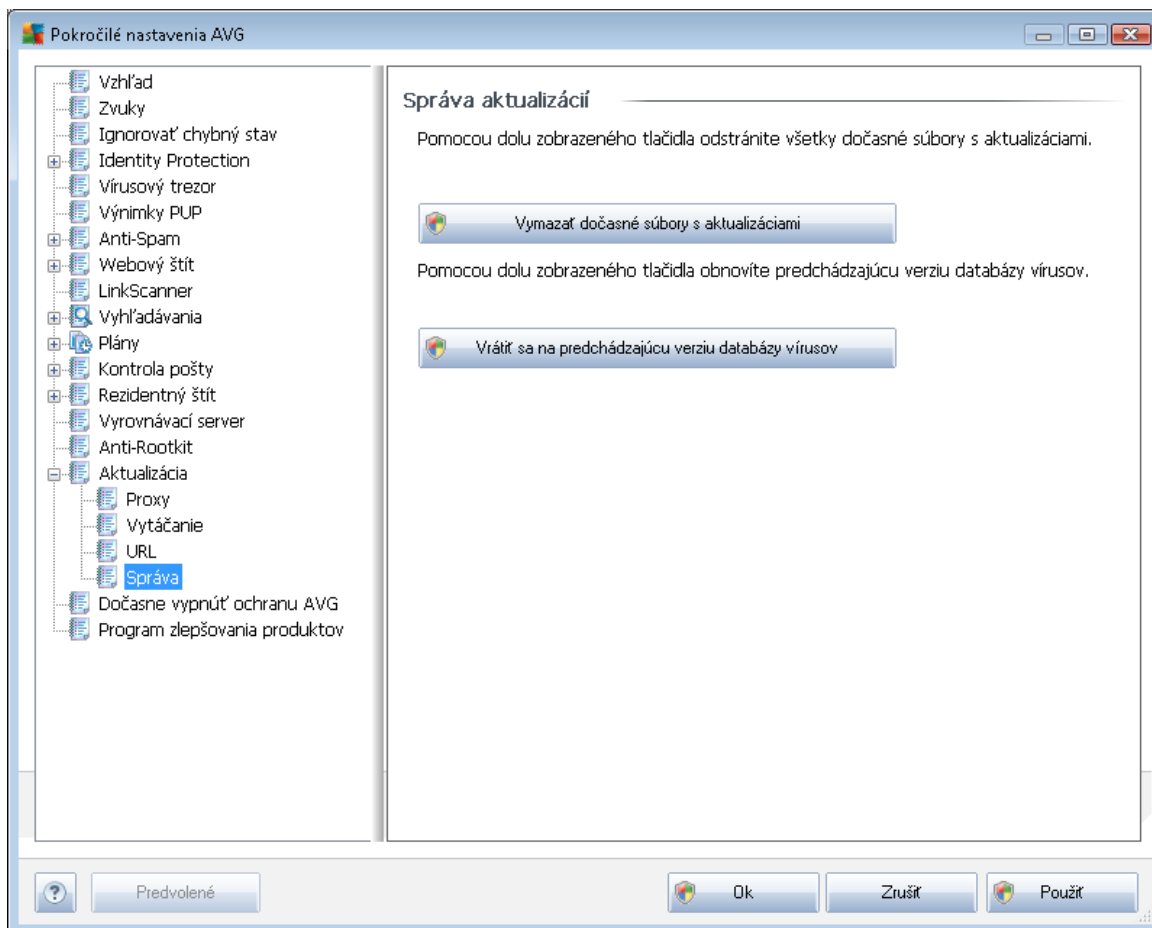


Dialógové okno **URL** uvádza zoznam internetových adries, odkiaľ si môžete prevziať aktualizčné súbory. Zoznam a jeho položky môžete zmeniť pomocou nasledujúcich ovládacích tlačidiel:

- **Pridať** - otvorí sa dialógové okno, kde môžete zadať novú URL adresu, ktorú chcete pridať do zoznamu
- **Upraviť** - otvorí sa dialógové okno, kde môžete upraviť parametre zvolenej URL adresy
- **Vymazať** - vymaže sa zvolená URL adresa zo zoznamu
- **Posunúť hore** - posunie zvolenú URL adresu o jednu pozíciu v zozname hore
- **Posunúť dole** - posunie zvolenú URL adresu o jednu pozíciu v zozname dole

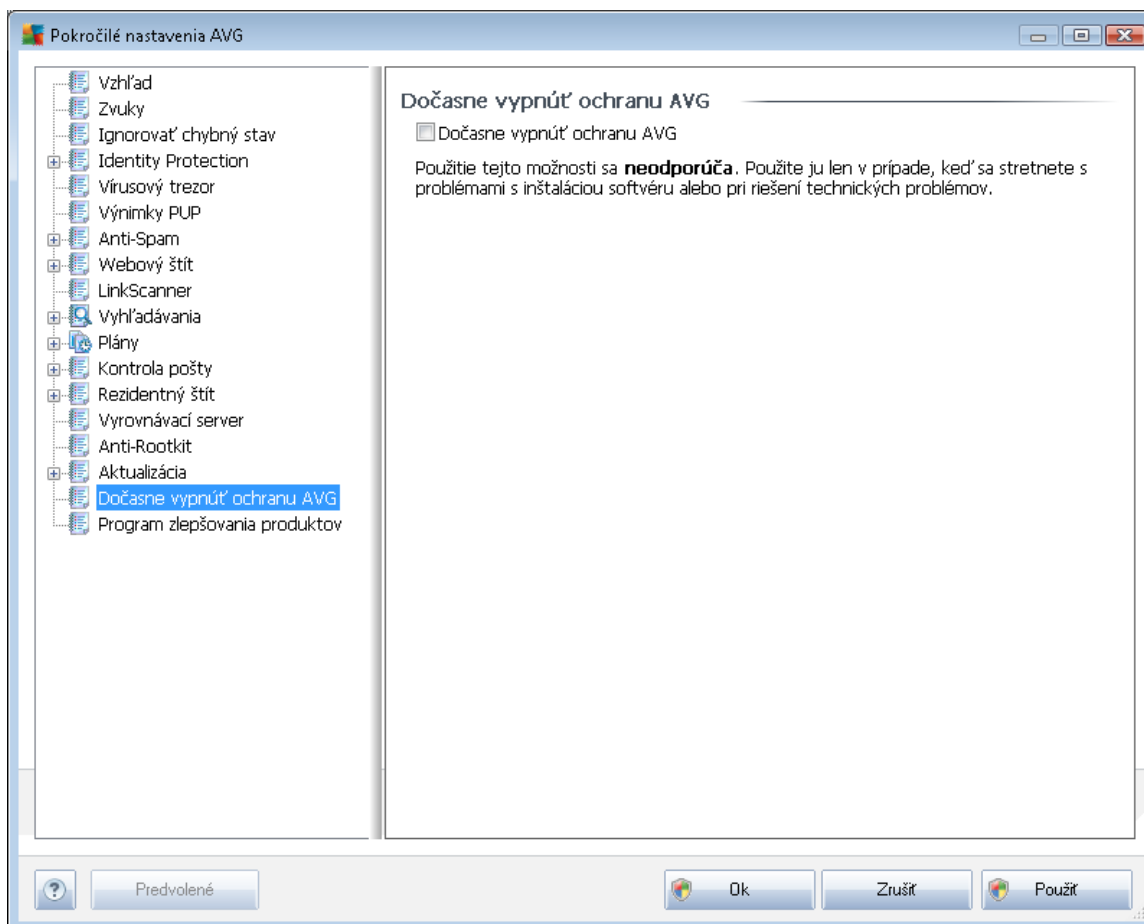
9.16.4. Správa

Dialógové okno **Správa** ponúka dve možnosti, ktoré sa sprístupnia pomocou dvoch tlačidiel:



- **Vymazať dočasné súbory aktualizácie:** Stlačením tohto tlačidla sa vymažú všetky redundantné súbory aktualizácie z pevného disku (*štandardne, tieto súbory zostanú uložené 30 dní*)
- **Obnoviť predchádzajúcu verziu databázy vírusov:** Stlačením tohto tlačidla sa vymaže najnovšia verzia databázy vírusov z pevného disku a obnoví sa predchádzajúca uložená verzia (*nová verzia databázy vírusov bude tvoriť súčasť nasledujúcej aktualizácie*).

9.17. Dočasné vypnutie ochrany AVG



Dialógové okno **Dočasné vypnutie ochrany AVG** umožňuje naraz vypnúť celú ochranu zabezpečovanú programom **AVG Internet Security 2011**.

Nepoužívajte túto možnosť, pokiaľ to nie je naozaj nevyhnutné!

Vo väčšine prípadov **nie je potrebné** vypnúť AVG pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, keď inštalačný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili spustené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak sa naozaj stretnete s problémom počas inštalácie, pokúste sa vypnúť najskôr súčasť [Rezidentný štít](#). Ak musíte dočasne vypnúť program AVG, zapnite ho hneď ako dokončíte pôvodnú činnosť. Ak ste pripojený na internet alebo k sieti v čase, keď je antivírusový softvér vypnutý, váš počítač je zraniteľný pred útokmi.

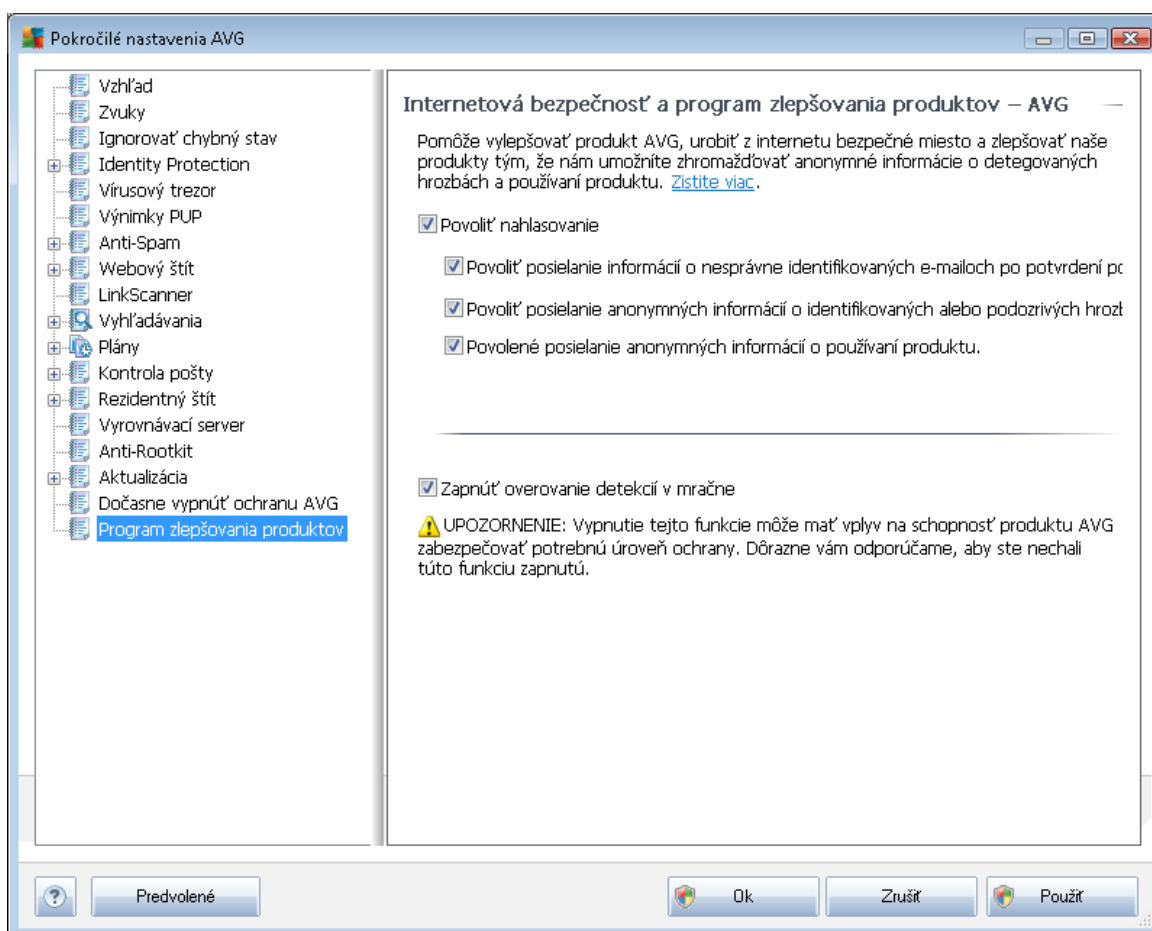
9.18. Program zlepšovania produktov

Dialógovým oknom **Internetová bezpečnosť a program zlepšovania produktov AVG** vás pozývame, aby ste sa zúčastnili programu zlepšovania produktov AVG a pomohli nám zvýšiť celkovú úroveň zabezpečenia internetu. Začiarknutím možnosti **Povolit' hlásenie** zapniete hlásenie detegovaných hrozieb do AVG. Táto funkcia nám pomáha zhromažďovať aktuálne informácie o



najnovších hrozbách od účastníkov z celého sveta a umožňuje nám zlepšovať ochranu pre každého jednotlivca.

Hlásenie prebieha automaticky, preto vás nijako nezaťažuje a v správach nie sú uvedené žiadne osobné údaje. Hlásenie detegovaných hrozieb je voliteľné, avšak žiadame vás, aby ste túto funkciu zapli, pretože nám pomáha zlepšovať ochranu nielen vás, ale aj ostatných používateľov produktov AVG.



V dnešnej dobe existuje oveľa viac hrozieb ako sú len jednoduché vírusy. Autori škodlivého kódu a nebezpečných internetových stránok sú však veľmi inovatívni a pomerne často sa objavujú nové typy hrozieb, pričom absolútna väčšina z nich sa vyskytuje na internete. Toto sú niektoré z najčastejšie sa vyskytujúcich hrozieb:

- **Vírus** je škodlivý kód, ktorý sa kopíruje a šíri často bez povšimnutia, až kým nenapácha škody. Niektoré vírusy predstavujú vážnu hrozbu, ktorá dokáže vymazať alebo zámerne zmeniť súbory, zatiaľ čo iné vírusy sú zdanlivo neškodné, napríklad zahrajú melódiu. Všetky vírusy sú však nebezpečné, pretože sa dokážu množiť. Jeden jediný vírus dokáže v okamihu zaplniť celú pamäť počítača a spôsobiť jeho zlyhanie.
- **Podkategóriou vírusu je červ**, ktorý, na rozdiel od vírusu, nepotrebuje „nosiča“, ku ktorému sa pripojí; sám sa rozosiela do ostatných počítačov, obvyčajne cez e-mail a v

dôsledku toho často preťažuje poštové servery a sieťové systémy.

- **Spyware** sú zvyčajne sprievodné programy kategórie malware (*malware* = *každý škodlivý softvér, vrátane vírusov*), zvyčajne trójske kone, ktoré sa používajú na odcudzenie osobných informácií, hesiel, čísel kreditných kariet, alebo na preniknutie do počítača a umožnenie útočníkovi ovládať počítač na diaľku; všetko samozrejme bez vedomia a súhlasu vlastníka počítača.
- **Potenciálne nežiaduce programy** je taký typ spywaru, ktorý môže, ale nemusí byť nevyhnutne nebezpečný pre počítač. Špecifickým príkladom PNP je adware, t. j. softvér určený na šírenie reklám, zvyčajne zobrazovaním reklamných prekryvacích okien, ktoré obťažujú, ale ktoré nie sú priamo škodlivé.
- **Sledovacie súbory cookies** sa môžu považovať za druh spywaru, pretože tieto malé súbory, uložené v internetovom prehliadači a automaticky posielané na „hlavnú“ internetovú stránku pri jej opätovnej návšteve, môžu obsahovať údaje ako je vaša história surfovania na internete a ďalšie podobné informácie.
- **Zneužitie** je škodlivý kód, ktorý využíva trhlínu alebo zraniteľnosť operačného systému, internetového prehliadača alebo iného základného programu.
- **Phishing** je pokus o získanie citlivých osobných údajov predstieraným zastupovaním dôveryhodnej a všeobecne známej organizácie. Potenciálne obeť sú často kontaktované prostredníctvom hromadných e-mailov, v ktorých sa od nich požaduje napr. aby si aktualizovali informácie o bankových účtoch. Na tento účel majú kliknúť na uvedený odkaz, ktorý potom vedie na falošnú internetovú stránku banky.
- **Hoax** je hromadný e-mail, ktorý obsahuje nebezpečné, alarmujúce alebo jednoducho len otravné a neúčinné informácie. Na šírenie väčšiny vyššie uvedených hrozieb sa používajú podvodné e-mailové správy typu hoax.
- **Škodlivé internetové stránky** sú napokon tie, ktoré úmyselne inštalujú škodlivý softvér do počítača a haknuté stránky robia to isté, ibaže ide o legítimne internetové stránky, ktoré boli zneužitú na infikovanie počítača návštevníkov.

Na účely ochrany pred všetkými týmito rôznymi druhmi hrozieb má AVG tieto špecializované súčasti:

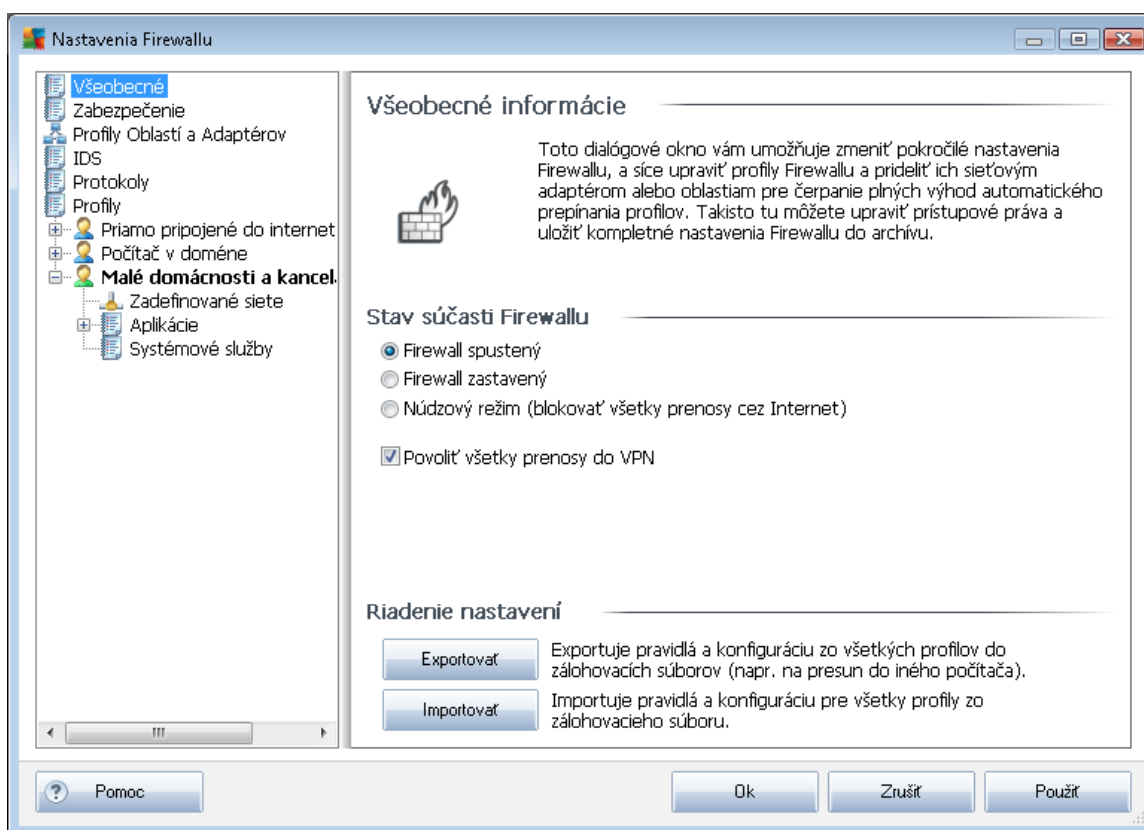
- **[Anti-Virus](#)** na ochranu počítača pred vírusmi.
- **[Anti-Spyware](#)** na ochranu počítača pred spywarom.
- **[Webový štít](#)** na ochranu pred vírusmi a spywarom počas surfovania na internete.
- **[LinkScanner](#)** na ochranu pred ostatnými online hrozbami uvedenými v tejto kapitole.

