



AVG AntiVirus

Používateľská príručka

Revízia dokumentu AVG.07 (25/11/2016)

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



Obsah

1. Úvod	3
2. Požiadavky na inštaláciu AVG	4
2.1 Podporované operačné systémy	4
2.2 Minimálne a odporúčané hardvérové požiadavky	4
3. Proces inštalácie AVG	5
3.1 Vitajte!	5
3.2 Zadaťte vaše licenčné číslo	6
3.3 Prispôbiť inštaláciu	8
3.4 Inštalácia AVG	9
3.5 Inštalácia dokončená	10
4. Po inštalácii	11
4.1 Aktualizácia vírusovej databázy	11
4.2 Registrácia produktu	11
4.3 Otvorenie používateľského rozhrania	11
4.4 Kontrola celého počítača	11
4.5 Test EICAR	11
4.6 Predvolená konfigurácia AVG	12
5. Používateľské rozhranie AVG	13
5.1 Horný navigačný rad	14
5.2 Informácie o stave zabezpečenia	17
5.3 Prehľad súčastí	18
5.4 Moje aplikácie	19
5.5 Kontrola/Aktualizovať rýchle odkazy	19
5.6 Ikona v paneli úloh	20
5.7 AVG Advisor	21
5.8 AVG Akcelerátor	21
6. Súčasti AVG	22
6.1 Ochrana počítača	22
6.2 Ochrana prezerania webu	25
6.3 Software Analyzer	27
6.4 Ochrana e-mailu	28
6.5 PC Analyzer	29
7. Rozšírené nastavenia AVG	31
7.1 Vzhľad	31
7.2 Zvuky	33
7.3 Dočasne vypnúť ochranu AVG	34
7.4 Ochrana počítača	35
7.5 Kontrola pošty	39



7.6 Ochrana prezerania webu	49
7.7 Software Analyzer	52
7.8 Kontroly	53
7.9 Plány	58
7.10 Aktualizácia	64
7.11 Výnimky	68
7.12 Vírusový trezor	70
7.13 AVG Sebaochrana	71
7.14 Preferencie ochrany osobných údajov	71
7.15 Ignorovať chybový stav	73
7.16 Advisor – známe siete	74
8. Kontrola AVG	75
8.1 Vopred definované kontroly	76
8.2 Kontrola z prieskumníka	86
8.3 Kontrola z príkazového riadka	86
8.4 Plánovanie kontrol	90
8.5 Výsledky kontrol	96
8.6 Podrobnosti výsledkov kontrol	97
9. AVG File Shredder	99
10. Vírusový trezor	100
11. História	101
11.1 Výsledky kontrol	101
11.2 Nálezy súčasti Rezidentný štít	102
11.3 Nálezy súčasti Identity Protection	105
11.4 Nálezy súčasti Ochrana e-mailu	106
11.5 Nálezy súčasti Webový štít	107
11.6 Protokol histórie udalostí	109
12. Aktualizácie AVG	110
13. Najčastejšie otázky a technická podpora	111



1. Úvod

Táto príručka je podrobnou používateľskou dokumentáciou pre produkt **AVG AntiVirus**.

AVG AntiVirus ponúka ochranu v reálnom čase pred najdômyselnejšími súčasnými hrozbami. Môžete v bezpečí chatovať, sťahovať a vymieňať si súbory, hrať hry a sledovať videá bez akéhokoľvek prerušenia. Môžete sťahovať a zdieľať súbory a bezpečne odosielať správy, používať sociálne siete a surfovať či vyhľadávať informácie s ochranou v reálnom čase.

Môžete využiť aj ďalšie zdroje informácií:

- **Súbor pomocníka:** Časť *Odstraňovanie problémov* je k dispozícii priamo v súbore pomocníka v produkte **AVG AntiVirus** (súbor pomocníka otvoríte stlačením klávesu *F1* v akomkoľvek dialógovom okne aplikácie). V tejto časti nájdete zoznam najčastejších situácií, v ktorých používateľ potrebuje vyhľadať profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím zobrazte podrobné pokyny vedúce k riešeniu daného problému.
- **Webová stránka centra podpory AVG:** Riešenie problému môžete prípadne vyhľadať aj na webovej stránke AVG (<http://www.avg.com/>). V časti **Podpora** nájdete prehľad tematických skupín zaoberajúcich sa otázkami týkajúcimi sa predaja, technickými otázkami, štruktúrovanú časť častých otázok a všetky dostupné kontakty.
- **AVG ThreatLabs:** Osobitná webová stránka spojená s AVG (<http://www.avg.com/about-viruses>) venovaná problémom s vírusmi, ktorá poskytuje štruktúrovaný prehľad informácií súvisiacich s hrozbami online. Môžete tu tiež nájsť pokyny na odstraňovanie vírusov, spyware a rady na zachovanie ochrany.
- **Diskusné fórum:** Môžete tiež využiť diskusné fórum používateľov AVG na adrese <http://community.avg.com/>.



2. Požiadavky na inštaláciu AVG

2.1. Podporované operačné systémy

AVG AntiVirus je určený na ochranu pracovných staníc s nasledujúcimi operačnými systémami:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (všetky edície)
- Windows 7 (všetky edície)
- Windows 8 (všetky edície)
- Windows 10 (všetky edície)

(a prípadne s novšími balíkmi Service Pack – platí pre určité operačné systémy)

2.2. Minimálne a odporúčané hardvérové požiadavky

Minimálne hardvérové požiadavky pre produkt **AVG AntiVirus**:

- Procesor Intel Pentium 1,5 GHz alebo rýchlejší
- 512 MB (Windows XP)/1 024 MB (Windows Vista, Windows 7) pamäte RAM
- 1,3 GB voľného miesta na pevnom disku (*na účely inštalácie*)

Odporúčané hardvérové požiadavky pre produkt **AVG AntiVirus**:

- Procesor Intel Pentium 1,8 GHz alebo rýchlejší
- 512 MB (Windows XP)/1 024 MB (Windows Vista, Windows 7) pamäte RAM
- 1,6 GB voľného miesta na pevnom disku (*na účely inštalácie*)



3. Proces inštalácie AVG

Na nainštalovanie programu **AVG AntiVirus** do počítača sa musí použiť najnovší inštalačný súbor. Aby ste sa uistili, že inštalujete najnovšiu verziu aplikácie **AVG AntiVirus**, odporúčame vám stiahnuť inštalačný súbor priamo z webovej lokality spoločnosti AVG (<http://www.avg.com/>). V časti **Podpora** sa nachádza štruktúrovaný prehľad inštalačných súborov pre každú z edícií AVG. Po stiahnutí a uložení inštalačného súboru na váš pevný disk môžete spustiť proces inštalácie. Postup inštalácie predstavuje rad následných jednoduchých a prehľadných dialógových okien. Každé dialógové okno obsahuje stručné informácie o jednotlivých krokoch procesu inštalácie. Ďalej ponúkame podrobné vysvetlenia každého z dialógových okien:

3.1. Vitajte!

Proces inštalácie začína dialógovým oknom **Víta vás AVG Internet Security**:



Výber jazyka

V tomto dialógovom okne zvolíte jazyk, ktorý sa použije pri procese inštalácie. Kliknutím na rozbaľovacie pole pri možnosti **Jazyk** zobrazíte ponuku jazykov. Vyberte požadovaný jazyk a proces inštalácie bude pokračovať ďalej v jazyku podľa vášho výberu. Aplikácia bude taktiež komunikovať vo vybranom jazyku, pričom budete mať možnosť prepnúť do angličtiny, ktorá sa vždy inštaluje automaticky.

Licenčná zmluva s koncovým používateľom a Ochrana osobných údajov

Odporúčame vám, aby ste sa pred tým, ako budete pokračovať v procese inštalácie, zoznámili s dokumentmi **Licenčná zmluva s koncovým používateľom** a **Ochrana osobných údajov**. Prístup k obojm dokumentom získate prostredníctvom aktívnych odkazov v spodnej časti dialógového okna. Kliknite na ktorýkoľvek z hypertextových odkazov, aby ste otvorili nové dialógové okno/nové okno prehliadača, v ktorom bude uvedené



plné znenie príslušnej listiny. Pozorne si prečítajte tieto právne záväzné dokumenty. Kliknutím na tlačidlo **Pokračovať** potvrdíte, že súhlasíte s týmito dokumentmi.

Pokračujte v inštalácii

Na pokračovanie inštalácie jednoducho kliknite na tlačidlo **Pokračovať**. Budete požiadaní o vaše licenčné číslo a potom bude inštalčný proces prebiehať v plne automatickom režime. Pre väčšinu používateľov sa odporúča, aby použili túto štandardnú možnosť inštalácie **AVG AntiVirus**, v ktorej všetky nastavenia vopred definoval dodávateľ programu. Táto konfigurácia poskytuje maximálne zabezpečenie s optimálnym využitím zdrojov. Ak v budúcnosti budete potrebovať zmeniť konfiguráciu, vždy to bude možné priamo v aplikácii.

Prípadne máte k dispozícii možnosť **Vlastná inštalácia**, a to vo forme hypertextového odkazu umiestneného pod tlačidlom **Pokračovať**. Vlastnú inštaláciu by mali používať len skúsení používatelia, ktorí majú skutočný dôvod inštalovať aplikáciu s neštandardnými nastaveniami, napr. na účely prispôsobenia konkrétnym systémovým potrebám. Ak sa rozhodnete pre tento spôsob, po vyplnení licenčného čísla budete presmerovaní na dialógové okno **Prispôbiť inštaláciu**, kde môžete zadať svoje nastavenia.

3.2. Zadajte vaše licenčné číslo

V dialógovom okne **Zadajte vaše licenčné číslo** budete vyzvaní aktivovať si svoju licenciu jej vpísaním (alebo použitím metódy kopírovať a prilepiť) do príslušného textového poľa:

Kde nájdem svoje licenčné číslo?

Predajné číslo sa nachádza na obale disku CD v škatuli **AVG AntiVirus**. Licenčné číslo sa bude nachádzať v potvrdzovacom e-maile, ktorý ste dostali po zakúpení produktu **AVG AntiVirus** 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.



Ako používať metódu Kopírovať a prilepiť

Pomocou metódy **Kopírovať a prilepiť** zadajte licenčné číslo **AVG AntiVirus** do programu. Tak zabezpečíte zadanie správneho čísla. Postupujte podľa nasledujúcich pokynov:

- Otvorte e-mail s vaším licenčným číslom.
- Kliknite ľavým tlačidlom myši na začiatok licenčného čísla, podržte tlačidlo stlačené a presuňte kurzor myši na koniec čísla. Potom tlačidlo uvoľnite. Číslo by sa malo teraz zvýrazniť.
- Stlačte a podržte kláves **Ctrl**, a potom stlačte kláves **C**. Tým číslo skopírujete.
- Nasmerujte kurzor a kliknite na miesto, kam chcete skopírované číslo vložiť, t. j. do textového poľa dialógového okna **Zadajte vaše licenčné číslo**.
- Stlačte a podržte kláves **Ctrl** a potom stlačte kláves **V**. Tým prilepíte číslo na vybrané miesto.

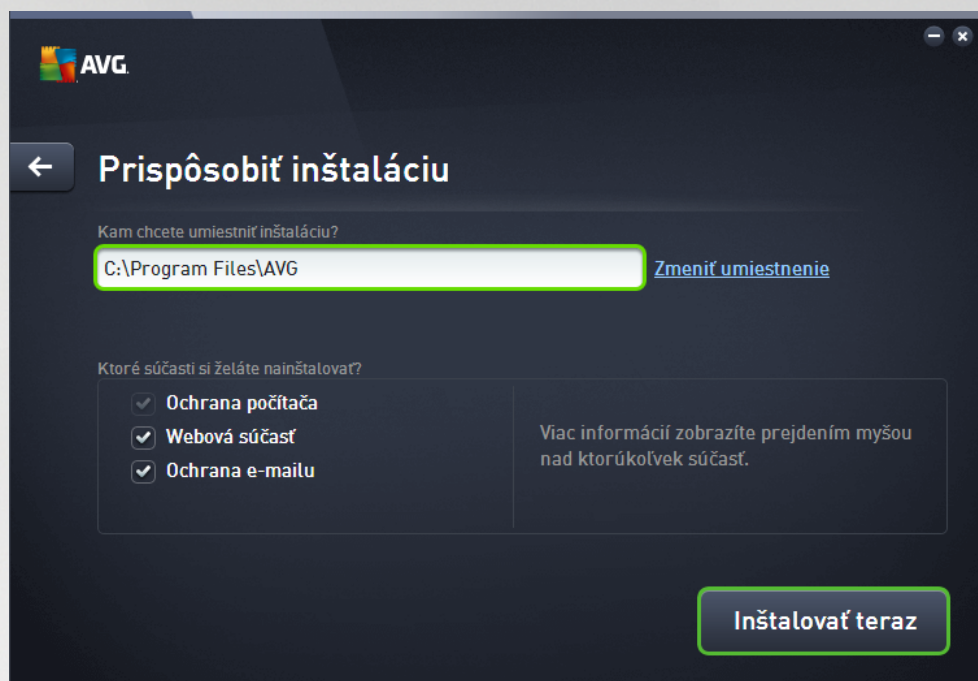
Pokračujte v inštalácii

V dolnej časti dialógového okna vidíte tlačidlo **Inštalovať teraz**. Tlačidlo sa aktivuje zadáním vášho licenčného čísla. Po aktivácii jednoducho kliknite na toto tlačidlo, aby ste spustili proces inštalácie. V prípade, že nemáte k dispozícii platné licenčné číslo, môžete si vybrať možnosť inštalácie bezplatnej edície aplikácie **AVG AntiVirus Free Edition**. Bezplatné edície však žiaľ nepodporujú všetky funkcie, ktoré sú k dispozícii v plnej profesionálnej verzii. Preto môžete zvážiť návštevu webovej stránky AVG (<http://www.avg.com/>) a dozvedieť sa tu podrobné informácie o nákupe a upgrade AVG.



3.3. Prispôbiť inštaláciu

Dialógové okno **Prispôbiť inštaláciu** vám umožňuje nastaviť podrobné parametre inštalácie:



Kam chcete umiestniť inštaláciu?

Tu môžete určiť, kam chcete nainštalovať túto aplikáciu. Adresa v textovom poli označuje navrhnuté umiestnenie v priečinku Programové súbory. Ak by ste sa rozhodli pre iné umiestnenie, kliknite na odkaz **Zmeniť umiestnenie**, ktorým otvoríte nové okno so stromovou štruktúrou vášho disku. Potom prejdite na želané umiestnenie a potvrdte.

Ktoré súčasti si želáte nainštalovať?

Táto časť uvádza prehľad všetkých súčastí, ktoré je možné inštalovať. Ak vám predvolené nastavenia nevyhovujú, môžete odstrániť konkrétne súčasti. Môžete však vyberať len zo súčastí, ktoré sú zahrnuté v produkte AVG AntiVirus. Jedinou výnimkou je súčasť **Ochrana počítača**, ktorú nie je možné z inštalácie vylúčiť. Po zvýraznení akejkoľvek položky v tejto časti sa na pravej strane zobrazí krátky popis danej súčasti. Ďalšie informácie o funkciách jednotlivých súčastí sa nachádzajú v kapitole [Prehľad súčastí](#) v tejto dokumentácii.

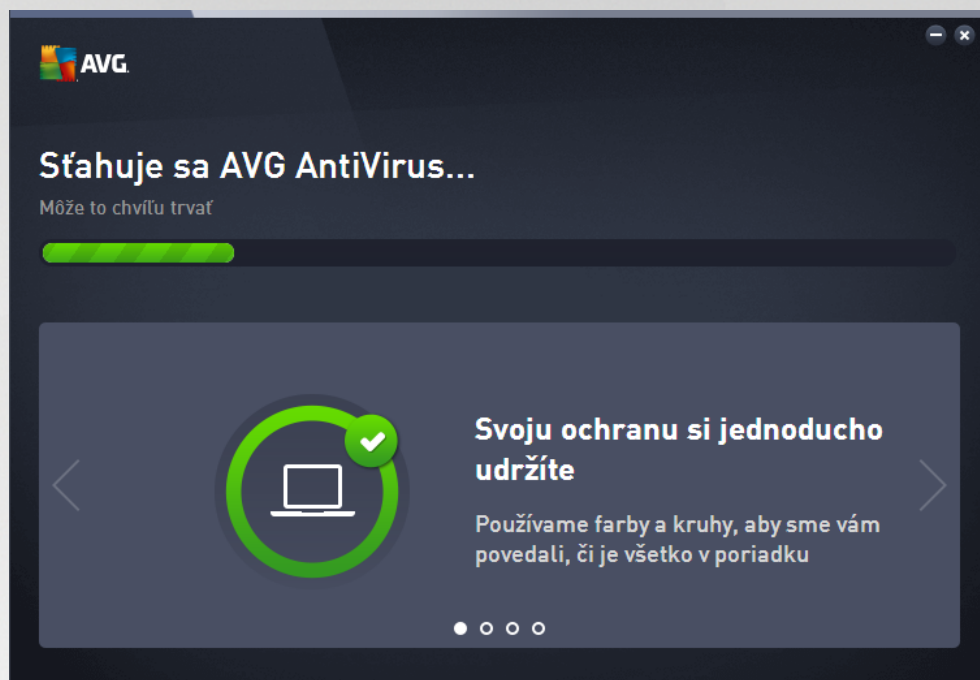
Pokračujte v inštalácii

Na pokračovanie inštalácie jednoducho kliknite na tlačidlo **Inštalovať teraz**. Prípadne, ak potrebujete zmeniť či overiť vaše jazykové nastavenia, sa môžete vrátiť o jeden krok na predchádzajúce dialógové okno pomocou tlačidla šípky  v hornej časti tohto dialógového okna.



3.4. Inštalácia AVG

Po potvrdení spustenia inštalácie v predchádzajúcom dialógovom okne sa spustí proces inštalácie v plne automatickom režime a nevyžaduje žiadne zásahy:

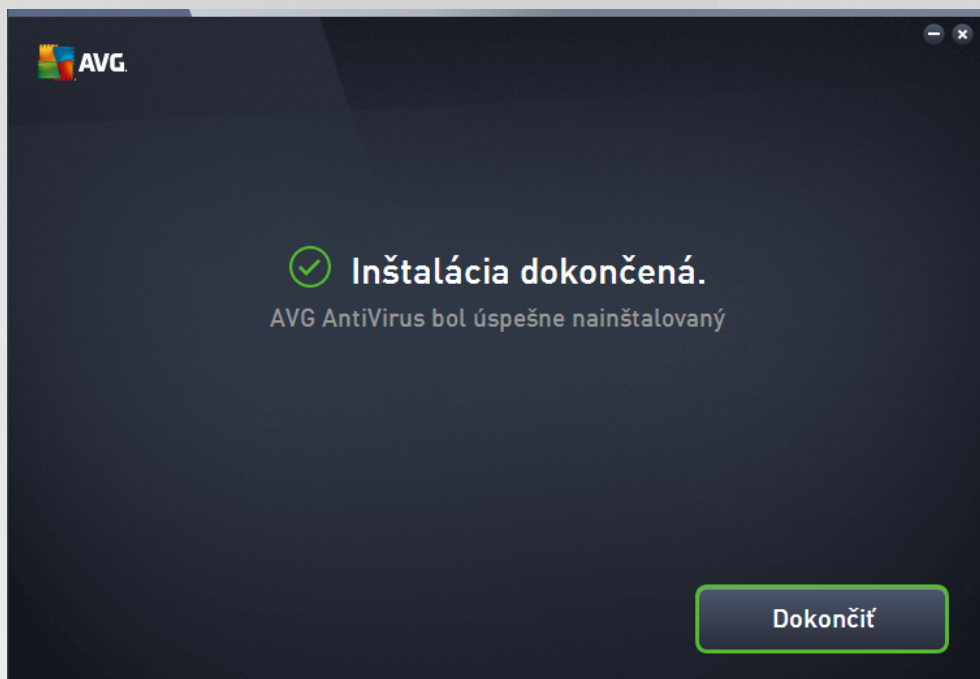


Po dokončení procesu inštalácie budete automaticky presmerovaní na ďalšie dialógové okno.



3.5. Inštalácia dokončená

Dialógové okno **Inštalácia dokončená** potvrdí, že je program AVG AntiVirus plne nainštalovaný a nastavený:



Kliknutím na tlačidlo **Dokončiť** dokončíte proces inštalácie.



4. Po inštalácii

4.1. Aktualizácia vírusovej databázy

Upozorňujeme, že po inštalácii (po reštarte počítača, ak sa vyžaduje) **AVG AntiVirus** automaticky aktualizuje svoju vírusovú databázu a všetky súčasti a pripravuje ich na použitie. To môže trvať niekoľko minút. Keď proces aktualizácie prebieha, budete na to upozornení informáciou, ktorá sa zobrazí v hlavnom dialógovom okne. Počkajte chvíľu, pokiaľ neskončí proces aktualizácie a nebudete mať **AVG AntiVirus** úplne spustený a pripravený na to, aby vás chránil!

4.2. Registrácia produktu

Po nainštalovaní produktu **AVG AntiVirus** zaregistrujte produkt on-line na webovej lokalite AVG (<http://www.avg.com/>). Registráciou získate úplný prístup k používateľskému účtu AVG, informáciám o aktualizáciách AVG a ďalším službám poskytovaným výhradne registrovaným používateľom. Najjednoduchší spôsob registrácie je priamo z používateľského rozhrania aplikácie **AVG AntiVirus**. Označte položku [v hornom navigačnom pruhu Možnosti/Zaregistrovať teraz](#). Budete presmerovaní na stránku **Registrácia** na webovej lokalite AVG (<http://www.avg.com/>). Postupujte podľa pokynov na tejto stránke.

4.3. Otvorenie používateľského rozhrania

[Hlavné dialógové okno AVG](#) sa otvára niekoľkými spôsobmi:

- dvakrát kliknite na ikonu AVG AntiVirus v [paneli úloh](#),
- dvakrát kliknite na ikonu AVG Protection na pracovnej ploche,
- z ponuky *Štart/Všetky programy/AVG/AVG Protection*.

4.4. Kontrola celého počítača

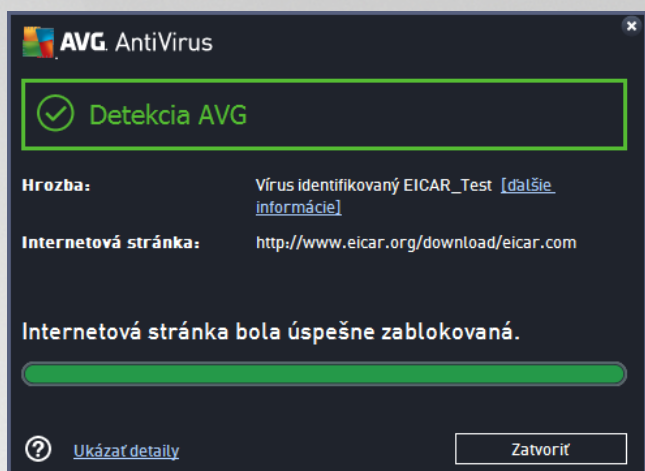
Existuje potenciálne riziko, že sa do vášho počítača dostal počítačový vírus ešte pred nainštalovaním produktu **AVG AntiVirus**. Z tohto dôvodu by ste mali spustiť [Kontrolu celého počítača](#), aby sa vylúčila možnosť existencie infekcie v počítači. Prvá kontrola môže istý čas trvať (približne hodinu), no odporúča sa ju nechať dokončiť, aby ste sa uistili, že váš počítač nie je v ohrození. Pokyny na spustenie [Kontroly celého počítača](#) sa nachádzajú v kapitole [Kontrola programom AVG](#).

4.5. Test EICAR

Pre potvrdenie správnej inštalácie **AVG AntiVirus** môžete vykonať test EICAR.

Test EICAR je štandardná a absolútne bezpečná metóda, ktorá sa používa na testovanie funkcie antivírusového systému. Je bezpečná, pretože v skutočnosti nejde o vírus a neobsahuje žiadne fragmenty vírusového kódu. Väčšina produktov naň reaguje ako keby išlo o vírus (aj keď ho obyčajne označia jasným názvom, ako napríklad „EICAR-AV-Test“). Vírus EICAR si môžete stiahnuť na internetových stránkach EICAR na adrese www.eicar.com, kde nájdete aj všetky potrebné informácie o teste EICAR.

Stiahnite si súbor *eicar.com* a uložte ho na pevný disk počítača. Hneď po potvrdení stiahnutia testovacieho súboru **AVG AntiVirus** naň zareaguje varovaním. Zobrazenie tohto oznámenia znamená, že je program AVG správne nainštalovaný v počítači.



Ak sa programu AVG nepodarí identifikovať testovací súbor EICAR ako vírus, skontrolujte ešte raz konfiguráciu programu!

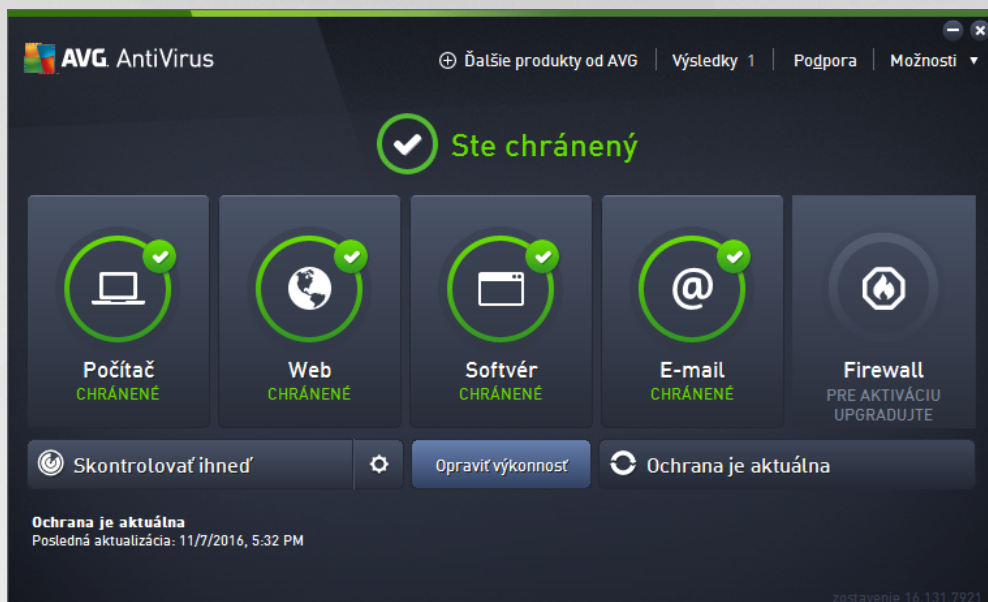
4.6. Predvolená konfigurácia AVG

Predvolenú konfiguráciu, (t. j. nastavenie aplikácie bezprostredne po inštalácii) produktu **AVG AntiVirus**, nastavil dodávateľ softvéru tak, aby všetky súčasti a funkcie fungovali optimálnym spôsobom. **Nemeňte konfiguráciu AVG, ak na to nemáte vážny dôvod! Zmeny nastavení by mali vykonávať len skúsení používatelia.** Ak chcete upraviť konfiguráciu programu AVG podľa svojich potrieb, prejdite do časti [Rozšírené nastavenia programu AVG](#): vyberte položku Hlavnej ponuky Možnosti/Rozšírené nastavenia a upravte konfiguráciu programu AVG v novootvorenom dialógovom okne [Rozšírené nastavenia programu AVG](#).



5. Používateľské rozhranie AVG

AVG AntiVirus otvorí hlavné okno:



Hlavné okno je rozdelené na niekoľko častí:

- **Navigácia v hornom riadku** obsahuje štyri aktívne odkazy zoradené v hornej časti hlavného okna (*Ďalšie produkty od AVG*, *Správy*, *Podpora*, *Možnosti*). [Podrobnosti >>](#)
- **Informácie o stave zabezpečenia** je časť so základnými informáciami o aktuálnom stave vášho **AVG AntiVirus**. [Podrobnosti >>](#)
- **Prehľad nainštalovaných súčastí** nájdete vo vodorovnom pruhu blokov v strednej časti hlavného okna. Súčasti sú zobrazené ako zelené obdĺžniky s ikonou príslušnej súčasti. Poskytujú informácie o jej stave. [Podrobnosti >>](#)
- **Moje aplikácie** sú graficky znázornené v dolnom pruhu hlavného okna a obsahujú prehľad aplikácií dopĺňujúcich **AVG AntiVirus**, ktoré sú na počítači buď už nainštalované, alebo sa ich inštalácia odporúča. [Podrobnosti >>](#)
- **Rýchle odkazy Kontrola/Oprava/Aktualizácia** sa nachádzajú v dolnom pruhu hlavného okna. Tieto tlačidlá umožňujú okamžitý prístup k väčšine najdôležitejších a najčastejšie používaných funkcií programu AVG. [Rýchle odkazy Podrobnosti>>](#)

Okrem hlavného okna **AVG AntiVirus** existuje ešte jedna kontrolná súčasť, cez ktorú máte prístup k aplikácii:

- **Ikona v paneli úloh** sa nachádza v pravom dolnom rohu monitora (*v paneli úloh*) a zobrazuje aktuálny stav **AVG AntiVirus**. [Podrobnosti >>](#)



5.1. Horný navigačný rad

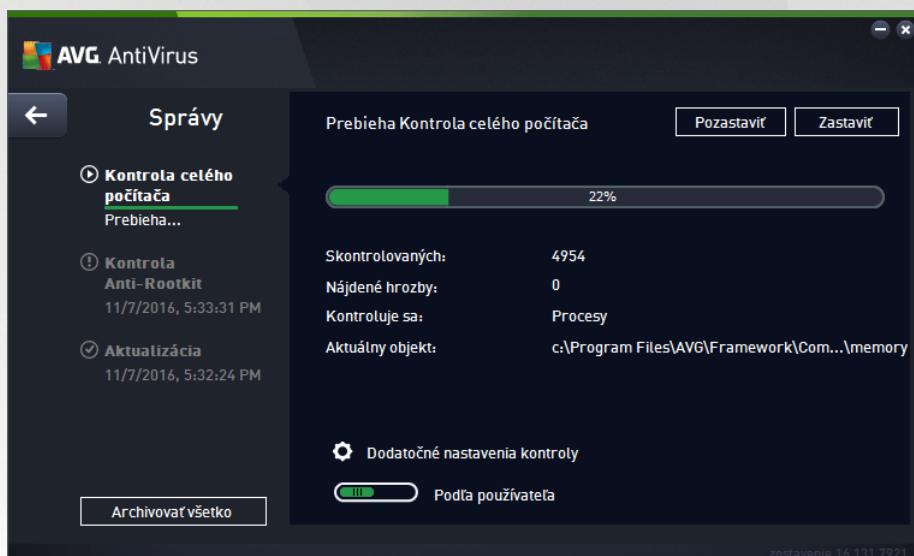
Horný navigačný rad sa skladá z radu viacerých aktívnych odkazov v hornej časti hlavného okna. Navigácia obsahuje tieto tlačidlá:

5.1.1. Ďalšie produkty od AVG

Jedným kliknutím na odkaz sa pripojíte ku webovej stránke AVG, kde nájdete všetky informácie o ochrane AVG pre vašu maximálnu bezpečnosť na internete.

5.1.2. Správy

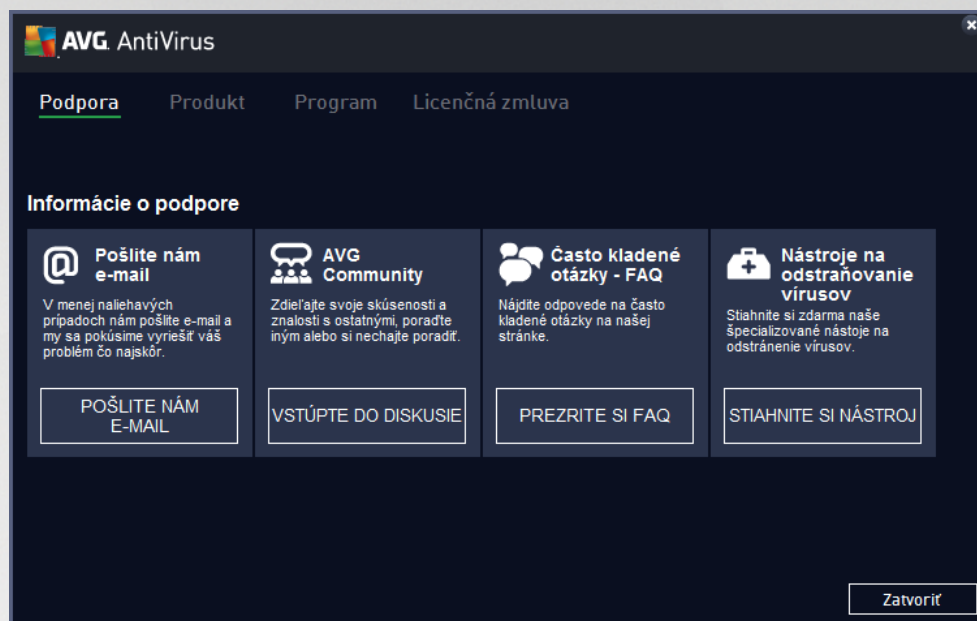
Otvorí sa nové dialógové okno **Správy** s prehľadom všetkých dôležitých správ o predchádzajúcich kontrolách a aktualizáciách. Ak práve prebieha kontrola alebo aktualizácia, vedľa textu **Správy** v hornom navigačnom pruhu [hlavného používateľského rozhrania](#) sa zobrazí otáčajúci sa krúžok. Kliknutím na tento krúžok sa zobrazí dialógové okno s informáciami o stave prebiehajúceho procesu:





5.1.3. Podpora

Otvorí sa nové dialógové okno rozdelené na štyri karty, v ktorých sa nachádzajú všetky dôležité informácie o aplikácii **AVG AntiVirus**:



- **Licencia a podpora** – táto karta poskytuje informácie o názve produktu, licenčnom čísle a dátume ukončenia platnosti. V dolnej časti dialógového okna nájdete tiež zrozumiteľne zostavený prehľad všetkých dostupných kontaktov na zákaznícku podporu. V tejto karte sa nachádzajú tieto aktívne odkazy a tlačidlá:
 - o **Znovu aktivovať** – kliknutím otvoríte nové dialógové okno **Aktivovať softvér AVG**. Vyplňte licenčné číslo do príslušného políčka a nahradte tak predajné číslo (ktoré používate počas inštalácie AVG AntiVirus) alebo zmeňte aktuálne licenčné číslo na iné (napr. pri upgradovaní na vyšší produkt AVG).
 - o **Kopírovať do schránky** – tento odkaz použijete na skopírovanie licenčného čísla, aby ste ho potom mohli prilepiť na miesto, kam potrebujete. Takto zaistíte, že licenčné číslo zadáte správne.
 - o **Predĺžiť teraz** – odporúčame vám, aby ste si kúpili predĺženie licencie **AVG AntiVirus** v dostatočnom predstihu, aspoň jeden mesiac pred vypršaním platnosti aktuálnej licencie. O blížiacom sa vypršaní platnosti budete informovaní. Po kliknutí na tento odkaz budete presmerovaní na webovú lokalitu AVG (<http://www.avg.com/>), kde nájdete podrobné informácie o stave vašej licencie, dátume konca jej platnosti a ponuku na predĺženie/upgrade.
- **Produkt** – na tejto karte sa nachádza prehľad najdôležitejších technických údajov **AVG AntiVirus**, týkajúcich sa informácií o antivírusovom produkte, nainštalovaných súčiastiach a nainštalovanej ochrane e-mailu.
- **Program** – na tejto karte nájdete podrobné technické informácie o nainštalovanom produkte **AVG AntiVirus**, ako napríklad číslo hlavnej verzie produktu a zoznam všetkých čísel verzií všetkých príslušných produktov (napr. *Zen*, *PC TuneUp* atď.). Ďalej sa na tejto karte uvádza prehľad všetkých



nainštalovaných súčastí a konkrétne informácie o zabezpečení (číslo verzií vírusovej databázy a nástroja Link Scanner).

- **Licenčná zmluva** – na tejto karte sa nachádza plné znenie licenčnej zmluvy medzi vami a spoločnosťou AVG Technologies.

5.1.4. Možnosti

Údržba **AVG AntiVirus** je dostupná prostredníctvom položky **Možnosti**. Kliknutím na šípku otvoríte rozbaľovaciu ponuku:

- **Skontrolovať počítač** – spustí kontrolu celého počítača.
- **Skontrolovať vybraný priečinok...** – prepne na rozhranie kontroly AVG a pomocou stromovej štruktúry počítača umožní definovať, ktoré súbory a priečinky sa majú kontrolovať.
- **Skontrolovať súbor...** – umožňuje vám spustiť na požiadanie test jedného konkrétneho súboru. Kliknutím na túto možnosť sa otvorí nové okno so stromovou štruktúrou disku. Vyberte požadovaný súbor a potvrdte spustenie kontroly.
- **Aktualizácia** – automaticky spustí proces aktualizácie **AVG AntiVirus**.
- **Aktualizácia z adresára...** – spustí proces aktualizácie z aktualizčných súborov, ktoré sa nachádzajú v určenom priečinku na miestnom disku. 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 zvolte priečinok, do ktorého ste predtým uložili aktualizčný súbor, a spustíte proces aktualizácie.
- **Vírusový trezor** – otvorí rozhranie úložiska karantény (Vírusový trezor), do ktorého AVG odstraňuje všetky zistené infekcie. V tejto karanténe sú infikované súbory izolované a je zaručená bezpečnosť vášho počítača. Zároveň sú infikované súbory uložené pre ich budúcu možnú opravu.
- **História** – ponúka ďalšie špeciálne možnosti podponuky:
 - o **Výsledky kontroly** – otvorí dialógové okno s prehľadom výsledkov kontrol.
 - o **Nálezy súčasti Rezidentný štít** – otvorí dialógové okno s prehľadom hrozieb detegovaných Rezidentným štítom.
 - o **Nálezy súčasti Software Analyzer** – otvorí dialógové okno s prehľadom hrozieb detegovaných súčastou Software Analyzer.
 - o **Nálezy súčasti Ochrana e-mailu** – otvorí dialógové okno s prehľadom príloh e-mailových správ označených súčastou Ochrana e-mailu ako nebezpečné.
 - o **Nálezy súčasti Webový štít** – otvorí dialógové okno s prehľadom hrozieb detegovaných Webovým štítom.
 - o **Protokol histórie udalostí** – otvorí rozhranie protokolu histórie s prehľadom všetkých zaznamenaných činností **AVG AntiVirus**.



- **Rozšírené nastavenia...** – otvorí dialógové okno s rozšírenými nastaveniami AVG, kde môžete upraviť konfiguráciu **AVG AntiVirus**. V zásade vám neodporúčame meniť predvolené nastavenia aplikácie definované dodávateľom softvéru.
- **Obsah pomocníka** – otvorí súbory pomocníka AVG.
- **Získajte podporu** – otvorí [dialógové okno podpory](#), ktoré poskytuje všetky dostupné kontakty a informácie podpory.
- **Vaša AVG webová stránka** – otvorí webovú stránku AVG (<http://www.avg.com/>).
- **O vírusoch a hrozbách** – otvorí online vírusovú encyklopédiu na webovej stránke AVG (<http://www.avg.com/>), v ktorej môžete vyhľadať podrobné informácie o identifikovanom víruse.
- **(Znova) aktivovať** – otvorí sa dialógové okno aktivácie s licenčným číslom, ktoré ste zadali počas procesu inštalácie. Toto dialógové okno sa používa na úpravu licenčného čísla buď pri nahradení predajného čísla (s ktorým ste nainštalovali produkt AVG), alebo pri nahradení starého licenčného čísla (napr. pri uprade na nový produkt AVG). Ak používate skúšobnú verziu **AVG AntiVirus**, uvedené dve položky sa zobrazia ako **Kúpiť teraz** a **Aktivovať** a umožnia vám zakúpiť si ihneď úplnú verziu programu. Ak je **AVG AntiVirus** nainštalovaný pomocou predajného čísla, položky sa zobrazia ako **Registrovat'** a **Aktivovať**.
- **Zaregistrovať teraz/MyAccount** – spojí vás s registračnou stránkou na webovej stránke AVG (<http://www.avg.com/>). Vyplňte vaše registračné údaje; nárok na bezplatnú technickú podporu získajú len tí zákazníci, ktorí si produkt AVG zaregistrujú.
- **O AVG** – otvorí nové dialógové okno s tromi záložkami s údajmi o zakúpenej licencií a informáciami o dostupnej podpore, produkte a programe. Uvedené je tu tiež plné znenie licenčnej zmluvy. (Rovnaké dialógové okno môžete otvoriť pomocou odkazu [Podpora](#) v hlavnej navigácii.)

5.2. Informácie o stave zabezpečenia

Časť **Informácie o stave zabezpečenia** sa nachádza v hornej časti hlavného okna **AVG AntiVirus**. V tejto časti vždy nájdete informácie o aktuálnom stave zabezpečenia vášho **AVG AntiVirus**. Pozrite si prehľad ikon, ktoré sa môžu nachádzať v tejto časti, a ich význam:



– zelená ikona informuje, že váš **AVG AntiVirus** je **úplne funkčný**. Váš počítač je plne chránený, aktuálny a všetky nainštalované súčasti fungujú správne.



– žltá ikona upozorňuje, že **jedna súčasť alebo niekoľko súčastí je nesprávne nakonfigurovaných** a treba venovať pozornosť ich vlastnostiam alebo nastaveniam. Neexistuje žiaden kritický problém s produktom **AVG AntiVirus** a pravdepodobne ste sa rozhodli z nejakého dôvodu vypnúť niektorú súčasť. Stále ste chránení. Venujte však pozornosť nastaveniam problémovej súčasti! Nesprávne nastavená súčasť sa zobrazí s varovným oranžovým pruhom v [hlavnom používateľskom rozhraní](#).

Žltá ikona sa zobrazí aj vtedy, keď ste sa z nejakého dôvodu rozhodli ignorovať chybový stav súčasti. Voľba **Ignorovať chybný stav** je dostupná vo vetve [Rozšírené nastavenia/Ignorovať chybný stav](#). Tam máte možnosť potvrdiť, že ste si vedomí chybového stavu súčasti, ale z nejakého dôvodu chcete nechať program **AVG AntiVirus** v tomto stave a nechcete byť na to upozorňovaní. Môže sa vyskytnúť situácia,



keď bude potrebné použiť túto možnosť; dôrazne vám však odporúčame, aby ste funkciu **Ignorovať chybný stav** čo najskôr znova vyplili!

Žltá ikona sa zobrazí aj vtedy, ak **AVG AntiVirus** vyžaduje reštart počítača (**Je potrebný reštart**). Tomuto varovaniu by ste mali venovať pozornosť a reštartovať počítač.



– Oranžová ikona upozorňuje, že sa vyskytol vážny stav produktu **AVG AntiVirus**! Jedna alebo viac súčastí nefunguje správne a **AVG AntiVirus** nedokáže chrániť váš počítač. Venujte okamžitú pozornosť odstráneniu uvedeného problému! Ak nedokázate opraviť chybu sami, kontaktujte tím [technickej podpory AVG](#).

Ak nie je program **AVG AntiVirus** nastavený tak, aby poskytoval optimálny výkon, vedľa informácie o stave zabezpečenia sa zobrazí nové tlačidlo s názvom **Kliknutím opraviť** (alebo **Kliknutím opraviť všetko**, ak sa problém týka viacerých súčastí). Stlačením tlačidla spustíte automatický proces kontroly a konfigurácie programu. Je to jednoduchý spôsob nastavenia optimálneho výkonu **AVG AntiVirus** a dosiahnutia maximálnej úrovne 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 produktu **AVG AntiVirus** môžete zistiť kedykoľvek pomocou [ikony v paneli úloh systému](#).

5.3. Prehľad súčastí

Prehľad nainštalovaných súčastí nájdete vo vodorovnom pruhu blokov v strednej časti [hlavného okna](#). Súčasti sú zobrazené ako zelené obdĺžniky označené ikonou príslušnej súčasti. Každý obdĺžnik obsahuje informácie o aktuálnom stave ochrany. Ak je súčasť správne nakonfigurovaná a plne funkčná, informácie sú uvedené zelenými písmenami. Ak je súčasť pozastavená, má obmedzenú funkčnosť alebo má poruchu, zobrazí sa varovný text v oranžovom textovom poli. **Dôrazne sa odporúča, aby ste venovali pozornosť príslušným nastaveniam súčastí!**

Presuňte kurzor myši nad súčasť. V dolnej časti [hlavného okna](#) sa zobrazí krátky text. Text uvádza základný popis funkcie súčasti. Obsahuje tiež informácie o aktuálnom stave súčasti a uvádza, ktorá zo služieb súčasti nie je správne nakonfigurovaná.

Zoznam nainštalovaných súčastí

V **AVG AntiVirus** v časti **Prehľad súčastí** sa nachádzajú informácie o nasledujúcich súčastiach:

- **Počítač** – tieto súčasti sa týkajú dvoch služieb: **AntiVirus Shield** deteguje vírusy, spyware, červy, trójske kone, neželané spustiteľné súbory či knižnice v systéme a chráni vás pred škodlivým adware. **Anti-Rootkit** kontroluje nebezpečné rootkity ukryté vnútri aplikácií, ovládačov alebo knižníc. [Podrobnosti >>](#)
- **Prezeranie webu** – chráni vás pred útokmi na webe pri vyhľadávaní a surfovaní na internete. [Podrobnosti >>](#)
- **Softvér** – táto súčasť spúšťa službu **Software Analyzer**, ktorá neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete. [Podrobnosti >>](#)



- **E-mail** – kontroluje prichádzajúce e-mailové správy, či neobsahujú nevyžiadajúcu poštu, a blokuje vírusy, phishingové útoky či iné hrozby. [Podrobnosti >>](#)

Dostupné činnosti

- **Presunutím kurzora myši nad ktorúkoľvek ikonu súčasti** sa príslušná ikona zvýrazní v prehľade súčastí. V spodnej časti [používateľského rozhrania](#) sa zároveň zobrazí popis základných funkcií súčasti.
- **Jedným kliknutím na ikonu súčasti** otvoríte rozhranie s údajmi o jej aktuálnom stave. Súčasne tu máte prístup ku konfigurácii a štatistickým údajom.

5.4. Moje aplikácie

V oblasti **Moje aplikácie** (v rade zelených obdĺžnikov pod súpravou súčastí) nájdete prehľad ďalších aplikácií AVG, ktoré sú buď na vašom počítači nainštalované, alebo sa ich inštalácia odporúča. Obdĺžniky sa zobrazujú podmienené a môžu predstavovať niektoré z týchto aplikácií:

- **Mobilná ochrana** je aplikácia, ktorá chráni mobilný telefón proti vírusom a malware. Poskytuje tiež možnosť diaľkového sledovania smartfónu, pokiaľ by ste s ním stratili kontakt.
- **PC TuneUp** je vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon.

Podrobnosti o niektorej aplikácii z radu **Moje aplikácie** zobrazíte po kliknutí na príslušný obdĺžnik. Budete presmerovaní na príslušnú webovú stránku AVG, kde si môžete súčasť priamo stiahnuť.

5.5. Kontrola/Aktualizovať rýchle odkazy

Rýchle odkazy sa nachádzajú v spodnom riadku tlačidiel [používateľského rozhrania AVG AntiVirus](#). Tieto odkazy poskytujú okamžitý prístup k najdôležitejším a najčastejšie používaným funkciám aplikácie, teda kontrole a aktualizácii. Rýchle odkazy sú dostupné zo všetkých dialógových okien používateľského rozhrania:

- **Skontrolovať teraz** – tlačidlo je graficky rozdelené na dve časti. Odkazom **Skontrolovať teraz** okamžite spustíte [Kontrolu celého počítača](#), a môžete sledovať jej priebeh a výsledky v automaticky otvorenom okne [Správy](#). Tlačidlo **Možnosti** otvorí dialógové okno **Možnosti kontroly**, kde môžete [spravovať naplánované kontroly](#) a upraviť parametre [Kontroly celého počítača/Kontroly súborov/priečinkov](#). (Podrobnosti nájdete v kapitole [Kontrola AVG](#))
- **Opraviť výkon** – Týmto tlačidlom vstúpite do služby [PC Analyzer](#), vyspelého nástroja na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon.
- **Aktualizovať teraz** – stlačením tohto tlačidla okamžite spustíte aktualizáciu. O výsledkoch aktualizácie budete informovaní v oznámení nad ikonou AVG v paneli úloh. (Podrobnosti nájdete v časti [Aktualizácie AVG](#))



5.6. Ikona v paneli úloh

Ikona AVG v paneli úloh (v paneli úloh Windows v pravom dolnom rohu monitora) zobrazuje aktuálny stav produktu **AVG AntiVirus**. Vždy je v paneli úloh viditeľná, bez ohľadu na to, či je [používateľské rozhranie AVG AntiVirus](#) otvorené alebo zatvorené.

Zobrazenie ikony AVG v systémovom paneli úloh

-  Úplne vyfarbená ikona bez ďalších prvkov znamená, že všetky súčasti aplikácie **AVG AntiVirus** sú aktívne a úplne funkčné. Takáto ikona sa však môže zobrazit' aj vtedy, keď niektorá zo súčastí nie je úplne funkčná, ale používateľ sa rozhodol [ignorovať jej stav](#). (Ak ste potvrdili možnosť ignorovania stavu súčastí, potvrdzujete tým, že ste si vedomí [chybového stavu súčastí](#), ale z nejakého dôvodu ju tak chcete nechať a nechcete zobrazovať varovania týkajúce sa tejto situácie.)
-  Ikona s výkričníkom znamená, že súčasť (alebo viac súčastí) je v [chybovom stave](#). Takýmto výstrahám vždy venujte pozornosť a snažte sa odstrániť problém konfigurácie súčastí, ktorá nie je nastavená správne. Ak chcete zmeniť konfiguráciu súčastí, dvakrát kliknite na ikonu v paneli úloh. Otvorí sa [používateľské rozhranie aplikácie](#). Podrobné informácie o [chybovom stave](#) jednotlivých súčastí nájdete v časti [Informácie o stave zabezpečenia](#).
-  Ikona v paneli úloh sa môže ďalej zobrazit' plnofarebne s blikajúcim a otáčajúcim sa majákom. Táto grafická verzia signalizuje, že prebieha aktualizácia.
-  Plnofarebné zobrazenie ikony so šípkou znamená, že **AVG AntiVirus** práve prebieha kontrola.

Informácie ikony AVG v systémovom paneli úloh

Ikona AVG v paneli úloh uvádza aj údaje o aktuálnych aktivitách v **AVG AntiVirus** a možných zmenách stavu programu (napr. o *automatickom spustení plánu kontroly alebo aktualizácie, zmene stavu súčastí, výskyte chybového stavu, atď.*) pomocou kontextového okna, ktoré sa otvorí kliknutím na ikonu v paneli úloh.

Činnosti prístupné prostredníctvom ikony AVG v paneli úloh

Ikonu AVG v systémovom paneli úloh môžete použiť aj na rýchle zobrazenie [používateľského rozhrania AVG AntiVirus](#). Stačí dvakrát kliknúť na ikonu. Kliknutím pravým tlačidlom myši na ikonu sa otvorí krátko kontextová ponuka, ktorá vám sprístupňuje niektoré z najdôležitejších funkcií:

- **Otvoriť** – použite toto tlačidlo na otvorenie [hlavného používateľského rozhrania](#).
- **Skontrolovať teraz** – použite toto tlačidlo na okamžité spustenie [Kontroly celého počítača](#).
- **Ochrana** (aktivované  / deaktivované ) – použite tento prepínač, aby ste vypli súčasti **AVG AntiVirus**, ktoré zabezpečujú ochranu v reálnom čase. Potom budete mať možnosť určiť, ako dlho má byť **AVG AntiVirus** neaktívny. Ochranu **AVG AntiVirus** môžete kedykoľvek znovu aktivovať – jednoducho znovu kliknite na prepínač.



5.7. AVG Advisor

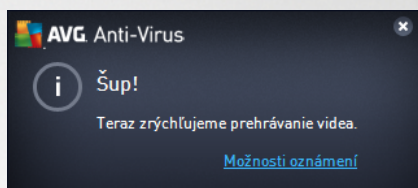
Súčasť **AVG Advisor** bola navrhnutá tak, aby detegovala problémy, ktoré môžu ohrozovať váš počítač a na odporúčanie akcií na riešenie daných situácií. **AVG Advisor** vidíte v podobe vysúvacieho kontextového okna nad panelom úloh. Služba deteguje pravdepodobnú **neznámu sieť so známym názvom**. To sa obvykle týka len tých používateľov, ktorí sa pripájajú k rôznym sieťam, obvyčajne pomocou prenosných počítačov. V prípade, že nová neznáma sieť má rovnaký názov ako dobre známa a často používaná sieť (*napríklad Doma alebo MojeWifi*), môže nastať omyl a nechtiac sa môžete pripojiť do úplne neznámej a potenciálne nebezpečnej siete. **AVG Advisor** tomu môže predísť tak, že vás varuje, že známy názov v skutočnosti označuje novú sieť. Samozrejme, ak sa rozhodnete, že neznáma sieť je bezpečná, môžete ju uložiť do zoznamu známych sietí **AVG Advisor**, aby v budúcnosti nebola znovu nahlasovaná.

Podporované internetové prehliadače

Táto funkcia funguje v nasledujúcich internetových prehliadačoch: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Akcelerátor

Služba **AVG Akcelerátor** umožňuje stabilnejšie prehrávanie on-line videa a uľahčuje ďalšie sťahovania. Ak prebieha akcelerácia videa, v paneli úloh vás upozorní kontextové okno.



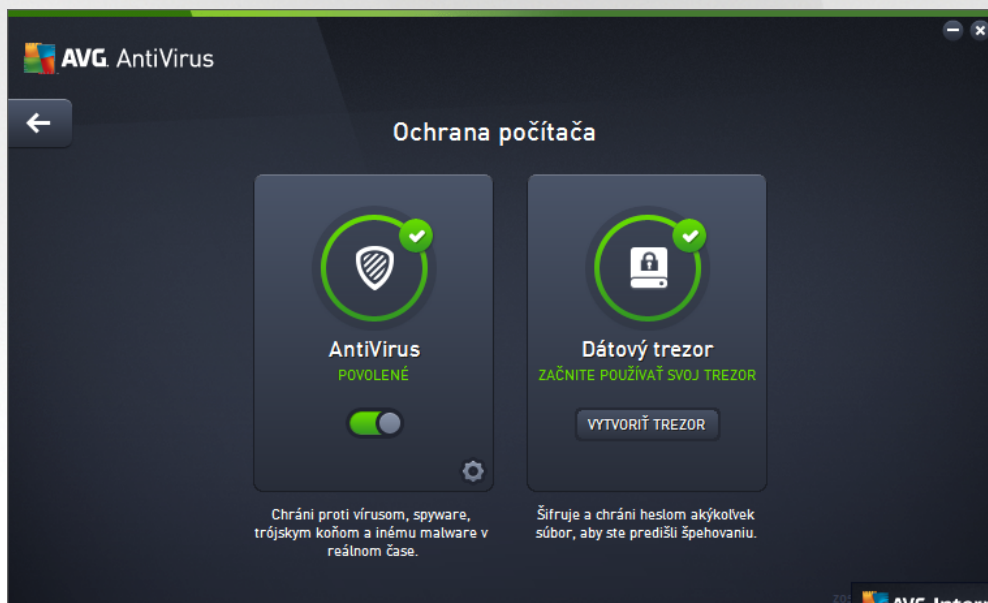


6. Súčasti AVG

6.1. Ochrana počítača

Súčasť **Počítač** sa týka dvoch hlavných bezpečnostných služieb: **AntiVirus** a **Dátový trezor**:

- **AntiVirus** sa skladá z kontrolného jadra, ktoré stráži všetky súbory, systémové oblasti počítača a vymeniteľné médiá (*disk flash a pod.*) a kontroluje známe vírusy. Každý zistený vírus sa zablokuje, aby nemohol vykonávať žiadnu činnosť, a potom sa vymaže alebo sa premiestni do [Vírusového trezora](#). Normálne tento proces ani nezbadáte, pretože rezidentná ochrana je „spustená v pozadí“. Súčasť AntiVirus používa tiež heuristickú kontrolu, pri ktorej sa v súboroch kontrolujú charakteristiky typické pre vírusy. To znamená, že súčasť AntiVirus dokáže detegovať nový, neznámy vírus, ak tento nový vírus obsahuje isté typické vlastnosti existujúcich vírusov. **AVG AntiVirus** dokáže tiež analyzovať a detegovať spustiteľné aplikácie alebo knižnice DLL, ktoré by sa v systéme nemali nachádzať (rôzne typy spyware, adware a pod.). AntiVirus ďalej kontroluje podozrivé záznamy v registri, dočasné internetové súbory a spracuje všetky potenciálne škodlivé položky rovnakým spôsobom ako každú inú infekciu.
- **Dátový trezor** vám umožňuje vytvárať bezpečné virtuálne trezory na uchovávanie citlivých údajov. Obsah Dátového trezora je šifrovaný a chránený heslom, ktoré si vyberiete, aby k údajom nikto nemal prístup bez povolenia.



Ovládacie prvky dialógového okna

Ak chcete prepínať medzi oboma časťami dialógového okna, stačí kliknúť kdekkoľvek na príslušný servisný panel. Panel sa zvýrazní v svetlejšom odtieni modrej. V oboch častiach dialógového okna nájdete tieto ovládacie prvky. Ich funkcia je rovnaká bez ohľadu na to, do ktorej bezpečnostnej služby patria (*AntiVirus alebo Dátový trezor*):

 **Zakázané/povolené** – tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav **Povolené**, čo znamená, že bezpečnostná služba AntiVirus je aktívna a plne funkčná. Červená farba predstavuje stav **Zakázané**, t. j.



služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným **varovným** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. **Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.**

 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. [AntiVirus](#). V rozšírených nastaveniach môžete upraviť všetky konfigurácie každej bezpečnostnej služby **AVG AntiVirus**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

 **Šípka** – pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do [hlavného používateľského rozhrania](#) s prehľadom súčastí.

Ako vytvoriť dátový trezor

V časti **Dátový trezor** dialógového okna **Ochrana počítača** nájdete tlačidlo **Vytvoriť trezor**. Kliknutím na tlačidlo otvoríte nové dialógové okno s rovnakým názvom, do ktorého môžete zadať parametre plánovaného trezora. Vyplňte všetky potrebné informácie a postupujte podľa pokynov v aplikácii:



Najprv je potrebné zadať názov trezora a vytvoriť silné heslo:

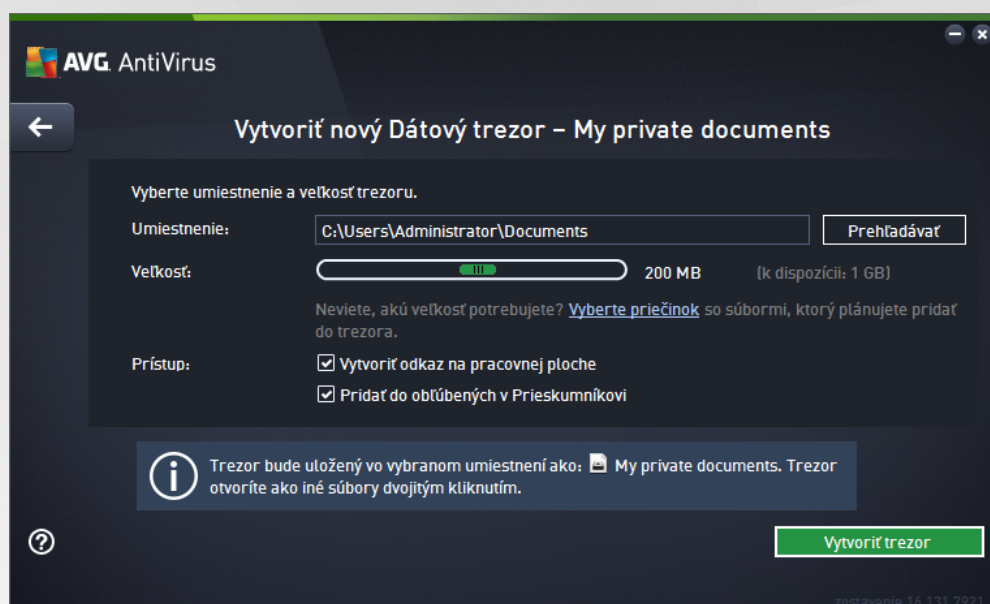
- **Názov trezora** – ak chcete vytvoriť nový dátový trezor, najprv je potrebné vybrať preň vhodný názov, aby ste ho rozpoznali. Ak sa delíte o počítač s ostatnými členmi rodiny, môžete doň zahrnúť svoje meno a slovo označujúce jeho obsah, napríklad *Ockove e-maily*.
- **Vytvoriť heslo/Znovu zadať heslo** – vytvorte heslo pre dátový trezor a napíšte ho do príslušných textových polí. Grafický indikátor vpravo vám oznámi, či je heslo slabé (*pomerne jednoducho prelomiteľné pomocou špeciálnych softvérových nástrojov*) alebo silné. Odporúčame zvoliť si heslo s minimálne strednou silou. Heslo môžete urobiť silnejším, ak bude obsahovať veľké písmená, čísla a iné znaky, ako napríklad bodky, pomlčky, atď. Ak chcete zabezpečiť, že napíšete želané heslo



správne, môžete zaškrtnúť políčko **Zobraziť heslo** (samozrejme, nikto iný sa nesmie pozerat' na vašu obrazovku).

- **Pomôcka pre heslo** – dôrazne odporúčame, aby ste si vytvorili aj pomôcku pre heslo, ktorá vám pomôže spomenúť si naň v prípade, že by ste ho zabudli. Pamätajte, že Dátový trezor je určený na zabezpečenie súborov a umožňuje k nim prístup len so zadaním hesla. Túto ochranu nemožno nijako obísť a ak zabudnete heslo, nebudete mať prístup do dátového trezora!

Po zadaní všetkých požadovaných údajov do textových polí kliknite na tlačidlo **Ďalej** a pokračujte ďalším krokom:

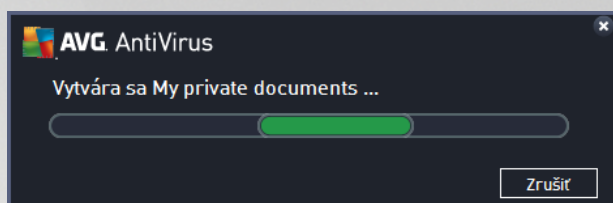


Toto dialógové okno poskytuje nasledovné možnosti konfigurácie:

- **Umiestnenie** – uvádza, kde bude dátový trezor fyzicky umiestnený. Nájdite vhodné miesto na pevnom disku alebo ponechajte preddefinované umiestnenie v priečinku *Dokumenty*. Upozorňujeme, že keď dátový trezor vytvoríte, jeho umiestnenie už nemôžete zmeniť.
- **Veľkosť** – môžete prednastaviť veľkosť dátového trezora, čím sa vyhradí potrebné miesto na disku. Nastavená hodnota by nemala byť príliš malá (*nedostatočná pre vaše potreby*) ani príliš veľká (*aby trezor nezaberal zbytočne priveľa miesta na disku*). Ak už viete, čo chcete do dátového trezora umiestniť, môžete dať všetky príslušné súbory do jedného priečinka a potom pomocou odkazu **Vybrať priečinok** automaticky vypočítať celkovú veľkosť. Veľkosť však môžete neskôr zmeniť podľa svojich potrieb.
- **Prístup** – začiarkavacie políčka v tejto časti umožňujú vytvoriť pohodlné skratky k dátovému trezoru.

Ako používať dátový trezor

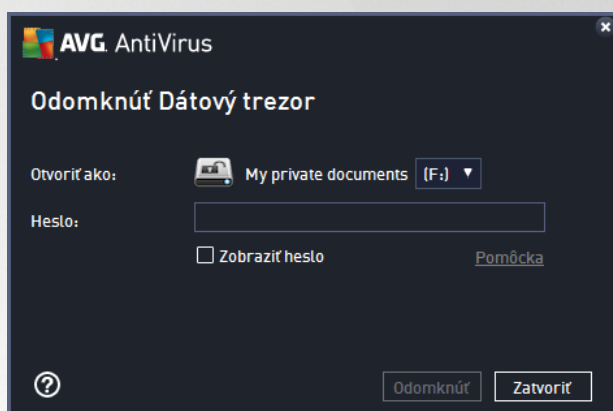
Keď budete s nastaveniami spokojní, kliknite na tlačidlo **Vytvoriť trezor**. Otvorí sa nové dialógové okno **Váš dátový trezor je teraz pripravený** a oznámi vám, že daný trezor je pripravený na ukladanie súborov. Práve teraz je trezor otvorený a môžete k nemu ihneď pristupovať. Pri každom ďalšom pokuse o prístup do trezora budete vyzvaní na odomknutie trezora pomocou hesla, ktoré ste určili:



Pred použitím nového dátového trezora ho musíte najskôr otvoriť – kliknite na tlačidlo **Otvoriť teraz**. Po otvorení sa dátový trezor objaví vo vašom počítači ako nový virtuálny disk. V rozbaľovacej ponuke mu priradíte písmeno podľa vášho výberu (*budete môcť vybrať spomedzi aktuálne voľných diskov*). Obvykle si nebudete môcť vybrať písmeno C (*zvyčajne priradené pevnému disku*), A (*disketová mechanika*) alebo D (*jednotka diskov DVD*). Pri každom odomknutí dátového trezora si môžete vybrať iné dostupné písmeno.

Ako odomknúť dátový trezor

Pri ďalšom pokuse o prístup do dátového trezora budete vyzvaní na odomknutie trezora pomocou hesla, ktoré ste určili:



Do textového poľa s cieľom overenia vašej osoby napíšete heslo a kliknete na tlačidlo **Odomknúť**. Ak potrebujete pripomenúť heslo, kliknite na položku **Pomôcka**, čím zobrazíte pomôcku k heslu, ktorú ste si určili pri vytváraní dátového trezora. Nový dátový trezor sa zobrazí v prehľade vašich dátových trezorov ako ODOMKNUTÝ a budete môcť podľa potreby pridávať a odstraňovať súbory.