10. Nastavenia súčasti Firewall

Konfigurácia [Firewallu](#) sa otvorí v novom okne, kde môžete vo viacerých dialógových oknách nastaviť veľmi pokročilé parametre komponentu. **Zmena rozšírenej konfigurácie je však určená len pre odborníkov a skúsených používateľov.**

10.1. Všeobecné informácie

Dialógové okno **Všeobecné informácie** je rozdelené na dve časti:



Stav súčasti Firewall

Časť **Stav súčasti Firewall** umožňuje prepnúť stav súčasti [Firewall](#) vtedy, keď nastane potreba:

- **Súčasť Firewall zapnutá** – vyberte túto možnosť, ak chcete povoliť komunikáciu tým aplikáciám, ktoré sú nastavené ako „povolené“ v skupine pravidiel definovaných vo vybranom [profile súčasti Firewall](#)
- **Súčasť Firewall vypnutá** – táto možnosť úplne vypne [Firewall](#), všetky sieťové prenosy sa povolia, ale nebudú sa kontrolovať!
- **Núdzový režim (blokovat' všetky prenosy na internete)** – vyberte túto možnosť, ak chcete blokovat' prenosy na všetkých sieťových portoch; súčasť [Firewall](#) zostane spustená, ale

všetky prenosy v sieti sa zastavia.

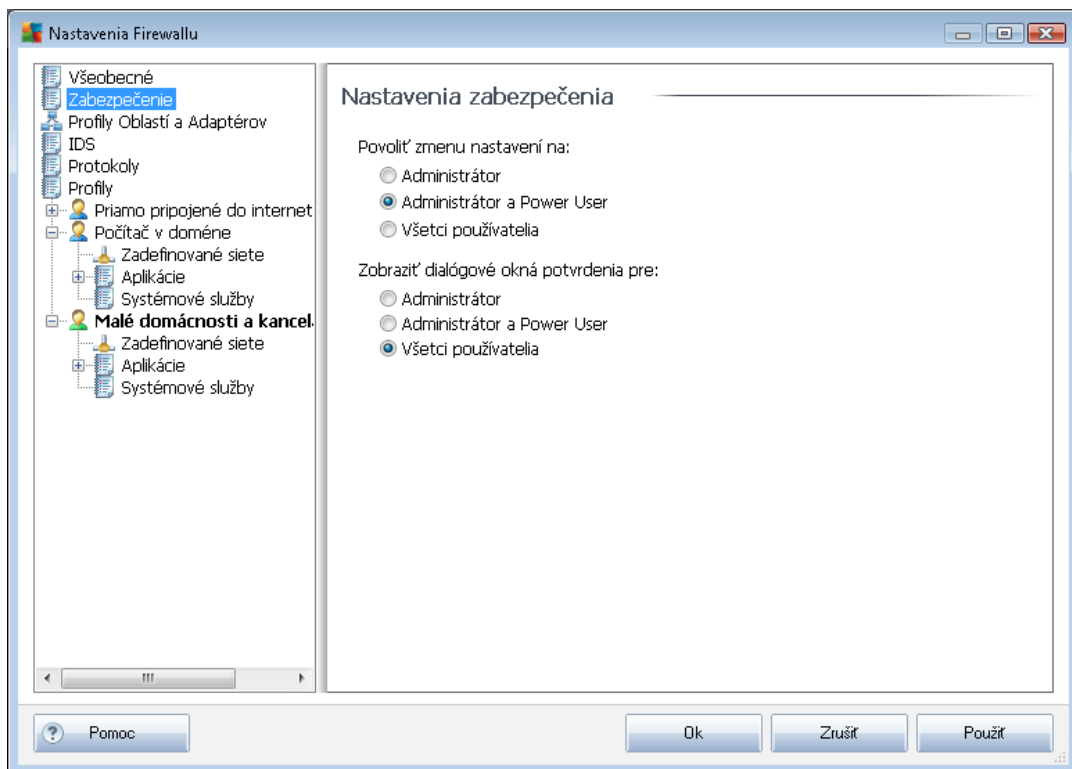
- **Povolit' všetky prenosy do VPN** – ak používate pripojenie VPN (virtuálna privátna sieť), napr. na pripojenie sa do kancelárie z domu, odporúčame vám, aby ste začiarkli toto okienko. **AVG Firewall** automaticky preskúma vaše sieťové adaptéry a vyhľadá tie, ktoré sú používané pre pripojenie VPN, a umožní všetkým aplikáciám pripájať sa k cieľovej sieti (platí len pre aplikácie bez prideleného špeciálneho pravidla súčasti Firewall). V štandardnom operačnom systéme s bežnými sieťovými adaptérmí, tento jednoduchý postup vám ušetrí prácu s nastavením podrobného pravidla pre každú aplikáciu, ktorú používate v sieti VPN.

Poznámka: Aby pripojenie VPN vôbec fungovalo, je potrebné povoliť komunikáciu na týchto systémových protokoloch: GRE, ESP, L2TP, PPTP. Robí sa to v dialógovom okne Systémové služby.

Správa nastavení

Časť **Riadenie nastavení** umožňuje **exportovať** a **importovať** konfiguráciu súčasti **Firewall**, t. j. exportovať definované pravidlá a nastavenia súčasti **Firewall** do zálohovacích súborov, alebo importovať celý zálohovací súbor.

10.2. Zabezpečenie



V dialógovom okne **Nastavenia zabezpečenia** môžete zadať všeobecné pravidlá správania **Firewallu** bez ohľadu na zvolený profil:

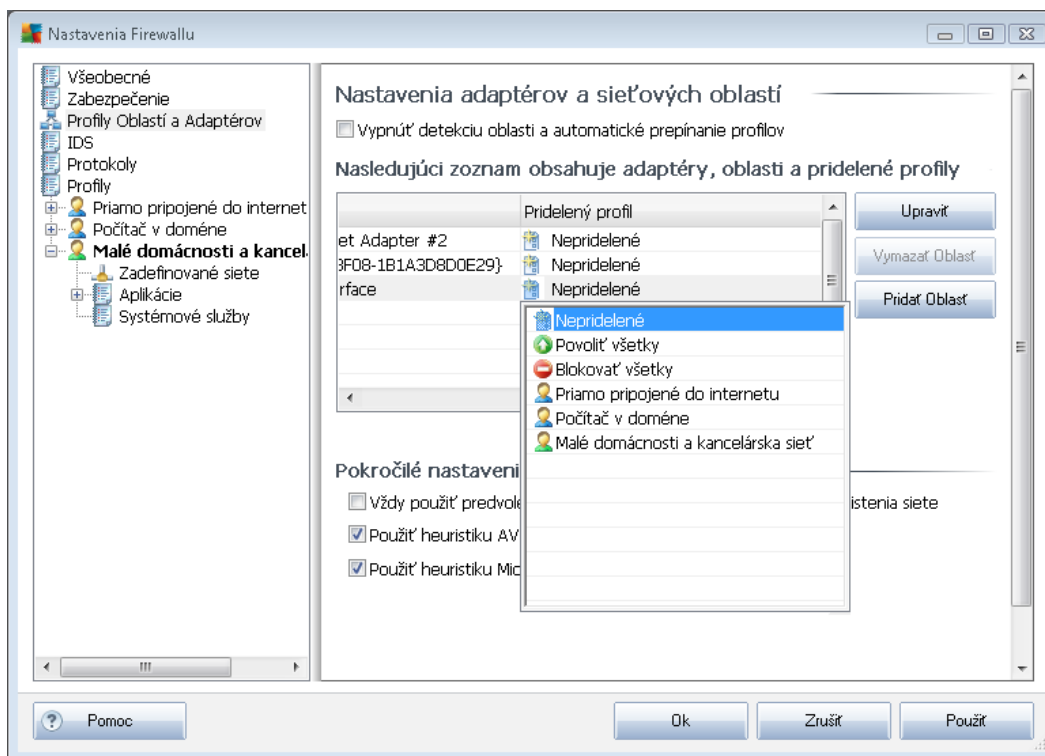
- **Povolit' zmenu nastavení komu** - zadajte, kto má právo meniť konfiguráciu [Firewallu](#)
- **Zobrazit' dialógové okno potvrdenia pre** - zadajte, komu by sa mali zobrazovať dialógové okná potvrdenia (dialógové okná, ktoré si vyžadujú rozhodnutie v situácii, ktorá nie je pokrytá zadaným pravidlom [Firewallu](#))

V obidvoch prípadoch môžete pridať špecifické právo jednej z nasledovných skupín používateľov.

- **Administrátor** - kompletne riadi počítač a má právo zaraďovať používateľov do skupín so špecificky definovanými oprávneniami
- **Administrátor a Power User** - administrátor môže zaradiť používateľa do danej skupiny (Power User) a definovať oprávnenia členov skupiny
- **Všetci používatelia** - ostatní používatelia, ktorí nie sú zaradení do žiadnej skupiny

10.3. Profily oblastí a sieťových kariet

Dialógové okná **Nastavenia sieťových kariet a sieťových oblastí** sa používajú na zmenu nastavení súvisiacich s pridelovaním definovaných profilov konkrétnym sieťovým kartám a súvisiacim sieťam:



- **Vypnúť detegovanie oblastí a automatické prepínanie profilů** – každému typu sieťového rozhrania resp. každej oblasti môžete pridať jeden definovaný profil. Ak nechcete definovať konkrétne profily, potom sa použije jeden spoločný profil. Ak sa však

rozhodnete rozlišovať profily a prideliť ich konkrétnym sieťovým kartám a oblastiam a neskôr, z nejakého dôvodu, budete chcieť túto konfiguráciu dočasne prepnúť, označte možnosť **Vypnúť detekciu oblastí a automatické prepínanie profilov**.

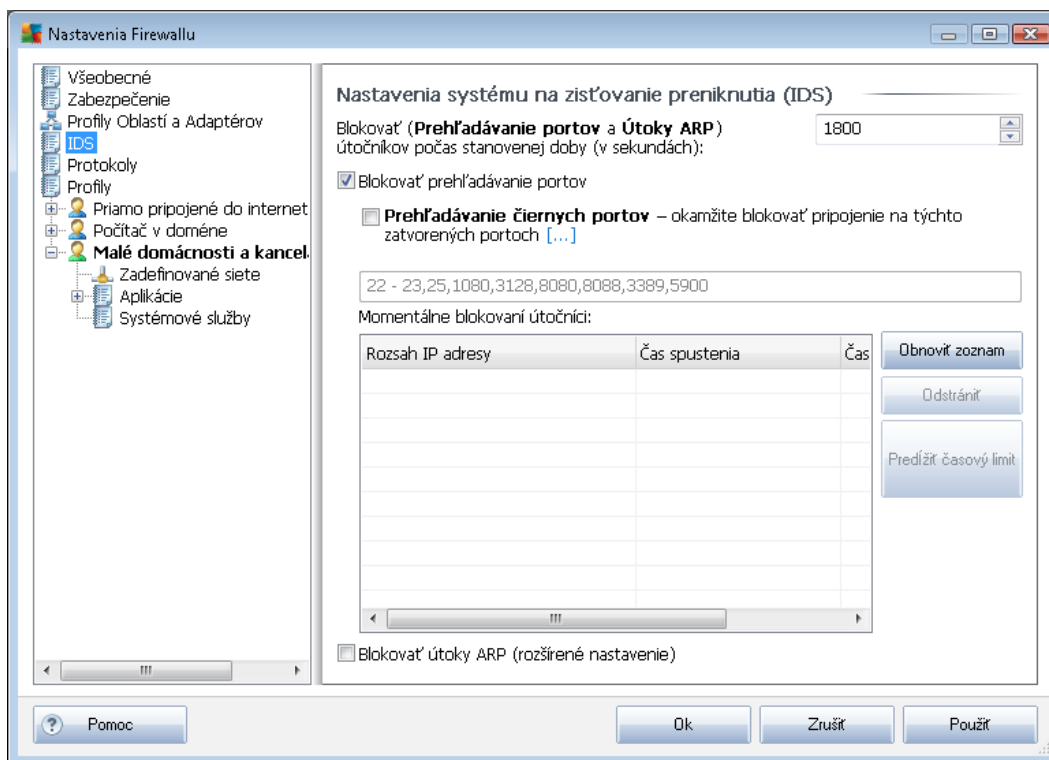
- **Zoznam sieťových kariet, oblastí a pridelených profilov** – v tomto zozname sa nachádza prehľad zistených sieťových kariet a oblastí. Každý tejto položke môžete prideliť konkrétny profil z ponuky definovaných profilov. Na otvorenie tejto ponuky kliknite na príslušnú položku v zozname sieťových kariet a vyberte profil.

Rozšírené nastavenia

- o **Vždy použiť predvolený profil a neotvoriť okno zistenia novej sieťovej oblasti** – vždy, keď sa počítač pripojí k novej sieti, vás [Firewall](#) upozorní a otvorí dialógové okno, ktoré vám umožní vybrať typ sieťového pripojenia, a prideliť jej [profil súčasti Firewall](#). Ak si neželáte, aby sa toto dialógové okno otváralo, začiarňte toto okienko.
- o **Používať heuristiku spoločnosti AVG na zisťovanie nových sietí** – zapína zhromažďovanie informácií o novej zistenej sieti pomocou vlastného mechanizmu produktu AVG (táto možnosť je však dostupná len pod operačným systémom VISTA a novšími).
- o **Používať heuristiku spoločnosti Microsoft na zisťovanie nových sietí** – zapína zhromažďovanie informácií o novej zistenej sieti od služby operačného systému Windows (táto možnosť je dostupná len pod operačným systémom Windows Vista a novšími).

10.4. IDS

Systém na detekciu preniknutia je špeciálna funkcia na analýzu správania, ktorej účelom je identifikovať a blokovat' podozrivé pokusy o komunikáciu na konkrétnych portoch počítača. Parametre funkcie IDS sa nastavujú v tomto rozhraní:



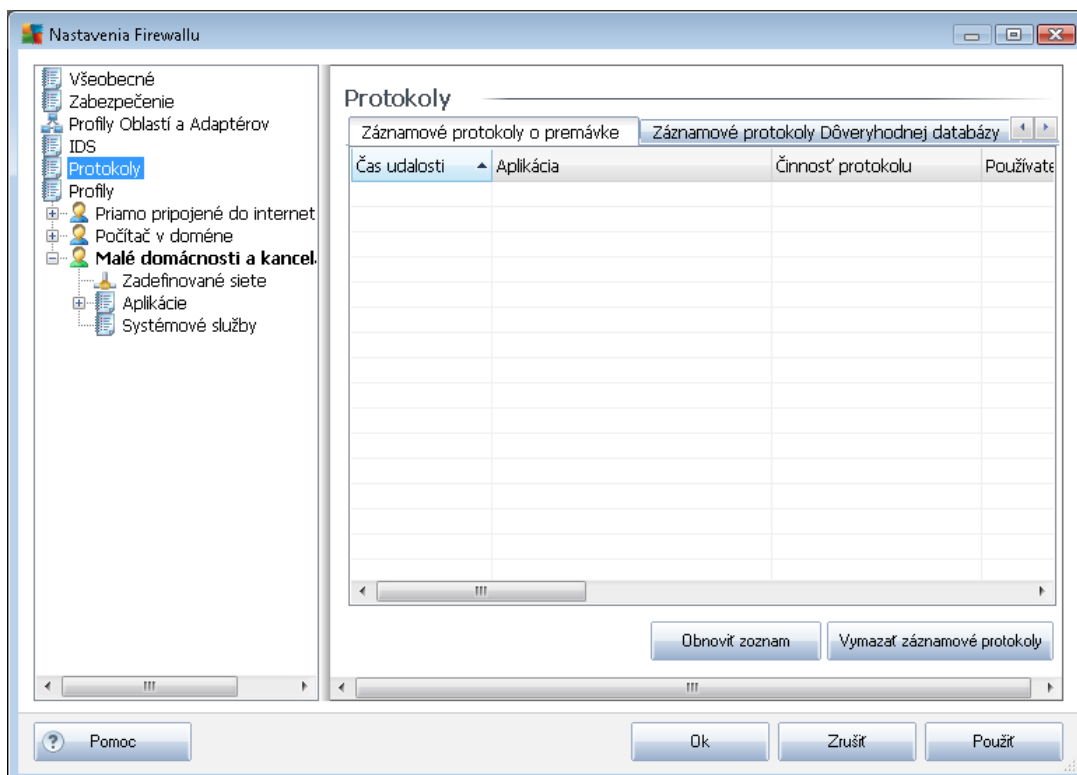
V dialógovom okne **Nastavenia systému na zisťovanie preniknutia (IDS)** sa nachádzajú tieto možnosti konfigurácie:

- **Blokovať útočníkov počas stanovenej doby** – umožňuje nastaviť dobu v sekundách, počas ktorej bude port blokovaný vždy, keď sa na ňom deteguje podozrivý pokus o komunikáciu. Štandardne je nastavený časový interval 1 800 sekúnd (30 minút).
- **Blokovať kontrolu portov** – začiarknutím tohto okienka sa zablokuje pokusy o komunikáciu na všetkých portoch TCP a UDP prichádzajúce do počítača zvonka. Pre každé takéto pripojenie sa povolí päť pokusov a šiesty sa zablokuje.
 - o **Kontrola čiernych portov** – začiarknutím tohto okienka sa okamžite zablokuje pokusy o komunikáciu na portoch uvedených v textovom poli nižšie. Jednotlivé porty alebo intervaly portov sa musia oddeliť čiarkou. Program má preddefinovaný zoznam odporúčaných portov pre prípad, ak by ste chceli túto funkciu používať.
 - o **Momentálne blokovaní útočníci** – v tejto časti sa nachádza zoznam pokusov o komunikáciu, ktoré sú momentálne blokované súčasťou **Firewall**. Celá história blokovaných pokusov sa nachádza v dialógovom okne **Protokoly** (na karte **Protokoly kontroly portov**).
- **Blokovať útoky ARP** zapne blokovanie špeciálnych druhov pokusov o komunikáciu v miestnej sieti, ktoré boli detegované funkciou **IDS** ako potenciálne nebezpečné. Použije sa čas nastavený v možnosti **Blokovať útočníkov počas stanovenej doby**. Odporúča sa, aby túto funkciu používali len skúsení používatelia, ktorí sú oboznámení s typom a úrovňou rizika používanej miestnej siete.

Ovládacie tlačidlá

- **Obnoviť zoznam** – stlačením tohto tlačidla sa aktualizuje zoznam (vrátane všetkých najnovších blokových pokusov)
- **Odstrániť** – stlačením tohto tlačidla sa zruší vybrané blokovanie
- **Predĺžiť časový limit** – stlačením sa predĺži doba, počas ktorej sa vybraný pokus blokuje. Otvorí sa nové dialógové okno s rozšírenými možnosťami, ktoré umožňuje nastaviť konkrétny čas a dátum alebo neobmedzené trvanie.

10.5. Protokoly



Dialógové okno **Protokoly** umožňuje zobraziť zoznam všetkých zaznamenaných akcií a udalostí súčasti **Firewall** a obsahuje podrobný opis súvisiacich parametrov (čas udalosti, názov aplikácie, príslušnú protokolovú činnosť, názov používateľa, PID, smer prenosu, typ protokolu, čísla vzdialených a miestnych portov a pod.) na štyroch kartách:

- **Protokoly prenosu** – zobrazí informácie o činnosti všetkých aplikácií, ktoré sa pokúsili pripojiť k sieti.
- **Protokoly Dôveryhodnej databázy** – Dôveryhodná databáza je interná databáza AVG, ktorá zhromažďuje informácie o certifikovaných a dôveryhodných aplikáciách, ktorým sa môže vždy povoliť komunikácia online. Pri prvom pokuse novej aplikácie o pripojenie k sieti



(t. j. ak doposiaľ nebolo vytvorené pravidlo súčasti Firewall súvisiace s touto aplikáciou) je potrebné zistiť, či sa má povoliť sieťová komunikácia príslušnej aplikácie. AVG najskôr nahliadne do *Dôveryhodnej databázy* a ak je v nej aplikácia uvedená, potom sa jej automaticky povolí prístup k sieti. Až potom, a pod podmienkou, že sa v databáze nenachádzajú informácie o tejto aplikácii, sa zobrazí dialógové okno, v ktorom sa vás program opýta, či chcete povoliť aplikácii prístup k sieti.

- **Protokoly kontroly portov** – obsahujú záznamy o všetkých aktivitách [Systému na detekciu preniknutia](#).
- **Protokoly ARP** – záznamy o blokovaní špeciálnych druhov pokusov o komunikáciu v miestnej sieti (možnosť [Blokovať útoky ARP](#)) detegovaných [Systémom na detekciu preniknutia](#) ako potenciálne nebezpečné.

Ovládacie tlačidlá

- **Obnoviť zoznam** – všetky zaznamenané parametre sa dajú usporiadať podľa vybraného atribútu: chronologicky (*dátumy*) alebo abecedne (*ostatné stĺpce*) – stačí kliknúť na hlavičku príslušného stĺpca. Použite tlačidlo **Obnoviť zoznam** na aktualizovanie práve zobrazených informácií.
- **Vyprázdniť zoznam** – vymaže všetky záznamy v tabuľke.

10.6. Profily

V dialógovom okne **Nastavenia profilov** sa nachádza zoznam všetkých dostupných profilov.



Všetky ostatné [profily](#) sa potom dajú editovať priamo v tomto dialógovom okne pomocou týchto ovládacích tlačidiel:

- **Aktivovať profil** – toto tlačidlo nastaví vybraný profil ako činný, čo znamená, že [Firewall](#) použije konfiguráciu vybraného profilu na ovládanie prenosov v sieti.
- **Kopírovať profil** – vytvorí identickú kópiu vybraného profilu; neskôr môžete editovať a premenovať kópiu na vytvorenie nového profilu na základe vybraného pôvodného profilu.
- **Prenenovať profil** – umožňuje definovať nový názov vybraného profilu.
- **Vymazať profil** – vymaže vybraný profil zo zoznamu.
- **Prepnúť na Dôveryhodnú databázu** – môžete nastaviť, aby sa pre zvolený profil použili informácie Dôveryhodnej databázy (Dôveryhodná databáza je interná databáza spoločnosti AVG, ktorá zhromažďuje informácie o dôveryhodných a certifikovaných aplikáciách, ktorým môže byť vždy povolené komunikovať online.).
- **Exportovať profil** – zaznamená konfiguráciu vybraného profilu v súbore, ktorý sa uloží a bude môcť použiť na neskoršie účely.
- **Importovať profil** – konfiguruje nastavenia vybraného profilu na základe údajov



exportovaných zo zálohovacieho súboru konfigurácie.

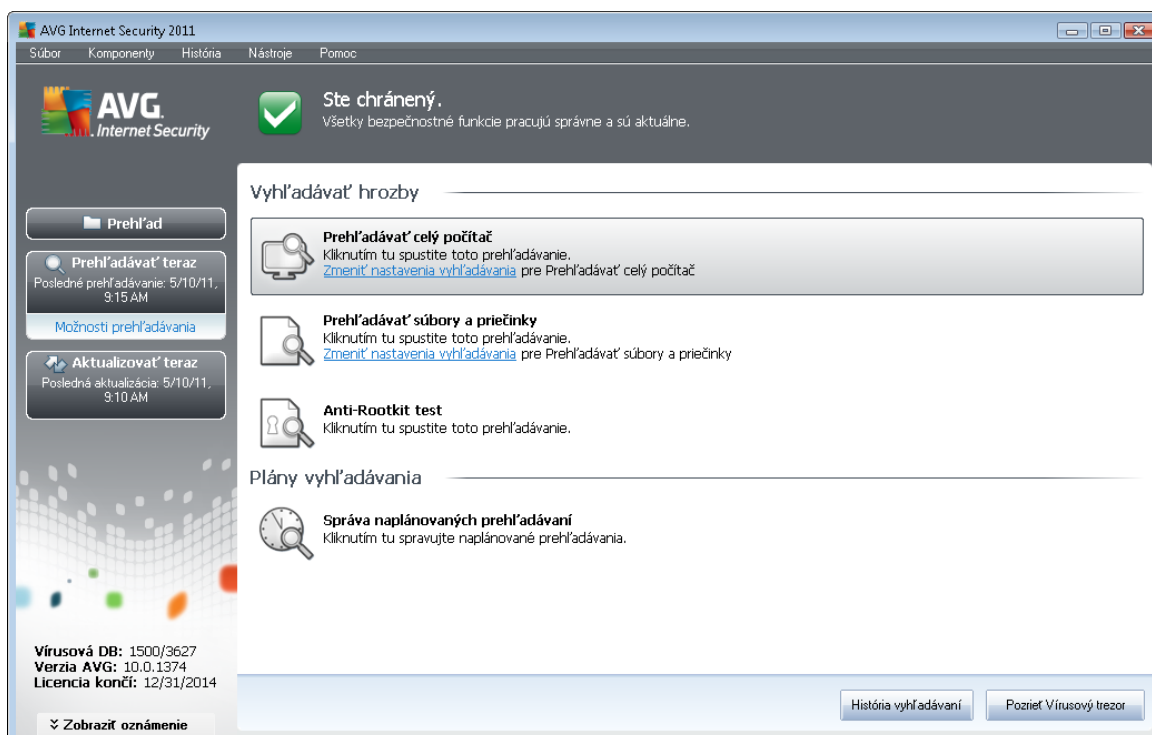
V spodnej časti tohto dialógového okna sa nachádza opis profilu, ktorý je momentálne vybraný vo vyššie uvedenom zozname.

Na základe počtu definovaných profilov, ktoré sa nachádzajú v zozname v dialógovom okne **Profil**, sa zmení štruktúra ľavej navigačnej ponuky. Každý definovaný profil vytvorí špecifickú vetvu pod položkou **Profil**. Jednotlivé profily sa potom dajú editovať v týchto dialógových oknách (sú rovnaké pre všetky profily):

11. Kontrola AVG

Prehľadávanie predstavuje rozhodujúcu časť funkcionality produktu **AVG Internet Security 2011**. Umožňuje spúšťať testy na požiadanie a [naplávať ich pravidelné spúšťanie](#) vo vhodnom čase.

11.1. Rozhranie kontroly



Rozhranie kontroly programom AVG sa otvára [rýchlým odkazom](#) ***Možnosti kontroly***. Kliknutím na tento odkaz otvorte dialógové okno ***Kontrola hrozieb***. V tomto dialógovom okne sa nachádzajú tieto položky:

- prehľad [preddefinovaných kontrol](#) – tri druhy kontrol definované dodávateľom softvéru sú pripravené na použitie okamžitým výberom alebo ako naplánované:
 - o [Kontrola celého počítača](#)
 - o [Kontrola špecifických súborov alebo priečinkov](#)
 - o [Kontrola súčasťou Anti-Rootkit](#)
-  [plánovanie kontrol](#) – tu môžete definovať nové testy a vytvoriť nové plány podľa potreby.

Ovládacie tlačidlá

V testovacom rozhraní sa nachádzajú tieto tlačidlá:



- **História kontrol** – otvorí dialógové okno [Prehľad výsledkov kontrol](#) s celou históriou kontrol.
- **Otvoriť Vírusový trezor** – otvorí nové okno s [Vírusovým trezorom](#), t. j. miesto, na ktorom sú uložené v karanténe detegované infekcie.

11.2. Preddefinované kontroly

Jednou z hlavných funkcií produktu **AVG Internet Security 2011** je kontrola na požiadanie. Testy na požiadanie sú určené na kontrolu rôznych častí počítača pri každom podozrení na možný výskyt vírusovej infekcie. Odporúčame vám, aby ste robili tieto testy pravidelne, aj keď si myslíte, že sa v počítači nenájde žiaden vírus.

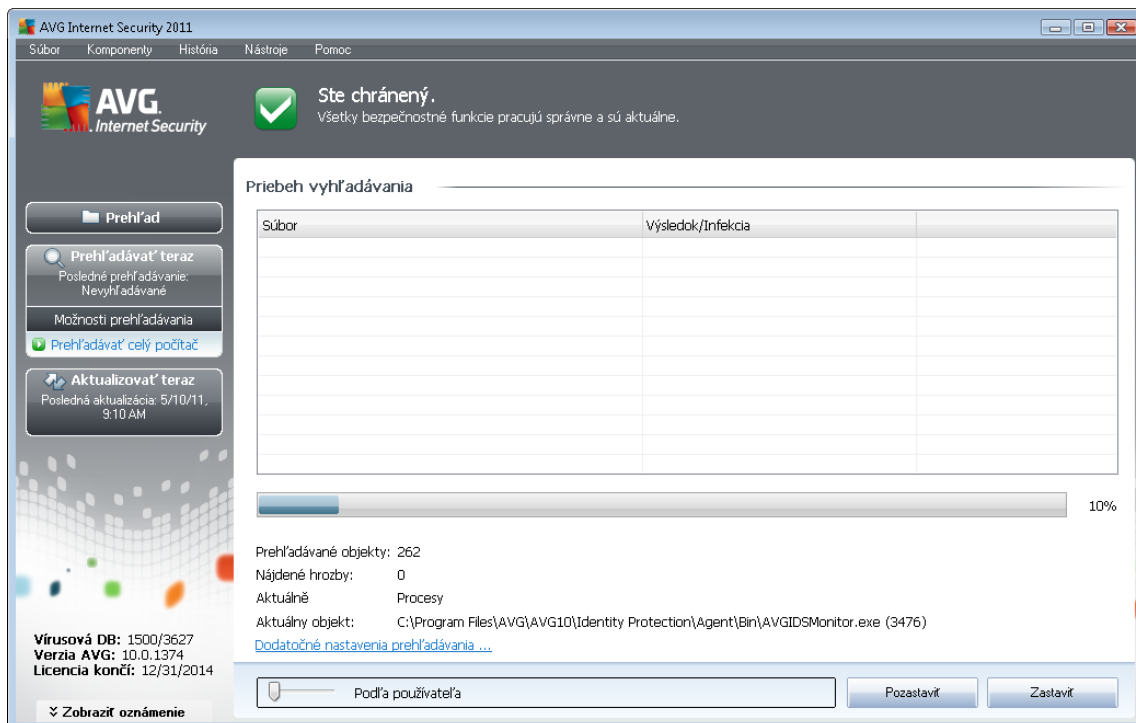
V produkte **AVG Internet Security 2011** sa nachádzajú tieto typy kontrol prednastavené dodávateľom softvéru:

11.2.1. Kontrola celého počítača

Kontrola celého počítača – skontroluje možné infekcie resp. potenciálne nežiaduce programy v celom počítači. Tento test bude kontrolovať všetky pevné disky počítača, deteguje vírusy a vylieči všetky nájdené vírusy alebo ich odstráni do [Vírusového trezora](#). Odporúčame vám, aby ste naplánovali program takým spôsobom, aby sa kontrola celého počítača spustilo najmenej raz za týždeň.

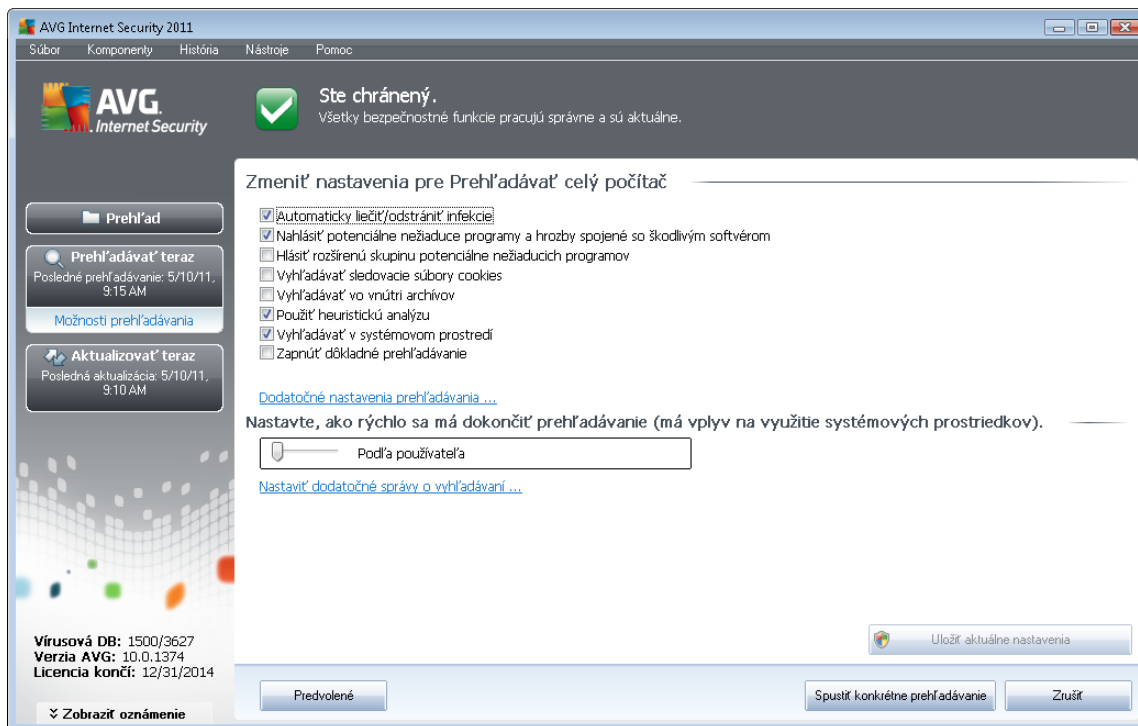
Spustenie kontroly

Kontrola celého počítača sa spúšťa priamo v [rozhraní kontroly](#) kliknutím na ikonu kontroly. Pre tento typ kontroly nie je potrebné konfigurovať žiadne ďalšie konkrétne nastavenia, kontrola sa spustí ihneď v dialógovom okne **Prebieha kontrola** (pozri snímku obrazovky). V prípade potreby môžete kontrolu dočasne prerušiť (tlačidlo **Pozastaviť**) alebo zrušiť (tlačidlo **Zastaviť**).



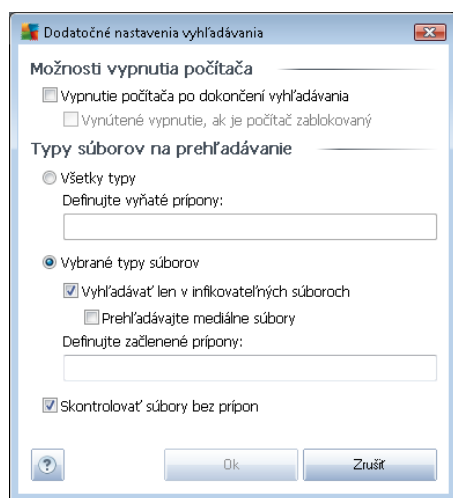
Zmena konfigurácie kontroly

Program umožňuje editovať vopred definované predvolené nastavenia funkcie **Kontrola celého počítača**. Kliknutím na odkaz **Zmeniť nastavenia kontroly** otvorte dialógové okno **Zmena nastavení kontroly celého počítača** (otvára sa v [rozhraní kontroly](#) pomocou odkazu **Zmeniť nastavenia kontroly funkcie Kontrola celého počítača**). **Odporúčame vám, aby ste zachovali predvolené nastavenia, ak nemáte vážny dôvod na ich zmenu!**



- **Parametre kontroly** – v zozname parametrov kontroly môžete zapnúť alebo vypnúť konkrétne parametre podľa potreby:
 - o **Automaticky liečiť/odstrániť infekciu** (štandardne zapnuté) – ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
 - o **Hlásiť potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté) – začiarknite toto okienko, ak chcete zapnúť súčasť [Anti-Spyware](#) a kontrolovať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
 - o **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – začiarknite toto okienko, ak sa má detegovať rozšírená skupina [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovat' dobré programy, a preto je táto funkcia štandardne vypnutá.
 - o **Kontrolovať sledovacie súbory cookies** (štandardne vypnuté) – tento parameter súčasť [Anti-Spyware](#) zapína funkciu na detegovanie súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).

- o **Kontrolovať vo vnútri archívov** (štandardne vypnuté) – tento parameter určuje, že sa majú počas kontroly overovať všetky súbory uložené vo vnútri archívov, napr. ZIP, RAR...
 - o **Používať heuristiku** (štandardne zapnuté) – heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detegovanie vírusov počas kontroly.
 - o **Kontrolovať systémové prostredie** (štandardne zapnuté) – počas kontroly sa budú kontrolovať aj systémové oblasti počítača.
 - o **Zapnúť dôkladnú kontrolu** (štandardne vypnuté) – v určitých situáciách (napr. pri podozrení na infikovanie počítača) môžete začiarknutím tohto okienka zapnúť algoritmus najdôkladnejšej kontroly, ktorá kontroluje aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Ďalšie nastavenia kontroly** – tento odkaz otvorí nové dialógové okno **Ďalšie nastavenia kontroly**, ktoré sa používa na nastavenie týchto parametrov.

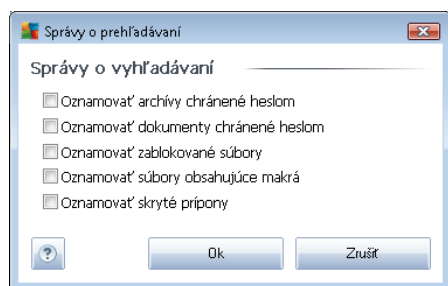


- o **Možnosť vypnutia počítača** – rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútené vypnutie počítača, keď je zamknutý**).
- o **Definovať typy súborov pre kontrolu** – ďalej môžete rozhodnúť, či sa majú kontrolovať:
 - **Všetky typy súborov** s možnosťou definovať výnimky kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.
 - **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory), vrátane mediálnych súborov (video, audio

súborov – ak necháte toto okienko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete nastaviť (podľa prípony), ktoré súbory sa majú kontrolovať vždy.

➤ Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

- **Nastaviť rýchlosť dokončenia kontroly** – pomocou posúvača zmeňte prioritu procesu kontroly. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „podľa používateľa“. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie počítačových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).
- **Vytvoriť ďalšie správy o kontrole** – odkaz otvorí nové dialógové okno **Správy o kontrole**, v ktorom môžete určiť, aké typy možných nálezov sa majú uviesť v správach:



Upozornenie: Tieto nastavenia kontroly sa zhodujú s parametrami novo definovanej kontroly; pozri informácie v kapitole [Kontrola programom AVG/Plánovanie kontroly/Ako kontrolovať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **Kontrola celého počítača**, potom môžete vaše nové nastavenie uložiť ako predvolenú konfiguráciu, ktorá sa použije pre všetky ďalšie kontroly celého počítača.

11.2.2. Kontrola špecifických súborov alebo priečinkov

Kontrola špecifických súborov alebo priečinkov – kontrolovať sa budú len vami vybrané oblasti počítača (vybrané priečinky, pevné disky, diskety, disky CD a pod.). Priebeh kontroly pri detegovaní vírusu a jeho liečba sú rovnaké ako pri kontrole celého počítača: [všetky nájdené vírusy sa vyliečia alebo odstránia do Vírusového trezora](#). Kontrolu špecifických súborov alebo priečinkov môžete použiť na nastavenie vlastných testov a ich plánov v závislosti od konkrétnych potrieb.