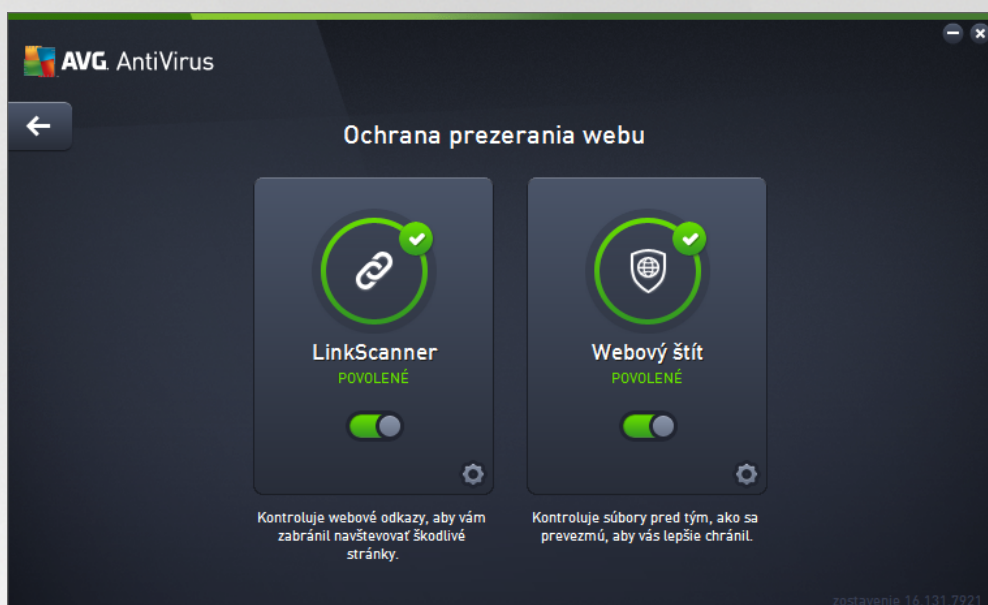
6.2. Ochrana prezerania webu

Ochrana prezerania webu sa skladá z dvoch služieb: **LinkScanner Surf-Shield** a **Webový štít**:

- **LinkScanner Surf-Shield** vás 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 prezeráte, a stará sa o to, aby boli bezpečné práve v momente, keď je to najviac dôležité – v momente, keď sa chystáte kliknúť na odkaz. **LinkScanner Surf-Shield nie je určený na ochranu serverových platforiem!**
- **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 stiahnu do počítača. Webový štít zistí prítomnosť nebezpečného kódu JavaScript na stránke, ktorú sa práve chystáte navštíviť, a neumožní stránku zobraziť. Zároveň rozpozná škodlivý softvér, ktorý sa nachádza na tejto stránke, a ihneď zastaví jeho sťahovanie, aby sa nikdy nedostal do počítača. Táto účinná ochrana zablokuje škodlivý kód každej webovej stránky, ktorú sa pokúšate otvoriť, a zabráni jeho stiahnutiu 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 pamätať na to, že zneužívané stránky môžu infikovať váš počítač už len tým, že ich navštívite. **Webový štít nie je určený na ochranu serverových platforiem!**



Ovládacie prvky dialógového okna

Ak chcete prepínať medzi oboma časťami dialógového okna, stačí kliknúť kdekoľvek na príslušný servisný panel. Panel sa zvýrazní v svetlejšom odtieni modrej. V oboch častiach dialógového okna nájdete tieto ovládacie prvky. Ich funkcia je rovnaká bez ohľadu na to, do ktorej bezpečnostnej služby patria (*LinkScanner Surf-Shield* alebo *Webový štít*):

 **Zakázané/povolené** – tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav **Povolené**, čo znamená, že bezpečnostná služba LinkScanner Surf-Shield/Webový štít je aktívna a plne funkčná. Červená farba predstavuje stav **Zakázané**, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným **varovným** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. **Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.**

 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. [LinkScanner Surf-Shield](#) alebo [Webový štít](#). V rozšírených nastaveniach môžete upraviť všetky konfigurácie každej bezpečnostnej služby **AVG AntiVirus**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

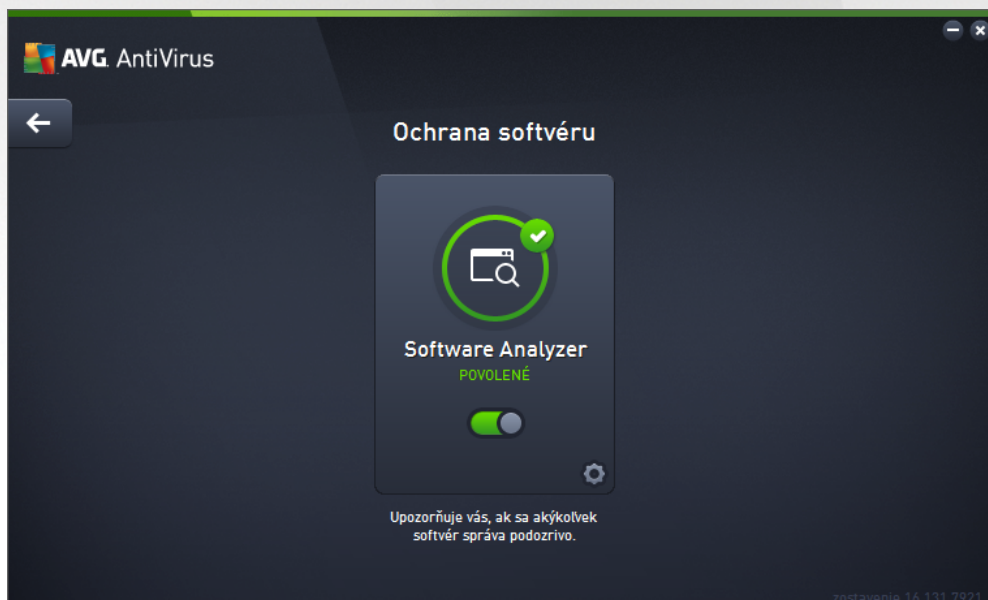


← **Šípka** – pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do [hlavného používateľského rozhrania](#) s prehľadom súčastí.

6.3. Software Analyzer

Súčasť **Software Analyzer** neustále chráni vaše digitálne aktíva pred novými a neznámymi hrozbami na internete:

- **Software Analyzer** je služba na ochranu pred malware, ktorá vás chráni pred všetkými druhmi malware (*spyware*, *softvérové roboty*, *krádež identity* atď.) s použitím technológií monitorovania správania a poskytuje okamžitú ochranu pred novými vírusmi. Identity Protection zabraňuje páchatelom počítačovej trestnej činnosti v oblasti odcudzenia identity, aby odcudzili vaše heslá, podrobnosti o bankových účtoch, čísla kreditných kariet a iné cenné osobné digitálne údaje zo všetkých druhov škodlivého softvéru (*malware*), ktorý útočí na váš počítač. Zabezpečuje správne fungovanie všetkých spustených programov na počítači alebo zdieľanej sieti. Software Analyzer neustále zaznamenáva a blokuje podozrivé správanie a chráni váš počítač pred každým novým malware. Software Analyzer chráni váš počítač pred novými a dokonca aj neznámymi hrozbami v reálnom čase. Monitoruje všetky procesy (*vrátane skrytých*) a viac ako 285 rôznych modelov správania a dokáže zistiť, či sa v počítači nevyskytuje niečo škodlivé. Preto dokáže odhaliť hrozby, ktoré ešte nie sú opísané vo vírusovej databáze. Keď sa do počítača dostane neznámy kód, program ho ihneď začne sledovať z hľadiska škodlivého správania. Ak sa súbor označí ako škodlivý, Software Analyzer presunie kód do [Vírusového trezora](#) a vráti späť všetky zmeny vykonané v systéme (*vloženia kódu, zmeny v registri, otvorenie portov a pod.*). Na dosiahnutie ochrany nemusíte spúšťať kontrolu. Technológia má veľmi aktívny prístup, len zriedka sa musí aktualizovať a vždy je v strehu.



Ovládacie prvky dialógového okna

V tomto dialógovom okne nájdete nasledujúce ovládacie prvky:



Aktivované/deaktivované – tlačidlo vám môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav **Aktivované**, čo



znamená, že bezpečnostná služba Software Analyzer je aktívna a plne funkčná. Červená farba predstavuje stav **Zakázané**, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným **varovným** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. **Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.**

 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. [Software Analyzer](#). V rozhraní rozšírených nastavení môžete upraviť všetky konfigurácie každej bezpečnostnej služby v **AVG AntiVirus**, no akúkoľvek konfiguráciu odporúčame iba skúseným používateľom!

 **Šípka** – pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do [hlavného používateľského rozhrania](#) s prehľadom súčastí.

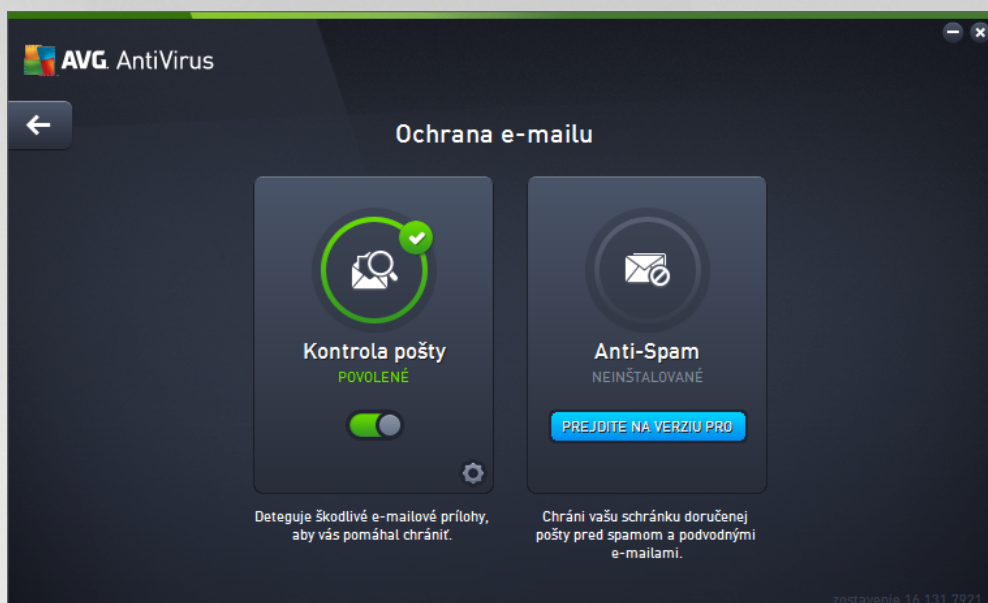
V **AVG AntiVirus** nie je služba Identity Alert žiaľ zahrnutá. Ak chcete používať tento typ ochrany, stlačte tlačidlo **Pre aktiváciu upgradujte**, ktoré vás presmeruje na príslušnú webovú stránku, kde si môžete zakúpiť licenciu Identity Alert.

Berte, prosím, do úvahy, že aj v edíciách AVG Premium Security je služba Identity Alert momentálne dostupná iba vo vybraných oblastiach: USA, Spojené kráľovstvo, Kanada a Írsko.

6.4. Ochrana e-mailu

Súčasť **Ochrana e-mailu** obsahuje nasledujúce dve služby zabezpečenia: **Kontrola pošty** a **Anti-Spam** (služba Anti-Spam je dostupná len v edíciách Internet/Premium Security).

- **Kontrola pošty:** Jeden z najbežnejších zdrojov vírusov a trójskych koňov je e-mail. Ohrozenia typu phishing a spam ďalej zvyšujú riziko e-mailu. Bezplatné e-mailové účty sú náchylnejšie na prijímanie takýchto škodlivých e-mailov (pretože málokedy využívajú technológiu na ochranu pred nevyžiadanou poštou) 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 útokom cez e-mail. Spoločnosti obvyčajne využívajú hromadné emailové účty a používajú antispamové filtre, atď., aby toto riziko znížili. Súčasť Ochrana e-mailu sa stará o kontrolu jednotlivých doručených alebo odoslaných e-mailových správ a vždy, keď zistí prítomnosť vírusu, ihneď presunie správu do [Vírusového trezora](#). Táto súčasť dokáže zároveň filtrovať niektoré typy e-mailových príloh a pridať text certifikácie k správam bez infekcie. **Kontrola pošty nie je určená pre serverové platformy!**
- **Anti-Spam** kontroluje všetku prichádzajúcu poštu a nechcené správy označí ako spam (Spam označuje nevyžiadajú poštu, ktorá väčšinou propaguje produkty či služby a ktorá je hromadne zasielaná na veľké množstvo e-mailových adries súčasne. Podobné správy plnia poštové schránky príjemcov. Spam sa nevztahuje na legálne komerčné e-maily, s ktorými zákazníci súhlasia.). Anti-Spam dokáže zmeniť predmet e-mailovej správy (ktorá bola označená ako nevyžiadaná pošta) pridaním špeciálneho textového reťazca. Môžete filtrovať e-mailové správy v e-mailovom klientovi. Súčasť Anti-Spam používa niekoľko metód analýzy na spracovanie jednotlivých e-mailových správ a prináša najvyššiu možnú úroveň ochrany pred nevyžiadanými e-mailovými správami. Anti-Spam používa pravidelne aktualizovanú databázu na detekciu nevyžiadanej pošty. 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 blokových (vždy označiť ako spam) adries.



Ovládacie prvky dialógového okna

Ak chcete prepínať medzi oboma časťami dialógového okna, stačí kliknúť kdekoľvek na príslušný servisný panel. Panel sa zvýrazní v svetlejšom odtieni modrej. V oboch častiach dialógového okna nájdete tieto ovládacie prvky. Ich funkcia je rovnaká bez ohľadu na to, do ktorej bezpečnostnej služby patria (*Kontrola pošty* alebo *Anti-Spam*):

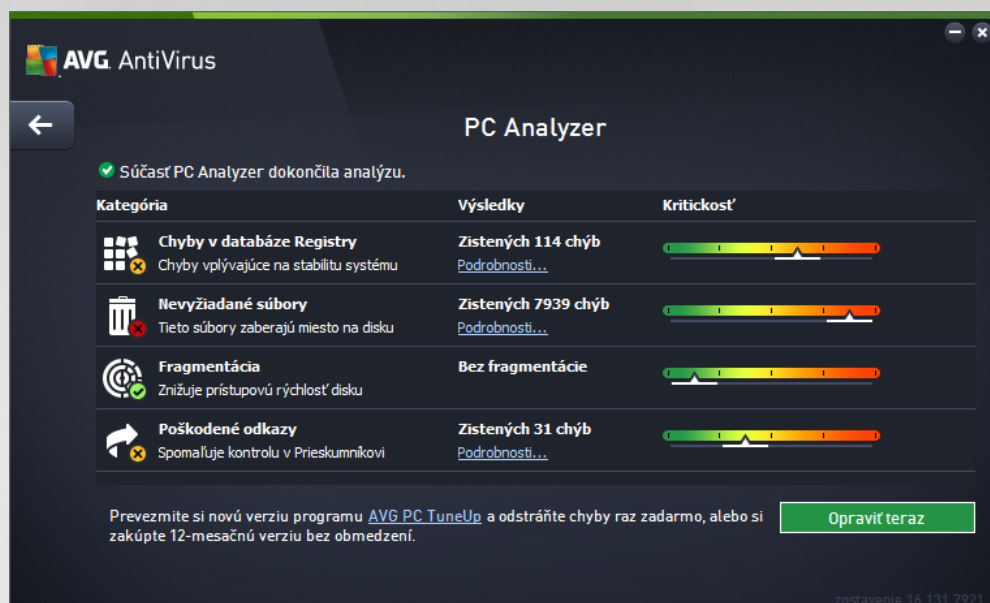
 **Zakázané/povolené** – tlačidlo môže pripomínať semafor vzhľadom aj funkciou. Kliknutím môžete prepínať medzi jeho dvomi polohami. Zelená farba symbolizuje stav **Povolené**, čo znamená, že bezpečnostná služba je aktívna a plne funkčná. Červená farba predstavuje stav **Zakázané**, t. j. služba je vypnutá. Ak nemáte dobrý dôvod na vypnutie služby, výrazne odporúčame, aby ste ponechali predvolené nastavenia pre všetky konfigurácie zabezpečenia. Predvolené nastavenia zaručujú optimálny výkon aplikácie a maximálnu bezpečnosť. Ak z nejakého dôvodu chcete vypnúť službu, budete upozornení na možné riziká červeným **varovným** nápisom a oznámením faktu, že momentálne nie ste úplne chránení. **Nezabudnite, že by ste službu mali znovu aktivovať čo najskôr.**

 **Nastavenia** – kliknutím na tlačidlo budete presmerovaní na rozhranie [rozšírených nastavení](#). Otvorí sa príslušné dialógové okno a budete môcť nakonfigurovať vybranú službu, t. j. [Kontrola pošty](#) alebo *Anti-Spam*. V rozšírených nastaveniach môžete upraviť všetky konfigurácie každej bezpečnostnej služby **AVG AntiVirus**, no akékoľvek nastavenie odporúčame iba skúseným používateľom!

 **Šípka** – pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do [hlavného používateľského rozhrania](#) s prehľadom súčastí.

6.5. PC Analyzer

PC Analyzer je vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon. Otvára sa prostredníctvom tlačidla **Opraviť výkon**, ktoré sa nachádza v [hlavnom dialógovom okne používateľského rozhrania](#) alebo prostredníctvom rovnakej možnosti uvedenej v kontextovej ponuke [ikony AVG v paneli úloh](#). Potom si budete môcť pozrieť priebeh analýzy a výsledky priamo v tabuľke:



Umožňuje analyzovať tieto oblasti: chyby v databáze Registry, nevyžiadané súbory, fragmentácia a poškodené odkazy:

- **Chyby v databáze Registry** informujú o počte chýb v databáze Registry operačného systému Windows, ktoré môžu spomaľovať váš počítač alebo spôsobovať zobrazenie chybových hlásení.
- **Nevyžiadané súbory** informujú o počte súborov, ktoré zaberajú miesto na disku, a ktoré sa pravdepodobne môžu vymazať. Zvyčajne ide o mnohé typy dočasných súborov a súbory v Koši.
- **Fragmentácia** vypočíta podiel pevného disku, ktorý je fragmentovaný, t. j. používal sa dlhý čas a väčšina súborov je umiestnená na rôznych miestach fyzického disku.
- **Poškodené odkazy** vyhľadávajú odkazy, ktoré už nie sú funkčné, vedú na neexistujúce miesta atď.

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

Ovládacie tlačidlá

- **Zastaviť analýzu** (zobrazí sa počas spustenej analýzy) – stlačením tohto tlačidla sa ihneď preruší analýza počítača.
- **Opraviť teraz** (zobrazí sa po dokončení analýzy) – ľutujeme, ale funkcia PC Analyzer v rámci **AVG AntiVirus** je obmedzená na analýzu súčasného stavu vášho počítača. AVG však poskytuje vyspelý nástroj na podrobnú analýzu a opravu systému, ktorý sa používa na hľadanie možností, ako zvýšiť rýchlosť počítača a zlepšiť jeho celkový výkon. Kliknite na tlačidlo, aby ste boli presmerovaní na vyhradenú webovú stránku pre ďalšie informácie.

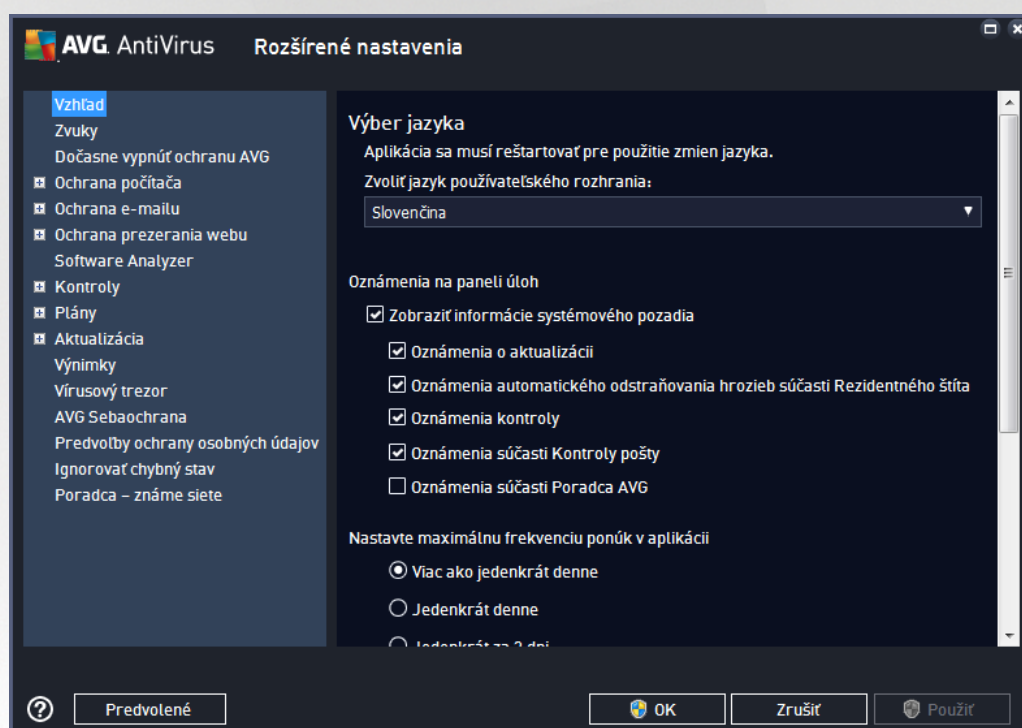


7. Rozšírené nastavenia AVG

Dialógové okno s rozšírenou konfiguráciou produktu **AVG AntiVirus** 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 konkrétnej časti), otvorte dialógové okno editovania v pravej časti okna.

7.1. Vzhľad

Prvá položka v navigačnej štruktúre, **Vzhľad**, sa týka všeobecných nastavení používateľského rozhrania **AVG AntiVirus** a niektorých základných možností správania sa aplikácie:



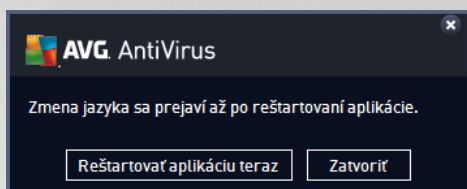
Výber jazyka

V časti **Výber jazyka** môžete v rozbaľovacej ponuke vybrať požadovaný jazyk. Vybraný jazyk sa potom použije pre celé používateľské rozhranie **AVG AntiVirus**. V rozbaľovacej ponuke sa nachádzajú len tie jazyky, ktoré ste už nainštalovali počas procesu inštalácie, plus angličtina (tá sa *inštaluje štandardne*). Zmenu jazyka **AVG AntiVirus** dokončíte reštartovaním aplikácie. Postupujte podľa nasledujúcich pokynov.

- V rozbaľovacej ponuke vyberte požadovaný jazyk aplikácie
- Potvrďte výber stlačením tlačidla **Použiť** (v pravom hornom rohu dialógového okna)
- Potvrďte stlačením tlačidla **OK**
- Zobrazí sa nové dialógové okno s informáciami o zmene jazyka aplikácie a potrebe reštartovať **AVG AntiVirus**



- Stlačením tlačidla **Reštartovať AVG teraz** súhlasíte s reštartovaním programu. Počkajte chvíľu, kým sa zmena jazyka prejaví:



Oznámenia na paneli úloh

V tejto časti môžete zrušiť zobrazovanie oznámení v paneli úloh o stave aplikácie **AVG AntiVirus**. V predvolenom nastavení je zobrazovanie oznámení v paneli úloh povolené. Dôrazne odporúčame toto nastavenie nemeniť! Systémové oznámenia informujú napríklad o spustení kontroly, spustení aktualizácie procesu alebo o zmene súčasti **AVG AntiVirus**. Týmto oznámeniam by ste rozhodne mali venovať pozornosť.

Ak sa však z nejakého dôvodu rozhodnete tieto informácie nezobrazovať alebo ak chcete zobrazovať iba niektoré oznámenia (týkajúce sa konkrétnej súčasti **AVG AntiVirus**), môžete definovať a určiť vlastné predvoľby označením/zrušením označenia príslušných možností:

- **Zobrazovať oznámenia v paneli úloh** (predvolene zapnuté) – predvolene sa zobrazujú všetky oznámenia. Ak chcete úplne vypnúť zobrazovanie všetkých oznámení, zrušte začiarknutie tejto položky. Po zapnutí môžete ďalej vybrať konkrétne oznámenia, ktoré sa majú zobrazovať:
 - o **Oznámenia o aktualizáciách** (predvolene zapnuté) – rozhodnite sa, či sa majú zobrazovať informácie týkajúce sa spustenia, postupu a dokončenia procesu aktualizácie **AVG AntiVirus**.
 - o **Oznámenia automatického odstraňovania hrozieb Rezidentným štítom** (predvolene zapnuté) – rozhodnite sa, či sa majú alebo nemajú zobrazovať informácie súvisiace s procesmi ukladania, kopírovania a otvárania súborov (toto nastavenie sa zobrazuje, len keď je v súčasti Rezidentný štít zapnutá možnosť *Liečiť automaticky*).
 - o **Oznámenia o kontrole** (predvolene zapnuté) – rozhodnite sa, či sa majú zobrazovať informácie pri automatickom spustení plánu kontroly, jeho priebehu a výsledkoch.
 - o **Oznámenia Kontroly pošty** (predvolene zapnuté) – rozhodnite sa, či sa majú zobrazovať informácie po každej kontrole prichádzajúcich a odchádzajúcich e-mailových správ.
 - o **Štatistické oznámenia** (predvolene zapnuté) – nechajte políčko začiarknuté, ak sa majú zobrazovať pravidelné štatistické prehľadové oznámenia v paneli úloh.
 - o **Oznámenia AVG Advisor** (predvolene zapnuté) – rozhodnite sa, či sa informácie o aktivite [AVG Advisor](#) majú zobrazovať v paneli úloh.

Režim hrania

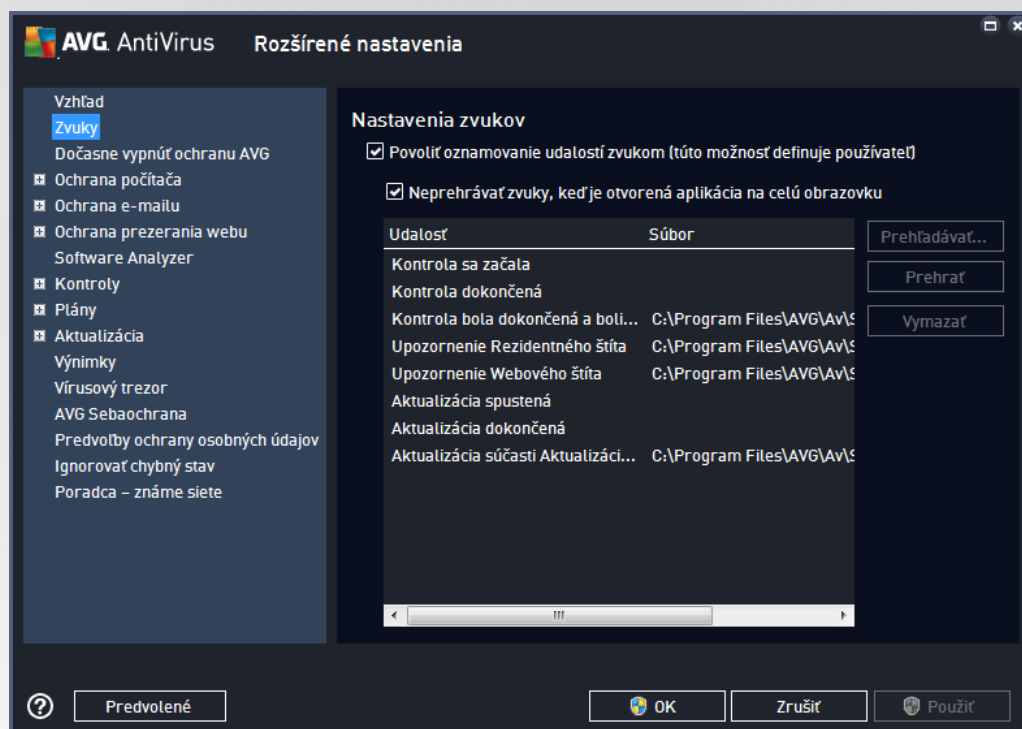
Táto funkcia programu AVG sa používa v súvislosti s aplikáciami spustenými na celú obrazovku, ktorých spustenie by sa mohlo narušiť (aplikácia by sa minimalizovala alebo by sa porušila grafika) zobrazením informačnej bubliny programu AVG (ktorá sa zobrazí napr. pri spustení plánu kontroly). Ak sa chcete vyhnúť



podobným situáciám, nechajte začiarkavacie políčko možnosti **Povolit' režim hrania, ak beží aplikácia v režime na celú obrazovku** označené (predvolené nastavenie).

7.2. Zvuky

Dialógové okno **Nastavenia zvukov** sa používa na zapnutie zvukových upozornení informujúcich o konkrétnych činnostiach programu **AVG AntiVirus**:



Tieto nastavenia sú platné len pre účet aktuálneho používateľa. To znamená, že každý používateľ na počítači bude mať svoje vlastné nastavenia zvukov. Ak chcete povoliť zvukové oznamy, nechajte označenú možnosť **Povolit' oznamovanie udalostí zvukom** (táto možnosť je predvolene zapnutá), aby ste aktivovali zoznam všetkých dôležitých činností. Ďalej môžete označiť možnosť **Neprehrávať zvuky, keď je aktívna aplikácia na celú obrazovku**, ak chcete potlačiť zvukové upozornenia v situáciách, keď by mohli vyrušovať (pozrite si tiež časť **Režim hry** v kapitole [Rozšírené nastavenia/Vzhľad](#) v tomto dokumente).

Ovládacie tlačidlá

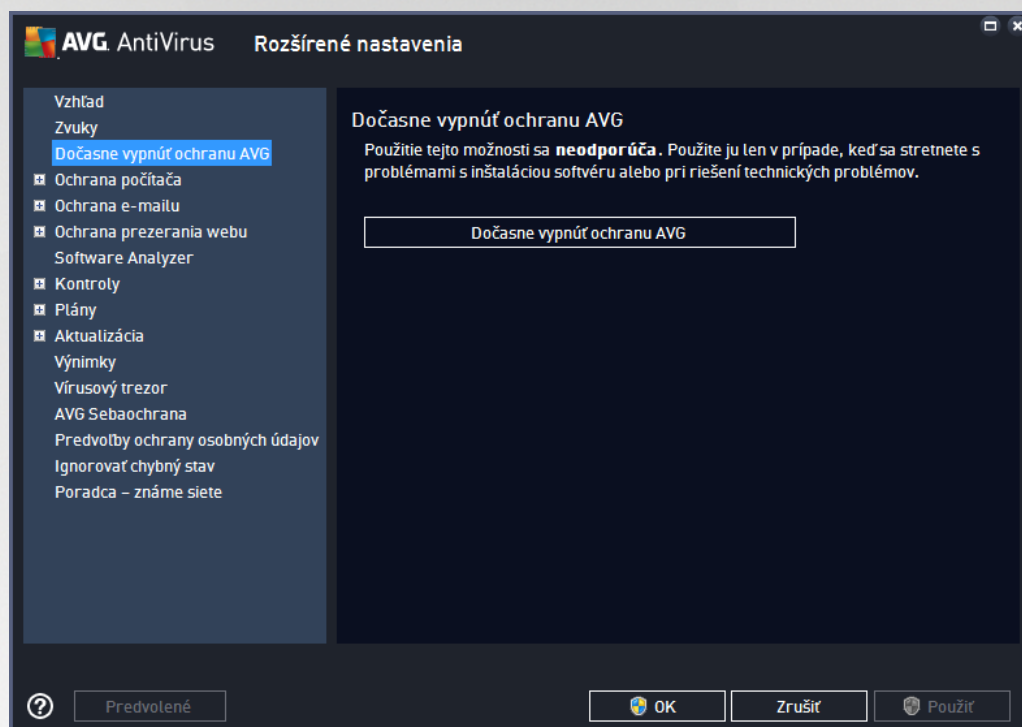
- **Prehľadávať...** – po označení príslušnej udalosti zo zoznamu pomocou tlačidla **Prehľadávať** nájdete na disku požadovaný zvukový súbor, ktorý chcete udalosti priradiť. (Upozorňujeme, že v súčasnosti sú podporované iba zvuky vo formáte *.wav!)
- **Prehrať** – ak si chcete vypočuť zvolený zvuk, zvýraznite udalosť v zozname a stlačte tlačidlo **Prehrať**.
- **Vymazať** – na odstránenie zvuku priradeného ku konkrétnej udalosti použite tlačidlo **Vymazať**.



7.3. Dočasne vypnúť ochranu AVG

Dialógové okno **Dočasne vypnúť ochranu AVG** umožňuje naraz vypnúť celú ochranu, ktorú zaisťuje **AVG AntiVirus**.

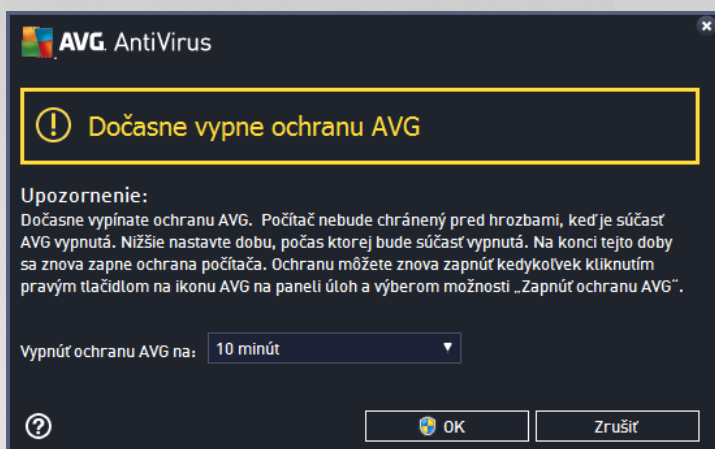
Nepoužívajte túto možnosť, ak to nie je naozaj nevyhnutné!



Vo väčšine prípadov **nie je potrebné** deaktivovať **AVG AntiVirus** pred inštaláciou nového softvéru alebo ovládačov, a to ani v prípade, keď inštalračný program alebo sprievodca inštaláciou softvéru odporúča, aby sa najskôr zatvorili spustené programy a aplikácie z dôvodu možného nežiaduceho prerušenia procesu inštalácie. Ak skutočne budete mať pri inštalácii problémy, pokúste sa najskôr [deaktivovať rezidentnú ochranu](#) (v dialógovom okne, do ktorého smeruje odkaz, zrušte začiarknutie položky **Povolit' Rezidentný štít**). Ak musíte dočasne vypnúť ochranu **AVG AntiVirus**, znova ju zapnite bezprostredne po dokončení úloh, pre ktoré ste ju vypli. Ak ste pripojení na internet alebo k sieti v čase, keď je antivírusový softvér vypnutý, váš počítač nie je chránený pred útokmi.

Ako vypnúť ochranu AVG

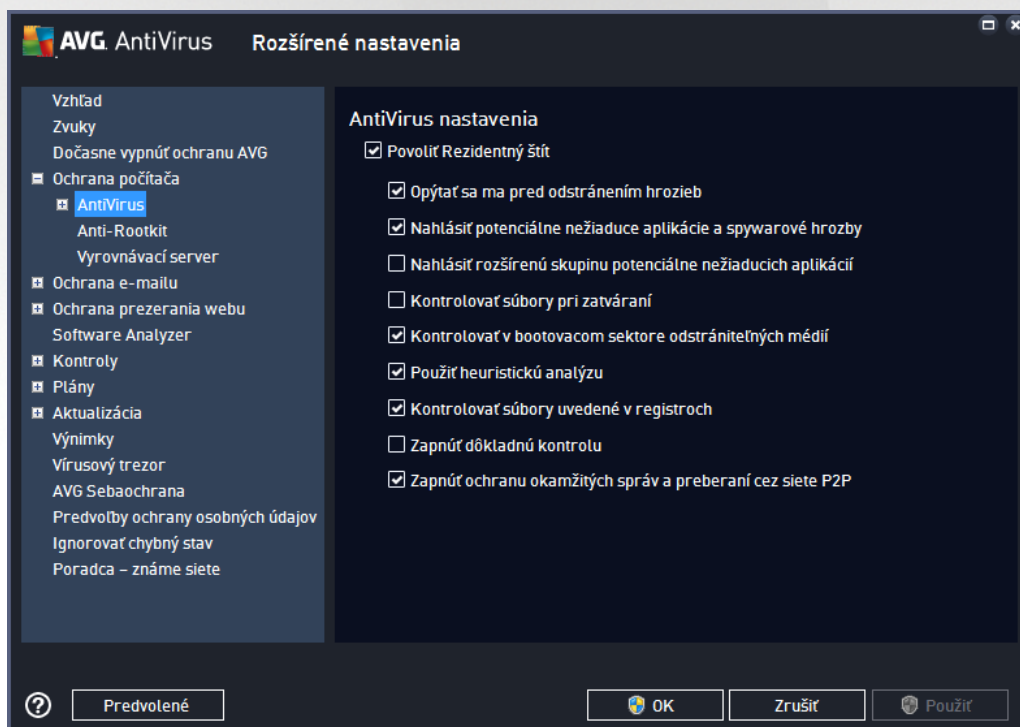
Označte začiarkavacie políčko **Dočasne vypnúť ochranu AVG** a potvrdte voľbu stlačením tlačidla **Použiť**. V novom otvorenom dialógovom okne **Dočasne vypnúť ochranu AVG** zadajte čas, na aký chcete vypnúť ochranu **AVG AntiVirus**. V predvolenom nastavení sa ochrana vypne na 10 minút, čo by malo stačiť na dokončenie bežných úloh, ako je inštalácia nového softvéru a pod. Môžete sa rozhodnúť pre dlhší časový úsek, ale táto možnosť sa neodporúča, ak to nie je naozaj potrebné. Potom sa všetky vypnuté súčasti automaticky znova aktivujú. Nanajvýš môžete vypnúť ochranu AVG až do najbližšieho reštartovania počítača.



7.4. Ochrana počítača

7.4.1. AntiVirus

AntiVirus spolu s **Rezidentným štítom** nepretržite chráni váš počítač pred všetkými známymi druhmi vírusov, spyware a malware (vrátane takzvaného spiaceho alebo neaktívneho malware, čo je malware, ktorý bol stiahnutý, ale nebol ešte aktivovaný).



Dialógové okno **Nastavenia súčasti Rezidentný štít** umožňuje úplne aktivovať alebo vypnúť rezidentnú ochranu začiatkom/zrušením začiatku položky **Povolit Rezidentný štít** (táto funkcia je predvolene zapnutá). Okrem toho môžete určiť, ktoré funkcie rezidentnej ochrany chcete aktivovať:

- **Opýtať sa ma pred odstránením hrozieb** (predvolene zapnuté) – začiatkom pre zabezpečenie, že Rezidentný štít nebude vykonávať žiadne akcie automaticky, a namiesto toho zobrazí dialógové okno



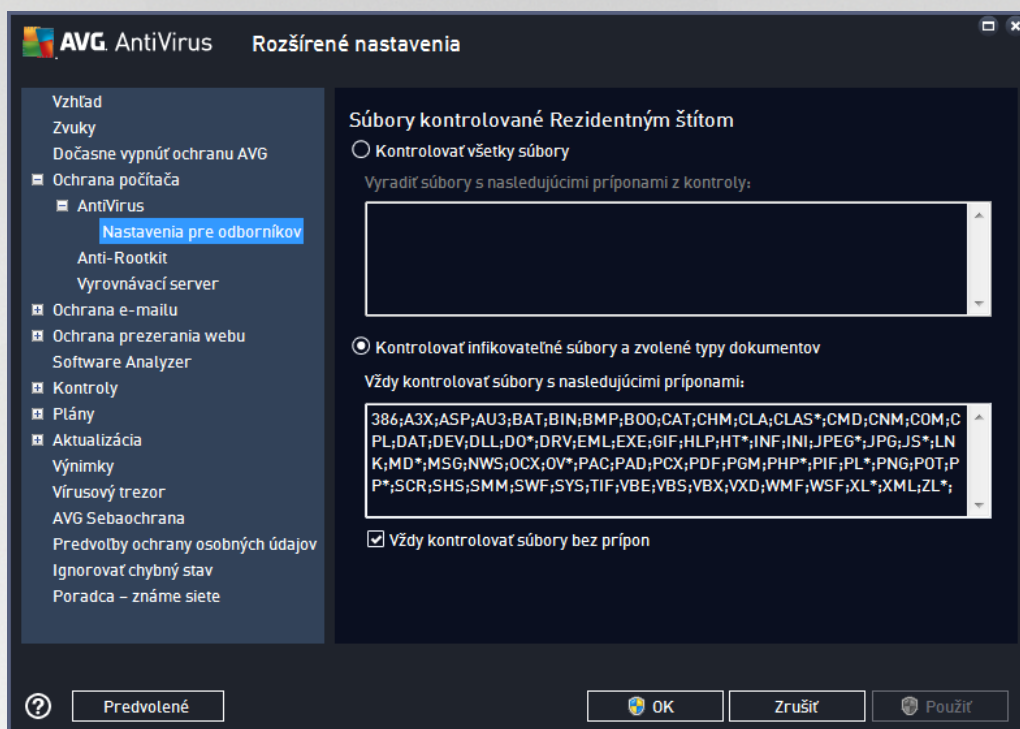
popisujúce detegovanú hrozbu a umožní vám tak rozhodnúť sa, aká akcia by mala byť vykonaná. Ak ponecháte políčko nezačiarknuté, **AVG AntiVirus** bude automaticky liečiť infekcie, a ak to nebude možné, bude objekt premiestnený do [Vírusového trezora](#).

- **Nahlásiť potenciálne nežiaduce aplikácie a hrozby spyware** (predvolene zapnuté) – začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (predvolene vypnuté) – začiarknite toto políčko, 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 legitímne programy, a preto je táto funkcia predvolene vypnutá.
- **Kontrolovať súbory pri zatváraní** (predvolene vypnuté) – kontrola pri zatvorení zabezpečí, že AVG skontroluje aktívne objekty (napr. aplikácie, dokumenty, atď.), keď sa otvárajú alebo zatvárajú; táto funkcia pomáha chrániť počítač pred niektorými druhmi sofistikovaných vírusov.
- **Kontrolovať v bootovacom sektore odstrániteľných médií** (predvolene zapnuté) – označte túto možnosť, ak sa majú kontrolovať zavádzacie sektory pripojených USB kľúčov, externých diskových jednotiek a iných odstrániteľných médií z hľadiska výskytu hrozieb.
- **Použiť heuristickú analýzu** (predvolene zapnuté) – na detekciu sa použije heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu v prostredí virtuálneho počítača).
- **Kontrolovať súbory uvedené v registroch** (predvolene zapnuté) – tento parameter určuje, že AVG bude kontrolovať všetky spustiteľné súbory pridané do registra na spúšťanie pri štarte počítača, aby sa známa infekcia nemohla spustiť pri ďalšom spustení počítača.
- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté) – v určitých situáciách (napr. v stave mimoriadnej núdze) môžete začiarknutím tohto políčka aktivovať algoritmus najdôkladnejšej kontroly, ktorý skontroluje všetky možné nebezpečné objekty do hĺbky. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Zapnúť ochranu okamžitých správ a sťahovaní cez sieť P2P** (predvolene zapnuté) – začiarknite toto políčko, ak chcete overiť, že komunikácie cez okamžité správy (t. j. AIM, Yahoo!, ICQ, Skype, MSN Messenger, atď.) a dáta stiahnuté sieťami typu peer-to-peer (siete umožňujúce priame pripojenie medzi klientmi bez serverov, ktoré môžu byť nebezpečné. Obyčajne sa používajú na zdieľanie hudobných súborov) neobsahujú vírusy.

Poznámka: Ak je AVG nainštalované vo Windowse 10, nachádza sa v zozname jedna položka navyše, nazvaná **Aktivovať Windows Antimalware Scan Interface (AMSI) pre dôkladnejšie kontroly softvéru** – táto funkcia zlepšuje ochranu pred vírusmi, keďže umožňuje Windowsu a AVG užiť spolupracovať pri odhaľovaní škodlivého kódu, vďaka čomu je ochrana spoľahlivejšia a znižuje sa počet nesprávnych detekcií.



V dialógovom okne **Súbory kontrolované Rezidentným štítom** môžete nastaviť, ktoré súbory sa budú kontrolovať (podľa konkrétnych prípon):

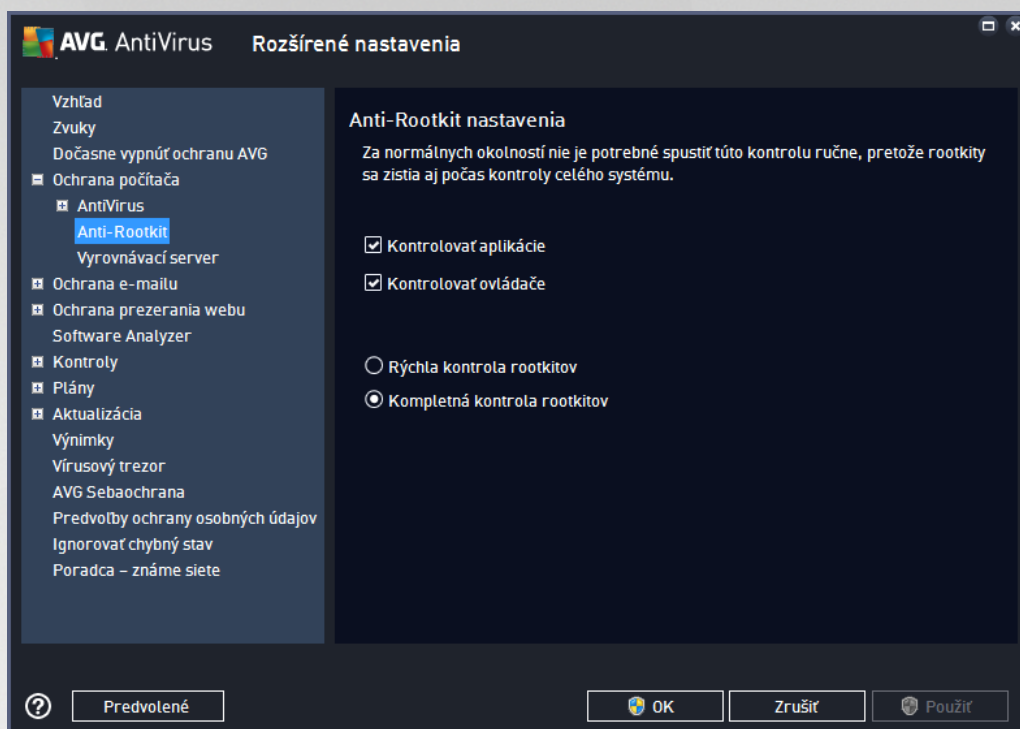


Označte príslušné začiarkavacie políčko podľa toho, či chcete použiť možnosť **Kontrolovať všetky súbory** alebo **Kontrolovať infikovateľné súbory a zvolené typy dokumentov**. Ak chcete urýchliť kontrolu a súčasne zabezpečiť maximálnu úroveň ochrany, odporúčame zachovať predvolené nastavenia. Takto sa budú kontrolovať iba infikovateľné súbory. V príslušnej časti dialógového okna nájdete aj upraviteľný zoznam prípon súborov, ktoré sa majú začleniť do kontroly.

Začiarknite možnosť **Vždy kontrolovať súbory bez prípon** (predvolené zapnutá), ak má Rezidentný štít kontrolovať aj súbory bez prípony a súbory neznámeho formátu. Odporúčame mať túto možnosť zapnutú, pretože súbory bez prípon sú podozrivé.

7.4.2. Anti-Rootkit

V dialógovom okne **Nastavenia nástroja Anti-Rootkit** môžete upraviť konfiguráciu služby **Anti-Rootkit** a konkrétne parametre kontroly. Kontrola nástrojom Anti-Rootkit je predvolený proces spustený pri [Kontrolu celého počítača](#):



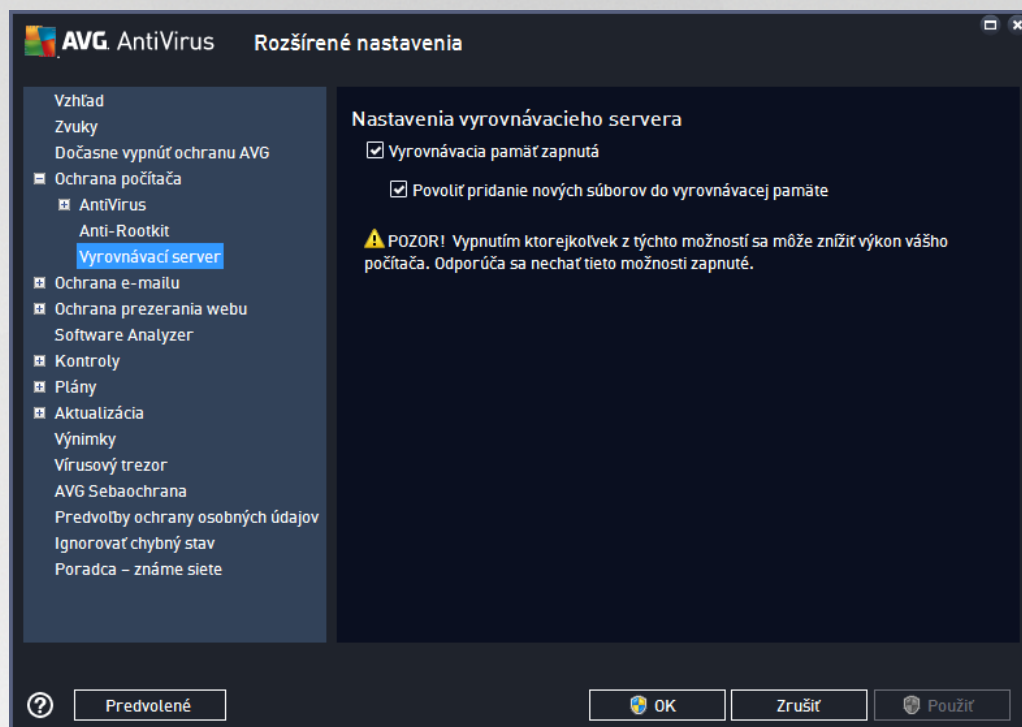
Možnosti **Kontrolovať aplikácie** a **Kontrolovať ovládače** vám umožňujú podrobne zadať, čo by malo byť súčasťou kontroly Anti-Rootkit. Tieto nastavenia sú určené pre skúsených používateľov, odporúčame vám, aby ste nechali všetky možnosti zapnuté. Môžete tiež vybrať režim kontroly rootkitov.

- **Rýchla kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače a systémový priečinok (zvyčajne c:\Windows)
- **Kompletná kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače, systémový priečinok (zvyčajne c:\Windows), a navyše všetky miestne disky (vrátane pamäťových médií, nie však disketové jednotky/jednotky CD-ROM)



7.4.3. Server vyrovnávacej pamäte

Dialógové okno **Nastavenia servera vyrovnávacej pamäte** sa týka procesu servera vyrovnávacej pamäte určeného na zrýchlenie všetkých typov kontrol **AVG AntiVirus**:



Ukladá údaje zozbierané serverom a uchováva informácie o dôveryhodných súboroch (*súbor sa pokladá za dôveryhodný, ak je podpísaný digitálnym podpisom z dôveryhodného zdroja*). Tieto súbory sa potom automaticky pokladajú za bezpečné a nie je potrebné ich kontrolovať. Preto sa počas kontroly vynechávajú.

Dialógové okno **Nastavenie servera vyrovnávacej pamäte** ponúka nasledujúce možnosti konfigurácie:

- **Vyrovnávacia pamäť zapnutá** (*predvolene zapnuté*) – zrušením označenia tohto políčka sa vypne **server vyrovnávacej pamäte** a vyprázdni sa vyrovnávacia pamäť. Upozorňujeme, že sa týmto môže spomaliť kontrola a znížiť celkový výkon počítača, pretože každý jeden používaný súbor sa najskôr skontroluje, či neobsahuje vírusy a spyware.
- **Povoliť pridanie nových súborov do vyrovnávacej pamäte** (*predvolene zapnuté*) – zrušením označenia tohto políčka sa zastaví pridávanie ďalších súborov do vyrovnávacej pamäte. Všetky súbory už vložené do vyrovnávacej pamäte sa zachovávajú a budú sa používať do úplného vypnutia ukladania do vyrovnávacej pamäte alebo do ďalšieho aktualizovania vírusovej databázy.

Ak nemáte oprávnený dôvod na vypnutie servera vyrovnávacej pamäte, dôrazne odporúčame zachovať predvolené nastavenia a nechať obe možnosti zapnuté. Inak môžete zaznamenať výrazné spomalenie rýchlosti a výkonu systému.

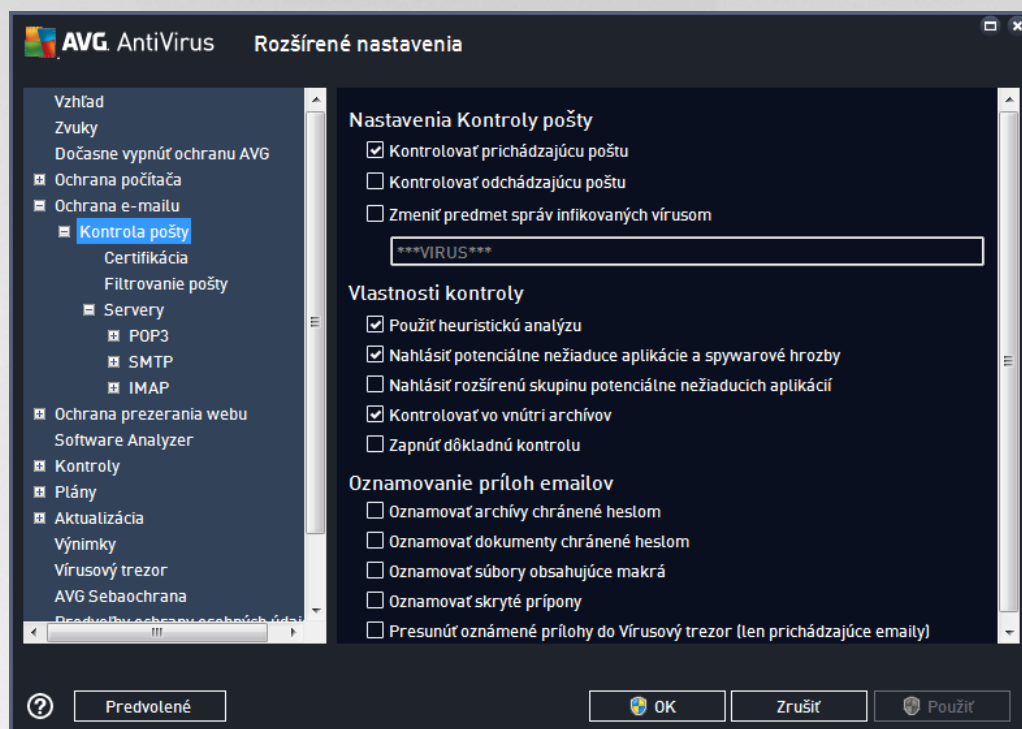
7.5. Kontrola pošty

V tejto časti môžete upraviť podrobnosti konfigurácie nástroja [Kontrola pošty](#) a Anti-Spam:



7.5.1. Kontrola pošty

Dialógové okno **Kontrola pošty** je rozdelené na tri časti:



Kontrola pošty

Táto časť umožňuje definovať tieto základné nastavenia pre prichádzajúcu alebo odchádzajúcu poštu:

- **Kontrolovať prichádzajúcu poštu** (predvolene zapnuté) – začiarknutím zapnete resp. vypnete funkciu na kontrolu všetkých e-mailových správ doručených do vášho e-mailového klienta
- **Kontrolovať odchádzajúcu poštu** (predvolene vypnuté) – začiarknutím zapnete resp. vypnete funkciu na kontrolu všetkých e-mailov poslaných z vašej poštovej aplikácie
- **Zmeniť predmet správ infikovaných vírusom** (predvolene vypnuté) – ak chcete byť informovaní 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 kontroly

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

- **Použiť heuristickú analýzu** (predvolene zapnuté) – začiarknite túto možnosť, ak chcete používať metódu heuristickej detekcie pri kontrole 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](#).



- **Nahlásiť potenciálne nežiaduce aplikácie a hrozby spyware** (predvolene zapnuté) – začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (predvolene vypnuté) – začiarknite toto políčko, 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 predvolene vypnutá.
- **Kontrolovať vo vnútri archívov** (predvolene zapnuté) – začiarknite toto políčko, ak sa má kontrolovať obsah archívov priložených k e-mailovým správam.
- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté) – v určitých situáciách (napr. pri podozrení na infikovanie počítača vírusom alebo zneužitím) môžete začiarknutím tohto políčka aktivovať algoritmus najdôkladnejšej kontroly, ktorá skontroluje aj tie oblasti počítača, ktoré bývajú infikované len vo výnimočných prípadoch – len pre istotu. Upozorňujeme však, že tento spôsob je náročný na čas.

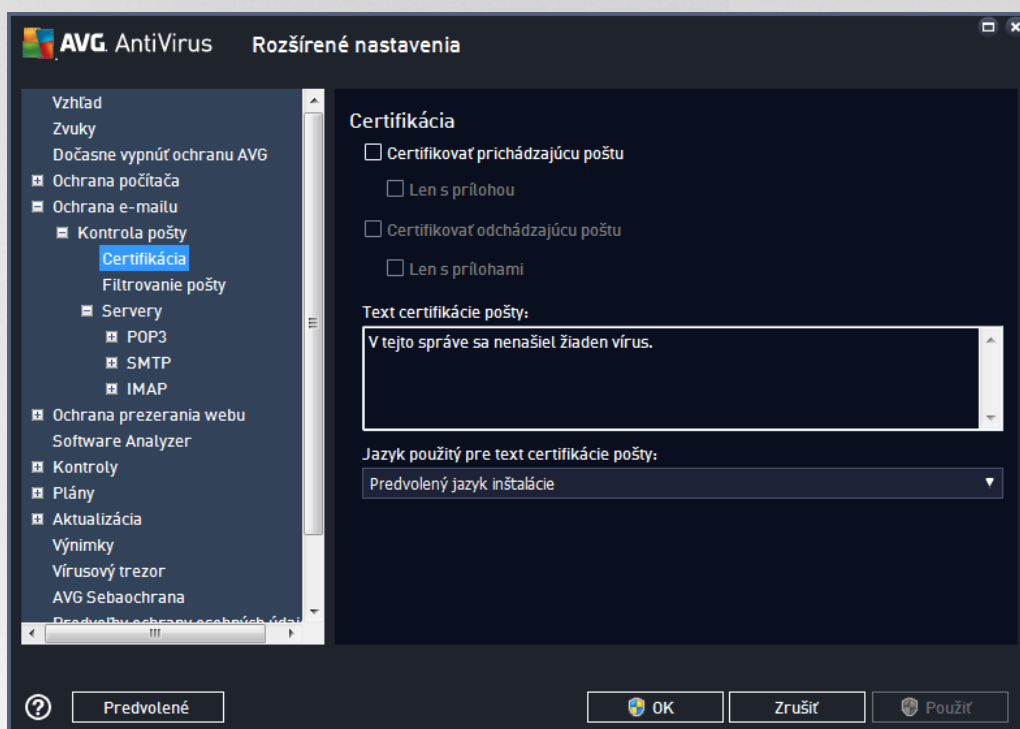
Hlásenie príloh e-mailov

Táto časť umožňuje nastaviť ďalšie správy o súboroch, ktoré môžu byť potenciálne nebezpečné alebo podozrivé. Nezobrazí sa žiadne dialógové okno, na koniec e-mailovej správy sa len pridá text certifikácie a všetky takéto správy budú uvedené v dialógovom okne [Nálezy súčasti Ochrana e-mailu](#):

- **Oznamovať archívy chránené heslom** – archívy (ZIP, RAR, atď.) chránené heslom sa nedajú skontrolovať na prítomnosť vírusov, začiarknite toto políčko, ak sa majú oznamovať tieto archívy ako potenciálne nebezpečné.
- **Oznamovať dokumenty chránené heslom** – dokumenty chránené heslom sa nedajú skontrolovať na prítomnosť vírusov, začiarknite toto políčko, ak sa majú oznamovať tieto dokumenty ako potenciálne nebezpečné.
- **Oznamovať súbory obsahujúce makrá** – makro je vopred definovaný sled krokov, ktoré zjednodušujú konkrétne úlohy používateľovi (makrá používané v MS Word sú veľmi známe). Makro ako také môže obsahovať potenciálne nebezpečné inštrukcie, a preto je vhodné začiarknuť toto políčko, aby sa súbory s makrami oznamovali ako podozrivé.
- **Oznamovať 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 políčko, ak sa majú tieto súbory oznamovať ako potenciálne nebezpečné.
- **Premiestniť hlásené prílohy do Vírusového trezora** – nastavte, či si želáte byť informovaní e-mailom o archívoch chránených heslom, dokumentoch chránených heslom, súboroch s makrami alebo súboroch so skrytou príponou, ktoré boli detegované ako príloha kontrolovanej e-mailovej správy. Ak sa takáto správa identifikuje počas kontroly, uveďte, či sa má detegovaný infikovaný objekt presunúť do [Vírusového trezora](#).

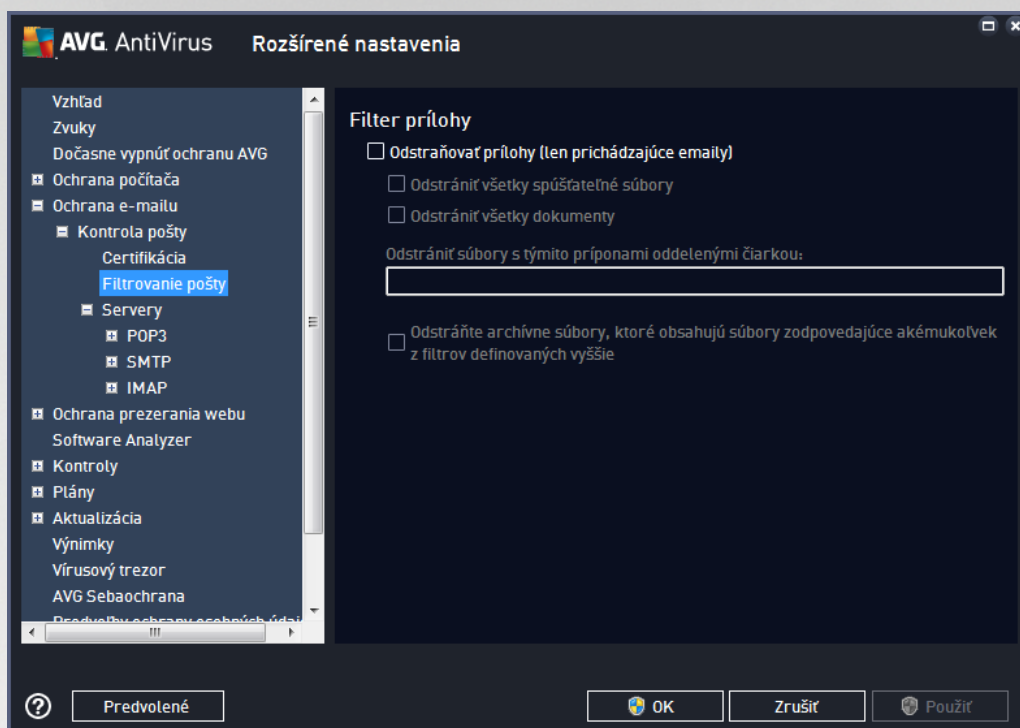


V dialógovom okne **Certifikácia** môžete označiť konkrétne začiarkavacie políčka a určiť, či chcete certifikovať prichádzajúcu poštu (**Certifikovať prichádzajúcu poštu**) alebo odchádzajúcu poštu (**Certifikovať odchádzajúcu poštu**). Pri každej možnosti môžete ďalej určiť parameter **Len s prílohami**. Vtedy sa certifikácia bude týkať iba e-mailových správ s prílohami:



Predvolene text certifikácie obsahuje iba základnú informáciu: *V tejto správe sa nenašiel žiadny vírus*. Tieto informácie však podľa potreby môžete rozšíriť alebo zmeniť: do poľa **Text e-mailovej certifikácie** napíšete požadovaný text certifikácie. V časti **Jazyk použitý pre text e-mailovej certifikácie** môžete ďalej definovať, v akom jazyku sa má automaticky vytváraná časť certifikácie (*V tejto správe sa nenašiel žiadny vírus*) zobrazit'.

Poznámka: Pamätajte, že v požadovanom jazyku sa zobrazí iba predvolený text. Váš vlastný text sa automaticky nepreloží!



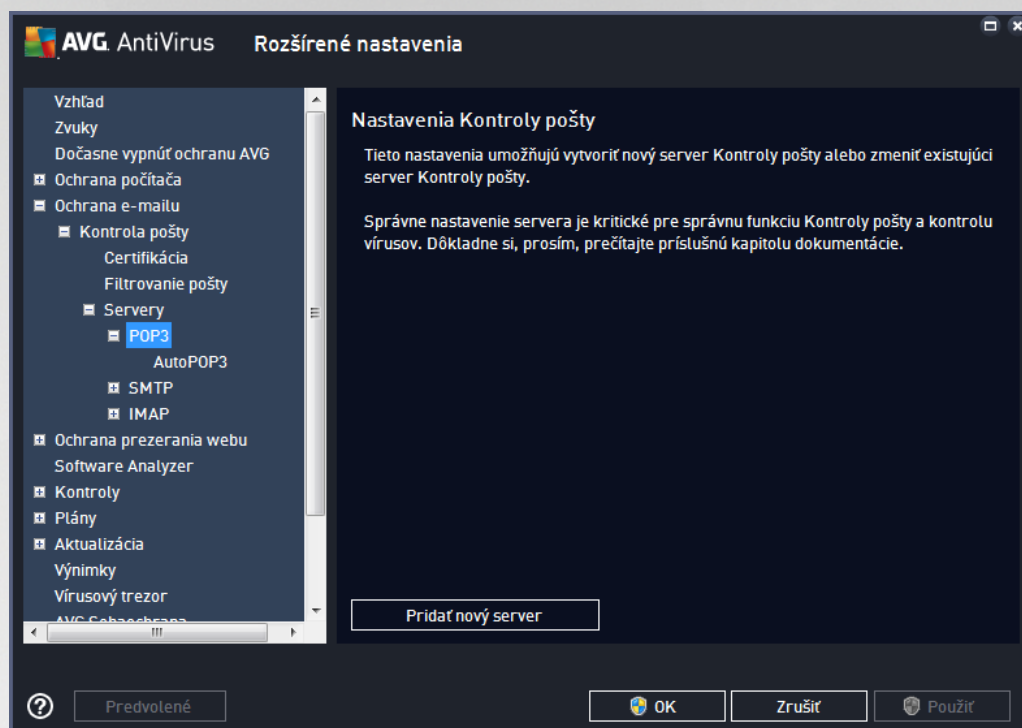
Dialógové okno **Filter príloh** vám umožňuje nastaviť parametre pre kontrolu príloh e-mailových správ. V predvolenom nastavení je možnosť **Odstrániť prílohy** vypnutá. Ak sa rozhodnete ju aktivovať, všetky prílohy e-mailových správ detegované ako infekcie alebo potenciálne nebezpečné programy sa automaticky odstraňujú. Ak chcete definovať konkrétne typy príloh, ktoré sa majú odstrániť, vyberte príslušnú možnosť:

- **Odstrániť všetky spúšťateľné 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

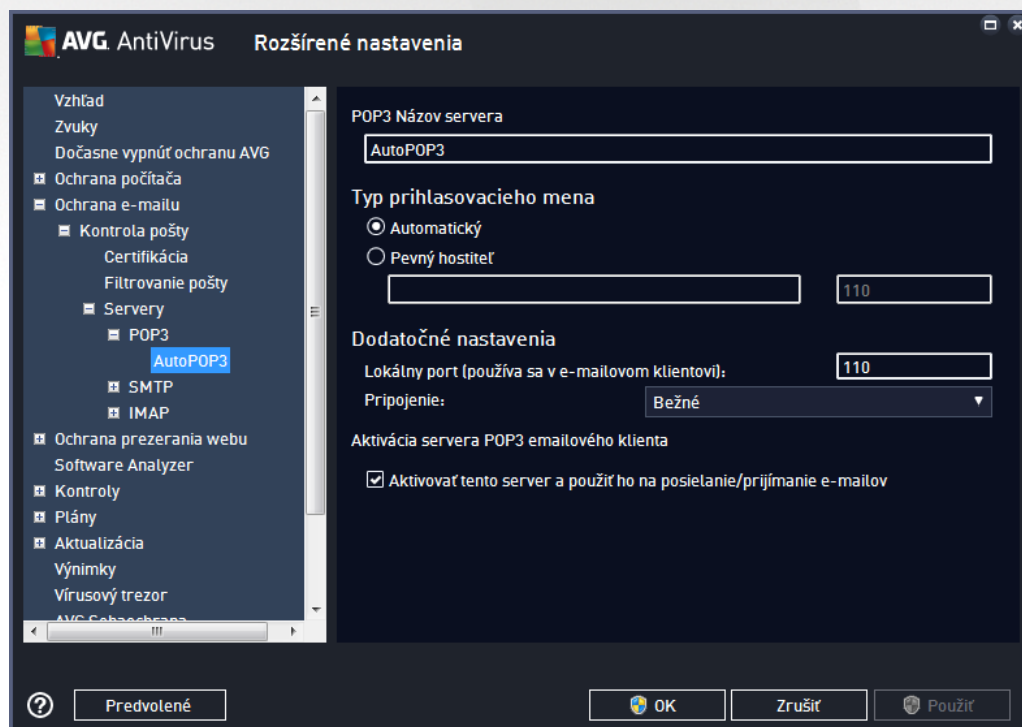
V časti **Servery** môžete upraviť parametre serverov súčasti [Kontrola pošty](#):

- [Server POP3](#)
- [Server SMTP](#)
- [Server IMAP](#)

Pomocou tlačidla **Pridať nový server** môžete definovať nové servery pre prichádzajúcu alebo odchádzajúcu poštu.