Spustenie kontroly

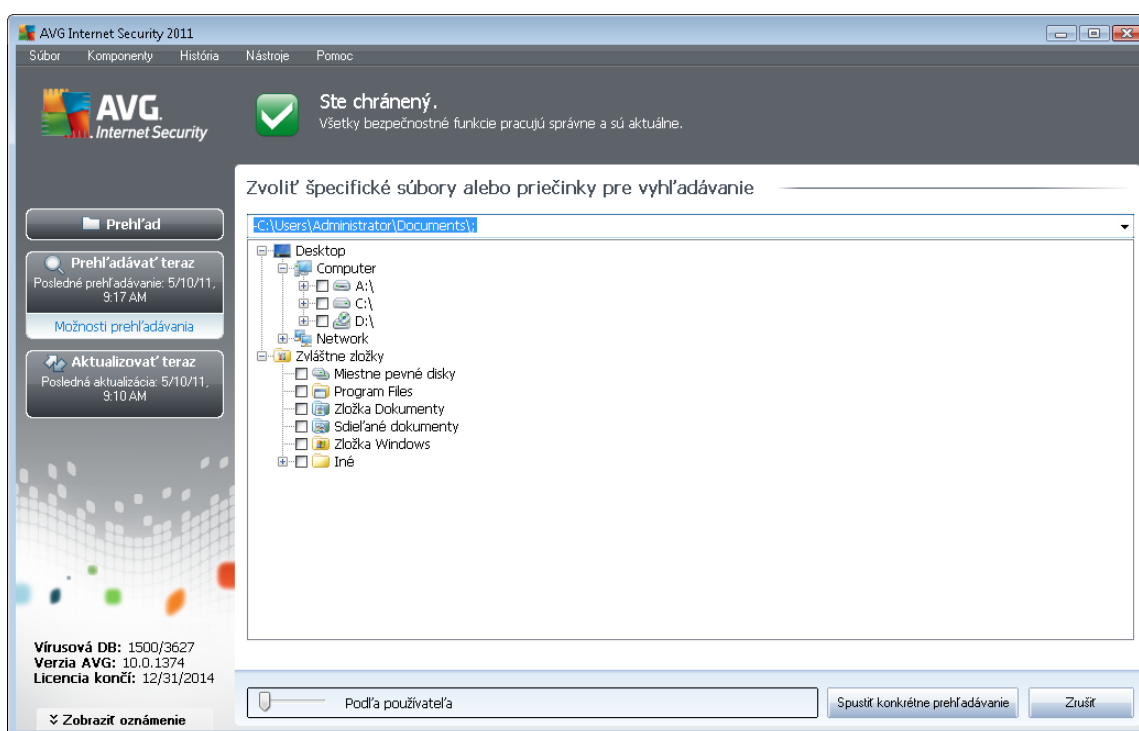
Kontrolu špecifických súborov alebo priečinkov môžete spustiť priamo v [rozhraní kontroly](#) kliknutím na ikonu kontroly. Otvorí sa nové dialógové okno s názvom **Výber konkrétnych súborov alebo priečinkov na kontrolu**. V stromovej štruktúre počítača vyberte tie priečinky, ktoré chcete



kontrolovať. Cesta ku každému vybranému priečinku sa vygeneruje automaticky a objaví sa v textovom okne v hornej časti tohto dialógového okna.

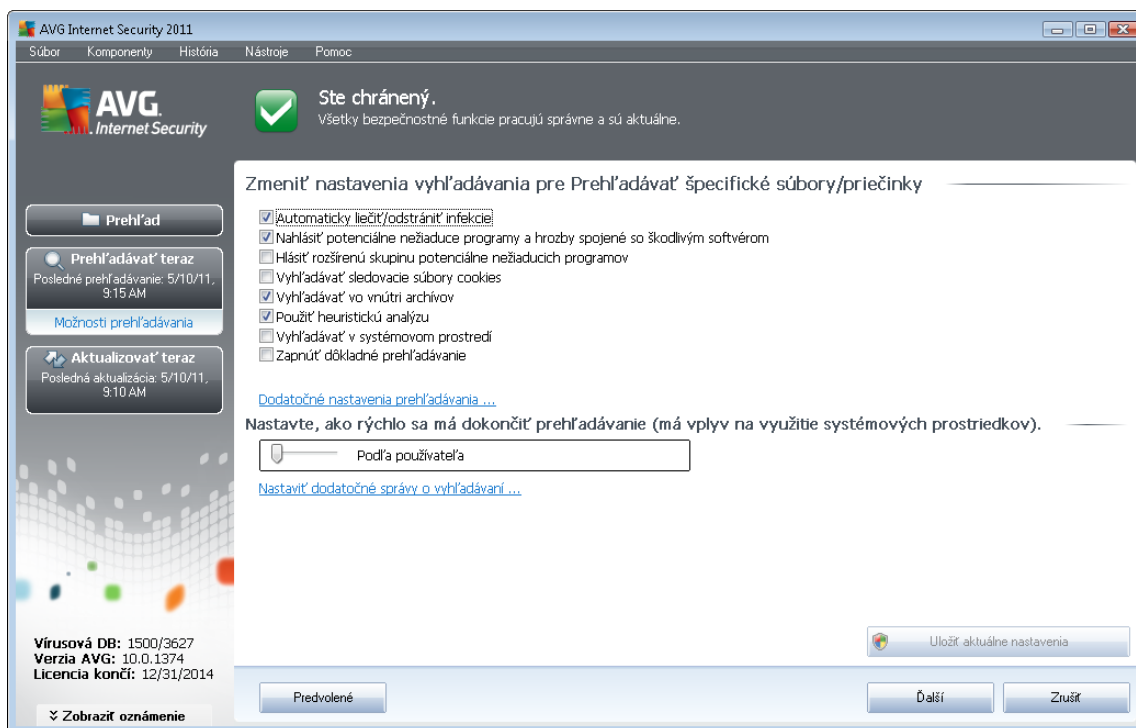
Rovnako môžete nastaviť kontrolu konkrétneho priečinka a zároveň vylúčiť všetky jeho podpriečinky z kontroly; v tom prípade vložte znak mínus „-“ pred automaticky vygenerovanú cestu (*pozri snímku obrazovky*). Na vylúčenie celého priečinka z kontroly použite parameter „!“.

Napokon, ak chcete spustiť kontrolu, stlačte tlačidlo **Spustiť kontrolu**; samotný proces kontroly sa v podstate zhoduje s [kontrolou celého počítača](#).



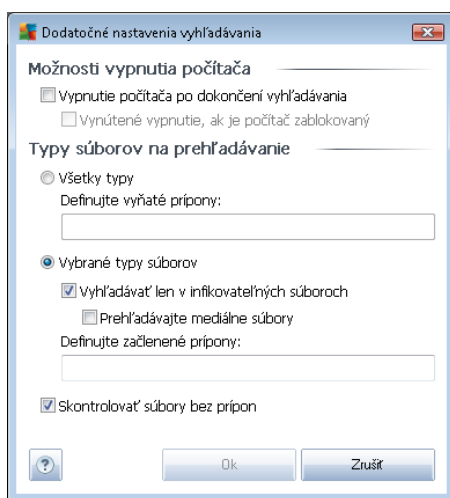
Zmena konfigurácie kontroly

Program umožňuje zmeniť preddefinované predvolené nastavenia funkcie na **kontrolu konkrétnych súborov alebo priečinkov**. Kliknutím na odkaz **Zmeniť nastavenia kontroly** otvorte dialógové okno **Zmena nastavení kontroly konkrétnych súborov alebo priečinkov**. **Odporúčame vám, aby ste zachovali predvolené nastavenia, ak nemáte vážny dôvod na ich zmenu!**



- **Parametre kontroly** – v zozname parametrov kontroly môžete zapnúť alebo vypnúť konkrétne parametre podľa potreby:
 - o **Automaticky liečiť/odstrániť infekciu** (štandardne zapnuté) – ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
 - o **Hlásiť potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté) – začiarknite toto okienko, ak chcete zapnúť súčasť [Anti-Spyware](#) a kontrolovať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
 - o **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté) – začiarknite toto okienko, ak sa má detegovať rozšírená skupina [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovat dobré programy, a preto je táto funkcia štandardne vypnutá.
 - o **Kontrolovať sledovacie súbory cookies** (štandardne vypnuté) – tento parameter súčasť [Anti-Spyware](#) zapína funkciu na detegovanie súborov cookies (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).

- o **Kontrolovať vo vnútri archívov** (štandardne zapnuté) – tento parameter určuje, že sa majú počas kontroly overovať všetky súbory uložené vo vnútri archívov, napr. ZIP, RAR...
 - o **Používať heuristiku** (štandardne vypnuté) – heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detegovanie vírusov počas kontroly.
 - o **Kontrolovať systémové prostredie** (štandardne vypnuté) – počas kontroly sa budú overovať aj systémové oblasti počítača.
 - o **Zapnúť dôkladnú kontrolu** (štandardne vypnuté) – v určitých situáciách (napr. pri podozrení na infikovanie počítača) môžete začiarknutím tohto okienka zapnúť algoritmus najdôkladnejšej kontroly, ktorý skontroluje aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Ďalšie nastavenia kontroly** – tento odkaz otvorí nové dialógové okno **Ďalšie nastavenia kontroly**, ktoré sa používa na nastavenie týchto parametrov.

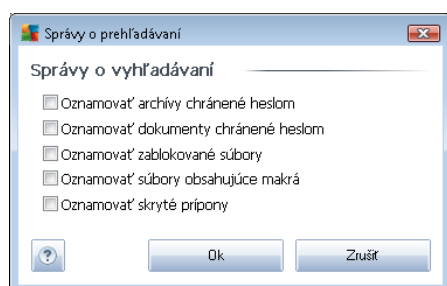


- o **Možnosti vypnutia počítača** – rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútené vypnutie počítača, keď je zamknutý**).
- o **Definovať typy súborov na kontrolu** – ďalej môžete rozhodnúť, či sa majú kontrolovať:
 - **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.
 - **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory), vrátane mediálnych súborov (video, audio

súborov – ak necháte toto okienko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete nastaviť (podľa prípony), ktoré súbory sa majú kontrolovať vždy.

- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

- **Priorita procesu kontroly** – použite posúvač na zmenu priority procesu kontroly. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „podľa používateľa“. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujímá vás, ako dlho bude kontrola trvať), alebo rýchlejšie s vyššími nárokmi na využívanie počítačových zdrojov (napr. keď sa počítač dočasne nepoužíva).
- **Vytvoriť ďalšie správy o kontrole** – odkaz otvorí nové dialógové okno **Správy o kontrole**, ktoré umožňuje nastaviť typy možných nálezov, ktoré sa majú hlásiť:



Upozornenie: Tieto nastavenia kontroly sa zhodujú s parametrami novo definovanej kontroly; pozri informácie v kapitole [Kontrola programom AVG/Plánovanie kontroly/Ako kontrolovať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **Kontrola špecifických súborov alebo priečinkov**, potom môžete uložiť vlastné nastavenia ako predvolenú konfiguráciu, ktorá sa použije pre všetky ďalšie kontroly konkrétnych súborov alebo priečinkov. Táto konfigurácia sa zároveň použije ako šablóna pre všetky vami novo naplánované kontroly ([všetky nastavené kontroly vychádzajú zo súčasnej konfigurácie kontroly vybraných súborov alebo priečinkov](#)).

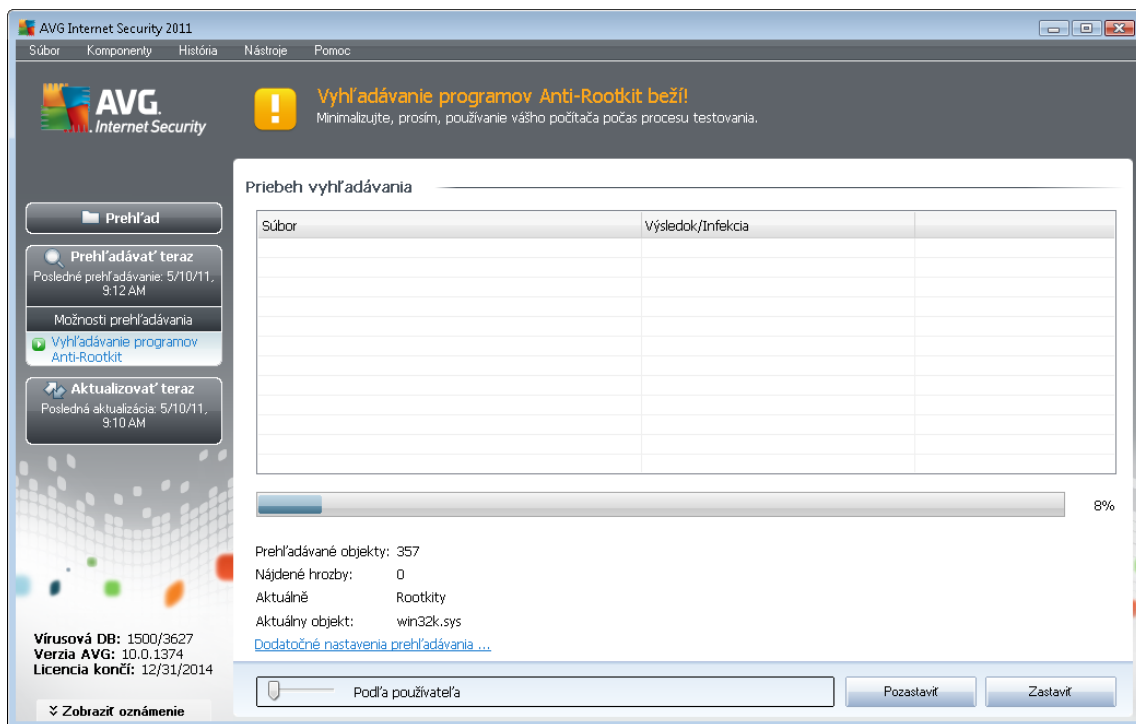
11.2.3. Kontrola súčasťou Anti-Rootkit

Kontrola súčasťou Anti-Rootkit skontroluje počítač a zisťuje prítomnosť potenciálnych rootkitov (programov a technológií, ktoré dokážu zakryť činnosť škodlivého programu v počítači). Keď program deteguje rootkit, nemusí to nevyhnutne znamenať, že je počítač infikovaný. V niektorých prípadoch sa môžu určité ovládače alebo časti bežných aplikácií nesprávne označiť ako rootkity.

Spustenie kontroly

Kontrola súčasťou Anti-Rootkit sa dá spustiť priamo v [rozhraní kontroly](#) kliknutím na ikonu kontroly. Pre tento typ kontroly nie je potrebné konfigurovať žiadne ďalšie konkrétne nastavenia, kontrola sa spustí ihneď v dialógovom okne **Priebeha kontrola** (pozri snímku obrazovky). V prípade

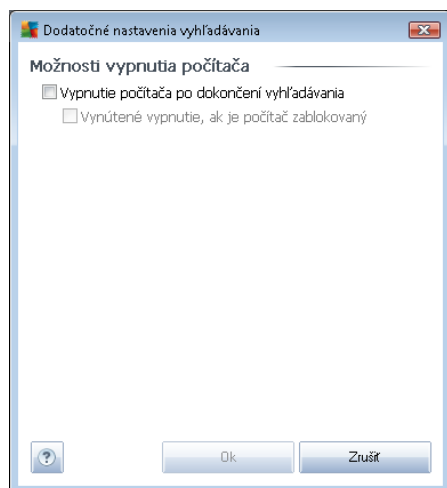
potreby môžete kontrolu dočasne prerušiť (tlačidlo **Pozastaviť**) alebo zrušiť (tlačidlo **Zastaviť**).



Zmena konfigurácie kontroly

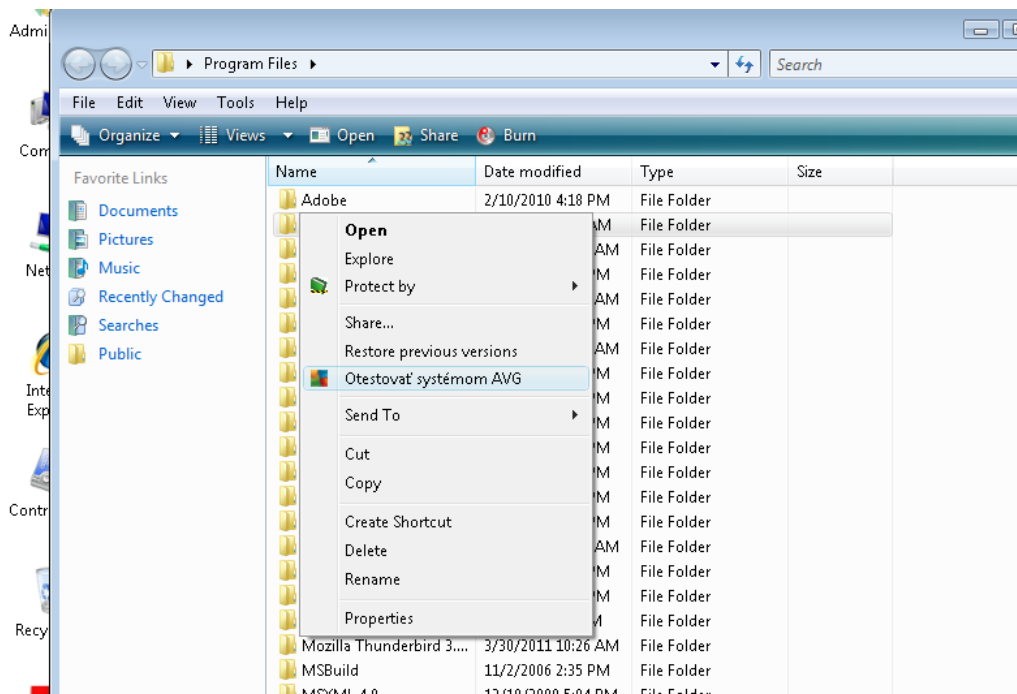
Kontrola súčast'ou Anti-Rootkit sa spustí vždy s predvolenými nastaveniami a zmenu parametrov kontroly je možné urobiť len v dialógovom okne [Rozšírené nastavenia/súčast' Anti-Rootkit](#). V rozhraní kontroly sa nachádza táto konfigurácia, ale len keď je spustená kontrola:

- **Automatická kontrola** – pomocou posúvača zmeňte prioritu procesu kontroly. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „podľa používateľa“. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie počítačových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).
- **Ďalšie nastavenia kontroly**– tento odkaz otvára nové dialógové okno **Ďalšie nastavenia kontroly**, ktoré sa používa na definovanie podmienok pre vypnutie počítača v súvislosti s funkciou **Kontrola súčast'ou Anti-Rootkit (Vypnúť počítač po dokončení kontroly alebo Vynútené vypnutie počítača, keď je zamknutý)**:



11.3. Kontrola v Prieskumníkovi

Okrem vopred definovaných kontrol spustených pre celý počítač alebo jeho vybrané oblasti, **AVG Internet Security 2011** zároveň umožňuje rýchlo kontrolovať konkrétny objekt priamo v prostredí programu Prieskumník. Ak chcete otvoriť neznámy súbor a nie ste si istý jeho obsahom, môžete ho skontrolovať na požiadanie. Postupujte podľa týchto pokynov.



- V programe Prieskumník zvýraznite súbor (alebo priečinok), ktorý chcete skontrolovať.
- Kliknutím pravým tlačidlom myši na objekt otvorte kontextovú ponuku.
- Výberom možnosti **Skontrolovať programom AVG** skontroluje súbor programom AVG.



11.4. Kontrola z príkazového riadka

Program **AVG Internet Security 2011** ponúka možnosť spustiť kontrolu z príkazového riadka. Túto funkciu môžete použiť napríklad na serveroch, alebo keď vytvárate dávkový skript, ktorý sa bude spúšťať automaticky po zavedení operačného systému. Príkazový riadok umožňuje spustiť kontrolu s väčšinou parametrov, ktoré sa nachádzajú aj v grafickom používateľskom rozhraní AVG.