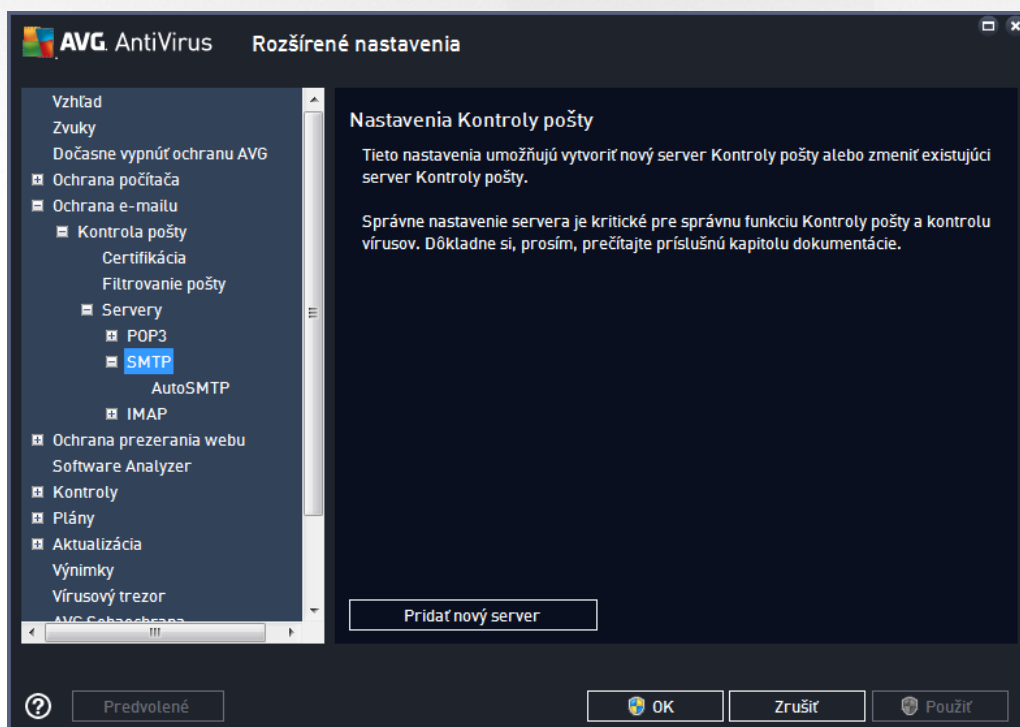


Toto dialógové okno umožňuje nastaviť pre súčasť [Kontrola pošty](#) nový server pomocou protokolu POP3 pre prichádzajúcu poštu:

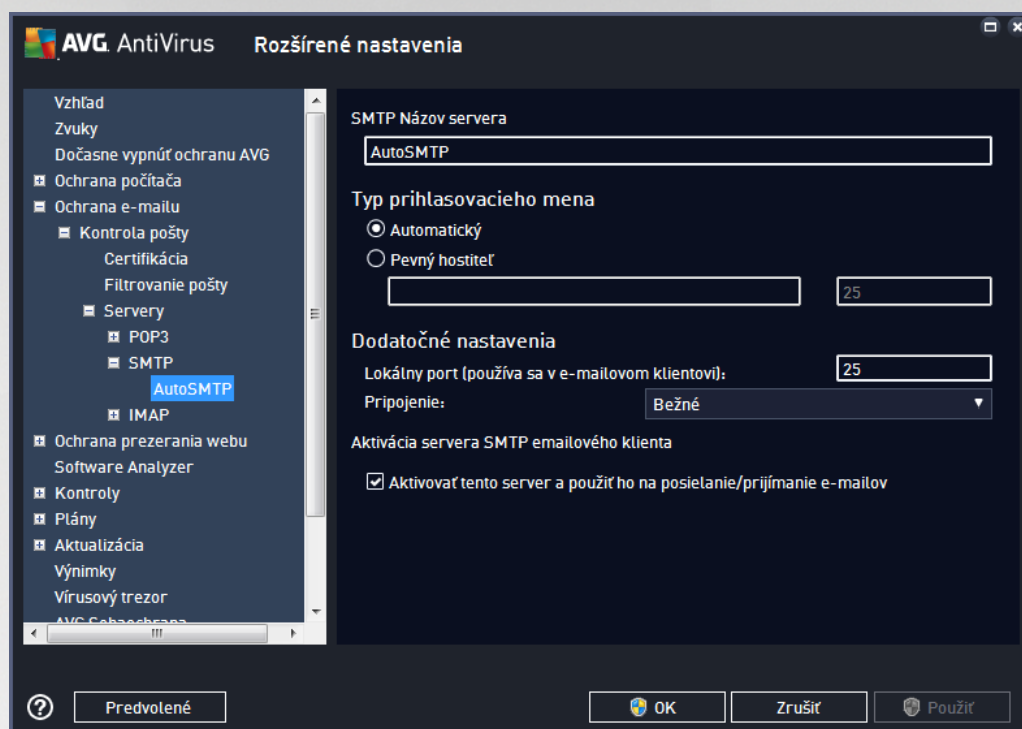




- **Názov servera POP3** – do tohto pol'a môžete zadať názov novo pridaných serverov (na pridanie servera POP3 kliknite pravým tlačidlom myši na položku POP3 v ľavej navigačnej ponuke).
- **Typ prihlásenia** – určuje metódu určovania e-mailového servera, ktorý sa používa pre prichádzajúcu poštu:
 - o **Automaticky** – prihlásenie sa uskutoční automaticky podľa nastavení vášho e-mailového klienta.
 - o **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadaťte adresu alebo názov svojho emailového serveru. Prihlasovacie meno zostane nezmenené. Ako názov môžete použiť názov domény (napríklad *pop.acme.com*), ako aj adresu IP (napríklad *123.45.67.89*). Ak poštový server používa neštandardný port, môžete zadať tento port za názvom servera a použité dvojbodku ako oddeľovací znak (napríklad *pop.acme.com:8200*). Štandardný port pre komunikáciu POP3 je 110.
- **Dodatočné nastavenia** – uvádza podrobnejšie parametre:
 - o **Lokálny port** – uvádza port, na ktorom sa očakáva komunikácia 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, ak ju podporuje cieľový poštový server.
- **Aktivácia servera POP3 v e-mailovom klientovi** – označením/zrušením označenia tejto položky sa aktivuje, resp. deaktivuje uvedený server POP3



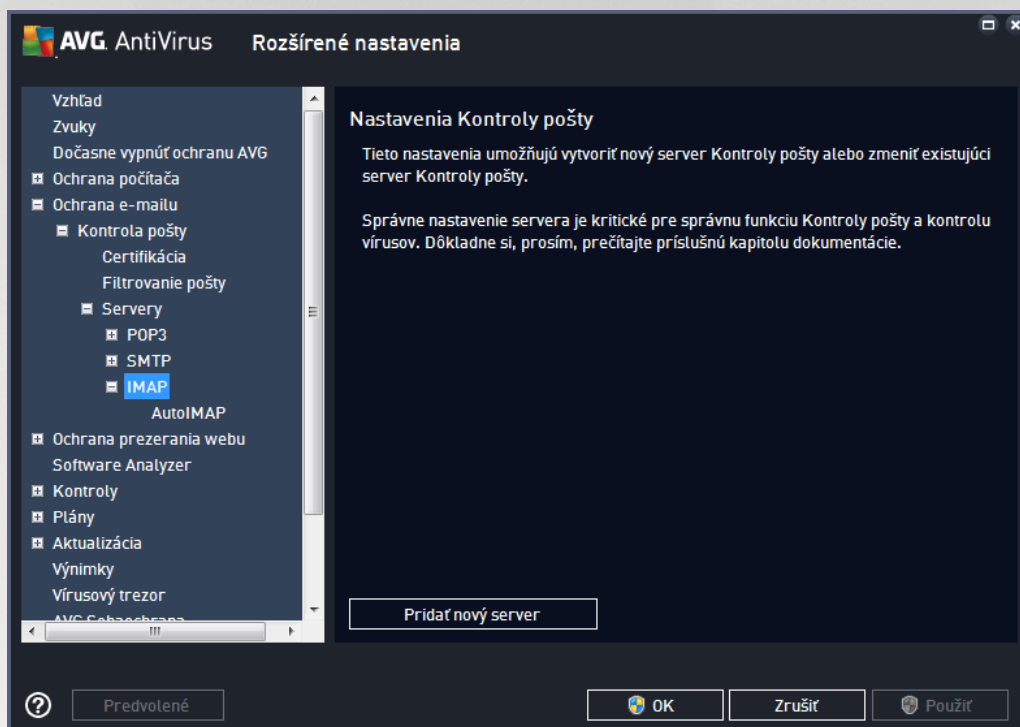
Toto dialógové okno umožňuje nastaviť pre súčasť [Kontrola pošty](#) nový server pomocou protokolu SMTP pre odchádzajúcu poštu:



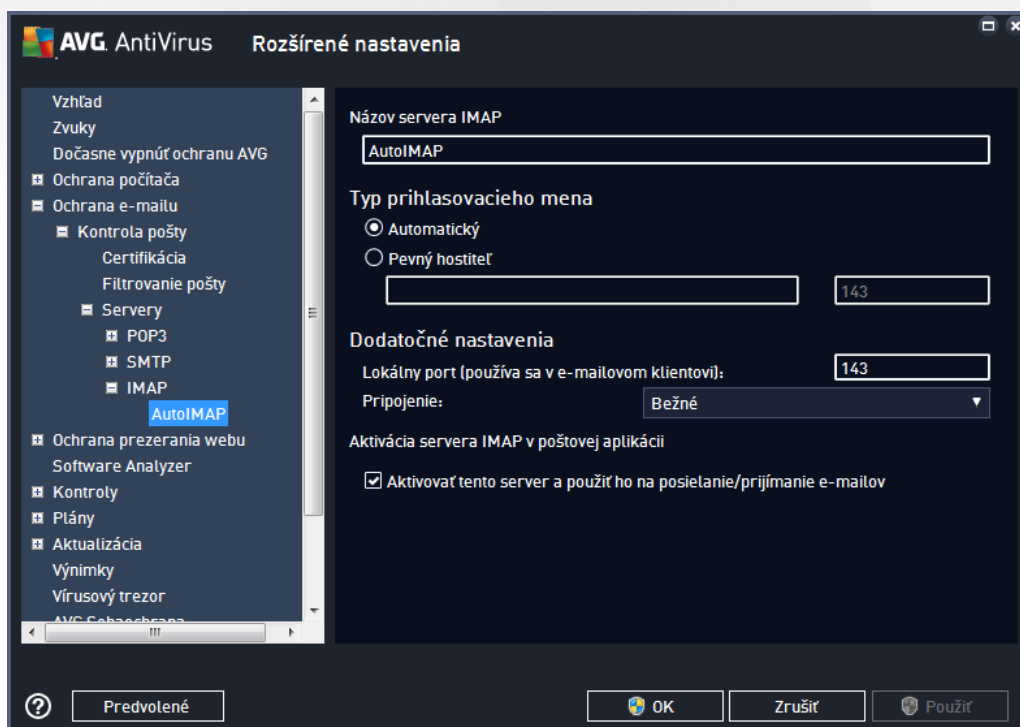
- **Názov servera SMTP** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie servera SMTP kliknite pravým tlačidlom myši na položku SMTP v ľavej navigačnej ponuke). Pre automaticky vytvorené servery „AutoSMTP“ je toto pole vypnuté.
- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre odchádzajúcu poštu:
 - o **Automaticky** – prihlásenie sa uskutoční automaticky podľa nastavení vášho e-mailového klienta
 - o **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov svojho emailového serveru. 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 pre komunikáciu SMTP je 25.
- **Dodatočné nastavenia** – uvádza podrobnejšie parametre:
 - o **Lokálny port** – uvádza port, na ktorom sa očakáva komunikácia 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, ktoré sa má použiť (bežné/SSL/predvolené SSL). 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.



- **Aktivácia servera SMTP v e-mailovom klientovi** – začiarknutím alebo zrušením začiarknutia tohto políčka sa aktivuje, resp. deaktivuje vyššie uvedený server SMTP



Toto dialógové okno umožňuje nastaviť pre súčasť [Kontrola pošty](#) nový server pomocou protokolu IMAP pre odchádzajúcu poštu:



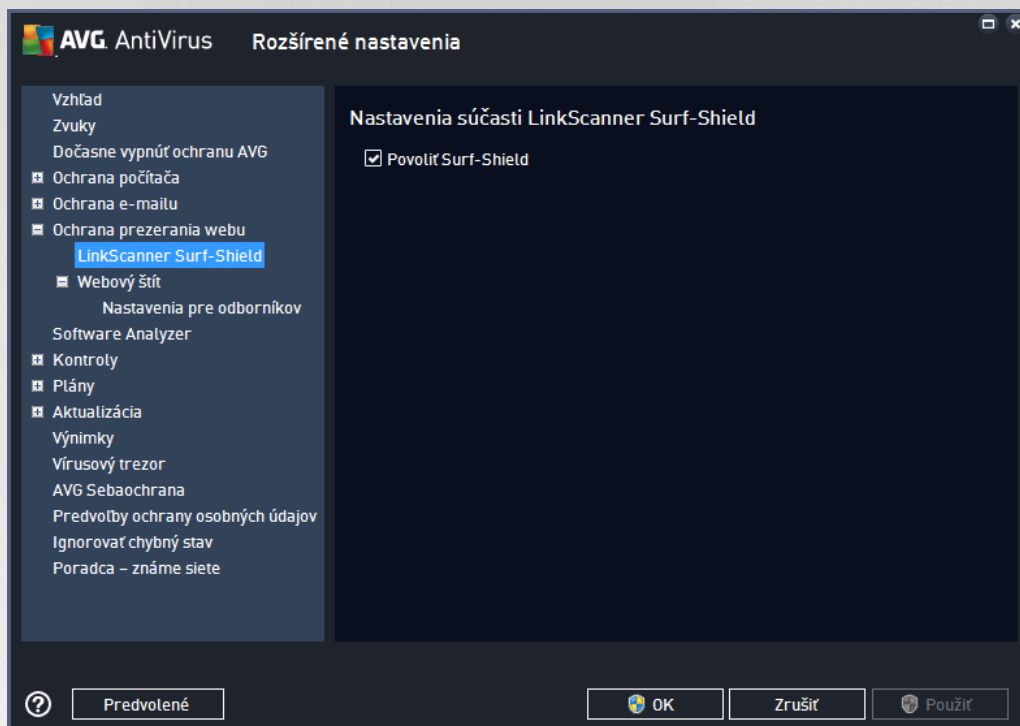


- **Názov servera IMAP** – do tohto poľa zadajte názov novo pridaných serverov (na pridanie servera IMAP kliknite pravým tlačidlom myši na položku IMAP v ľavej navigačnej ponuke).
- **Typ prihlásenia** – určuje spôsob zistenia poštového servera, ktorý sa používa pre odchádzajúcu poštu:
 - o **Automaticky** – prihlásenie sa uskutoční automaticky podľa nastavení vášho e-mailového klienta
 - o **Pevný hostiteľ** – v tomto prípade program vždy použije server, ktorý je tu uvedený. Zadajte adresu alebo názov svojho emailového serveru. 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 oddeľovacieho znaku (napríklad *imap.acme.com:8200*). Štandardný port pre komunikáciu IMAP je 143.
- **Dodatočné nastavenia** – uvádza podrobnejšie parametre:
 - o **Lokálny port používaný v** – určuje port, na ktorom sa má očakávať 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 typu pripojenia, ktoré sa má použiť (bežné/SSL/predvolené SSL). Ak si zvolíte pripojenie SSL, zaslané údaje budú zakódované bez rizika vystopovania alebo monitorovania treťou stranou. Táto funkcia je dostupná len vtedy, keď ju podporuje cieľový poštový server.
- **Aktivácia servera IMAP v e-mailovom klientovi** – začiatkom alebo zrušením začiatku tohto políčka sa aktivuje, resp. deaktivuje vyššie uvedený server IMAP



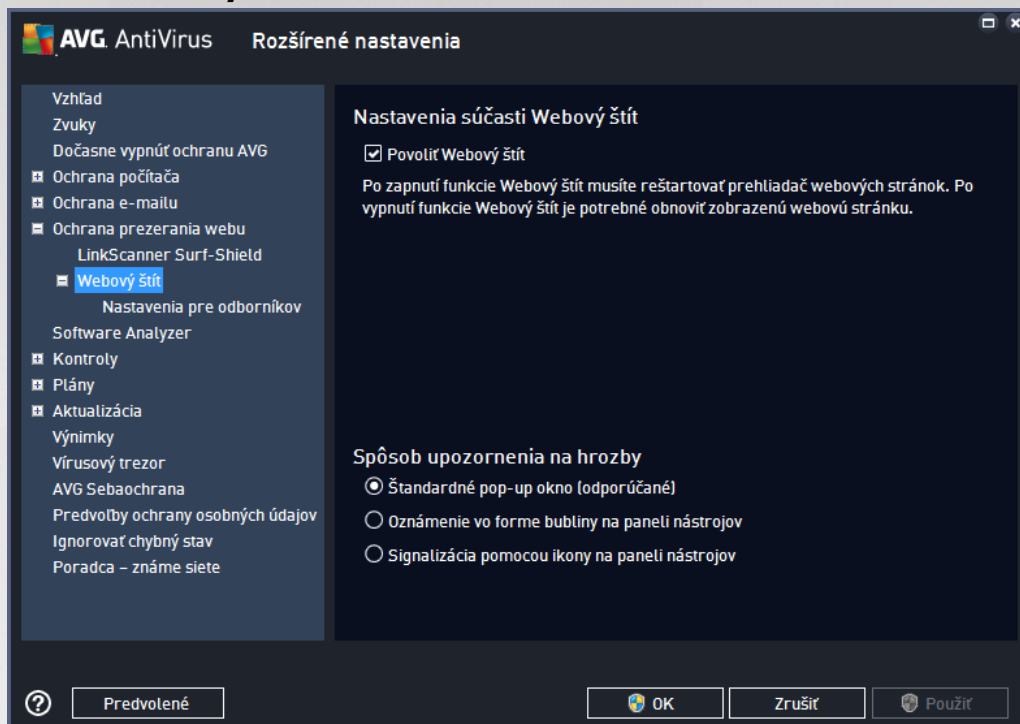
7.6. Ochrana prezerania webu

Dialógové okno s nastaveniami súčasti **LinkScanner** vám umožňuje zapnúť/vypnúť tieto funkcie:



- **Povolit' Surf-Shield** – (predvolene zapnuté): aktívna ochrana (v reálnom čase) pred webovými 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).

7.6.1. Webový štít

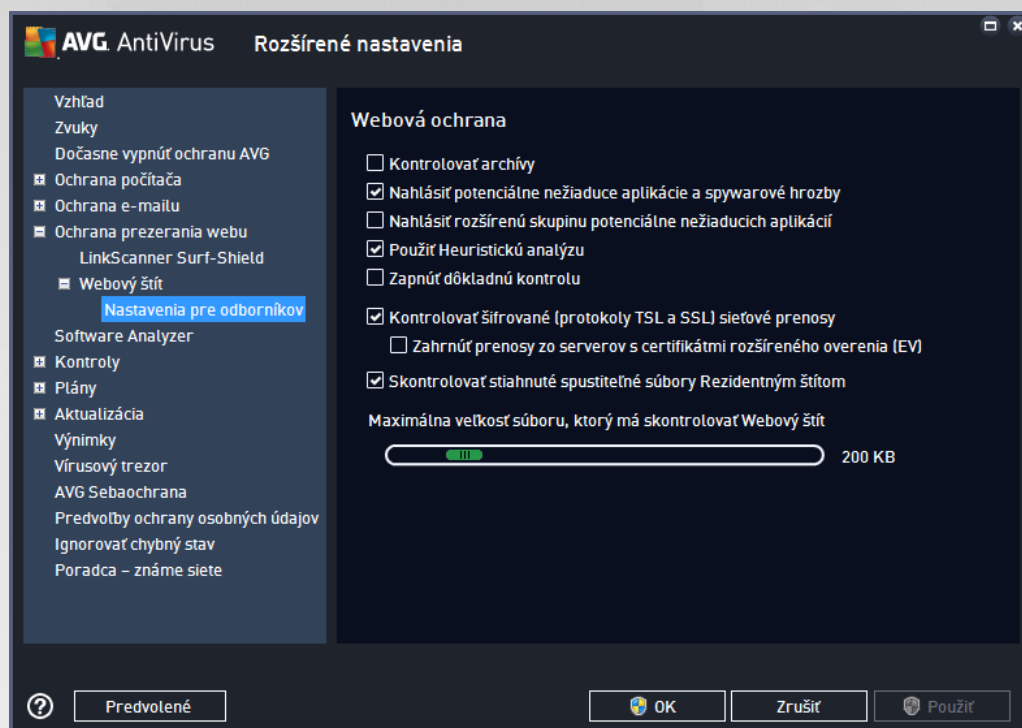


Dialógové okno **Webový štít** ponúka tieto možnosti:

- **Povolit Webový štít** (predvolene zapnuté) – aktivuje/deaktivuje celú službu **Webový štít**. Ďalšie rozšírené nastavenia **Webového štítu** nájdete v nasledujúcom dialógovom okne s názvom [Webová ochrana](#).

Spôsob upozornenia na hrozby

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



Dialógové okno **Webová ochrana** umožňuje upraviť konfiguráciu súčasti z hľadiska kontroly obsahu webových stránok. Rozhranie editácie umožňuje nastaviť tieto základné možnosti:

- **Kontrolovať archívy** – (predvolene vypnuté): kontrolovať obsah archívov, ktoré sa môžu nachádzať na otvorenej webovej stránke.
- **Nahlásiť potenciálne nežiaduce programy a spyware hrozby** – (predvolene zapnuté): zaškrtnite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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.
- **Nahlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** – (predvolene vypnuté): zaškrtnite toto políčko, 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 predvolene vypnutá.
- **Použiť heuristickú analýzu** – (predvolene zapnuté): kontroluje obsah zobrazovanej stránky pomocou metódy heuristickej analýzy (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí).
- **Zapnúť dôkladnú kontrolu** – (predvolene vypnuté): v určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obvyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.



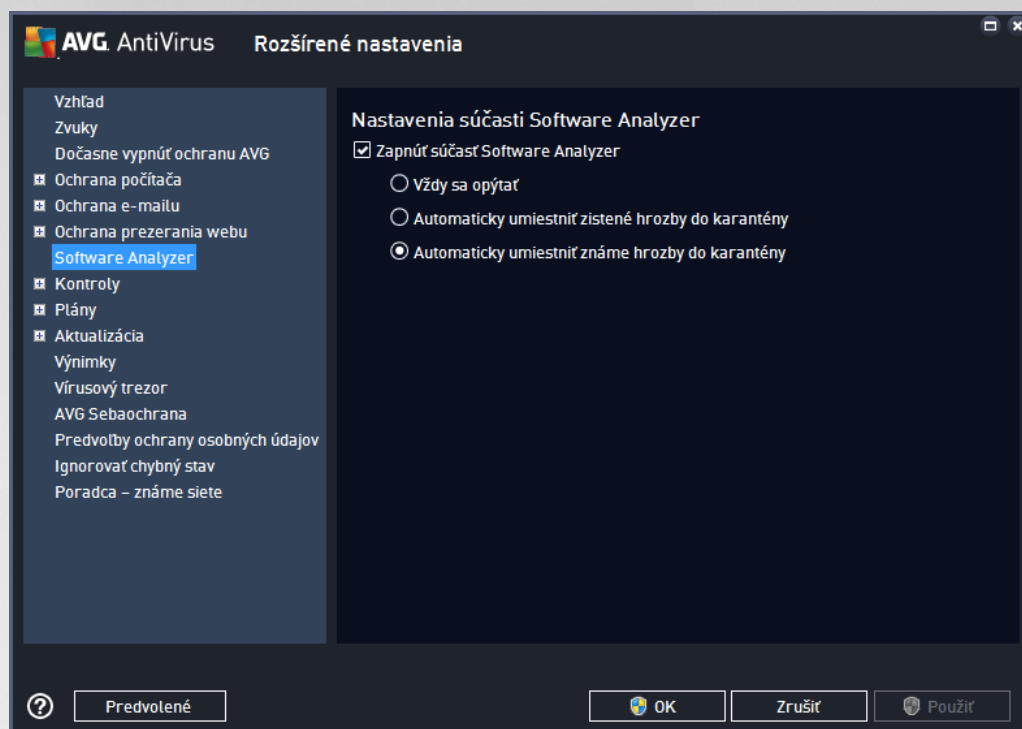
- **Kontrolovať šifrované (protokoly TSL a SSL) sieťové prenosy** – (predvolene zapnuté): nechajte označené, aby ste umožnili AVG kontrolovať taktiež všetku šifrovanú sieťovú komunikáciu, teda spojenia prostredníctvom zabezpečených protokolov (SSL a jeho novšia verzia TLS). Týka sa to webových stránok používajúcich protokol HTTPS a pripojení e-mailových klientov používajúcich protokol TLS/SSL. Zabezpečené prenosy sa dešifrujú, skontrolujú, či neobsahujú malware, znova sa zašifrujú a bezpečne sa odošlú do počítača. V rámci tejto možnosti sa môžete rozhodnúť **Zahrnúť prenosy zo serverov s certifikátmi rozšíreného overenia (EV)** a kontrolovať taktiež šifrovanú sieťovú komunikáciu so servermi, ktoré sú certifikované pomocou certifikátu rozšíreného overenia. Vydanie certifikátu EV vyžaduje predĺženú platnosť certifikačným orgánom a webové stránky prevádzkované na základe certifikátu sú preto omnoho dôveryhodnejšie (*je menej pravdepodobné, že budú prenášať malware*). Z tohto dôvodu sa môžete rozhodnúť nekontrolovať prenosy z certifikovaných serverov EV, čo by malo mierne zrýchliť šifrovanú komunikáciu.
- **Skontrolovať stiahnuté spustiteľné súbory Rezidentným štítom** – (predvolene zapnuté): kontrolovať spustiteľné súbory (typicky prípony exe, bat, com) po ich stiahnutí. Rezidentný štít kontroluje súbory pred stiahnutím, aby zabezpečil, že sa žiadny škodlivý kód nedostane do vášho počítača. Táto kontrola je však obmedzená **Maximálnou čiastkovou veľkosťou kontrolovaného súboru** – pozrite si nasledujúcu položku v tomto dialógovom okne. Preto sú veľké súbory kontrolované po častiach, a to isté platí aj pre väčšinu spustiteľných súborov. Spustiteľné súbory môžu vo vašom počítači vykonávať rôzne úlohy, a preto je nevyhnutne nutné, aby boli na 100 % bezpečné. To je možné zabezpečiť kontrolou častí súboru pred jeho stiahnutím a taktiež kontrolou ihneď po dokončení stiahnutia súboru. Odporúčame vám ponechať túto možnosť zaškrtnutú. Ak túto možnosť deaktivujete, stále môžete byť pokojní, že AVG nájde akýkoľvek potenciálne škodlivý kód. Len obvykle nebude schopný posúdiť spustiteľný súbor ako celok, takže môže ohlasovať niekoľko nesprávnych detekcií.

Posúvač v dolnej časti dialógového okna vám umožňuje určiť **Maximálnu čiastkovú veľkosť kontrolovaného súboru** – ak sa priložené súbory nachádzajú na otvorenej stránke, potom sa ich obsah môže zároveň skontrolovať ešte predtým, než sa súbory stiahnu do počítača. Kontrola veľkých súborov však chvíľu trvá a stiahnutie z internetovej stránky sa môže výrazne spomaliť. Pomocou posúvača môžete nastaviť maximálnu veľkosť súboru, ktorá sa má kontrolovať súčasťou **Webový štít**. Aj keď je stiahnutý súbor väčší než nastavená hodnota a z tohto dôvodu ho súčasť Webový štít neskontroluje, váš počítač je stále chránený: ak je súbor infikovaný, súčasť **Rezidentný štít** ho ihneď deteguje.

7.7. Software Analyzer

Software Analyzer je súčasťou na ochranu pred malware, ktorá vás chráni pred všetkými typmi malware (spyware, softvérové roboty, krádeže identity atď.). Používa behaviorálne technológie a poskytuje okamžitú ochranu pred novými vírusmi (podrobný popis funkcií tejto súčasti nájdete v kapitole [Software Analyzer](#)).

Dialógové okno **Nastavenia Software Analyzer** vám umožňuje zapnúť alebo vypnúť základné funkcie súčasti [Software Analyzer](#):



Aktivovať Software Analyzer (predvolene zapnuté) – zrušením začiarknutia sa vypne súčasť [Identita](#). **Odporúčame, aby ste tak učinili len v prípade, ak to je naozaj nevyhnutné!** Keď je súčasť Software Analyzer aktivovaná, môžete nastaviť, čo sa má urobiť pri detegovaní hrozby:

- **Vždy sa opýtať** – 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** – označte toto začiarkavacie políčko, ak si želáte všetky potenciálne zistené hrozby ihneď premiestniť na bezpečné miesto vo [Vírusovom trezore](#). Ponechaním predvolených nastavení sa vás pri zistení hrozby program opýta, či sa má hrozba premiestniť do karantény, aby nedošlo k neželanému odstráneniu aplikácií, ktoré chcete používať.
- **Automaticky umiestniť známe hrozby do karantény** (predvolene zapnuté) – nechajte toto začiarkavacie políčko označené, ak si želáte všetky aplikácie označené ako potenciálne škodlivé automaticky a ihneď premiestniť do [Vírusového trezora](#).

7.8. Kontroly

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

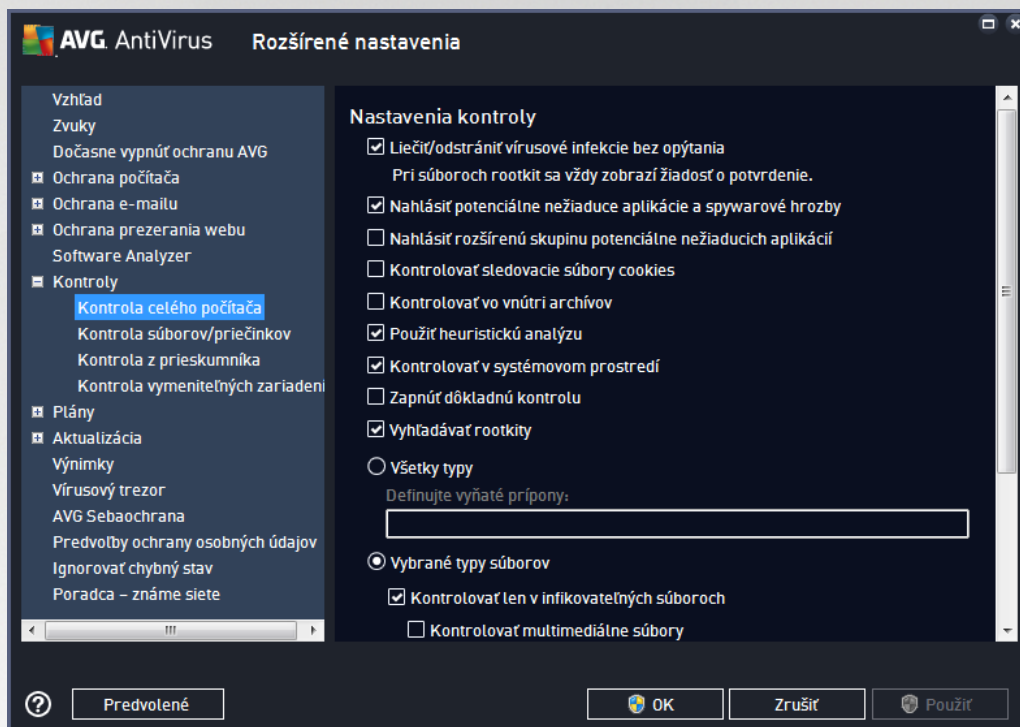
- [Kontrola celého počítača](#) – štandardná vopred definovaná kontrola celého počítača.
- [Kontrola súborov/priečinkov](#) – štandardná vopred definovaná kontrola vybraných oblastí počítača.
- [Kontrola z prieskumníka](#) – špeciálna kontrola vybraného objektu priamo v prostredí programu Windows Explorer.



- [Kontrola vymeniteľných zariadení](#) – špeciálna kontrola vymeniteľných zariadení zapojených do počítača.

7.8.1. Kontrola celého počítača

Funkcia **Kontrola celého počítača** umožňuje upraviť 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:

- **Liečiť/odstrániť vírusovú infekciu bez opýtania** (predvolene zapnuté) – ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a hrozby spyware** (predvolene zapnuté) – začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich programov** (predvolene vypnuté) – začiarknite toto políčko, 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 predvolene vypnutá.



- **Kontrolovať sledovacie súbory cookies** (predvolene vypnuté) – tento parameter súčasť zapína detekciu súborov cookies; (súbory 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 vo vnútri archívov** (predvolene vypnuté) – tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory uložené vnútri archívov, napr. ZIP, RAR, atď.
- **Použiť heuristickú analýzu** (predvolene zapnuté) – heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolovať v systémovom prostredí** (predvolene zapnuté) – počas kontroly sa overujú systémové oblasti počítača.
- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté – v určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obvyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Kontrolovať rootkity** (predvolene zapnuté) – [Anti-Rootkit](#) skontroluje počítač a zisťuje prítomnosť potenciálnych rootkitov, t. j. programov a technológií, ktoré dokážu zakryť činnosť malwaru 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.

Mali by ste tiež určiť, čo 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, sa nebudú kontrolovať), vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.
- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony** – táto možnosť je predvolene 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.

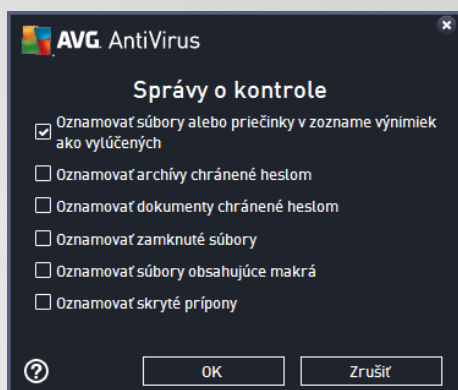
Nastaviť rýchlosť dokončenia kontroly

V časti **Nastaviť rýchlosť dokončenia kontroly** môžete ďalej nastaviť požadovanú rýchlosť kontroly v závislosti od využívania systémových zdrojov. Predvolene 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 systémových zdrojov a spomalia 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 systémových zdrojov predĺžením doby trvania kontroly.



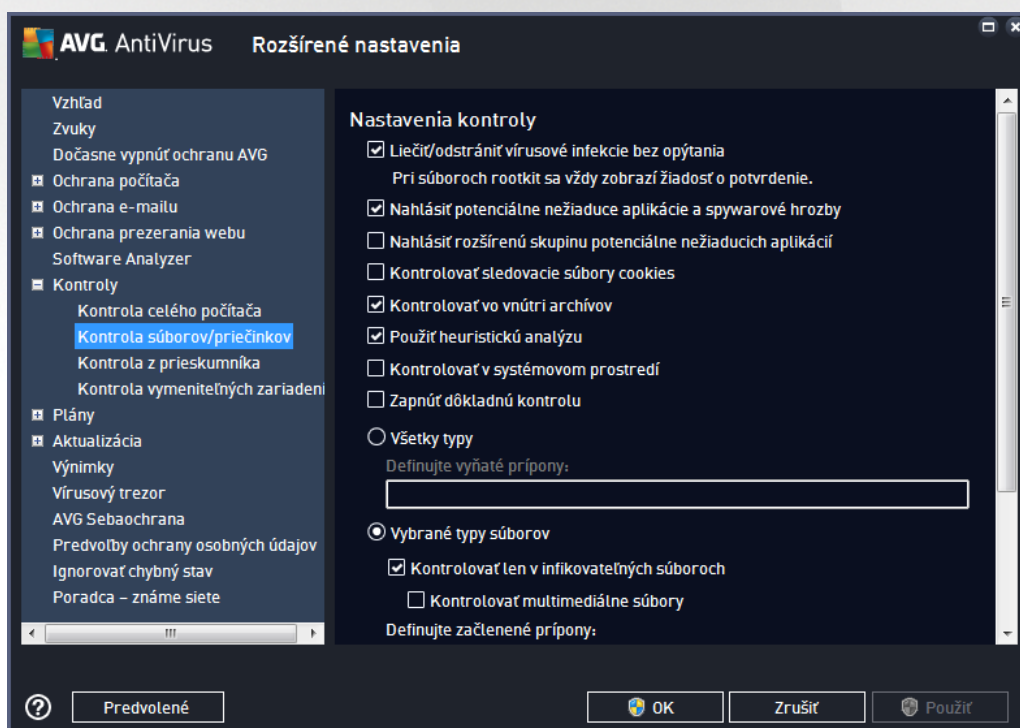
Vytvoriť ďalšie správy o kontrole...

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



7.8.2. Kontrola súborov/priečinkov

Rozhranie editácie na **Kontrolu súborov/priečinkov** je takmer rovnaké ako dialógové okno editácie s názvom [Kontrola celého počítača](#), avšak predvolené nastavenia sú pre možnosť [Kontrola celého počítača](#) prísnejšie:



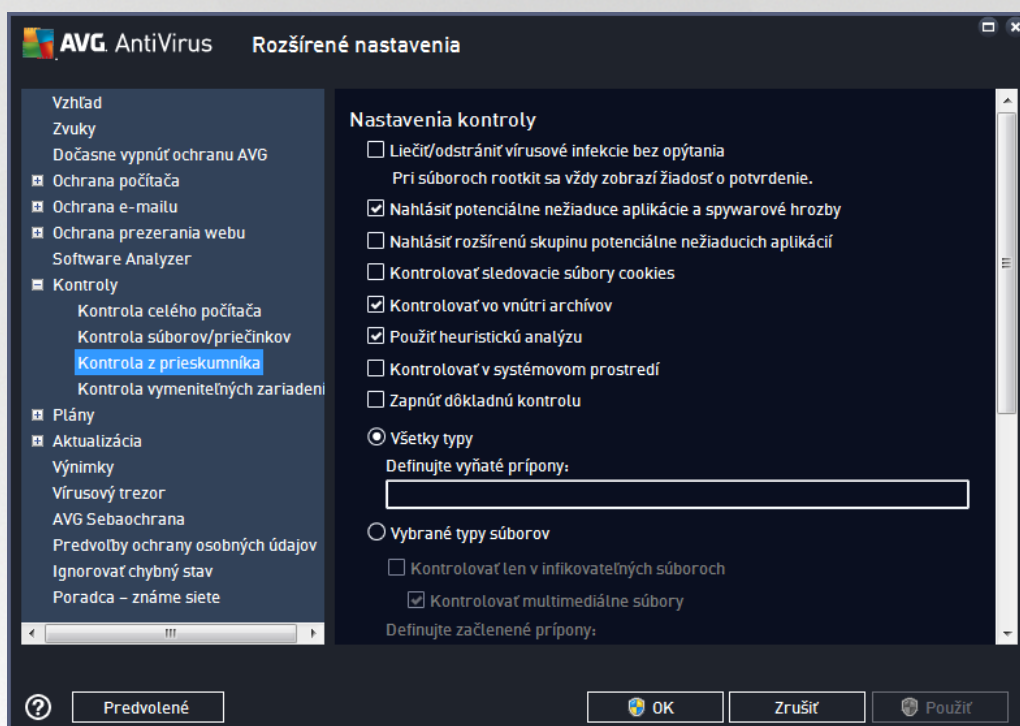
Všetky parametre nastavené v tomto dialógovom okne konfigurácie sa vzťahujú len na oblasti vybrané na kontrolu v dialógovom okne [Kontrola súborov/priečinkov](#)!



Poznámka: Informácie o konkrétnych parametroch nájdete v kapitole [Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača](#).

7.8.3. Kontrola z prieskumníka

Rovnako ako predchádzajúca funkcia, [Kontrola celého počítača](#), aj táto funkcia s názvom **Kontrola z prieskumníka** ponúka niekoľko možností na úpravu kontroly vopred definovanej dodávateľom softvéru. V tomto prípade súvisí konfigurácia s [kontrolou konkrétnych objektov spustených v prostredí programu Windows Explorer \(prieskumník\)](#), pozri kapitolu [Kontrola z prieskumníka](#):



Možnosti úpravy sú takmer rovnaké ako tie, ktoré sú k dispozícii pre možnosť [Kontrola celého počítača](#), avšak predvolené nastavenia sa líšia (napríklad *Kontrola celého počítača* predvolene nekontroluje archívy, ale kontroluje systémove prostredie, zatiaľ čo *Kontrola z prieskumníka* má presne opačné nastavenia).

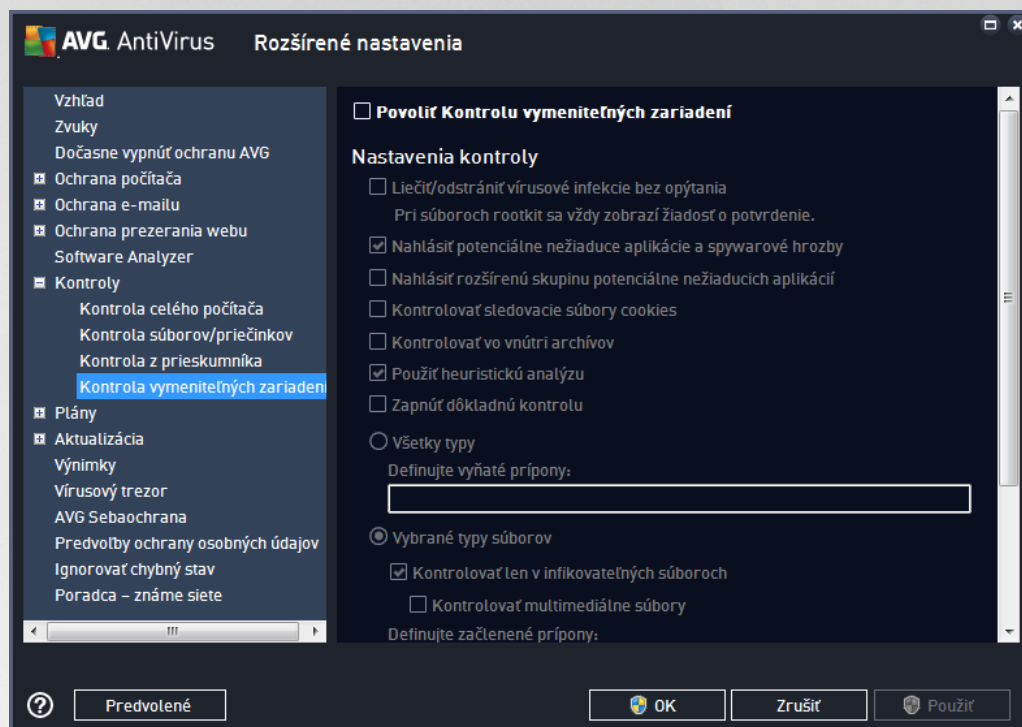
Poznámka: Informácie o konkrétnych parametroch nájdete v kapitole [Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača](#).

V porovnaní s dialógovým oknom [Kontrola celého počítača](#) sa v dialógovom okne **Kontrola z prieskumníka** nachádza aj časť s názvom **Zobrazenie postupu a výsledkov kontroly**, ktorá umožňuje nastaviť, či majú byť výsledky a priebeh kontroly prístupné v používateľskom rozhraní AVG. Zároveň umožňuje nastaviť, aby sa výsledky kontroly zobrazili len v prípade, keď sa počas kontrolovania deteguje infekcia.



7.8.4. Kontrola vymeniteľných zariadení

Rozhranie editácie **Kontrola vymeniteľných zariadení** je tiež veľmi podobné dialógovému oknu editácie [Kontrola celého počítača](#):



Kontrola vymeniteľných zariadení sa spustí automaticky po pripojení vymeniteľného zariadenia k počítaču. Táto kontrola je predvolene vypnutá. Kontrola vymeniteľných zariadení je však veľmi dôležitá z hľadiska potenciálnych hrozieb, pretože tieto predstavujú zdroj infekcie. Ak chcete, aby táto kontrola bola pripravená a spustila sa automaticky v prípade potreby, označte možnosť **Povolit kontrolu vymeniteľných zariadení**.

Poznámka: Informácie o konkrétnych parametroch nájdete v kapitole [Rozšírené nastavenia AVG/Kontroly/Kontrola celého počítača](#).

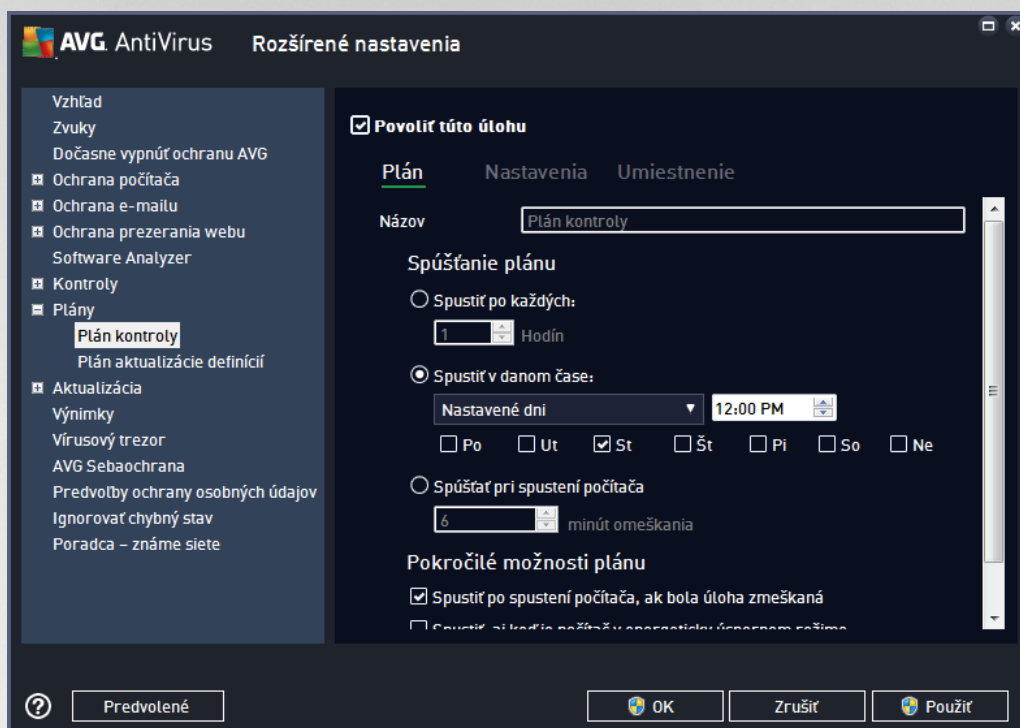
7.9. Plány

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

- [Plán kontroly](#)
- [Plán aktualizácie definícií](#)
- Plán aktualizácie programu

7.9.1. Plán kontroly

Parametre plánu kontroly sa dajú upraviť (alebo sa dá nastaviť nový plán) v troch kartách. Na každej karte najskôr začiarknutím, resp. zrušením začiarknutia položky **Povolit túto úlohu** dočasne vypnete naplánovaný test a znova ho zapnete, keď je potrebný:



Vo vedľajšom textovom poli **Názov** (neaktívne pre všetky predvolené plány) sa nachádza názov, ktorý tomuto konkrétnemu plánu pridelil dodávateľ programu. Pre novo pridané plány (nový plán sa pridá kliknutím pravým tlačidlom myši nad položkou **Plán kontroly** 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 kontroly, aby sa dali neskôr ľahšie navzájom odlíšiť.

Napríklad: nie je vhodné nazývať kontrolu „Nová kontrola“ alebo „Moja kontrola“, pretože tieto názvy sa nevzťahujú na to, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod. Takisto nie je potrebné zadať do názvu kontroly, či ide o kontrolu celého počítača, alebo vybraných súborov, alebo priečinkov, pretože vaše vlastné kontroly budú vždy predstavovať špeciálnu verziu [kontroly vybraných súborov alebo priečinkov](#).

Toto dialógové umožňuje ďalej definovať tieto parametre prehľadávania:

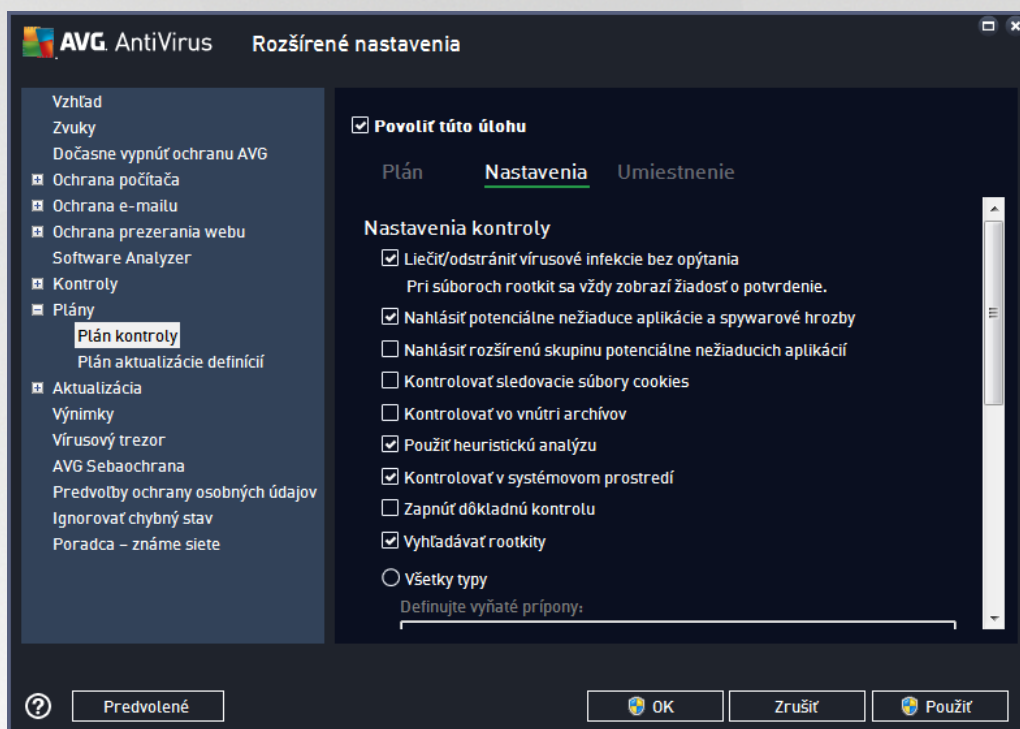
Spúšťanie naplánovaných úloh

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

Rozšírené možnosti plánu



- **Spustiť po spustení počítača, ak bola úloha zmeškaná** – ak naplánujete úlohu, aby sa spustila v istom čase, táto možnosť zabezpečí, že sa následne vykoná kontrola v prípade, že sa počítač v naplánovanom čase vypne.
- **Spustiť, aj keď je počítač v energeticky úspornom režime** – úloha sa má vykonať v naplánovanom čase, aj keď je počítač napájaný batériou.



V karte **Nastavenia** nájdete zoznam parametrov kontrolovania, ktoré sa dajú voliteľne zapnúť/vypnúť. Predvolene je väčšina parametrov zapnutá a príslušná funkcia sa použije počas kontroly. **Ak nemáte závažný dôvod meniť tieto nastavenia, odporúčame vám ponechať vopred definovanú konfiguráciu:**

- **Liečiť/odstrániť vírusové infekcie bez opýtania** (predvolene zapnuté): ak sa počas kontroly identifikuje vírus, môže sa automaticky vyliečiť, ak je dostupná liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a spywarové hrozby** (predvolene zapnuté): začiarňte toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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.
- **Nahlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolene vypnuté): začiarňte toto políčko, 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 predvolene vypnutá.



- **Kontrolovať sledovacie súbory cookies** (predvolene vypnuté): tento parameter súčasť zapína funkciu na detekciu súborov cookies počas kontroly; (súbory 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 vo vnútri archívov** (predvolene vypnuté): tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR, atď.
- **Použiť heuristickú analýzu** (predvolene zapnuté): heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolovať v systémovom prostredí** (predvolene zapnuté): počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté): v určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obvyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Kontrolovať rootkity** (predvolene zapnuté): Kontrola Anti-Rootkit kontroluje počítač a zisťuje prítomnosť potenciálnych rootkitov (programov a technológií, ktoré dokážu zakryť činnosť malwaru 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.

Mali by ste tiež určiť, čo 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, sa nebudú kontrolovať), vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.
- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony** – táto možnosť je predvolene 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.

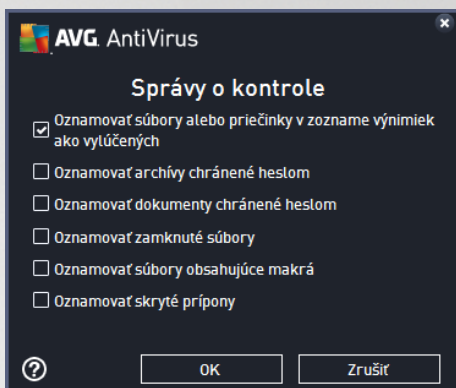
Nastaviť rýchlosť dokončenia kontroly

V tejto časti môžete ďalej špecifikovať želanú rýchlosť kontroly v závislosti od využívania systémových zdrojov. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Ak chcete, aby kontrola prebiehala rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie systémových zdrojov a spomalia 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 systémových zdrojov predĺžením doby trvania kontroly.



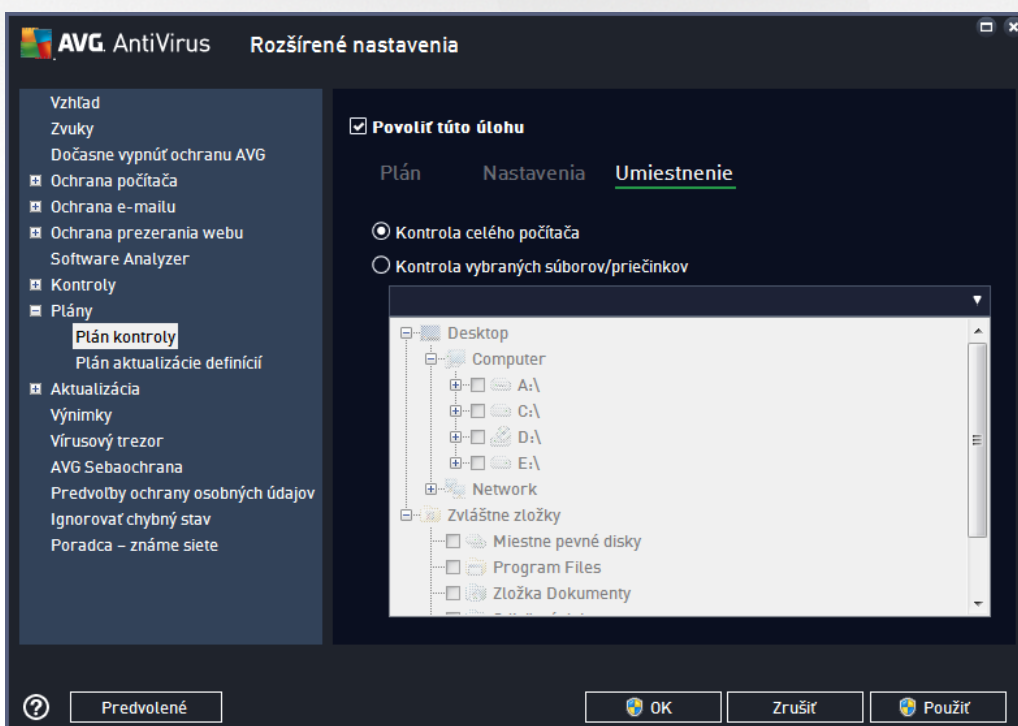
Vytvoriť ďalšie správy o kontrole

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



Možnosti vypnutia počítača

V časti **Možnosti vypnutia počítača** môžete rozhodnúť, 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 zablokovaný (**Vynútené vypnutie, ak je počítač zablokovaný**).

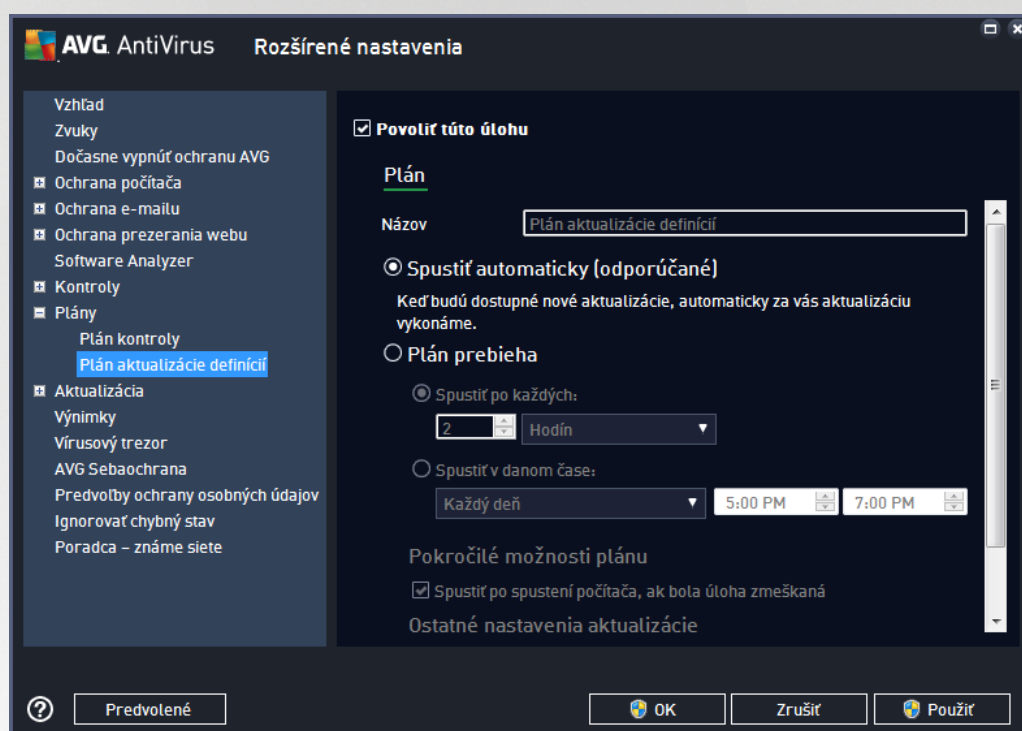




Na karte **Umiestnenie** môžete nastaviť, či chcete naplánovať [kontrolu celého počítača](#) alebo [kontrolu súborov/priečinkov](#). V prípade, že zvolíte kontrolu súborov/priečinkov, v spodnej časti tohto dialógového okna sa aktivuje zobrazená stromová štruktúra a môžete určiť priečinky, ktoré sa majú kontrolovať.

7.9.2. Plán aktualizácie definícií

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



Toto dialógové okno sa používa na nastavenie niektorých podrobných parametrov plánu aktualizácie. V textovom poli **Názov** (*neaktívne pre všetky predvolené plány*) sa nachádza názov, ktorý tomuto konkrétnemu plánu pridelil dodávateľ programu.

Spúšťanie naplánovaných úloh

Predvolene sa úloha spustí automaticky (**Spustiť automaticky**) hneď po tom, ako je k dispozícii nová aktualizácia definícií vírusov. Odporúčame vám nemeniť toto nastavenie, ak nemáte pádny dôvod na jeho zmenu. Potom môžete nastaviť úlohu na ručné spustenie a určiť časové intervaly, v ktorých sa bude spúšťať aktualizácia nových definícií. Časovanie sa definuje ako opakované spúšťanie aktualizácie po uplynutí určitého času (**Spustiť po každých ...**) alebo nastavením presného dátumu a času (**Spustiť v konkrétnom čase**).

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.

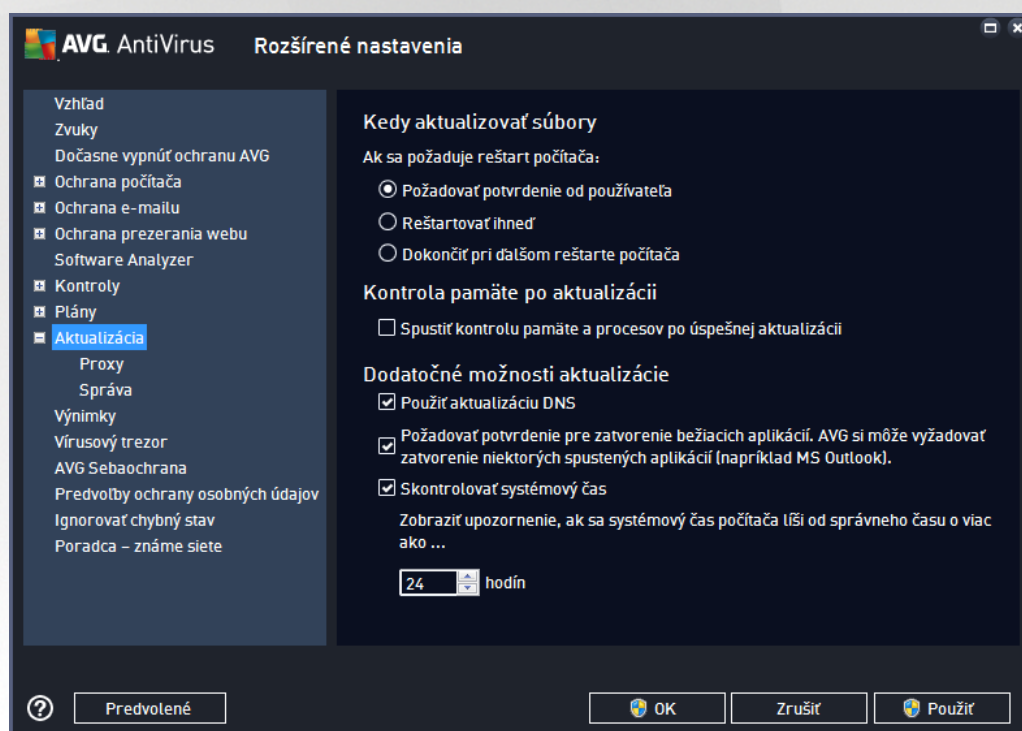


Ďalšie nastavenia aktualizácie

Nakoniec označte možnosť **Spustiť aktualizáciu znova hneď po obnovení internetového pripojenia**, ak sa má v prípade výpadku internetového pripojenia a neúspechu procesu aktualizácie ihneď po obnovení pripojenia okamžite spustiť. Po spustení naplánovanej aktualizácie vo vami nastavenom čase sa zobrazí informácia o tejto skutočnosti v automaticky otváranom okne nad [ikonou AVG v paneli úloh](#) (pod podmienkou, že sa nezmenila predvolená konfigurácia v dialógovom okne [Rozšírené nastavenia/Vzhľad](#)).

7.10. 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 možností, ktorá bude použitá v prípade, ak si proces aktualizácie vyžiada reštartovanie počítača. Dokončenie aktualizácie môžete naplánovať na ďalšie reštartovanie počítača alebo môžete ihneď reštartovať počítač:

- **Požadovať potvrdenie od používateľa** (predvolené) – zobrazí sa žiadosť, aby ste potvrdili reštartovanie počítača, ktoré je potrebné na dokončenie procesu [aktualizácie](#)
- **Reštartovať ihneď** – počítač sa automaticky reštartuje ihneď po dokončení procesu [aktualizácie](#) a nepožiadava vás o udelenie súhlasu



- **Dokončiť pri ďalšom reštarte počítača** – dokončenie procesu [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!

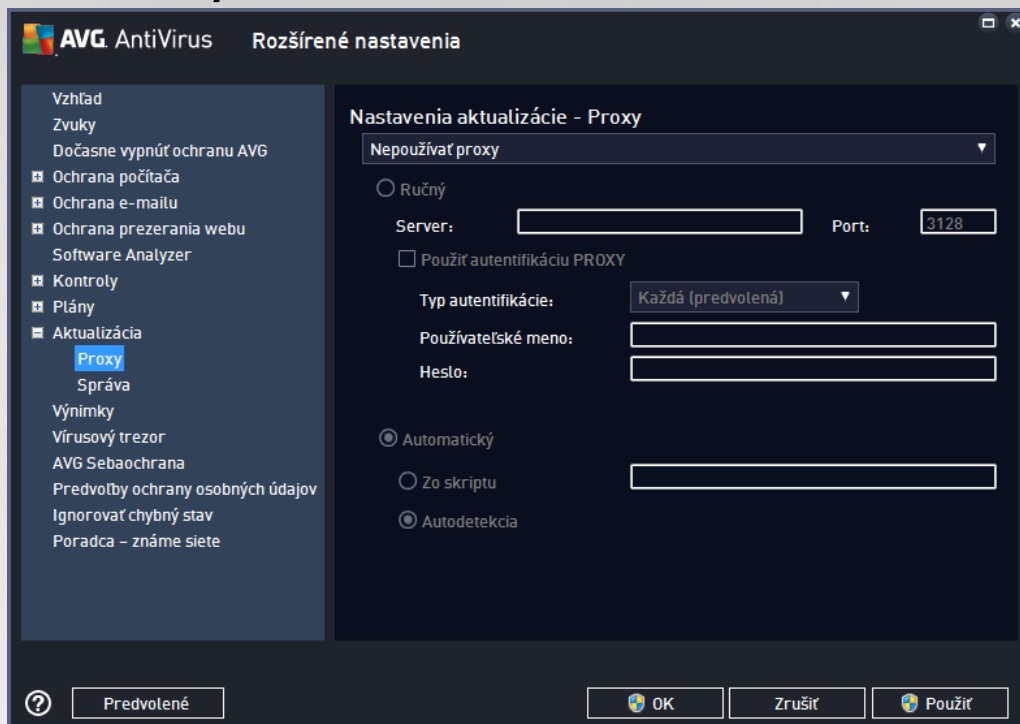
Kontrola pamäte po aktualizácii

Označte toto začiaravacie políčko, ak sa má nová kontrola pamäte spustiť po každej úspešnej aktualizácii. Najnovšia stiahnutá aktualizácia môže obsahovať nové definície vírusov, ktoré sa môžu ihneď použiť pri kontrole.