Na spustenie kontroly programom AVG z príkazového riadka spustíte tento príkaz v priečinku, v ktorom je nainštalovaný program AVG:

- **avgscanx** pre 32-bitové operačné systémy
- **avgscana** pre 64-bitové operačné systémy

Syntax príkazu

Toto je syntax príkazového riadka:

- **avgscanx /parameter** ... napr. **avgscanx /comp** na kontrolu celého počítača
- **avgscanx /parameter /parameter** ... Ak použijete niekoľko parametrov, zoradíte ich za sebou a oddelíte ich medzerou a lomkou.
- Ak sa musí uviesť konkrétna hodnota pre parameter (napr. parameter **/scan**, ktorý si vyžaduje informáciu o tom, ktoré oblasti počítača sa majú kontrolovať, a je potrebné uviesť presnú cestu k vybranej časti), potom sa hodnoty oddelia bodkočiarkou, napríklad:
avgscanx /scan=C:\;D:

Parametre kontroly

Ak chcete zobraziť úplný prehľad použiteľných parametrov, zadajte príslušný príkaz spolu s parameterom **/?** alebo **/HELP** (napr. **avgscanx /?**). Jediný povinný parameter je **/SCAN**, ktorý definuje oblasti počítača, ktoré sa majú kontrolovať. Podrobnejšie informácie o možnostiach sa nachádzajú v [prehľade parametrov príkazového riadka](#).

Na spustenie kontroly stlačte kláves **Enter**. Počas kontroly môžete zastaviť proces stlačením kombinácie klávesov **Ctrl+C** alebo **Ctrl+Pause**.

Kontrola z príkazového riadka spustené z grafického rozhrania

Ak používate operačný systém Windows a počítač je v núdzovom režime, môžete spustiť kontrolu z príkazového riadka z grafického používateľského rozhrania. Samotná kontrola sa spustí z príkazového riadka, dialógové okno **Command Line Composer** umožňuje zadať väčšinu parametrov kontroly len pomocou praktického grafického rozhrania.

Keďže sa dá toto dialógové okno otvoriť, len keď je počítač s operačným systémom Windows v núdzovom režime, na zobrazenie podrobných informácií o tomto dialógovom okne použite súbor

pomocníka, ktorý sa otvára priamo v dialógovom okne.

11.4.1. Parametre kontroly z príkazového riadka

Nasledujúce je zoznam všetkých parametrov použiteľných pri prehľadávaní z príkazového riadka:

- **/SCAN** [Prehľadávať konkrétne súbory alebo priečinky](#) /SCAN=path;path (napr. /SCAN=C:\;D:\)
- **/COMP** [Prehľadávať celý počítač](#)
- **/HEUR** Použiť [heuristickú analýzu](#)
- **/EXCLUDE** Vylúčiť cestu alebo súbory z prehľadávania
- **/@** Súbor s príkazmi /názov súboru/
- **/EXT** Prehľadávať tieto prípony /napríklad EXT=EXE,DLL/
- **/NOEXT** Neprehľadávať tieto prípony /napríklad NOEXT=JPG/
- **/ARC** Prehľadávať archívy
- **/CLEAN** Automaticky vyčistiť
- **/TRASH** Premiestniť infikované súbory do [Vírusového trezora](#)
- **/QT** Rýchly test
- **/MACROW** Hlásiť makrá
- **/PWDW** Hlásiť súbory chránené heslom
- **/IGNLOCKED** Ignorovať zamknuté súbory
- **/REPORT** Hlásiť do súboru /názov súboru/
- **/REPAPPEND** Pripojiť k súboru so správou
- **/REPOK** Označiť neinfikované súbory slovom OK
- **/NOBREAK** Nepovoliť prerušenie klávesmi CTRL-BREAK
- **/BOOT** Povolit' kontrolu MBR/BOOT
- **/PROC** Prehľadávať aktívne procesy
- **/PUP** Hlásiť „[potenciálne nežiaduce programy](#)“
- **/REG** Prehľadávať databázu Registry



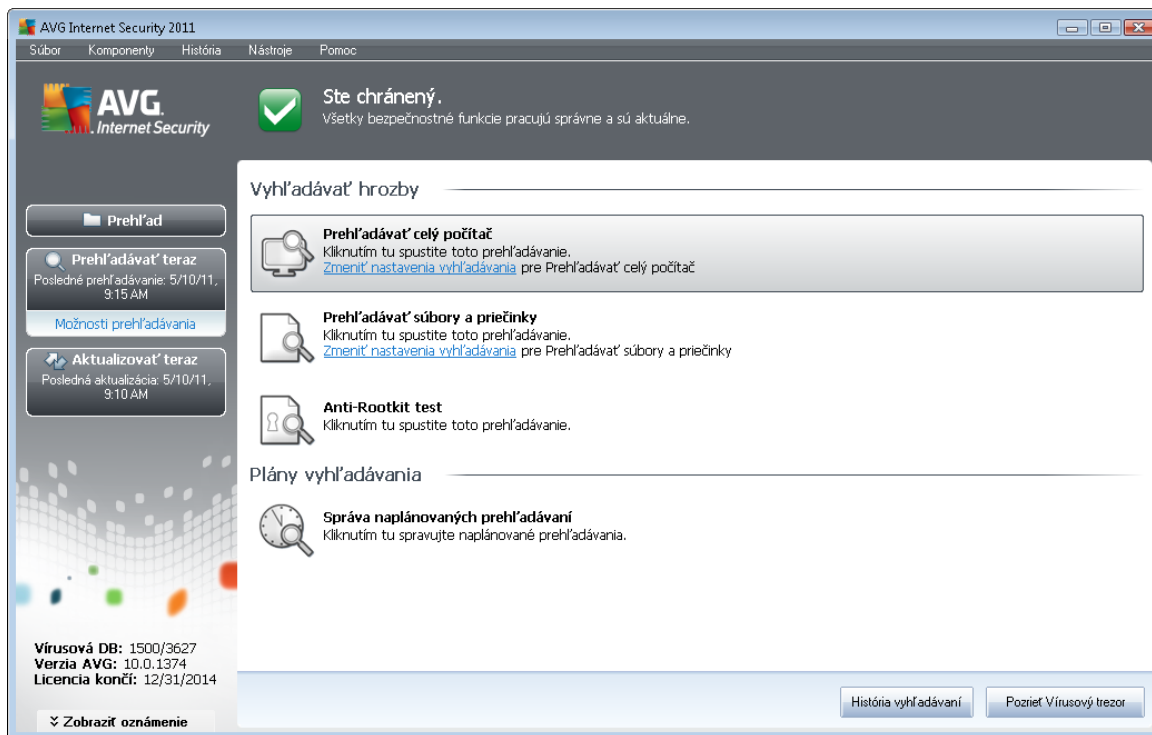
- **/COO** Prehľadávať súbory cookies
- **/?** Zobrazit' pomocníka pre túto tému
- **/HELP** Zobrazit' pomocníka pre túto tému
- **/PRIORITY** Nastaviť prioritu prehľadávania /nízka, automatická, vysoká/ (pozri časť [Rozšírené nastavenia/Prehľadávania](#))
- **/SHUTDOWN** Vypnúť počítača po dokončení prehľadávania
- **/FORCESHUTDOWN** Vynútené vypnutie počítača po dokončení prehľadávania
- **/ADS** Prehľadávať alternatívne dátové prúdy (len pre NTFS)
- **/ARCBOMBSW** Hlásiť opakovane komprimované archivačné súbory

11.5. Plánovanie kontroly

AVG Internet Security 2011 umožňuje spustiť kontrolu na požiadanie (napríklad, keď máte podozrenie, že sa do počítača dostala infekcia) alebo na základe vytvoreného plánu. Odporúčame vám, aby ste spúšťali kontroly podľa plánov. týmto spôsobom sa zabezpečí, že bude počítač chránený pred infikovaním a nebudete si musieť robiť starosti s tým, kedy a či vôbec máte spustiť kontrolu.

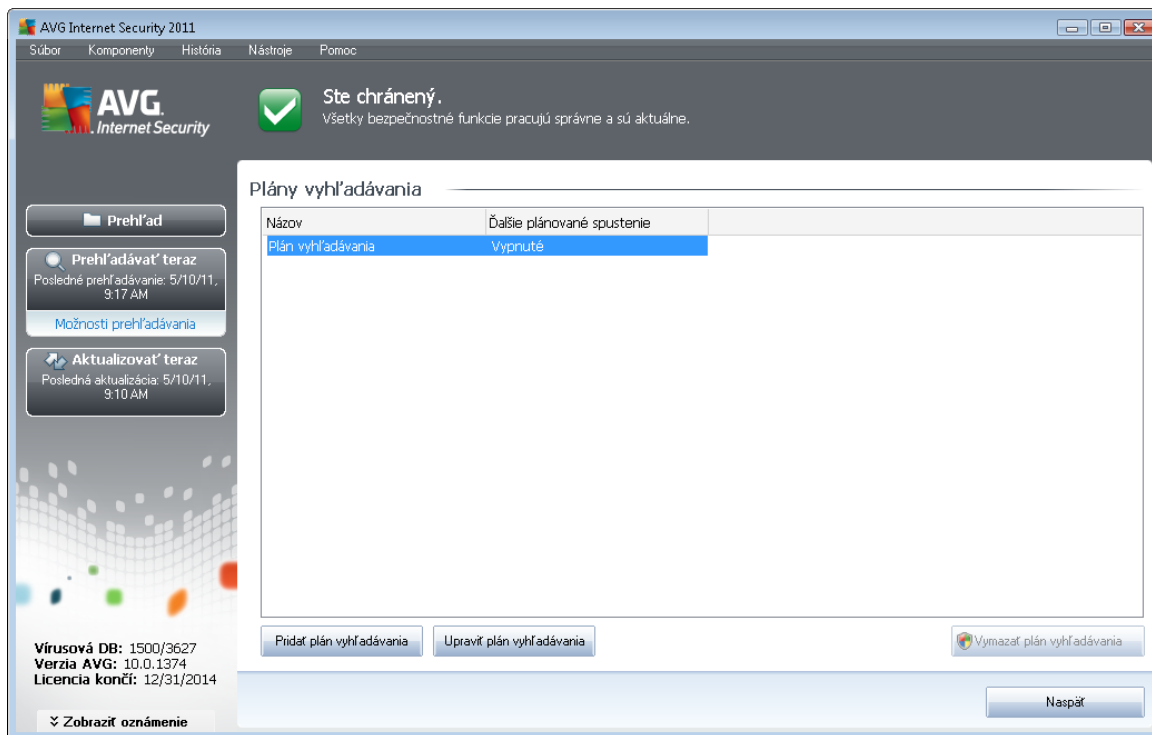
Odporúčame vám, aby ste pravidelne, najmenej raz za týždeň, spustili [kontrolu celého počítača](#). Podľa možností však spúšťajte kontrolu celého počítača každý deň – tak, ako je nastavené v predvolenej konfigurácii plánu kontroly. Ak je počítač „stále zapnutý“, potom môžete naplánovať kontrolu na čas, keď sa počítač nepoužíva. Ak je počítač v tomto čase vypnutý, potom sa zmeškaná naplánovaná kontrola spustí [pri spustení počítača](#).

Ak chcete vytvoriť nový plán kontroly, otvorte [rozhranie kontroly programom AVG](#) a prejdite na spodnú časť s názvom **Naplánovať kontroly**:



Naplánovať kontroly

Kliknutím na grafickú ikonu v časti **Naplánovať kontroly** otvorte nové dialógové okno **Naplánovať kontroly** so zoznamom všetkých momentálne naplánovaných kontrol.

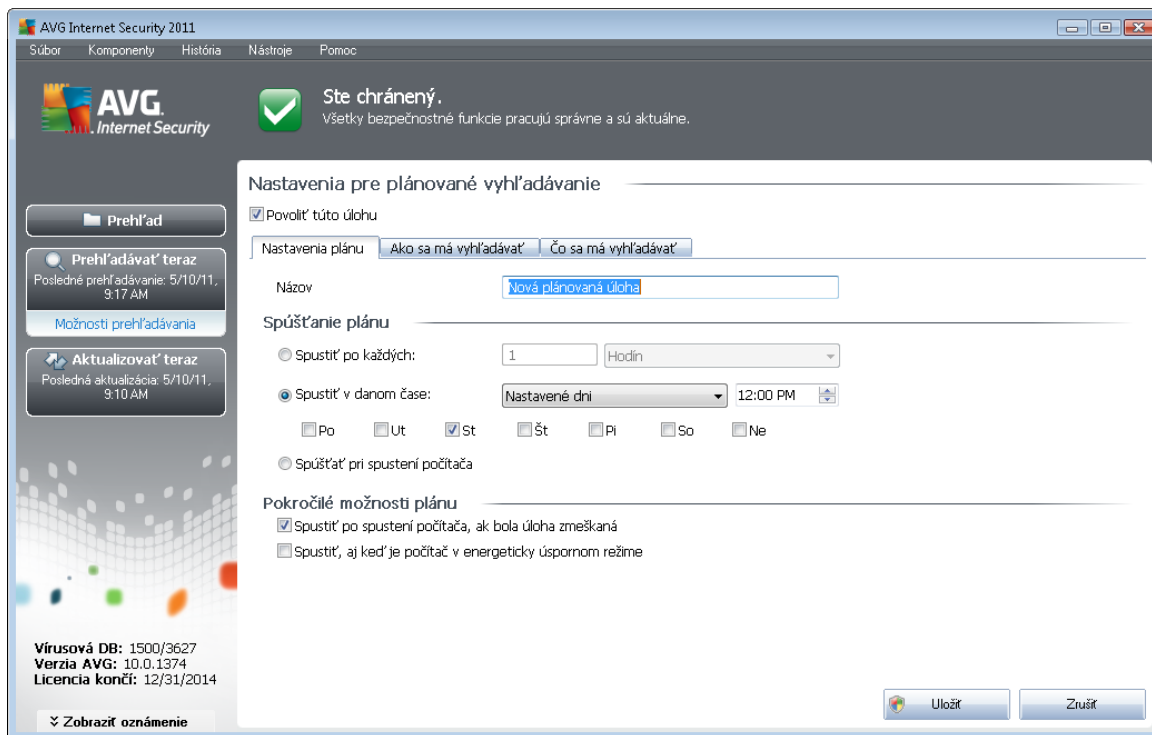


Umožňuje editovať a pridať kontroly pomocou týchto ovládacích tlačidiel:

- **Pridať plán kontroly** – toto tlačidlo otvorí dialógové okno **Nastavenia naplánovanej kontroly**, kartu [Nastavenia plánu](#). V tomto dialógovom okne nastavíte parametre novo definovaného testu.
- **Editovať plán kontroly** – toto tlačidlo je použiteľné len v prípade, ak ste už predtým vybrali existujúci test v zozname naplánovaných testov. V tom prípade sa tlačidlo použiteľné – kliknutím naň sa otvorí dialógové okno **Nastavenia plánovanej kontroly**, kartu [Nastavenia plánu](#). Parametre vybraného testu sú tu už nastavené a dajú sa editovať.
- **Vymazať plán kontroly** – toto tlačidlo je tiež použiteľné len v prípade, ak ste už predtým vybrali existujúci test v zozname naplánovaných testov. Tento test môžete potom vymazať zo zoznamu stlačením ovládacieho tlačidla. Môžete však odstrániť len vaše vlastné kontroly, **plán kontroly celého počítača** nastavený v predvolenej konfigurácii sa nedá nikdy vymazať.
- **Naspäť** – návrat na [používateľské rozhranie AVG](#)

11.5.1. Nastavenia plánu

Ak si želáte naplánovať nový test a jeho pravidelné spúšťanie, otvorte dialógové okno **Nastavenia plánovaného testu** (kliknite na tlačidlo **Pridať plán prehľadávania** v dialógovom okne **Naplánovať prehľadávania**). Dialógové okno je rozdelené na tri karty: **Nastavenia plánu** – pozri obrázok nižšie (predvolená karta, ktorá sa otvorí automaticky), [Ako sa má prehľadávať](#) a [Čo sa má prehľadávať](#).



Na karte **Nastavenia plánu** najskôr začiarknutím alebo zrušením začiarknutia položky **Povolit túto úlohu** jednoducho dočasne vypnete naplánovaný test a znova ho zapnete v prípade potreby.

Potom uveďte názov vytváraného prehľadávania a plánu. Zadať názov do textového poľa vedľa položky **Název**. Podľa možností použite stručné, opisné a vhodné názvy pre prehľadávania, aby sa neskôr dali ľahšie rozpoznať medzi ostatnými.

Príklad: Nie je vhodné nazvať prehľadávanie „Nové prehľadávanie“ alebo „Moje vyhľadávanie“, pretože tieto názvy nesúvisia s tým, čo prehľadávanie vlastne kontroluje. Na druhej strane, príkladom dobrého opisného názvu je „Prehľadávanie systémových oblastí“ a pod. Takisto nie je potrebné zadať do názvu prehľadávania, či ide o prehľadávanie celého počítača alebo prehľadávanie vybraných súborov alebo priečinkov, pretože vaše vlastné prehľadávania budú vždy predstavovať špeciálnu verziu prehľadávania vybraných súborov alebo priečinkov.

Toto dialógové umožňuje ďalej definovať tieto parametre prehľadávania:

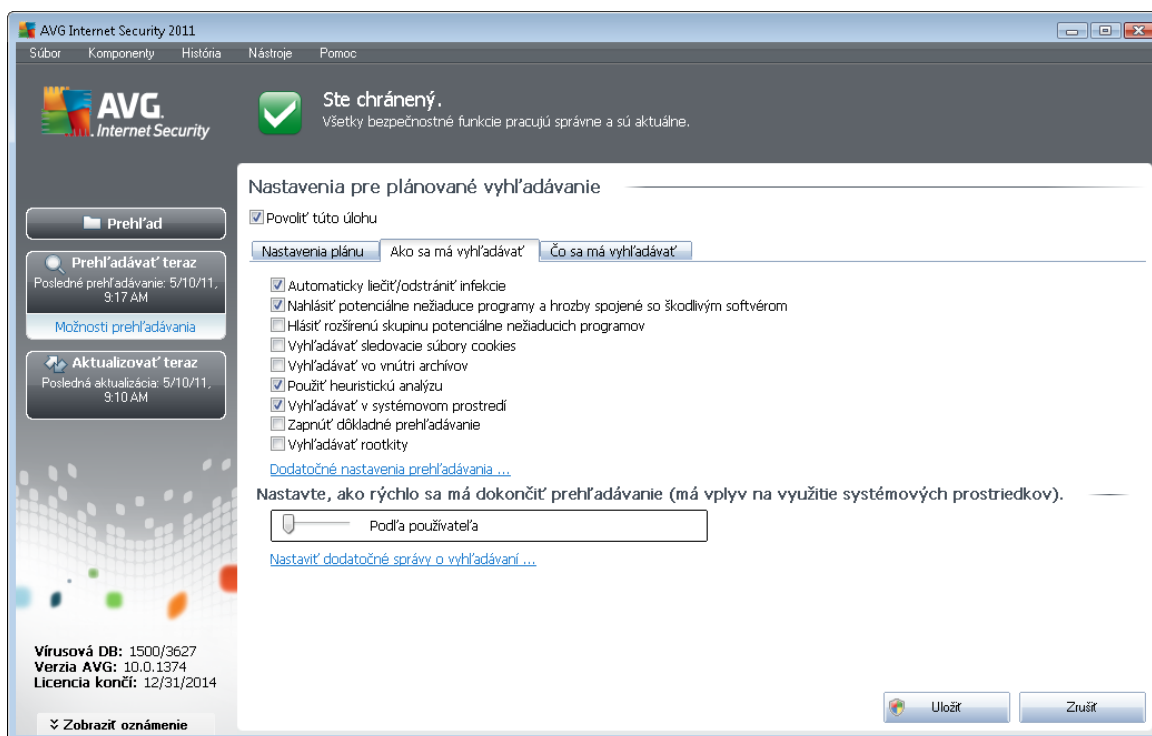
- **Spúšťanie naplánovaných úloh** – nastavte časové intervaly spúšťania novo naplánovaného prehľadávania. Čas spúšťania sa definuje ako opakované spúšťanie prehľadávania po uplynutí určitého času (**Spustiť každých...**), definovaním presného dátumu a času (**Spustiť v konkrétnom časovom intervale...**), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie prehľadávania (**Činnosť pri spustení počítača**).
- **Rozšírené možnosti plánu** – táto časť sa používa na definovanie podmienok, pri ktorých sa má resp. nemá spustiť prehľadávanie, keď je počítač v úspornom režime alebo úplne vypnutý.