Ďalšie možnosti aktualizácie

- **Vytvoriť nový bod obnovy systému pri každej aktualizácii programu** (*predvolene zapnuté*) – pred každým spustením aktualizácie programu AVG sa vytvorí bod obnovy systému. Ak proces aktualizácie zlyhá a operačný systém spadne, potom vám tento bod obnovenia umožní obnoviť stav operačného systému s pôvodnou konfiguráciou. Prístup k tejto možnosti je cez ponuku Štart/Všetky programy/Príslušenstvo/Systémové nástroje/Obnovenie systému, ale vykonať zmeny týchto nastavení sa odporúča len skúseným používateľom! Nechajte toto začiaravacie políčko označené, ak chcete používať túto funkcionality.
- **Použiť aktualizáciu DNS** (*predvolene zapnuté*) – ak je toto začiaravacie políčko označené, po spustení aktualizácie **AVG AntiVirus** vyhľadá informácie o najnovšej verzii vírusovej databázy a najnovšej verzii programu na serveri DNS. Až potom sa stiahnu a nainštalujú najmenšie nevyhnutne potrebné aktualizčné súbory. Týmto spôsobom sa minimalizuje celkový objem stiahnutých dát a zrýchli proces aktualizácie.
- **Požadovať súhlas so zatvorením spustených aplikácií** (*predvolene zapnuté*) – postará sa o to, aby sa žiadna spustená aplikácia nezatvorila bez vášho súhlasu, ak to je potrebné na dokončenie procesu aktualizácie.
- **Skontrolovať systémový čas** (*predvolene zapnuté*) – začiarajte túto možnosť, ak chcete byť informovaní v prípade, keď sa systémový čas líši od skutočného času o viac, ako je stanovený počet hodín.

7.10.1. Proxy



Server proxy je samostatný server alebo služba spustená na počítači, ktorá zaručuje bezpečnejšie pripojenie do internetu. Podľa zadaných pravidiel siete potom môžete prísť k Internetu buď priamo alebo cez proxy server, môžete využiť aj obidve možnosti zároveň. Potom v prvej položke dialógového okna **Nastavenia aktualizácie – Proxy** musíte nastaviť v ponuke, či chcete:

- **Nepoužívať proxy** – predvolené nastavenia
- **Použiť proxy**
- **Pokúsiť sa pripojiť pomocou proxy a ak sa to nepodarí, pripojiť priamo**

Ak si zvolíte niektorú možnosť pomocou proxy servera, 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** – zadajte IP adresu servera alebo názov servera
- **Port** – zadajte číslo portu, ktorý umožňuje prístup na internet (predvolene je toto číslo nastavené na hodnotu 3128, ale môžete nastaviť inú hodnotu; ak máte pochybnosti, kontaktujte správcu siete)



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

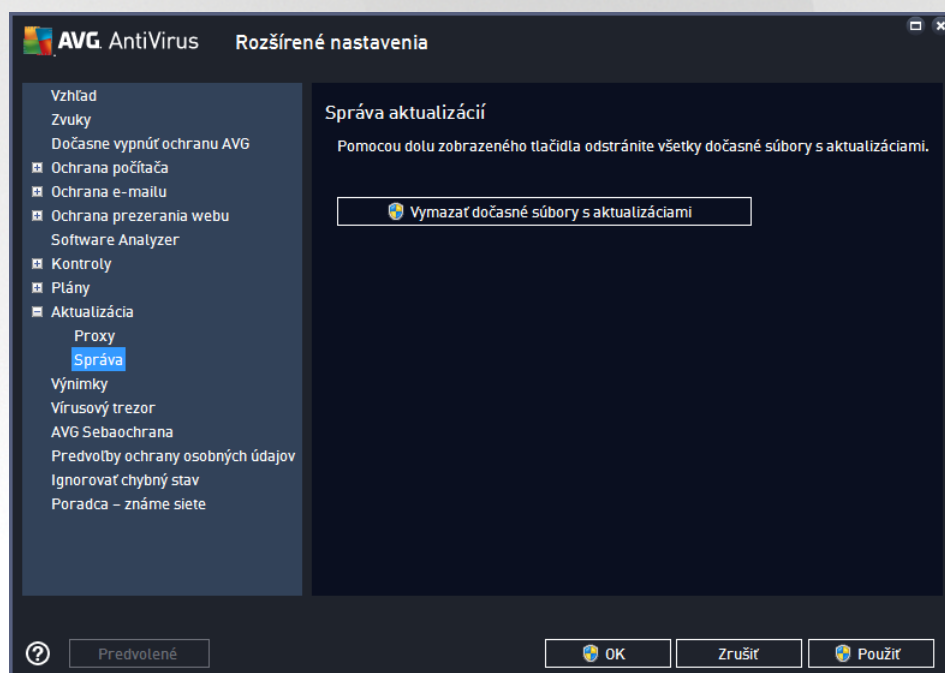
Automatická konfigurácia

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

- **Z prehliadača** – konfigurácia sa načíta z predvoleného internetového prehliadača
- **Zo skriptu** – konfigurácia sa prečíta zo stiahnutého skriptu s funkciou, ktorá vráti adresu proxy
- **Autodetekcia** – konfigurácia sa bude detegovať automaticky priamo zo servera proxy

7.10.2. Správa

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



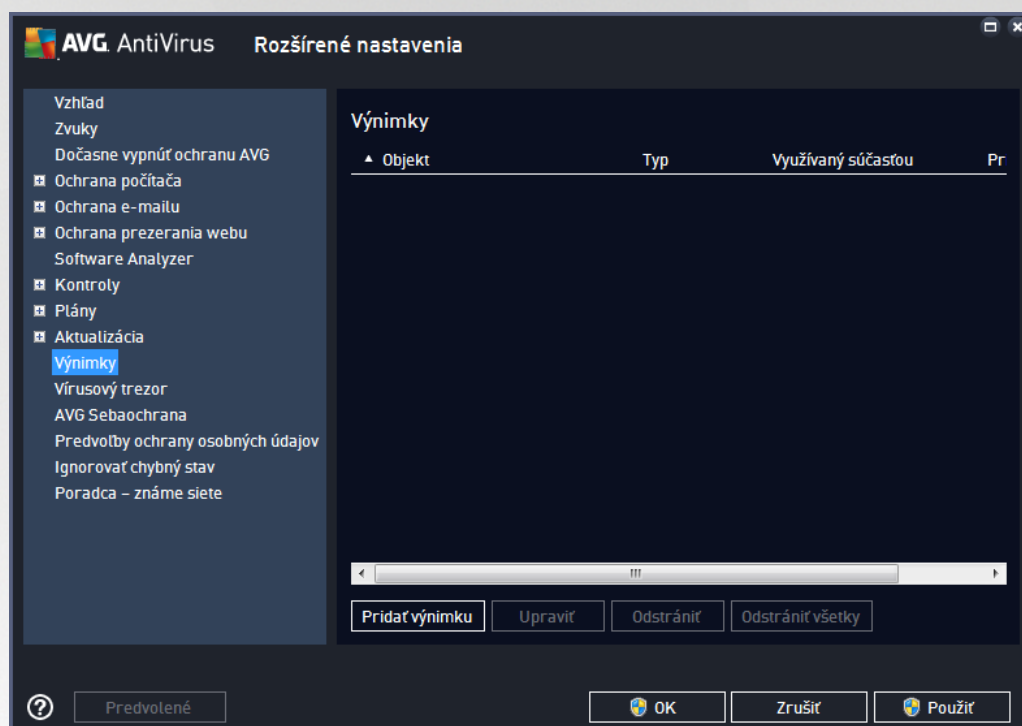
- **Vymazať dočasné súbory s aktualizáciami** – stlačením tohto tlačidla sa vymažú všetky nepotrebné súbory aktualizácie z pevného disku (v predvolenom nastavení zostanú tieto súbory uložené 30 dní)
- **Vrátiť sa na predchádzajúcu verziu databázy vírusov** – stlačením tohto tlačidla sa vymaže najnovšia verzia databázy vírusov z pevného disku a obnoví sa predchádzajúca uložená verzia (nová verzia databázy vírusov bude tvoriť súčasť nasledujúcej aktualizácie)



7.11. Výnimky

V dialógovom okne **Výnimky** môžete definovať výnimky, teda položky, ktoré **AVG AntiVirus** bude ignorovať. Obvykle budete musieť výnimku definovať, ak program AVG neustále deteguje program alebo súbor ako hrozbu alebo blokuje bezpečnú stránku ako nebezpečnú. Pridajte takýto súbor alebo stránku do tohto zoznamu výnimiek a program AVG ho už nebude označovať ani blokovať.

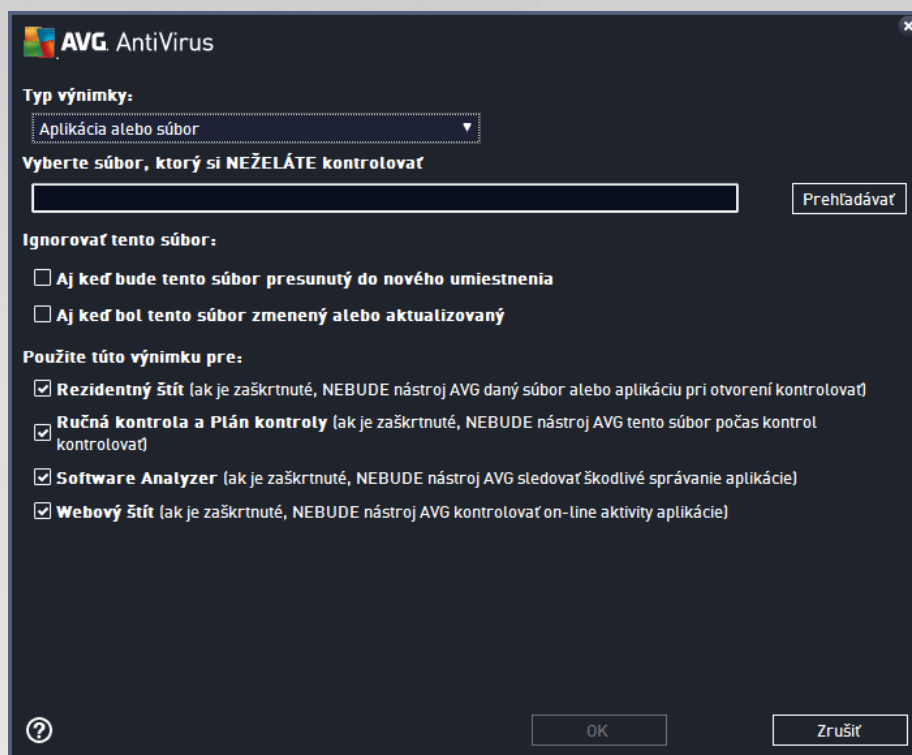
Vždy sa uistite, že daný súbor, program alebo stránka sú úplne bezpečné!



Hlavná časť stránky zobrazuje zoznam výnimiek, ak už boli nejaké definované. Vedľa každej položky sa nachádza začiarňavacie políčko. Keď je začiarňavacie políčko označené, potom sa výnimka používa; keď nie je, potom je výnimka len definovaná, ale momentálne sa nepoužíva. Kliknite na hlavičku stĺpca, aby sa položky zoradili podľa príslušného kritéria.

Ovládacie tlačidlá

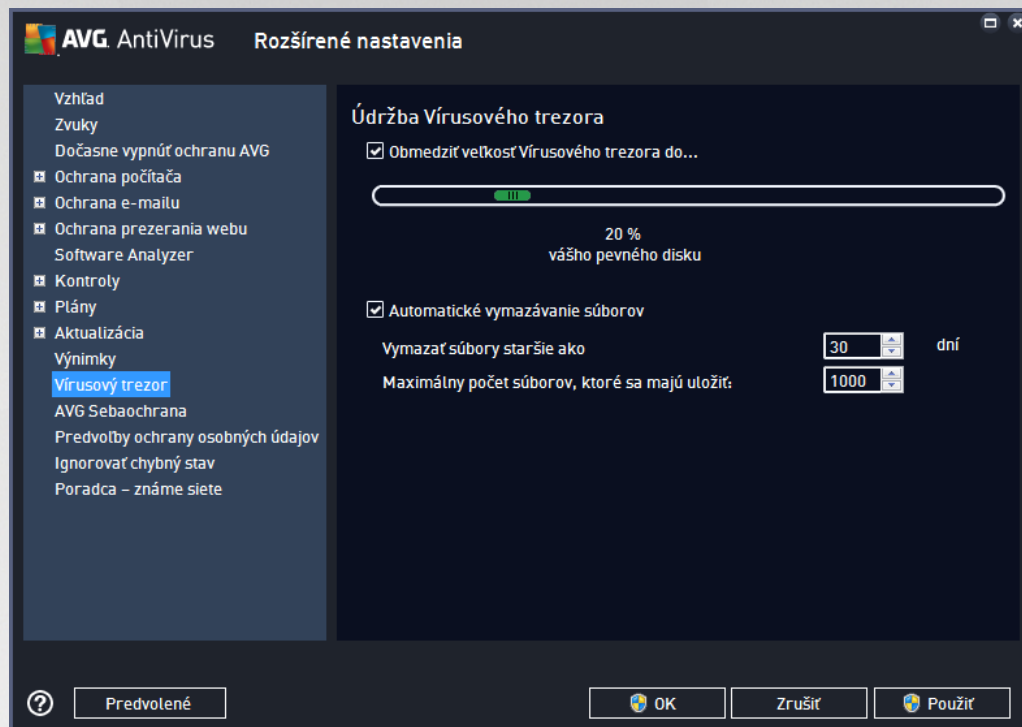
- **Pridať výnimku** – kliknutím otvoríte nové dialógové okno, kde môžete zadať položku, ktorá sa má vynechať z kontroly AVG:



Najskôr budete vyzvaní na zadanie typu objektu, t. j. či ide o aplikáciu alebo súbor, priečinok či certifikát. Potom na disku nájdite cestu k príslušnému objektu alebo napíšte URL. Nakoniec môžete zvoliť, ktoré funkcie AVG by mali vybraný objekt ignorovať (*Rezidentný štít*, *Ručná kontrola a Plán kontroly*, *Software Analyzer*, *Webový štít* a *Windows Antimalware Scan Interface*).

- **Upraviť** – toto tlačidlo je aktívne iba vtedy, ak už sú nadefinované nejaké výnimky a sú uvedené v tabuľke. Potom môžete týmto tlačidlom otvoriť dialógové okno úpravy vybranej výnimky a nastaviť jej parametre.
- **Odstrániť** – týmto tlačidlom zrušíte zadanú výnimku. Výnimky môžete odstrániť buď po jednej, alebo zvýrazniť niekoľko výnimiek v zozname a zrušiť ich naraz. Po zrušení výnimky bude AVG príslušný súbor, priečinok či adresu URL opäť kontrolovať. Upozorňujeme, že bude odstránená len výnimka, nie súbor alebo priečinok samotný!
- **Odstrániť všetky** – použite toto tlačidlo na vymazanie všetkých výnimiek definovaných v zozname.

7.12. Vírusový trezor

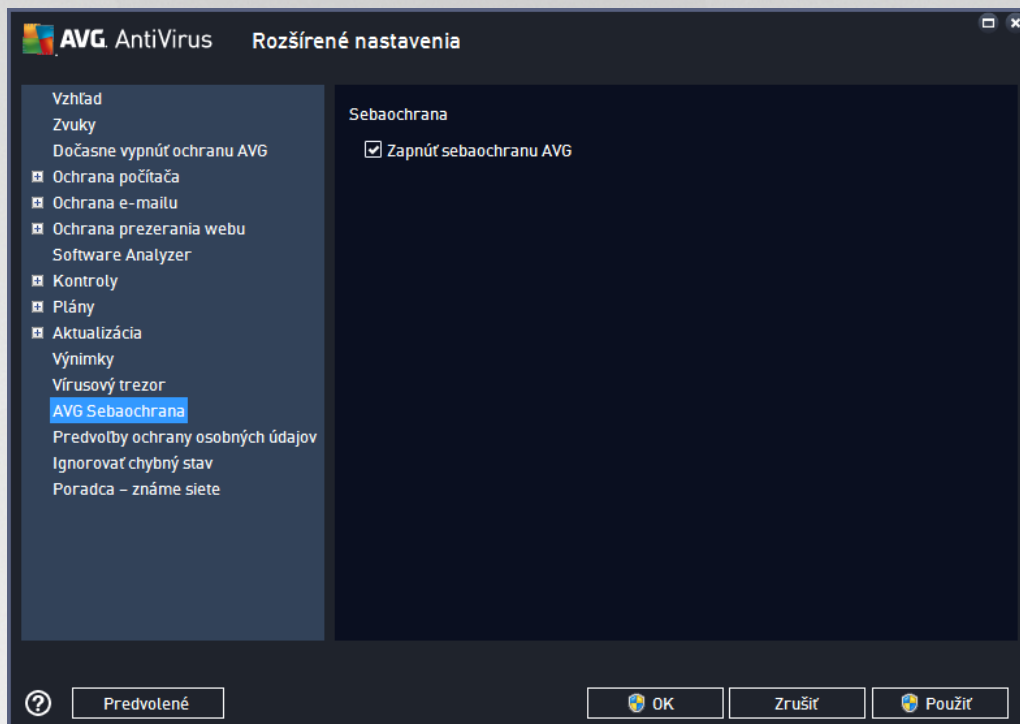


Dialógové okno **Správa Vírusového trezora** vám umožňuje zadať niekoľko parametrov ohľadom administrácie objektov uložených vo [Vírusovom trezore](#):

- **Obmedziť veľkosť Vírusového trezora** – použijete posúvač na nastavenie maximálnej veľkosti [Vírusového trezora](#). Táto veľkosť sa uvádza úmerne v porovnaní s veľkosťou vášho miestneho disku.
- **Automatické vymazávanie súborov** – v tejto časti môžete stanoviť maximálny časový úsek, 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**).



7.13. AVG Sebaochrana

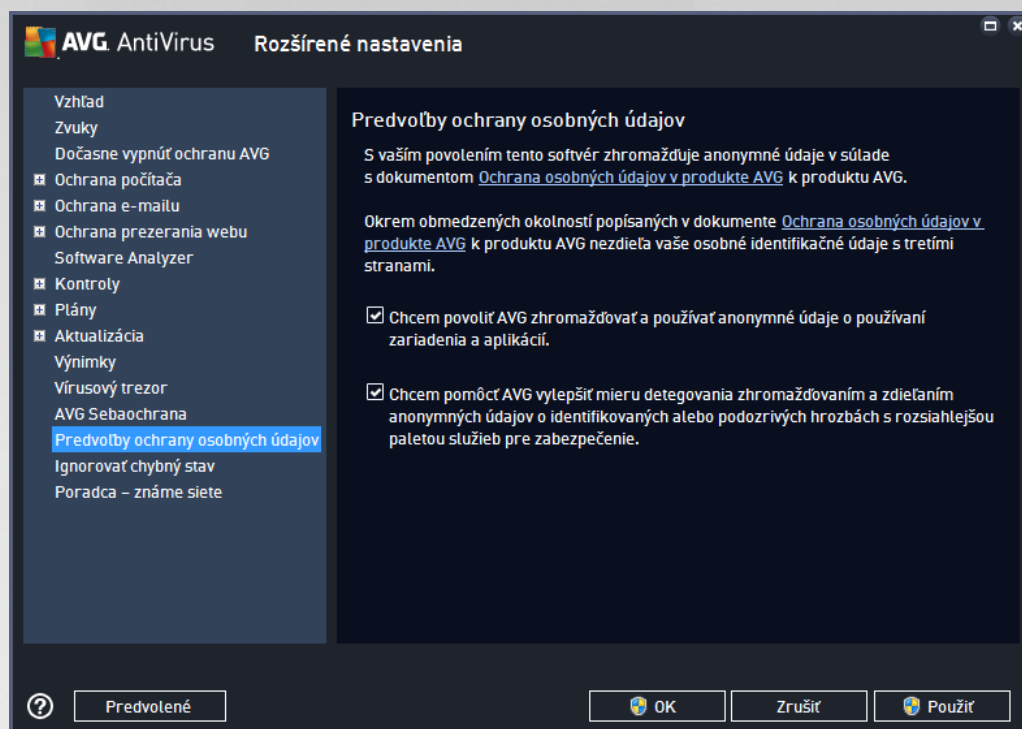


Funkcia **AVG Sebaochrana** umožňuje **AVG AntiVirus** chrániť svoje vlastné procesy, súbory, záznamy v registri a ovládače pred zmenou alebo deaktiváciou. Hlavným dôvodom pre tento druh ochrany je, že niektoré sofistikované hrozby sa snažia vypnúť antivírusovú ochranu, a potom nerušene poškodzujú vášho počítača.

Odporúčame vám túto funkciu ponechať zapnutú!

7.14. Preferencie ochrany osobných údajov

Dialógové okno **Preferencie ochrany osobných údajov** vám ponúkne možnosť účasti na programe zlepšovania služieb AVG, aby ste nám pomohli zlepšiť celkovú úroveň zabezpečenia na internete. Vaše hlásenia nám pomáhajú zhromažďovať aktuálne informácie o najnovších hrozbách od účastníkov z celého sveta a umožňuje nám to zlepšovať ochranu pre každého jednotlivca. Hlásenia sa vykonávajú automaticky a preto vám nespôsobia žiadne nepohodlie. Hlásenia neobsahujú žiadne osobné údaje. Hlásenie zistených hrozieb je voliteľné, radi by sme vás ale požiadali o jeho zapnutie. Pomáha zlepšiť nielen vašu ochranu, ale aj ochranu ostatných používateľov aplikácie AVG.



V dialógovom okne sú k dispozícii tieto možnosti nastavenia:

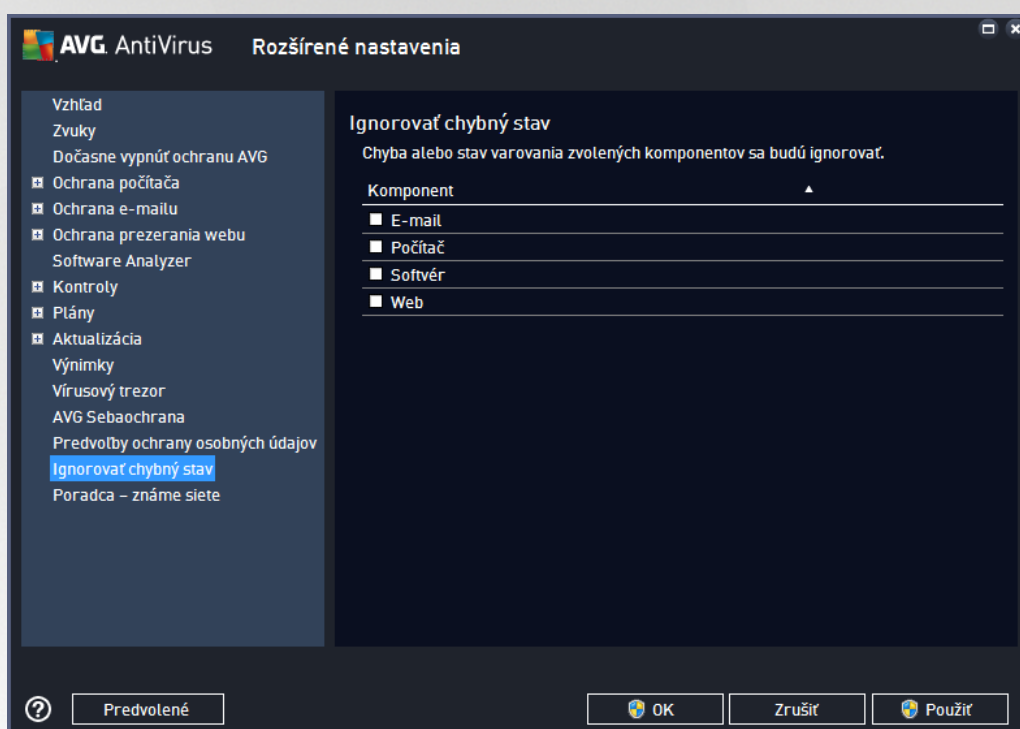
- **Želám si pomôcť spoločnosti AVG zlepšovať jej produkty a chcem sa zúčastniť Programu zlepšovania produktov AVG** (predvolene zapnuté) – ak nám chcete pomáhať v ďalšom zlepšovaní produktu **AVG AntiVirus**, nechajte toto políčko začiarknuté. Táto funkcia zapne oznamovanie všetkých zaznamenaných hrozieb do spoločnosti AVG a umožní nám zhromažďovať najnovšie informácie o malware od všetkých účastníkov z celého sveta a zlepšovať ochranu pre každého jednotlivca. Oznamovanie prebieha automaticky, preto vás nijako nezaťažuje, a v správach nie sú uvedené žiadne osobné údaje.
- o **Povoliť posielanie informácií o nesprávne identifikovaných e-mailoch po potvrdení používateľom** (predvolene zapnuté) – zasielať informácie o e-mailových správach, ktoré boli nesprávne označené ako nevyžiadaná pošta, alebo správach nevyžiadanej pošty, ktoré služba Anti-Spam nedetegovala. Pred poslaním tohto druhu informácií vás program požiada o potvrdenie.
- o **Povoliť posielanie anonymných informácií o identifikovaných alebo podozrivých hrozbách** (predvolene zapnuté) – zasielať informácie o podozrivom alebo pozitívne nebezpečnom kóde alebo vzore správania (môže ísť o vírus, spyware alebo škodlivé internetové stránky, ktoré sa pokúšate otvoriť) detegovanom na vašom počítači.
- o **Povoliť posielanie anonymných informácií o používaní produktu** (predvolene zapnuté) – odosielanie základných štatistík o používaní aplikácie, ako je počet nájdených hrozieb, spustených kontrol, úspešné či neúspešné kontroly a pod.
- **Zapnúť overovanie detekcií pomocou cloud computingu** (predvolene zapnuté) – detegované hrozby sa budú overovať, či sú naozaj infikované, aby sa vylúčili nesprávne detekcie.



- **Želám si, aby sa produkty AVG prispôsobili mojej práci zapnutím funkcie AVG Personalizácia (predvolene vypnutá)** – táto funkcia anonymne analyzuje správanie programov a aplikácií vo vašom počítači. Na základe tejto analýzy vám môže spoločnosť AVG ponúkať služby na mieru vašich potrieb, aby vám zabezpečila maximálnu bezpečnosť.

7.15. Ignorovať chybový stav

V dialógovom okne **Ignorovať chybný stav** môžete označiť tie súčasti, o ktorých nechcete byť informovaní:



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

- [ikona v paneli úloh](#) – ak všetky časti aplikácie AVG fungujú správne, ikona je zobrazená v štyroch farbách; ak sa však vyskytne chyba, ikona sa zobrazí so žltým výkričníkom,
- textový popis existujúceho problému v časti [Informácie o stave zabezpečenia](#) v hlavnom okne AVG

Môže nastať situácia, keď z nejakého dôvodu bude potrebné dočasne túto súčasť vypnúť. **To sa neodporúča, snažte sa mať neustále všetky súčasti trvalo zapnuté a v predvolenej konfigurácii.** Niekedy však sa takej situácii nemožno vyhnúť. V tom prípade ikona v 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.

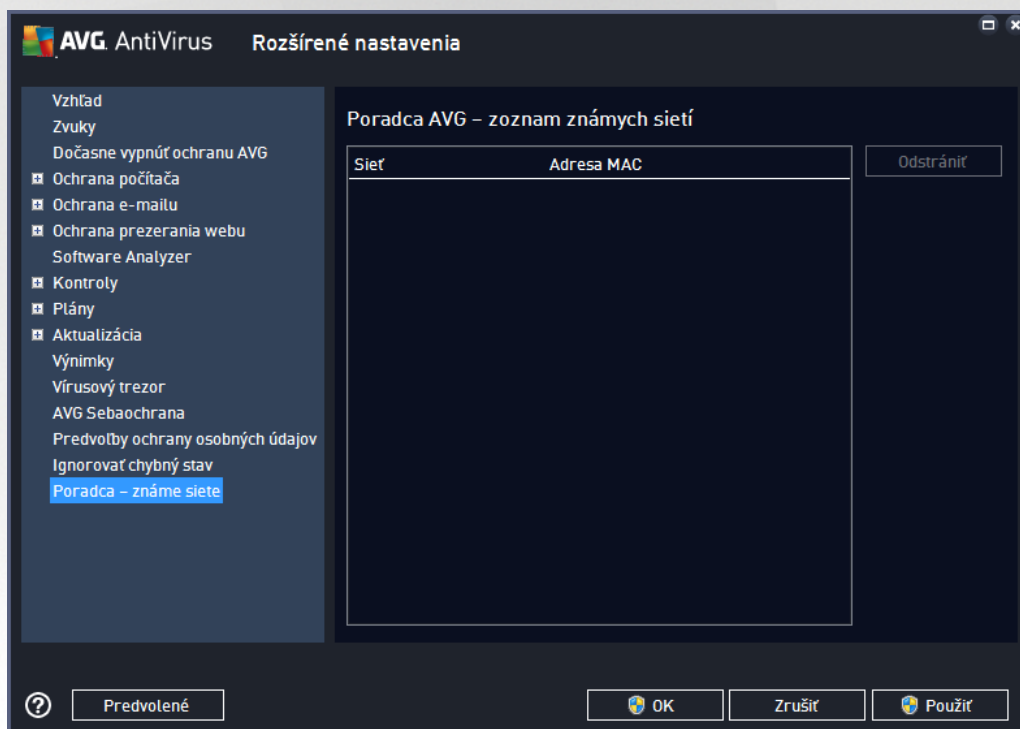
V tejto situácii môžete v dialógovom okne **Ignorovať chybný stav** vybrať súčasti, o ktorých prípadnom chybnom stave (alebo vypnutí) si neželáte byť informovaní. Kliknutím na tlačidlo **OK** potvrdíte zmeny.



7.16. Advisor – známe siete

[AVG Advisor](#) obsahuje funkciu sledovania sietí, ku ktorým sa pripájate. Ak nájde novú sieť (s už použitým názvom siete, čo môže viesť k omylu), upozorní vás a odporučí vám, aby ste skontrolovali zabezpečenie danej siete. Ak sa rozhodnete, že je bezpečné pripojiť sa k novej sieti, môžete ju tiež uložiť do tohto zoznamu. (Prostredníctvom odkazu v oblasti oznámení na paneli úloh AVG Advisor, ktoré sa vysunie nad panelom úloh pri rozpoznaní neznámej siete. Podrobnosti nájdete v kapitole [AVG Advisor](#)). [AVG Advisor](#) si zapamätá jedinečné atribúty siete (predovšetkým adresu MAC) a najbližšie už oznámenie nezobrazí. Každá sieť, ku ktorej sa pripojíte, sa bude automaticky považovať za známu a pridá sa do zoznamu. Jednotlivé záznamy môžete vymazať stlačením tlačidla **Odstrániť**. Daná sieť bude následne opäť považovaná za neznámu a potenciálne nebezpečnú.

V tomto dialógovom okne môžete skontrolovať, ktoré siete sa považujú za známe:



Poznámka: Funkcia známych sietí v AVG Advisor nie je podporovaná v 64-bitových systémoch Windows XP.

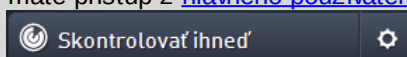


8. Kontrola AVG

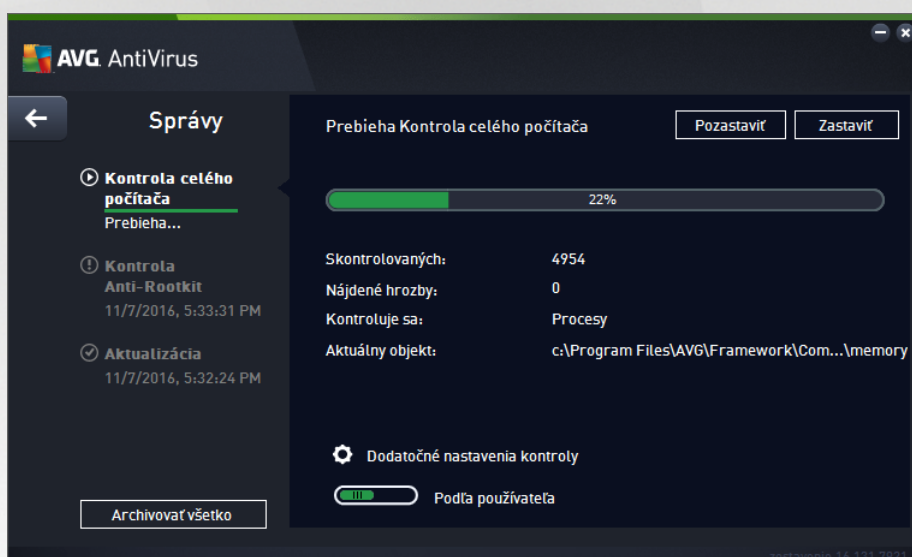
V predvolenom nastavení **AVG AntiVirus** nespúšťa žiadnu kontrolu, pretože po úvodnej kontrole (zobrazí sa vám návrh na jej spustenie) by ste mali byť dokonale chránení rezidentnými súčasťami **AVG AntiVirus**, ktoré sú vždy na stráží a nedovolia žiadnemu škodlivému kódu preniknúť do počítača. Samozrejme, že môžete [naplánovať kontrolu](#), ktorá sa bude spúšťať v pravidelných intervaloch, alebo manuálne kedykoľvek spustiť kontrolu podľa vlastných potrieb.