Ovládacie tlačidlá dialógového okna Nastavenia plánovaného prehľadovania

Na všetkých troch kartách dialógového okna **Nastavenia naplánovaného prehľadovania** (**Nastavenia plánu**, **Ako sa má prehľadávať** a **Čo sa má prehľadávať**) sa nachádzajú dve ovládacie tlačidlá, ktoré majú rovnakú funkciu bez ohľadu na to, ktorá karta je práve otvorená:

- **Uložiť** – uloží všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na [hlavné dialógové okno s rozhraním prehľadovania programu AVG](#). Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých potrebných možností.
- **Zrušiť** – zruší všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na [hlavné dialógové okno s rozhraním kontroly programu AVG](#).

11.5.2. Ako kontrolovať



Na karte **Ako kontrolovať** sa nachádza zoznam parametrov kontroly, ktoré sa dajú zapnúť resp. vypnúť. Štandardne je väčšina parametrov zapnutá a príslušná funkcia sa použije počas kontroly. Ak nemáte vážny dôvod meniť tieto nastavenia, potom vám odporúčame, aby ste zachovali prednastavenú konfiguráciu:

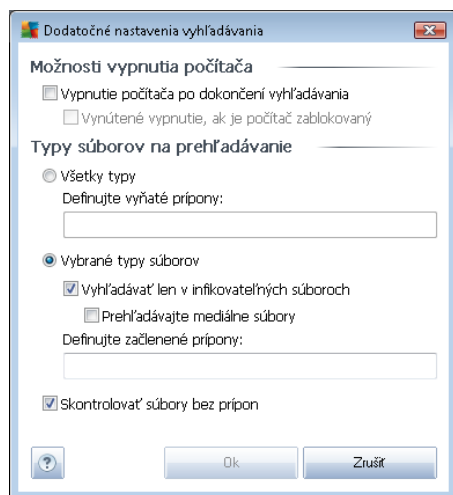
- **Automaticky liečiť/odstrániť infekcie** (štandardne zapnuté): ak sa počas kontroly zistí prítomnosť vírusu, môže sa automaticky vyliečiť, ak je k dispozícii liečba. Ak sa infikované súbory nedajú vyliečiť automaticky, alebo keď sa rozhodnete vypnúť túto funkciu, potom sa po detekcii vírusu zobrazí upozornenie a budete musieť rozhodnúť, čo sa má urobiť s

detegovanou infekciou. Odporúčame vám, aby ste infikovaný súbor odstránili do [Vírusového trezora](#).

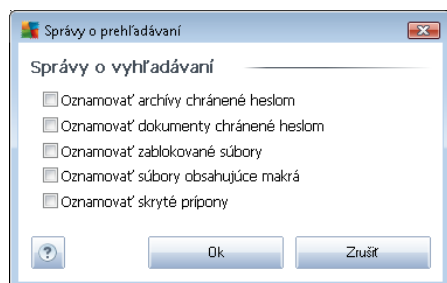
- **Hlásit' potenciálne nežiaduce programy a hrozby spyware** (štandardne zapnuté): začiaroknite toto okienko, ak chcete zapnúť súčasť [Anti-Spyware](#) a kontrolovať spyware a vírusy. [Spyware](#) predstavuje pochybnú kategóriu škodlivého softvéru: hoci v bežných situáciách predstavuje bezpečnostné riziko, niektoré takéto programy môžu byť nainštalované úmyselne. Odporúčame vám, aby ste nechali túto funkciu zapnutú, pretože zvyšuje úroveň zabezpečenia počítača.
- **Hlásit' rozšírenú skupinu potenciálne nežiaducich programov** (štandardne vypnuté): začiaroknite toto okienko, ak sa má detegovať rozšírená skupina [spywaru](#): programov, ktoré sú úplne v poriadku a neškodné, keď sa získajú priamo od výrobcu, ale neskôr sa dajú zneužiť na škodlivé účely. Toto je ďalšie opatrenie, ktoré ešte viac zvyšuje úroveň zabezpečenia počítača, ale môže blokovat' dobré programy, a preto je táto funkcia štandardne vypnutá.
- **Kontrolovať sledovacie súbory cookies** (štandardne vypnuté): tento parameter súčasť [Anti-Spyware](#) zapína funkciu na zisťovanie prítomnosti súborov cookies počas kontroly (*HTTP cookies sa používajú na overenie totožnosti, sledovanie a správu konkrétnych informácií o používateľoch, ako sú preferencie stránok alebo obsah elektronických nákupných košíkov*).
- **Kontrolovať v archívoch** (štandardne vypnuté): tieto parametre určujú, že sa majú počas kontroly overovať všetky súbory, aj keď sú zabalené vo vnútri určitých typov archívov, ako sú ZIP, RAR...
- **Používať heuristiku** (štandardne zapnuté): heuristická analýza (*dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí*) bude jedna z metód, ktoré sa použijú na detegovanie vírusov počas kontroly.
- **Kontrolovať systémové prostredie** (štandardne zapnuté): počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnúť dôkladnú kontrolu** (štandardne vypnuté) – v určitých situáciách (*napr. pri podozrení na infikovanie počítača*) môžete začiaroknutím tohto okienka zapnúť algoritmus najdôkladnejšej kontroly, ktorý overí aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.

Potom môžete zmeniť konfiguráciu kontroly podľa tohto postupu:

- **Ďalšie nastavenia kontroly** – tento odkaz otvorí nové dialógové okno **Ďalšie nastavenia kontroly** ktoré sa používa na nastavenie týchto parametrov.



- o **Možnosti vypnutia počítača** – rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútené vypnutie počítača, keď je zamknutý**).
- o **Definovať typy súborov pre kontrol** – ďalej môžete rozhodnúť, či sa majú kontrolovať:
 - **Všetky typy súborov** s možnosťou definovať výnimky kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.
 - **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (*súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory*), vrátane mediálnych súborov (*video, audio súborov – ak necháte toto okienko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá*). Znova môžete nastaviť (podľa prípony), ktoré súbory sa majú kontrolovať vždy.
 - Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony**. Táto možnosť je štandardne zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili, ak na to nemáte skutočný dôvod. Súbory bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.
- **Nastaviť rýchlosť dokončenia kontroly** – pomocou posúvača zmeňte prioritu procesu kontroly. Štandardne má tento parameter nastavenú úroveň automatického využívania zdrojov „podľa používateľa“. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*toto nastavenie je užitočné vtedy, ak potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššími nárokmi na využívanie počítačových zdrojov (*napr. keď sa počítač dočasne nepoužíva*).
- **Vytvoriť ďalšie správy o kontrole** – odkaz otvorí nové dialógové okno **Správy o kontrole**, v ktorom môžete určiť, aké typy možných nálezov sa majú uviesť v správach:



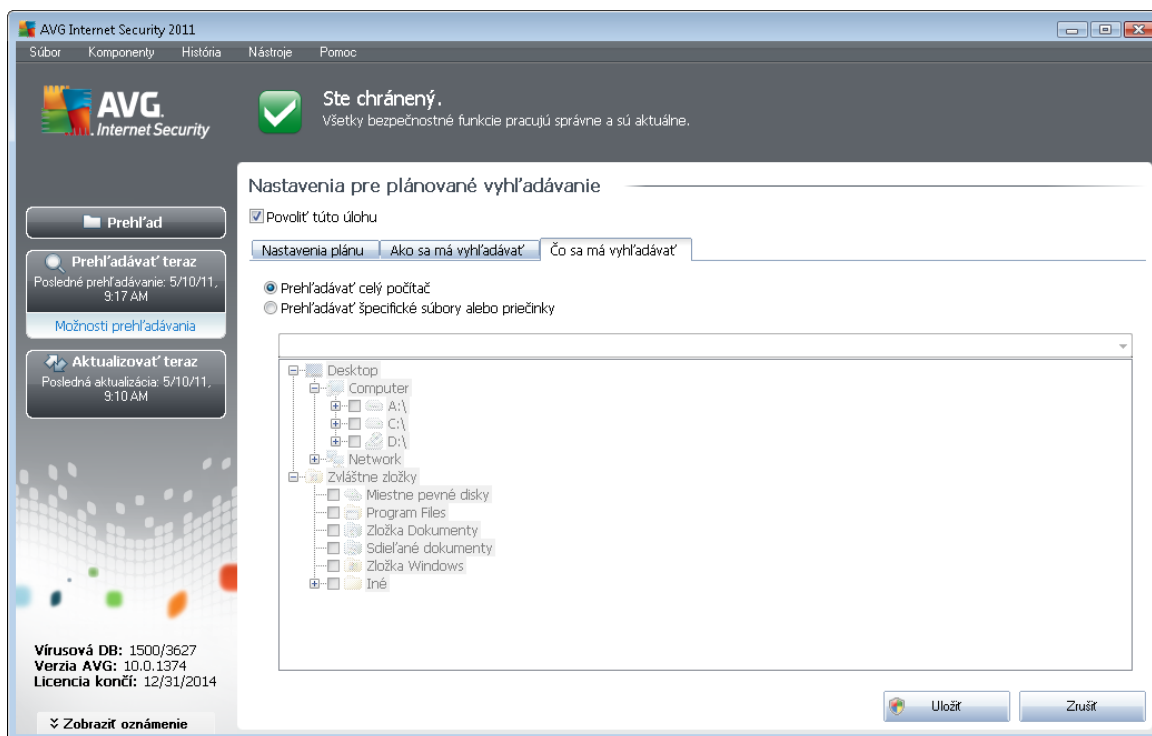
Poznámka: Konfigurácia kontroly je štandardne nastavená tak, aby sa dosahoval optimálny výkon. Ak nemáte vážny dôvod meniť nastavenia kontroly, potom vám odporúčame, aby ste zachovali prednastavenú konfiguráciu. Zmenu konfigurácie by mali robiť len skúsení používatelia. Ďalšie možnosti konfigurácie kontroly sa nachádzajú v dialógovom okne [Rozšírené nastavenia](#), ktoré sa otvára pomocou položky v hlavnej ponuke programu **Súbor/Rozšírené nastavenia**.

Ovládacie tlačidlá

Na všetkých troch kartách dialógového okna **Nastavenia naplánovanej kontroly** ([Nastavenia plánu](#), **Ako kontrolovať** a [Čo kontrolovať](#)) sa nachádzajú dve ovládacie tlačidlá, ktoré majú rovnakú funkciu bez ohľadu na to, ktorá karta je práve otvorená:

- **Uložiť** – uloží všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na [hlavné dialógové okno s rozhraním kontroly programom AVG](#). Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých potrebných možností.
- **Zrušiť** – zruší všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na [hlavné dialógové okno s rozhraním kontroly programom AVG](#).

11.5.3. Čo kontrolovať



Na karte **Čo kontrolovať** môžete nastaviť, či chcete naplánovať [kontrolu celého počítača](#) alebo [kontrolu špecifických súborov alebo priečinkov](#).

Keď vyberiete kontrolu špecifických súborov alebo priečinkov, potom sa v spodnej časti tohto dialógového okna aktivuje zobrazená stromová štruktúra, v ktorej môžete nastaviť priečinky, ktoré sa majú kontrolovať (*rozbaľte položky kliknutím na uzol so znakom plus a vyhľadajte priečinok, ktorý chcete kontrolovať*). Začiarknutím príslušných okienok môžete vybrať naraz niekoľko priečinkov. Vybrané priečinky sa zobrazia v textovom poli v hornej časti dialógového okna a do prekryvacej ponuky sa uloží história vami vybraných kontrol na neskoršie účely. Úplnú cestu k požadovanému priečinku môžete zadať aj ručne (*ak zadáte viac ciest, musíte ich oddeliť bodkočiarkou bez medzier*).

V stromovej štruktúre môžete zároveň vyhľadať vetvu s názvom **Špeciálne umiestnenia**. Toto je zoznam umiestnení, ktoré sa skontrolujú po začiarknutí príslušného začiarkovacieho okienka:

- **Pevné disky počítača** – všetky pevné disky počítača.
- **Programové súbory**
 - o C:\Program Files\
 - o v 64-bitovej verzii C:\Program Files (x86)
- **Priečinkov Moje dokumenty**



o vo Win XP: C:\Documents and Settings\Default User\Moje dokumenty\

o vo Windows Vista/7: C:\Users\používateľ\Dokumenty\

- **Zdieľané dokumenty**

o vo Win XP: C:\Documents and Settings\All Users\Dokumenty\

o vo Windows Vista/7: C:\Users\Public\Dokumenty\

- **Adresár Windows** – C:\Windows\

- **Iné**

o **Systémový disk** – pevný disk, na ktorom je nainštalovaný operačný systém (zvyčajne C:).

o **Systémový priečinok** – C:\Windows\System32\

o **Priečinok Temporary Files** – C:\Documents and Settings\User\Local\ (Windows XP) alebo C:\Users\používateľ\AppData\Local\Temp\ (Windows Vista/7)

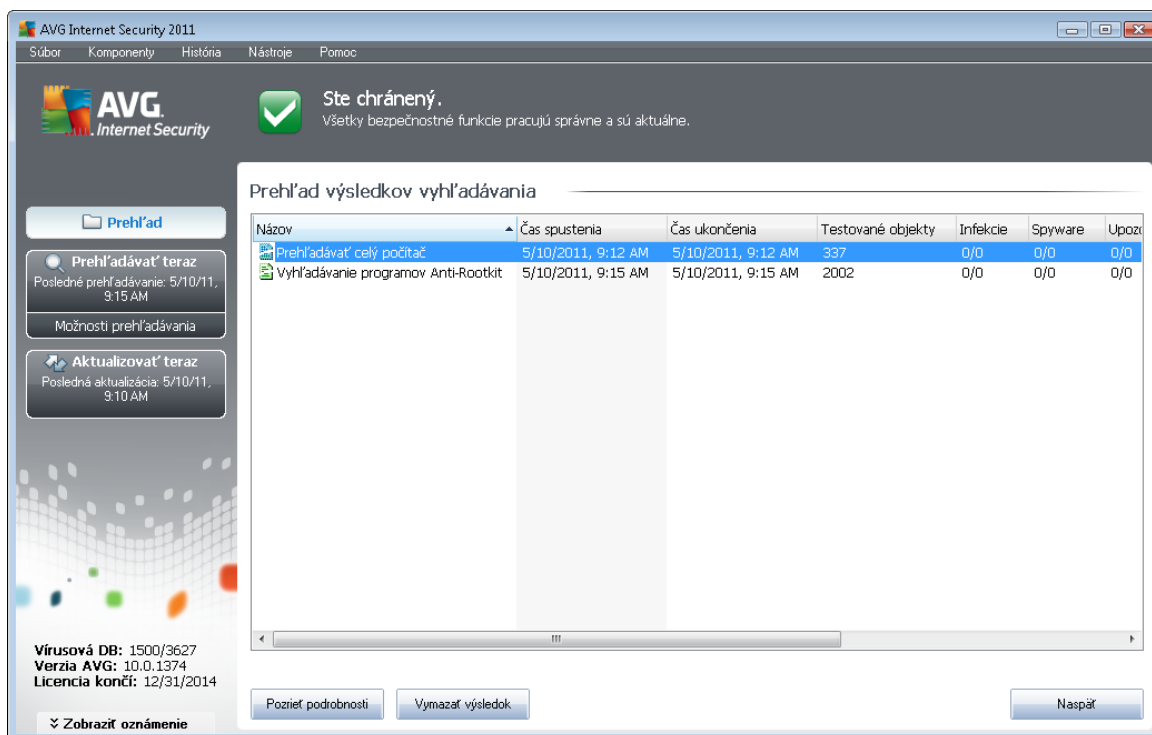
o **Temporary Internet Files** – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP) alebo C:\Users\používateľ\AppData\Local\Microsoft\Windows\Temporary Internet Files\ (Windows Vista/7)

Ovládacie tlačidlá dialógového okna Nastavenia naplánovanej kontroly

Na všetkých troch kartách dialógového okna **Nastavenia naplánovanej kontroly** ([Nastavenia plánu](#), [Ako kontrolovať](#) a [Čo kontrolovať](#)) sa nachádzajú dve ovládacie tlačidlá, ktoré majú rovnakú funkciu bez ohľadu na to, ktorá karta je práve otvorená:

- **Uložiť** – uloží všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na [hlavné dialógové okno s rozhraním kontroly programom AVG](#). Preto, ak chcete nastaviť parametre testu na všetkých kartách, stlačením tohto tlačidla ich uložte až po nastavení všetkých potrebných možností.
- **Zrušiť** – zruší všetky zmeny, ktoré ste urobili na tejto karte alebo na inej karte tohto dialógového okna a prepne naspäť na [hlavné dialógové okno s rozhraním kontroly programom AVG](#).

11.6. Prehľad výsledkov kontroly



Dialógové okno **Prehľad výsledkov prehľadávania** sa otvára v [rozhraní prehľadávania programom AVG](#) pomocou tlačidla **História prehľadávání**. V dialógovom okne sa nachádza zoznam všetkých doposiaľ spustených prehľadávání a informácie o ich výsledkoch:

- **Názov:** Označenie vyhľadávania; buď môže ísť o názov niektorého z [vopred definovaných prehľadávání](#) alebo o názov, ktorý ste priradilo [vlastnému naplánovanému prehľadávaniu](#). Každý názov obsahuje ikonu označujúcu výsledok prehľadávania:

 – Zelená ikona informuje, že počas prehľadávania nebola detegovaná žiadna infekcia.

 – Modrá ikona informuje, že počas prehľadávania bola detegovaná infekcia, ale infikovaný objekt bol automaticky odstránený.

 – Červená ikona upozorňuje, že počas prehľadávania bola detegovaná infekcia, ktorá sa nedala odstrániť!

Každá ikona môže byť buď celá alebo rozdelená na polovicu; celá ikona predstavuje dokončené a správne ukončené prehľadávanie; ikona rozdelená na polovicu predstavuje zrušené alebo prerušené prehľadávanie.

Poznámka: Podrobné informácie o každom prehľadaní sa nachádzajú v dialógovom okne [Výsledky prehľadávania](#), ktoré sa otvára pomocou tlačidla **Zobraziť podrobnosti** (v spodnej časti tohto dialógového okna).

- **Čas spustenia:** Dátum a čas, kedy bolo prehľadávanie spustené.
- **Čas skončenia:** Dátum a čas, kedy sa prehľadávanie skončilo.
- **Testované objekty:** Počet objektov, ktoré sa skontrolovali počas prehľadávania.
- **Infekcie:** Počet detegovaných/odstránených [vírusových infekcií](#)
- **Spyware:** Počet detegovaných/odstránených programov typu [spyware](#)
- **Upozornenia:** Počet detegovaných [podozrivých objektov](#)
- **Rootkity:** Počet detegovaných [rootkitov](#)
- **Informácie záznamového protokolu prehľadávania:** Informácie súvisiace s priebehom a výsledkami prehľadávania (obvyčajne s jeho dokončením alebo prerušením).

Ovládacie tlačidlá

Ovládacie tlačidlá pre dialógové okno **Prehľad výsledkov prehľadávania** sú nasledovné:

- **Zobraziť podrobnosti:** Stlačením tohto tlačidla sa otvorí dialógové okno [Výsledky prehľadávania](#) s podrobnými informáciami o zvolenom prehľadaní.
- **Vymazať výsledky:** Stlačením tohto tlačidla sa zvolená položka odstráni z prehľadu výsledkov prehľadávania.
- **Naspäť:** Prepne naspäť na hlavné dialógové okno [rozhrania prehľadávania programom AVG](#)

11.7. Podrobné výsledky kontroly

Ak v dialógovom okne [Prehľad výsledkov prehľadávania](#) zvolíte konkrétne prehľadávanie, potom môžete kliknutím na tlačidlo **Zobraziť podrobnosti** otvoriť dialógové okno **Výsledky prehľadávania** s podrobnými informáciami o priebehu a výsledkoch zvoleného prehľadávania.

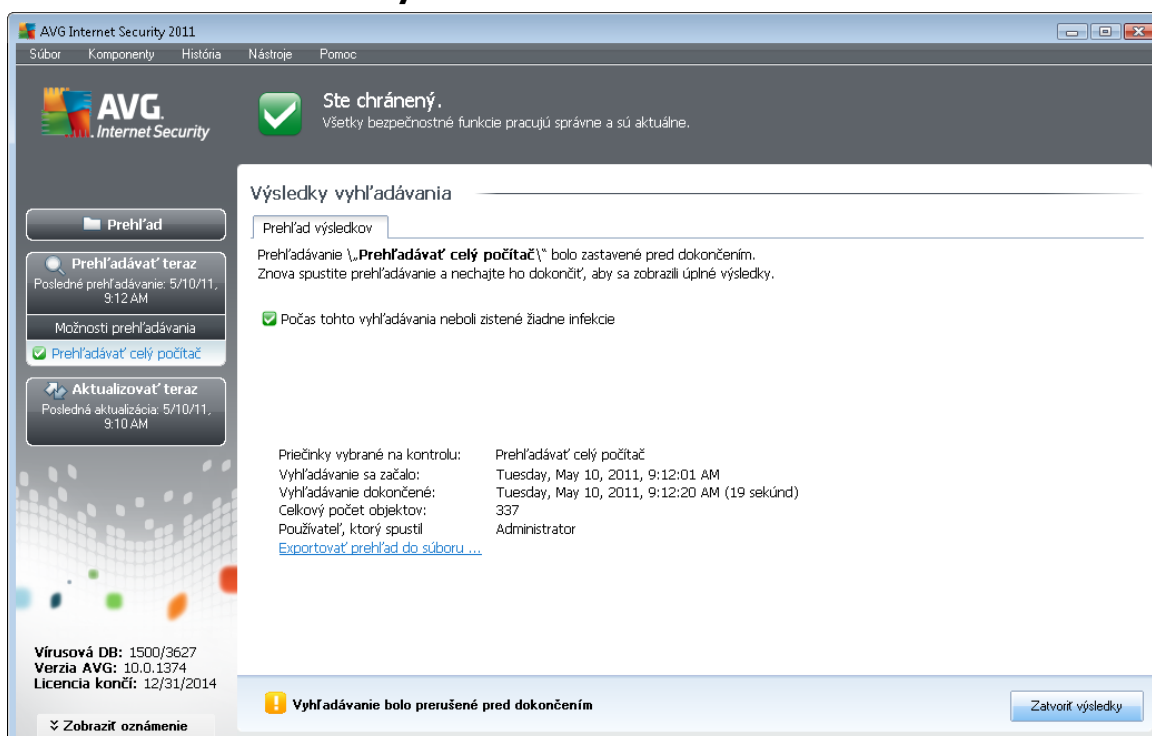
Toto dialógové okno je rozdelené na niekoľko kariet:

- **Prehľad výsledkov:** Táto karta sa tu nachádza vždy a poskytuje štatistické informácie o priebehu prehľadávania.
- **Infekcie:** Táto karta sa tu nachádza len vtedy, ak sa počas prehľadávania detegovala [vírusová infekcia](#)
- **Spyware:** Táto karta sa tu nachádza len vtedy, ak sa počas prehľadávania detegoval [spyware](#)
- **Upozornenia:** Táto karta sa tu nachádza len vtedy, ak sa počas prehľadávania detegovali súbory cookies.
- **Rootkity:** Táto karta sa tu nachádza len vtedy, ak sa počas prehľadávania detegovali o

[rootkity](#)

- **Informácie:** Táto karta sa tu nachádza len vtedy, ak sa detegovali niektoré potenciálne hrozby, ktoré sa však nedajú zaradiť do žiadnej z vyššie uvedených kategórií; na karte sa potom zobrazí upozornenie súvisiace s nálezom. Nachádzajú sa tu aj informácie o objektoch, ktoré nie je možné prehľadať (napr. heslom chránené archívy).

11.7.1. Karta Prehľad výsledkov



V karte **Výsledky vyhľadávania** môžete nájsť podobnú štatistiku s informáciami o:

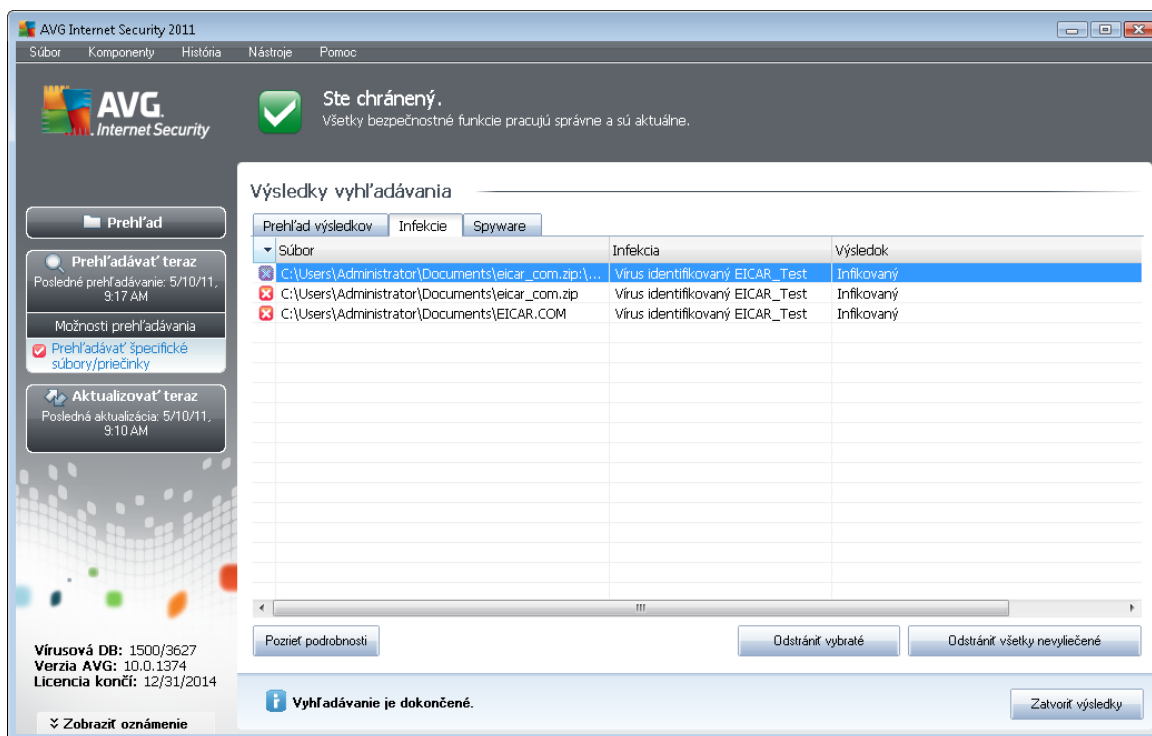
- detekovaných [vírusových infekciách](#) / [spyware](#)
- odstránených [vírusových infekciách](#) / [spyware](#)
- počte [vírusových infekcií](#) / [spyware](#), ktoré sa nedajú odstrániť alebo vyliečiť

Okrem toho nájdete informácie o dátume a presnom čase spustenia vyhľadávania, o celkovom počte prehľadaných objektov, o trvaní vyhľadávania a o počte chýb, ktoré sa vyskytli počas vyhľadávania.

Ovládacie tlačidlá

V tomto dialógovom okne je dostupné len jedno ovládacie tlačidlo. Tlačidlo **Naspäť** sa vráti do dialógového okna [Prehľad výsledkov vyhľadávania](#).

11.7.2. Karta Infekcie



Karta **Infekcie** sa nachádza v dialógovom okne **Výsledky prehľadávania** len v prípade, ak sa počas prehľadávania detegovala [vírusová infekcia](#). Táto karta je rozdelená na tri časti, na ktorých sa nachádzajú tieto informácie:

- **Súbor** – úplná cesta k pôvodnému umiestneniu infikovaného objektu.
- **Infekcie** – názov detegovaného [vírusu](#) (podrobnosti o konkrétnych vírusoch sa nachádzajú online vo [Vírusovej encyklopédii](#)).
- **Výsledok** – informuje o momentálnom stave infikovaného objektu, ktorý sa detegoval počas kontroly:
 - o **Infikovaný** – infikovaný objekt bol detegovaný a ponechal sa na pôvodnom mieste (napríklad ak ste [vypli funkciu na automatické liečenie](#) v nastavení konkrétnej kontroly).
 - o **Vyliečený** – infikovaný objekt sa automaticky vyliečil a ponechal na pôvodnom mieste.
 - o **Premiestnený do Vírusového trezora** – infikovaný objekt sa premiestnil do karantény vo [Vírusovom trezore](#)
 - o **Vymazaný** – infikovaný objekt sa vymazal.
 - o **Pridaný do výnimiek PNP** – zistený program bol označený ako výnimka a pridaný

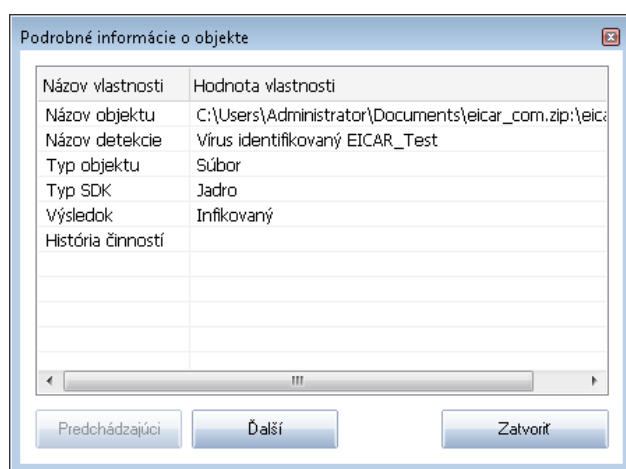
do zoznamu výnimiek PNP (nastavuje sa v dialógovom okne [Výnimky PNP](#) v rozšírených nastaveniach)

- o **Zamknutý súbor – netestovaný** – príslušný objekt je zamknutý a program AVG ho preto nedokáže skontrolovať.
- o **Potenciálne nebezpečný objekt** – objekt bol označený ako potenciálne nebezpečný, nie však infikovaný (môže obsahovať napríklad makrá); informáciu považujte len za upozornenie.
- o **Vyžaduje sa reštart na dokončenie akcie** – infikovaný objekt sa nedá odstrániť, na jeho úplné odstránenie musíte reštartovať počítač

Ovládacie tlačidlá

V tomto dialógovom okne sa nachádzajú tri ovládacie tlačidlá:

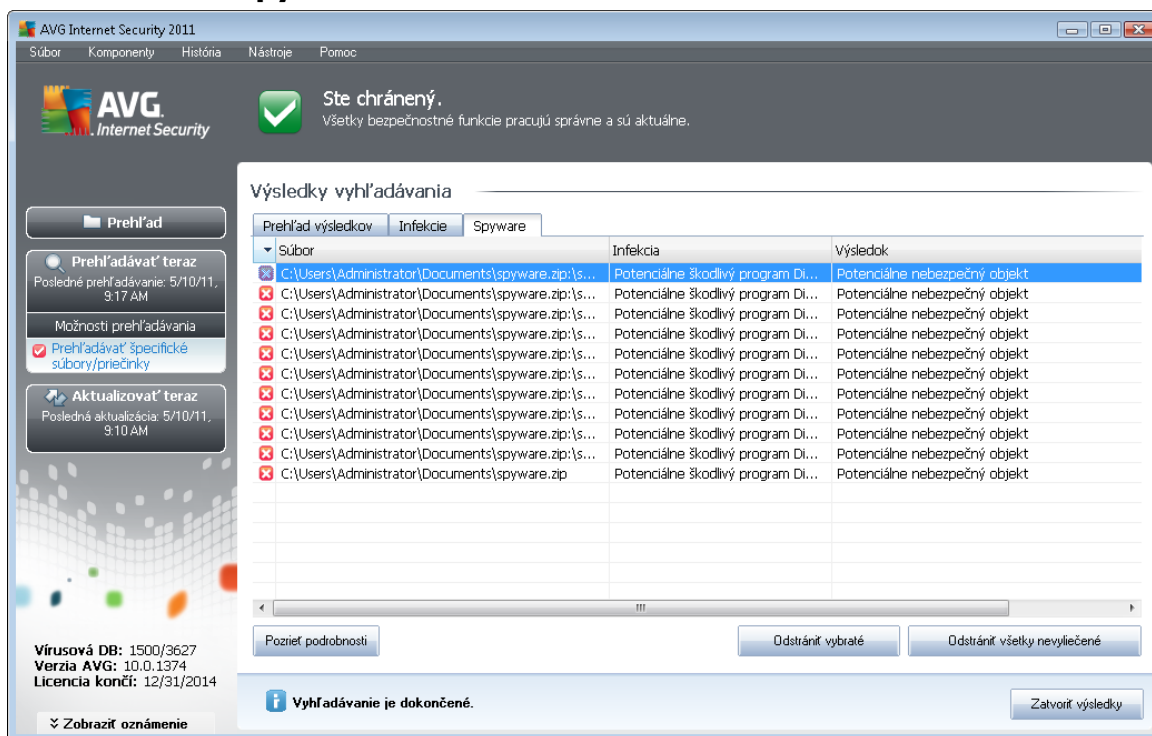
- **Zobraziť podrobnosti** – toto tlačidlo otvorí nové dialógové okno s názvom **Podrobné informácie o objekte**:



V tomto dialógovom okne sa nachádzajú podrobné informácie o detegovanom infikovanom objekte (napr. názov a umiestnenie infikovaného objektu, typ objektu, typ SDK, výsledky detekcie a história akcií súvisiacich s detegovaným objektom). Tlačidlá **Predchádzajúce/Ďalšie** sa používajú na zobrazenie informácií o konkrétnych nálezoch. Tlačidlo **Zatvoriť** sa používa na zatvorenie tohto dialógového okna.

- **Odstrániť vybrané** – toto tlačidlo sa používa na premiestnenie vybraného nálezu do [Vírusového trezora](#)
- **Odstrániť všetky nevylicované** – toto tlačidlo vymaže všetky nálezy, ktoré sa nedajú vyliečiť alebo premiestniť do [Vírusového trezora](#)
- **Zatvoriť výsledky** – zatvorí prehľad a otvorí pôvodné dialógové okno [Prehľad výsledkov kontroly](#).

11.7.3. Karta Spyware



Karta **Spyware** sa nachádza v dialógovom okne **Výsledky prehľadovania**, len ak sa počas prehľadovania detegoval [spyware](#). Táto karta je rozdelená na tri časti, na ktorých sa nachádzajú tieto informácie:

- **Súbor** – úplná cesta k pôvodnému umiestneniu infikovaného objektu.
- **Infekcie** – názov detegovaného [spywaru](#) (podrobnosti o konkrétnych vírusoch sa nachádzajú v online [Encyklopédii vírusov](#)).
- **Výsledok** – informuje o momentálnom stave infikovaného objektu, ktorý sa detegoval počas kontroly:
 - o **Infikovaný** – detegovaný infikovaný objekt sa ponechal na pôvodnom mieste (napríklad ak ste [vypli automatické liečenie](#) v nastavení konkrétnej kontroly).
 - o **Vyliečený** – infikovaný objekt sa automaticky vyliečil a ponechal na pôvodnom mieste.
 - o **Premiestnený do Vírusového trezora** – infikovaný objekt sa premiestnil do karantény vo [Vírusovom trezore](#).
 - o **Vymazaný** – infikovaný objekt sa vymazal.
 - o **Pridaný do výnimiek z PNP** – nález sa označil ako výnimka a pridal do zoznamu výnimiek z PNP (nastavuje sa v dialógovom okne [Výnimky z PNP](#) v rozšírených

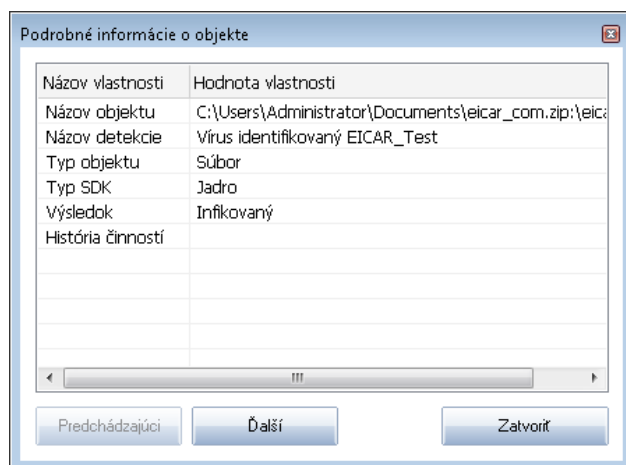
nastaveniach).

- o **Zamknutý súbor – netestovaný** – príslušný objekt je zamknutý a program AVG ho preto nedokáže skontrolovať.
- o **Potenciálne nebezpečný objekt** – objekt bol označený ako potenciálne nebezpečný, nie však infikovaný (môže obsahovať napríklad makrá); informácie považujte len za upozornenie.
- o **Vyžaduje sa reštart na dokončenie akcie** – infikovaný objekt sa nedá odstrániť, na jeho úplné odstránenie musíte reštartovať počítač

Ovládacie tlačidlá

V tomto dialógovom okne sa nachádzajú tri ovládacie tlačidlá:

- **Zobraziť podrobnosti** – toto tlačidlo otvorí nové dialógové okno s názvom **Podrobné informácie o objekte**:



V tomto dialógovom okne sa nachádzajú podrobné informácie o detegovanom infikovanom objekte (napr. názov a umiestnenie infikovaného objektu, typ objektu, typ SDK, výsledky detekcie a história akcií súvisiacich s detegovaným objektom). Tlačidlá **Predchádzajúce/Ďalšie** sa používajú na zobrazenie informácií o konkrétnych nálezoch. Pomocou tlačidla **Zatvoriť** zatvorte toto dialógové okno.

- **Odstrániť vybrané** – toto tlačidlo sa používa na premiestnenie vybraného nálezu do [Vírusového trezora](#)
- **Odstrániť všetky nevylicené** – toto tlačidlo vymaže všetky nálezy, ktoré sa nedajú vyliečiť alebo premiestniť do [Vírusového trezora](#)
- **Zatvoriť výsledky** – zatvorí prehľad a otvorí pôvodné dialógové okno [Prehľad výsledkov kontroly](#).



11.7.4. Karta Upozornenia

Karta **Varovania** zobrazuje informácie o "podozrivých" objektoch (*obyčajne súboroch*) detekovaných počas vyhľadávania. Po detekcii [Rezidentným štítom](#) sa tieto súbory zablokujú, aby k nim nebol možný prístup. Typické príklady týchto druhov nálezov sú: skryté súbory, cookies, podozrivé kľúče registrov, heslom chránené dokumenty alebo archívy, atď. Tieto súbory nepredstavujú priamu hrozbu pre váš počítač ani bezpečnostnú hrozbu. Informácie o týchto súboroch majú význam hlavne v prípade, ak sa zistí prítomnosť škodlivého softvéru typu adware alebo spyware v počítači. Ak sa zobrazujú len upozornenia týkajúce sa prípadov zistených počas testu AVG, nie je potrebné prijať žiadne opatrenie.

Toto je stručný popis najbežnejších príkladov takýchto objektov:

- **Skryté súbory** - skryté súbory sú štandardne neviditeľné v operačnom systéme Windows a niektoré vírusy alebo iné hrozby sa môžu pokúsiť vyhnúť detegovaniu tým, že svoje súbory uložia s týmto atribútom. Ak program AVG nájde skrytý súbor a máte podozrenie, že je škodlivý, môžete ho premiestniť do [Vírusového trezora AVG](#).
- **Cookies** - cookies sú jednoduché textové súbory, ktoré používajú webové stránky na ukladanie špecifických informácií o používateľovi, ktoré sa neskôr použijú na načítanie vlastného rozloženia webovej stránky, automatické vyplnenie mena používateľa a pod.
- **Podozrivé kľúče registrov** - niektorý škodlivý softvér ukladá svoje informácie do registrov operačného systému Windows, aby sa zabezpečilo jeho načítanie pri spustení operačného systému, alebo rozšíril jeho vplyv v operačnom systéme.

11.7.5. Karta Rootkity

Na karte **Rootkity** sa nachádzajú informácie o rootkitoch detegovaných počas [kontroly súčastí](#) [Anti-Rootkit](#).

[Rootkit](#) je program, ktorého cieľom je zmocniť sa základnej kontroly nad počítačom bez súhlasu vlastníka počítača a jeho legitímnych správcov. Prístup k hardvéru sa väčšinou nepožaduje, pretože účelom rootkitu je zmocniť sa kontroly nad operačným systémom spusteným na hardvéri. Rootkity zvyčajne maskujú svoju prítomnosť v systéme rozvratnou činnosťou, alebo vyhýbaním sa štandardným bezpečnostným mechanizmom operačného systému. Často ide aj o trójske kone, ktoré klamlivo presvedčia používateľov, že sa môžu bezpečne spustiť na počítači. Medzi metódy používané na dosiahnutie tohto cieľa patria utajenie spustených procesov pred sledovacími programami, alebo skrývanie súborov alebo systémových dát pred operačným systémom.

Štruktúra tejto karty je v podstate zhodná so štruktúrou [karty Infekcie](#) a [karty Spyware](#).

11.7.6. Karta Informácie

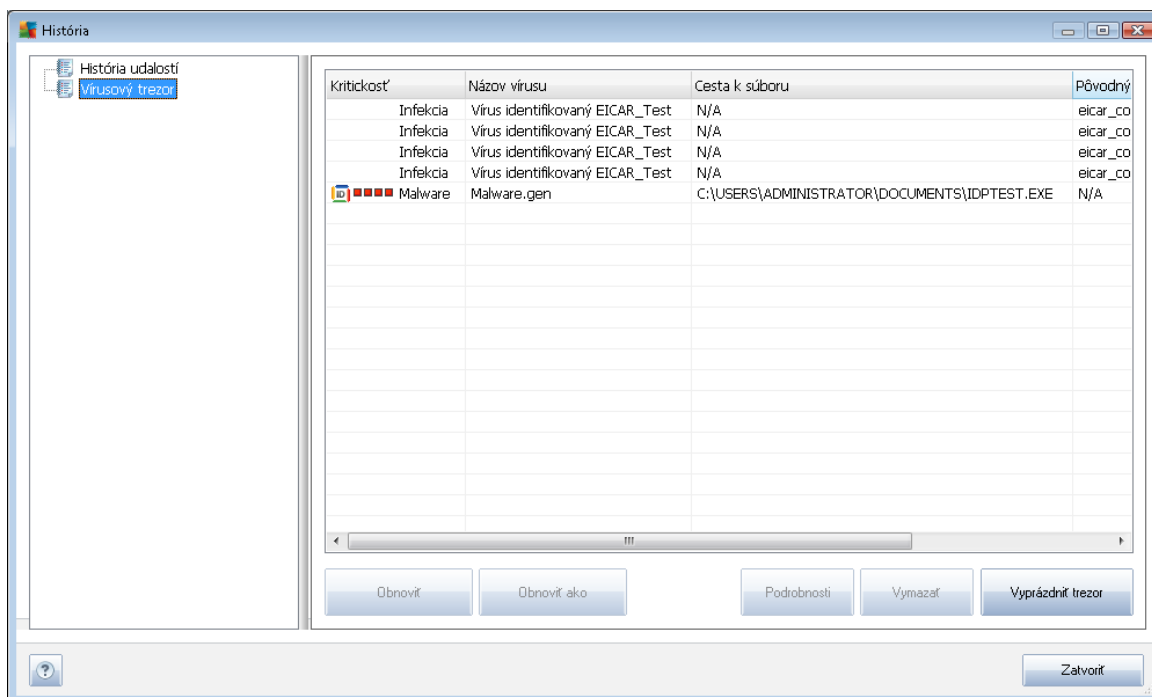
Karta **Informácie** obsahuje údaje o takýchto "nálezoč", ktoré sa nedajú hodnotiť ako infekcie, spyware, atď. Nedajú sa pozitívne označiť ako nebezpečné, zasluhujú si však vašu pozornosť. Programom AVG dokáže pri vyhľadávaní zistiť prítomnosť súborov, ktoré nemusia byť infikované, ale sú podozrivé. Informácia o týchto súboroch sa zobrazí buď ako [Upozornenie](#) alebo ako **Informácia**.

Informácia o závažnosti sa zobrazí pri výskyte ktorejkoľvek z nasledujúcich udalostí:



- **Komprimovaný za chodu** - Súbor bol komprimovaný jedným z menej bežne používaných komprimačných programov, čo môže naznačovať pokus o zabránenie kontrole tohto súboru. Nie každá takáto informácia však znamená výskyt vírusu.
- **Komprimovaný za chodu rekurzívny** - Podobné ako predchádzajúce, ale súbor bol komprimovaný menej často používaným softvérom spomedzi bežných programov. Tieto súbory sú podozrivé a je potrebné zvážiť možnosť odstrániť alebo poslať ich na analýzu.
- **Archív alebo dokument chránený heslom** - Program AVG (a v podstate ani žiaden program na kontrolu výskytu škodlivého kódu) nedokáže prehľadávať súbory chránené heslom.
- **Dokument obsahujúci makrá** - Nahlásený dokument obsahuje makrá, ktoré môžu byť škodlivé.
- **Skrytá prípona** - Súbory so skrytou príponou sa môžu javiť napr. ako obrázky, ale v skutočnosti predstavujú spustiteľné súbory (napr. *obrazok.jpg.exe*). Druhá prípona nie je pri štandardnom nastavení viditeľná pod operačným systémom Windows a AVG upozorní na tieto súbory, aby zabránil ich náhodnému spusteniu.
- **Nesprávna cesta k súboru** - Ak sa niektorý dôležitý systémový súbor spustí z iného ako štandardného umiestnenia (napr. *súbor winlogon.exe spustený z iného priečinka ako Windows*), program AVG upozorní na túto nezrovnalosť. V niektorých prípadoch vírusy používajú názvy štandardných systémových procesov, aby ich prítomnosť v systéme bola menej nápadná.
- **Zamknutý súbor** - Identifikovaný súbor je zamknutý, a preto ho AVG nemôže skontrolovať. Spravidla to znamená, že určitý súbor je neustále používaný systémom (napr. *swapový súbor*).

11.8. Vírusový trezor



Vírusový trezor je bezpečné prostredie na správu podozrivých a infikovaných objektov detegovaných počas testov vykonaných programom AVG. Ak sa počas kontroly deteguje podozrivý objekt a aplikácia AVG ho nedokáže automaticky vyliečiť, program sa vás opýta, čo sa má s podozrivým objektom urobiť. Odporúčame vám, aby ste premiestnili objekt do **Vírusového trezora** pre prípad, ak by ste ho chceli použiť v budúcnosti. Hlavným účelom **Vírusového trezora** je uchovať všetky vymazané súbory počas určitej doby, aby ste mali čas uistiť sa, že súbor naozaj nepotrebujete. Ak zistíte, že odstránenie súboru spôsobuje problémy, môžete ho poslať na analýzu, alebo obnoviť do pôvodného umiestnenia.

Rozhranie **Vírusového trezora** sa otvorí v samostatnom okne a poskytuje prehľad informácií o infikovaných objektoch v karanténe:

- **Úroveň závažnosti** – ak sa rozhodnete nainštalovať súčasť [Identity Protection](#) do programu **AVG Internet Security 2011**, potom sa v tejto časti bude nachádzať grafické znázornenie úrovne závažnosti zisteného nálezu na stupnici so štyrmi úrovňami, od vyhovujúcej (■□□□) až po veľmi nebezpečnú (■□■□); a informácie o type infekcie (na základe úrovne infikovateľnosti – všetky uvedené objekty môžu byť pozitívne alebo potenciálne infikované).
- **Názov vírusu** – uvádza názov detegovanej infekcie podľa [Encyklopédie vírusov](#) (online)
- **Cesta k súboru** – úplná cesta k pôvodnému umiestneniu detegovaného infikovaného súboru.
- **Pôvodný názov objektu** – všetky detegované objekty uvedené v tabuľke boli označené štandardným názvom prideleným programom AVG počas procesu kontroly. Ak mal objekt

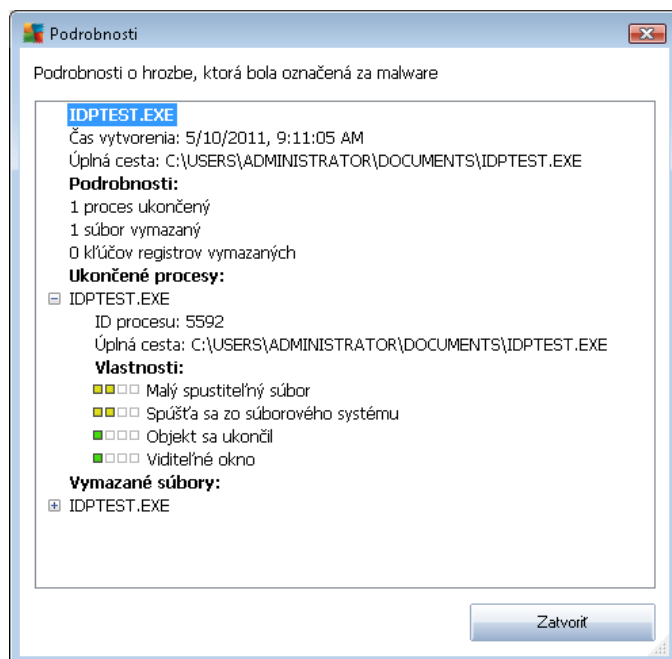
pridelený konkrétny pôvodný názov, ktorý je známy (napr. názov prílohy e-mailu, ktorý nezodpovedá skutočnému obsahu prílohy), bude uvedený v tomto stĺpci.

- **Dátum uloženia** – dátum a čas, kedy bol podozrivý súbor detegovaný a premiestnený do **Vírusového trezora**

Ovládacie tlačidlá

V rozhraní **Vírusového trezora** sa nachádzajú tieto ovládacie tlačidlá:

- **Obnoviť** – premiestni infikovaný súbor naspäť do pôvodného umiestnenia na disku.
- **Obnoviť ako** – premiestni infikovaný súbor do vybraného priečinka
- **Podrobnosti** – toto tlačidlo sa používa len v súvislosti s hrozbami detegovanými súčasťou **Identity Protection**. Po kliknutí sa zobrazí súhrnný prehľad informácií o hrozbe (ktoré súbory alebo procesy boli ovplyvnené, vlastnosti procesov atď.). Upozorňujeme, že pre všetky ostatné položky (okrem detegovaných súčastí Identity Protection) je toto tlačidlo sivé a neaktívne!



- **Vymazať** – dokonale a nenávratne odstráni infikovaný súbor z **Vírusového trezora**.
- **Vyprázdniť trezor** – dokonale vymaže celý obsah **Vírusového trezora**. Odstránením z **Vírusového trezora** sa súbory úplne a nenávratne odstránia z disku (nepremiestnia sa do Koša).



12. Aktualizácie AVG

Neustále aktualizovanie programu AVG je dôležité na to, aby sa čo najskôr detegovali novo objavené vírusy.

Keďže sa aktualizácie pre programy AVG nevydávajú podľa pevne stanoveného harmonogramu, ale skôr ako reakcia na počet a závažnosť nových hrozieb, odporúčame vám, aby ste kontrolovali nové aktualizácie najmenej raz za deň alebo ešte častejšie. Len týmto spôsobom získate istotu, že bude program **AVG Internet Security 2011** vždy aktualizovaný aj počas dňa.

12.1. Úrovne aktualizácie

AVG ponúka dve úrovne aktualizácie, z ktorých si môžete vybrať:

- **Aktualizácia definícií** obsahuje zmeny potrebné na dosiahnutie spoľahlivej ochrany pred vírusmi. Zvyčajne neobsahuje žiadne zmeny kódu a aktualizuje len databázu definícií. Táto aktualizácia by sa mala použiť čo možno najskôr.
- **Aktualizácia programu** obsahuje rôzne zmeny programu, doplnky a vylepšenia.

Pri [plánovaní aktualizácie](#) môžete nastaviť, ktorú úroveň priority chcete prevziať a použiť.

Poznámka: Ak sa čas naplánovanej aktualizácie programu náhodou prekrýva s naplánovaným prehľadávaním, potom má proces aktualizácie vyššiu prioritu a prehľadávanie sa preruší.

12.2. Typy aktualizácie

Rozlišujeme dva typy aktualizácie:

- **Aktualizácia na požiadanie** je okamžitá aktualizácia programu AVG, ktorú je možné spustiť vždy, keď je to potrebné.
- **Naplánovaná aktualizácia** – program AVG zároveň umožňuje [vopred nastaviť plán aktualizácie](#). Plánovaná aktualizácia sa potom bude vykonávať pravidelne podľa nastavenej konfigurácie. Keď sa na uvedenom mieste nachádzajú nové aktualizčné súbory, prevezmú sa buď priamo z internetu alebo sieťového adresára. Keď nie sú dostupné žiadne nové aktualizácie, nič sa nestane.

12.3. Proces aktualizácie

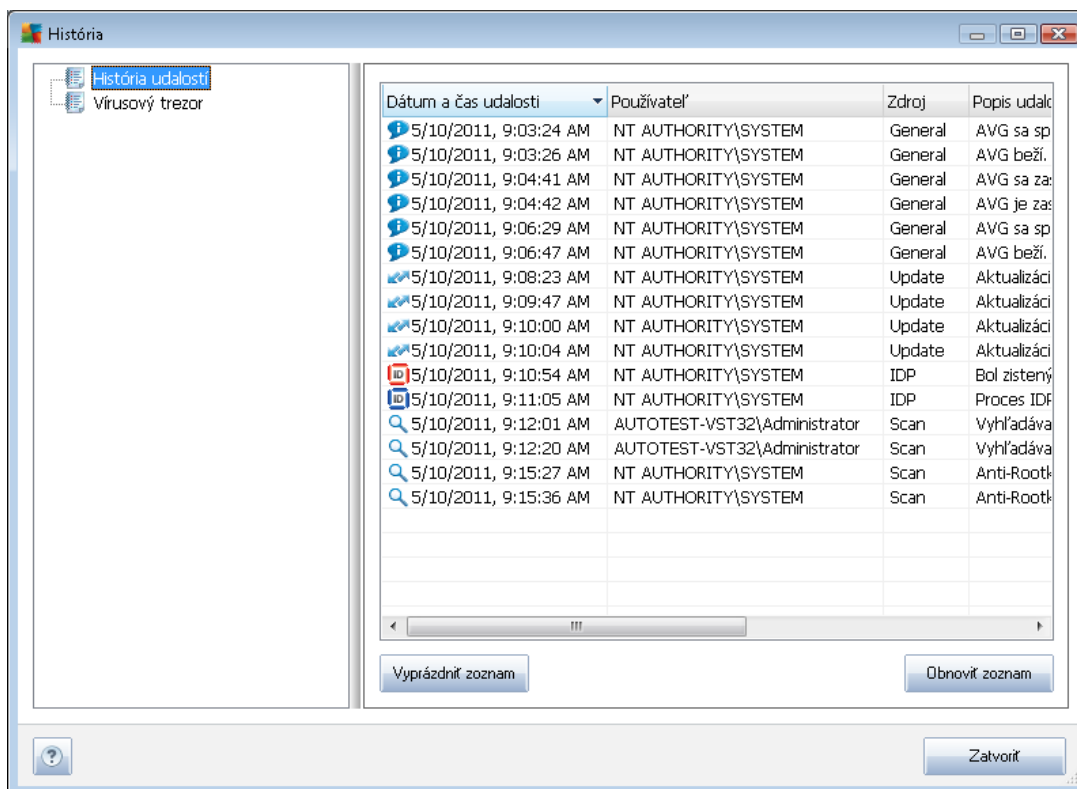
Proces aktualizácie môžete spustiť kedykoľvek podľa potreby kliknutím na [odkaz Aktualizovať teraz](#). Tento odkaz sa vždy nachádza v každom dialógovom okne [používateľského rozhrania AVG](#). Napriek tomu vám však odporúčame robiť aktualizácie pravidelne podľa plánu aktualizácie, ktorý sa nastavuje v súčasti [Update Manager](#).

Po spustení aktualizácie program AVG najskôr skontroluje, či sú k dispozícii nové aktualizčné súbory. Ak nájde nové aktualizácie, začne ich preberať a spustí samotný proces aktualizácie. Počas procesu aktualizácie sa otvorí rozhranie **aktualizácie**, ktoré informuje o priebehu procesu v grafickej podobe, a v ktorom sa zároveň nachádza prehľad súvisiacich štatistických parametrov (*veľkosť aktualizčného súboru, prijaté dáta, rýchlosť preberania, uplynutý čas...*).



Poznámka: Pred spustením aktualizácie programu AVG sa vytvorí bod obnovenia systému. Ak proces aktualizácie zlyhá a operačný systém spadne, tento bod obnovenia umožní obnoviť stav operačného systému s pôvodnou konfiguráciou. Prístup k tejto možnosti je cez ponuku Štart/Programy/Príslušenstvo/Systémové nástroje/Obnovenie systému. Zmeny týchto nastavení odporúčame robiť len skúseným používateľom!

13. História udalostí



Dialógové okno **História udalostí** sa otvára v [ponuke programu](#) kliknutím na položku **História/Protokol histórie udalostí**. V tomto dialógovom okne sa nachádza prehľad významných udalostí, ktoré sa vyskytli v čase, keď bol program **AVG Internet Security 2011** spustený. **História** zaznamenáva tieto typy udalostí:

- Informácie o aktualizáciách aplikácie AVG
- Spustenie, ukončenie a zastavenie prehľadávania (vrátane automaticky vykonávaných testov)
- Udalosti spojené s detekciou vírusov (súčasťou [Rezidentný štít](#) alebo [prehľadávanim](#)), vrátane miesta výskytu
- Iné významné udalosti

Každá udalosť má uvedené tieto informácie:

- **Dátum a čas udalosti** informuje o presnom dátume a čase výskytu udalosti.
- **Používateľ** informuje o osobe, ktorá spustila danú udalosť.
- **Zdroj** informuje o súčasti alebo inej časti systému AVG, ktorá pôvodne spustila udalosť.



- **Opis udalosti** obsahuje stručný prehľad o tom, čo sa v skutočnosti udialo.

Ovládacie tlačidlá

- **Vyprázdniť zoznam** – vymaže všetky položky zo zoznamu udalostí.
- **Obnoviť zoznam** – aktualizuje všetky položky zoznamu udalostí.



14. FAQ a technická podpora

Ak narazíte na problémy s programom AVG, či už obchodné alebo technické, nahliadnite do časti [FAQ](http://www.avg.com/) na webových stránkach AVG (<http://www.avg.com/>).

Ak ani tu nenájdete pomoc, kontaktujte oddelenie technickej pomoci e-mailom. Použite, prosím, kontaktný formulár dostupný v systémovej ponuke cez **Pomoc/Získať pomoc online**.