K rozhraniu kontroly AVG máte prístup z [hlavného používateľského rozhrania](#) prostredníctvom tlačidla graficky

rozdeleného na dve časti:



- **Skontrolovať teraz** – stlačte toto tlačidlo pre okamžité spustenie [Kontroly celého počítača](#) a sledujte jej priebeh a výsledky v automaticky otvorenom okne [Výsledky](#):



- **Možnosti** – vyberte toto tlačidlo (graficky zobrazené ako tri vodorovné čiary v zelenom poli), ktorým otvoríte dialógové okno **Možnosti kontroly**, kde môžete [upraviť naplánované kontroly](#) a parametre [Kontroly celého počítača/Kontroly súborov/priečinkov](#).



V dialógovom okne **Možnosti kontroly** sa nachádzajú tri hlavné časti konfigurácie kontroly:

- o **Upraviť naplánované kontroly** – kliknutím na túto možnosť sa otvorí nové [dialógové okno s prehľadom všetkých naplánovaných kontrol](#). Než zadefinujete vlastné kontroly, zobrazí sa v tabuľke iba jeden plán kontroly, ktorý vopred definoval dodávateľ softvéru. Táto kontrola je predvolene vypnutá. Ak ju chcete zapnúť, kliknite na ňu pravým tlačidlom a v kontextovej ponuke vyberte možnosť *Povoliť úlohu*. Po povolení plánu kontroly môžete [upraviť jej konfiguráciu](#) tlačidlom *Upraviť plán kontroly*. Taktiež môžete kliknúť na tlačidlo *Pridať plán kontroly*, aby ste vytvorili nový vlastný plán.
- o **Kontrola celého počítača/Nastavenia** – tlačidlo je rozdelené na dve časti. Kliknutím na položku *Kontrola celého počítača* okamžite spustíte kontrolu celého počítača (*podrobnosti o kontrole celého počítača nájdete v príslušnej kapitole s názvom [Vopred definované kontroly/Kontrola celého počítača](#)*). Kliknutím na časť *Nastavenia* sa zobrazí [konfiguračné okno, kde môžete nastaviť parametre kontroly celého počítača](#).
- o **Kontrola súborov/priečinkov/Nastavenia** – tlačidlo je opäť rozdelené na dve časti. Kliknutím na možnosť *Kontrola súborov/priečinkov* okamžite spustíte kontrolu vybraných oblastí počítača (*podrobnosti o kontrole súborov a priečinkov nájdete v príslušnej kapitole s názvom [Vopred definované kontroly/Kontrola súborov/priečinkov](#)*). Kliknutím na časť *Nastavenia* sa zobrazí [konfiguračné okno, kde môžete nastaviť parametre kontroly súborov a priečinkov](#).
- o **Skontrolovať počítač na prítomnosť rootkitov/Nastavenia** – ľavou časťou tlačidla označenou *Skontrolovať počítač na prítomnosť rootkitov* sa spustí okamžitá kontrola anti-rootkit (*podrobnosti o kontrole rootkitov nájdete v príslušnej kapitole pod názvom [Preddefinované kontroly/Skontrolovať počítač na prítomnosť rootkitov](#)*). Kliknutím na časť *Nastavenia* sa zobrazí konfiguračné okno, kde môžete [nastaviť parametre kontroly rootkitov](#).

8.1. Vopred definované kontroly

Jednou z hlavných funkcií programu **AVG AntiVirus** je kontrola na požiadanie. Testy na požiadanie sú určené na kontrolu rôznych častí počítača pri každom podozrení možného výskytu vírusovej infekcie. Odporúča sa vykonávať takéto testy pravidelne, aj keď si myslíte, že sa vo vašom počítači nenájdne žiadny vírus.



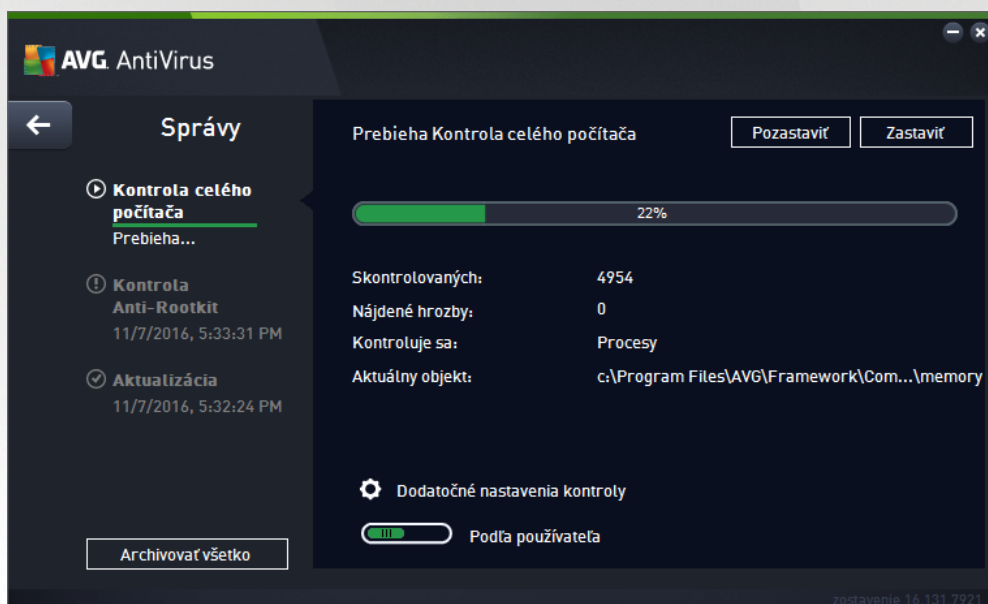
V produkte **AVG AntiVirus** sa nachádzajú tieto typy kontrol vopred definované dodávateľom softvéru:

8.1.1. Kontrola celého počítača

Kontrola celého počítača – skontroluje možné infekcie alebo potenciálne nežiaduce programy v celom počítači. Tento test bude kontrolovať všetky pevné disky vášho počítača, bude detegovať a liečiť všetky nájdené vírusy a odstráni detegovanú infekciu do [Vírusového trezora](#). Kontrola celého počítača by mala byť naplánovaná na pracovnej stanici aspoň raz do týždňa.

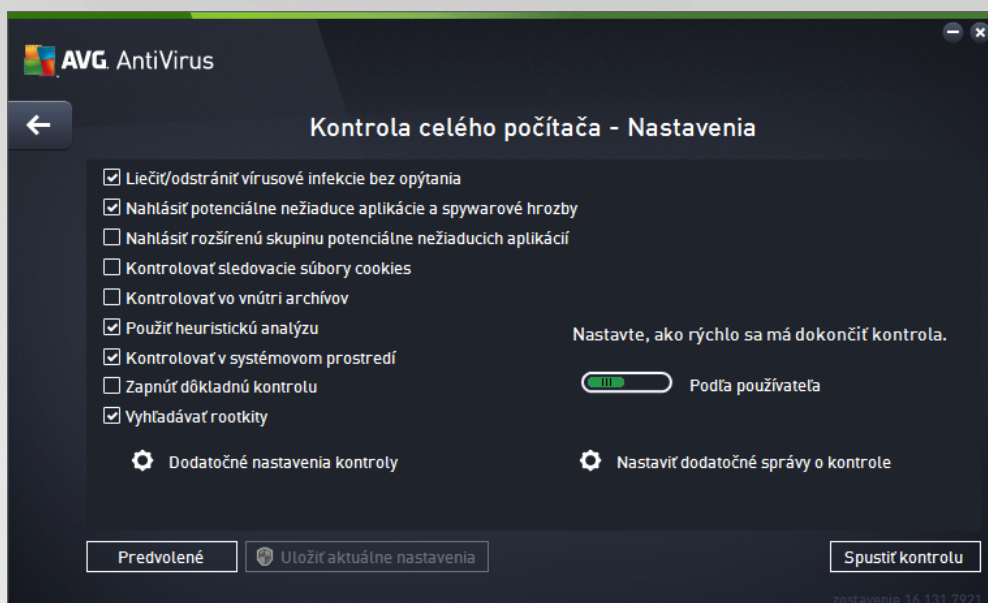
Spustenie kontroly

Kontrolu celého počítača môžete spustiť priamo z [hlavného používateľského rozhrania](#) kliknutím na tlačidlo **Skontrolovať teraz**. Pre tento typ kontroly netreba žiadne ďalšie nastavenia, kontrola sa spustí okamžite. V dialógovom okne **Priebeh kontrola celého počítača** (pozri snímku obrazovky) môžete sledovať priebeh a výsledky. V prípade potreby môžete kontrolu dočasne prerušiť (tlačidlo **Pozastaviť**) alebo zrušiť (tlačidlo **Zastaviť**).



Zmena konfigurácie kontroly

Konfiguráciu **kontroly celého počítača** môžete upraviť v dialógovom okne **Kontrola celého počítača – Nastavenia** (okno je prístupné cez odkaz **Nastavenia** pre Kontrolu celého počítača v rámci okna [Možnosti kontroly](#)). **Odporúča sa ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť!**

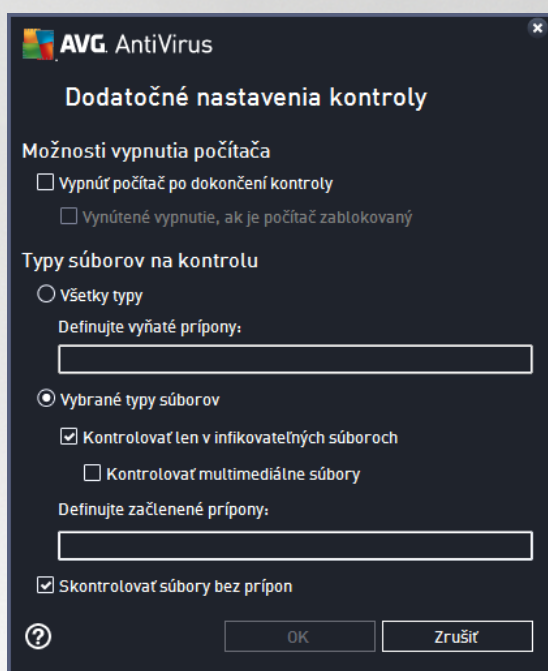


V zozname parametrov kontroly môžete zapnúť/vypnúť špecifické parametre podľa potreby:

- **Liečiť/odstrániť vírusovú infekciu bez opýtania** (predvolene zapnuté) – ak sa počas kontroly nájde vírus, môže byť automaticky vyliečený, pokiaľ je liek k dispozícii. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a hrozby spyware** (predvolene zapnuté) – začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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.
- **Hlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolene vypnuté) – začiarknite toto políčko, 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 predvolene vypnutá.
- **Kontrolovať sledovacie súbory cookies** (predvolene vypnuté) – tento parameter zapína funkciu na detekciu súborov cookies (cookies protokolu HTTP sa používajú na overenie totožnosti, sledovanie a uchovávanie konkrétnych informácií o používateľoch, akými sú napríklad preferencie alebo obsah elektronických nákupných košíkov).
- **Kontrolovať vo vnútri archívov** (predvolene vypnuté) – tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory uložené vnútri archívov, napr. ZIP, RAR, atď.
- **Použiť heuristickú analýzu** (predvolene zapnuté) – heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolovať v systémovej prostredí** (predvolene zapnuté) – počas kontroly sa budú overovať aj systémové oblasti počítača.



- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté) – v určitých situáciách (podozrenia na infikovanie počítača) môžete zaškrtnúť túto možnosť, aby ste aktivovali najdôkladnejšie kontrolné algoritmy, ktoré pre úplnú istotu skontrolujú aj tie oblasti počítača, ktoré sa obvyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Kontrolovať rootkity** (predvolene zapnuté) – zahŕňa kontrolu prítomnosti rootkitov do kontroly celého počítača. [Kontrola anti-rootkit](#) možno spustiť aj samostatne.
- **Dodatočné nastavenia kontroly** – tento odkaz otvorí nové dialógové okno Dodatočné nastavenia kontroly, ktoré sa používa na nastavenie nasledujúcich parametrov.

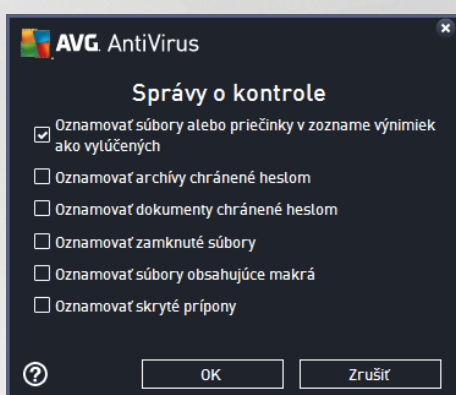


- o **Možnosti vypnutia počítača** – rozhodnite, či sa má počítač vypnúť automaticky po dokončení procesu kontroly. Po potvrdení tejto možnosti (**Vypnúť počítač po dokončení kontroly**) sa aktivuje nová možnosť, ktorá umožní vypnúť počítač, aj keď je momentálne zamknutý (**Vynútiť vypnutie počítača, keď je zamknutý**).
- o **Typy súborov na kontrolu** – mali by ste tiež určiť, čo chcete 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, sa nebudú kontrolovať), vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.
 - Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony**. Táto možnosť je predvolene zapnutá a odporúčame vám, aby ste toto nastavenie nikdy nemenili,



ak na to nemáte skutočný dôvod. Súborý bez prípony sú skôr podozrivé a mali by sa vždy kontrolovať.

- **Nastaviť rýchlosť dokončenia kontroly** – pomocou posúvača zmeňte prioritu procesu kontroly. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *podľa používateľa*. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (*užitočné vtedy, keď potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať*), alebo rýchlejšie s vyššou mierou využívania počítačových zdrojov (*napríklad, 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 hlásiť:



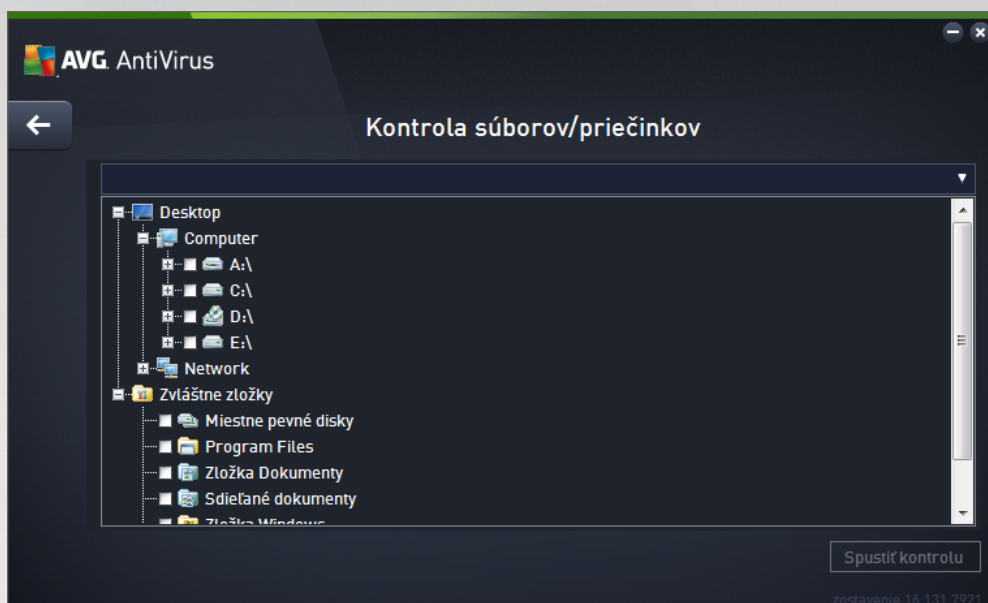
Varovanie: Tieto nastavenia kontroly sa zhodujú s parametrami novo definovanej kontroly; pozrite informácie [v kapitole Kontrola AVG/Plánovanie kontroly/Ako kontrolovať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **Kontrola celého počítača**, svoje nové nastavenie môžete uložiť ako predvolenú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

8.1.2. Kontrola súborov/priečinkov

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

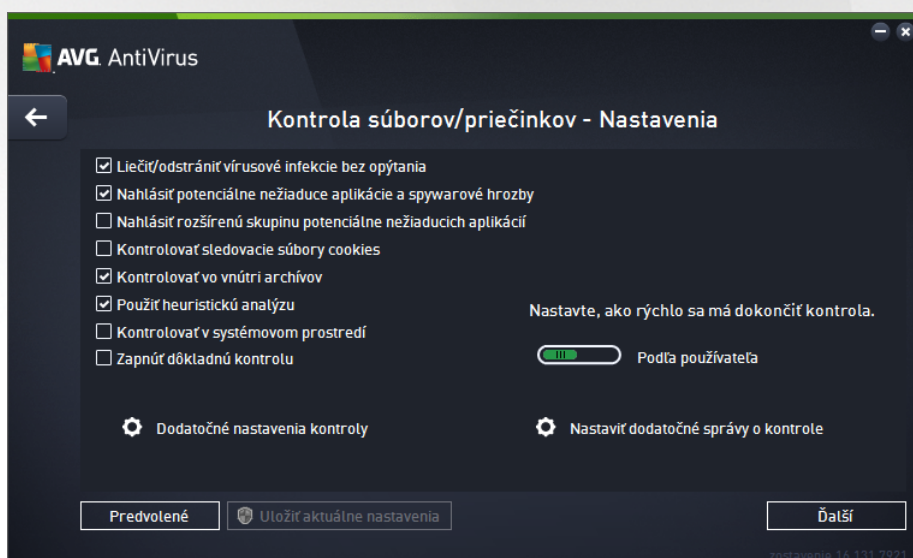
Spustenie kontroly

Funkciu **Kontrola súborov/priečinkov** môžete spustiť priamo z okna [Možnosti kontroly](#) kliknutím na tlačidlo **Kontrola súborov/priečinkov**. 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 zvolenému priečinku sa vygeneruje automaticky a objaví sa v textovom okne vo vrchnej časti tohto dialógového okna. Rovnako môžete nastaviť kontrolu konkrétneho priečinka, ktorého vnorené priečinky sa vylúčia z tejto kontroly; v tom prípade vložte znak mínus „-“ pred automaticky vygenerovanú cestu (*pozrite snímku obrazovky*). Na vynechanie celého priečinka z kontroly použite parameter „!“ Napokon, ak chcete spustiť kontrolu, stlačte tlačidlo **Spustiť kontrolu**; samotný proces kontrolovania sa v podstate zhoduje s [kontrolou celého počítača](#).



Zmena konfigurácie kontroly

Konfiguráciu **Kontroly súborov/priečinkov** môžete upraviť v dialógovom okne **Kontrola súborov/priečinkov – Nastavenia** (okno je prístupné cez odkaz **Nastavenia pre Kontrolu súborov/priečinkov** v rámci okna [Možnosti kontroly](#)). **Odporúča sa ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť!**



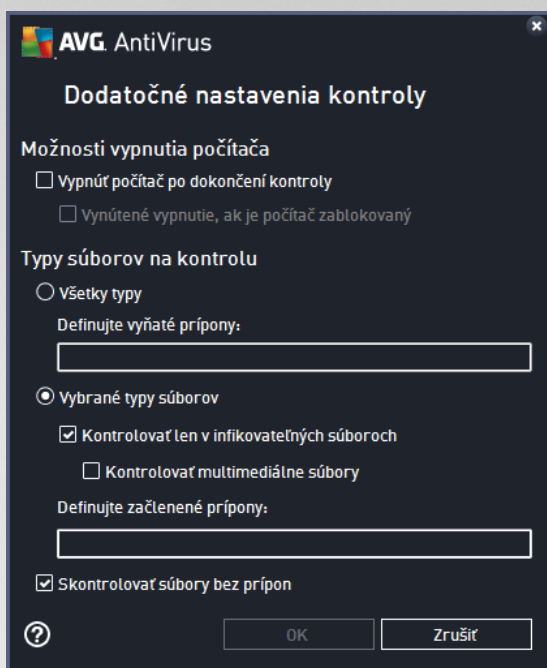
V tomto zozname parametrov kontroly môžete podľa potreby vypnúť alebo zapnúť konkrétne parametre:

- **Liečiť/odstrániť vírusové infekcie bez opýtania** (predvolene zapnuté): Ak sa počas kontroly identifikuje vírus, môže sa automaticky vyliečiť, ak je dostupná liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a spywarové hrozby** (predvolene zapnuté): Začiarknite toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu



malware: 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.

- **Nahlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolene vypnuté): Začiarknite toto políčko, 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 predvolene vypnutá.
- **Kontrolovať sledovacie súbory cookies** (predvolene vypnuté): Tento parameter súčasť zapína funkciu na detekciu súborov cookies (súbory 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 vo vnútri archívov** (predvolene zapnuté): Tento parameter definuje, že počas kontroly by sa mali kontrolovať všetky súbory, aj tie, ktoré sa nachádzajú vo vnútri archívov, napr. ZIP, RAR, atď.
- **Použiť heuristickú analýzu** (predvolene zapnuté): Heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolovať v systémovom prostredí** (predvolene vypnuté): Počas kontroly sa budú kontrolovať aj systémové oblasti vášho počítača.
- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté): V určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obvyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Dodatočné nastavenia kontroly** – tento odkaz otvorí nové dialógové okno **Dodatočné nastavenia kontroly**, ktoré sa používa na nastavenie nasledujúcich 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 zablokovaný (**Vynútené vypnutie, ak je počítač zablokovaný**).

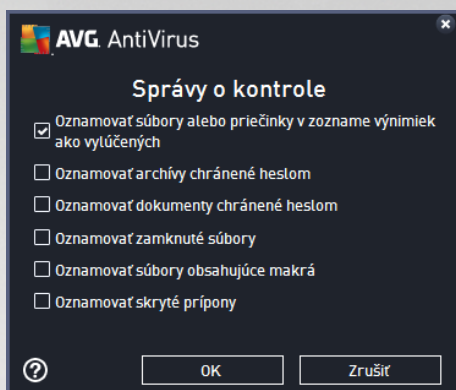
o **Typy súborov na kontrolu** – mali by ste tiež určiť, čo chcete kontrolovať:

- **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, sa nebudú kontrolovať), vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.
- Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony**. Táto možnosť je predvolene 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. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená podľa používateľa. Prípadne môžete spustiť procesy kontroly pomalšie, čím sa minimalizuje využívanie počítačových zdrojov (užitočné vtedy, keď potrebujete pracovať na počítači, ale nezaujíma vás, ako dlho bude kontrola trvať), alebo rýchlejšie s vyššou mierou využívania počítačových zdrojov (napr. keď sa počítač dočasne nepoužíva).



- **Vytvoriť ďalšie správy o kontrole** – odkaz otvorí nové dialógové okno **Správy o kontrole**, ktoré vám umožní nastaviť, ktoré typy možných nálezov sa majú hlásiť:



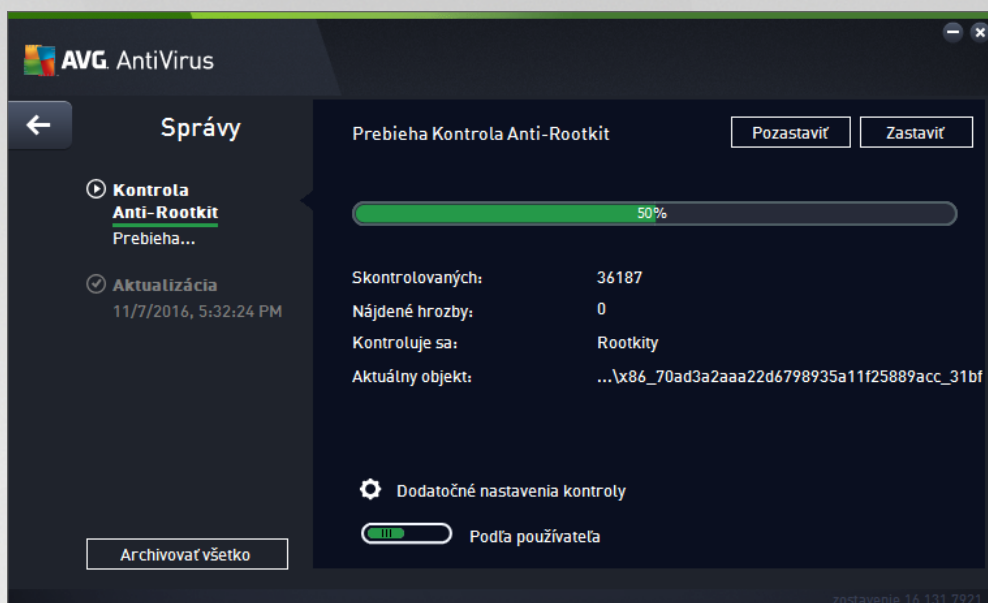
Varovanie: Tieto nastavenia kontroly sa zhodujú s parametrami novo definovanej kontroly; pozrite informácie v kapitole [Kontrola AVG/Plánovanie kontroly/Ako kontrolovať](#). Ak sa rozhodnete zmeniť predvolenú konfiguráciu funkcie **kontrola súborov/priečinkov**, svoje nové nastavenie môžete potom uložiť 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](#)).

8.1.3. Skontrolovať počítač na prítomnosť rootkitov

Kontrola počítača na prítomnosť rootkitov deteguje a účinne odstraňuje nebezpečné rootkity, t. j. programy a technológie, ktoré dokážu zamaskovať prítomnosť škodlivého softvéru vo vašom počítači. Rootkit je program určený na to, aby sa zmocnil základnej kontroly nad počítačovým systémom bez povolenia vlastníka systému a jeho právoplatných správcov. Kontrola dokáže zistiť prítomnosť rootkitov pomocou vopred definovanej skupiny pravidiel. Ak sa nájde rootkit, nemusí to nevyhnutne znamenať, že je infikovaný. Programy rootkit sa niekedy používajú ako ovládače, príp. tvoria súčasť správnych aplikácií.

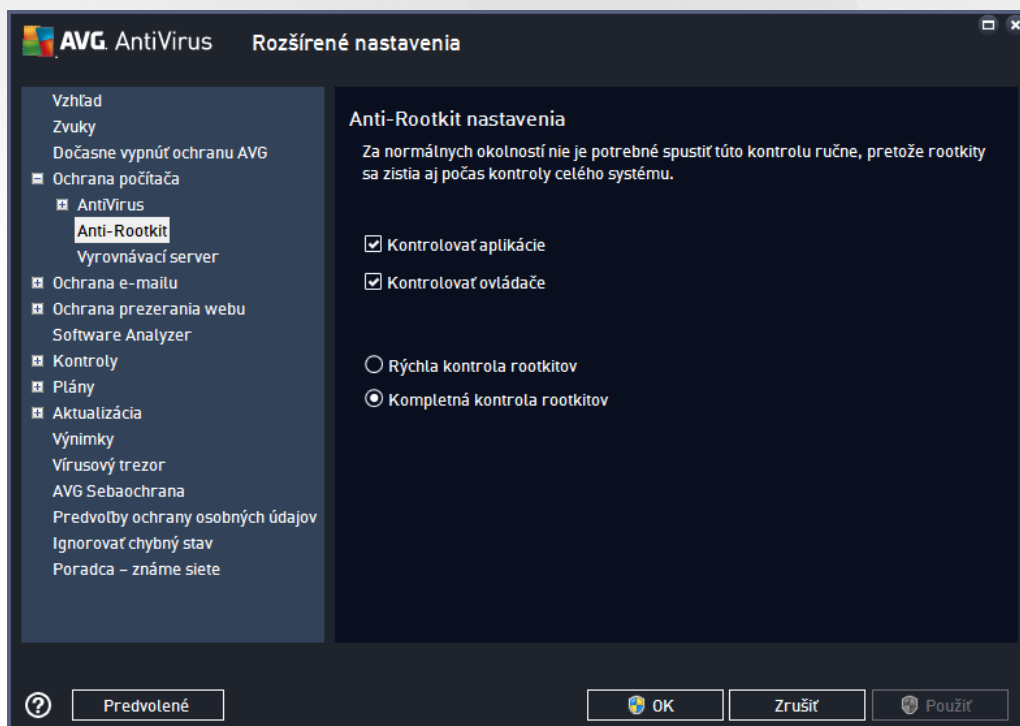
Spustenie kontroly

Kontrola počítača na prítomnosť rootkitov môže byť spustená priamo z dialógového okna [Možnosti kontroly](#) kliknutím na tlačidlo **Kontrola počítača na prítomnosť rootkitov**. Otvorí sa nové dialógové okno s názvom **Prebieha kontrola Anti-Rootkit**, v ktorom sa zobrazuje priebeh spustenej kontroly:



Zmena konfigurácie kontroly

Konfiguráciu kontroly Anti-Rootkit môžete upraviť v dialógovom okne **Nastavenia nástroja Anti-Rootkit** (dialógové okno je prístupné cez odkaz **Nastavenia** pre Kontrolu počítača na prítomnosť rootkitov v rámci dialógového okna [Možnosti kontroly](#)). **Odporúča sa ponechať predvolené nastavenia, ak nemáte závažný dôvod ich meniť!**



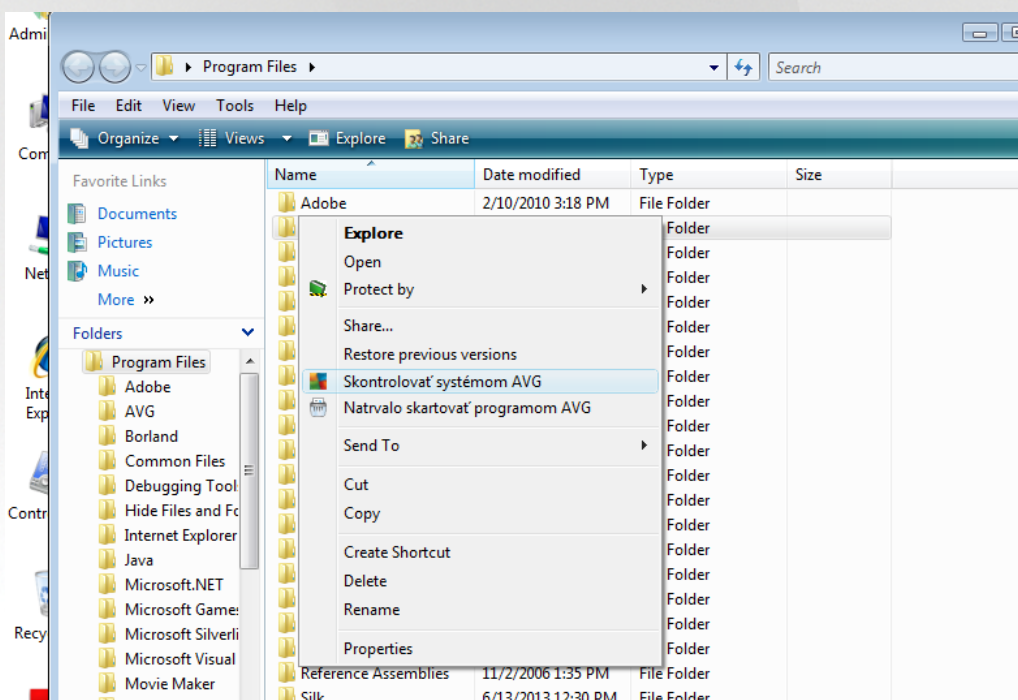


Možnosti **Kontrolovať aplikácie** a **Kontrolovať ovládače** vám umožňujú podrobne zadať, čo by malo byť súčasťou kontroly Anti-Rootkit. Tieto nastavenia sú určené pre skúsených používateľov, odporúčame vám, aby ste nechali všetky možnosti zapnuté. Môžete tiež vybrať režim kontroly rootkitov.

- **Rýchla kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače, a taktiež systémový priečinok (väčšinou *c:\Windows*)
- **Kompletná kontrola rootkitov** – kontroluje všetky spustené procesy, zavedené ovládače a taktiež systémový priečinok (väčšinou *c:\Windows*), a navyše všetky miestne disky (vrátane pamäťových médií, nie však disketové jednotky/jednotky CD)

8.2. Kontrola z prieskumníka

Okrem vopred definovaných kontrol spustených pre celý počítač alebo jeho vybrané oblasti, **AVG AntiVirus** 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 aplikácii Windows Explorer označte súbor (alebo priečinok), ktorý chcete skontrolovať.
- Kliknutím pravým tlačidlom myši na objekt otvorte kontextovú ponuku.
- Výberom možnosti **Skontrolovať programom AVG** skontrolujte súbor programom **AVG AntiVirus**

8.3. Kontrola z príkazového riadka

V **AVG AntiVirus** sa nachádza možnosť spustenia kontroly 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.



Pre spustenie kontroly AVG z príkazového riadka spustíte nasledovný príkaz v priečinku, kde je nainštalovaný program AVG:

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

8.3.1. Syntax príkazu

Toto je syntax príkazového riadka:

- **avgscanx /parameter** ... napr. **avgscanx /comp** pre 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:**

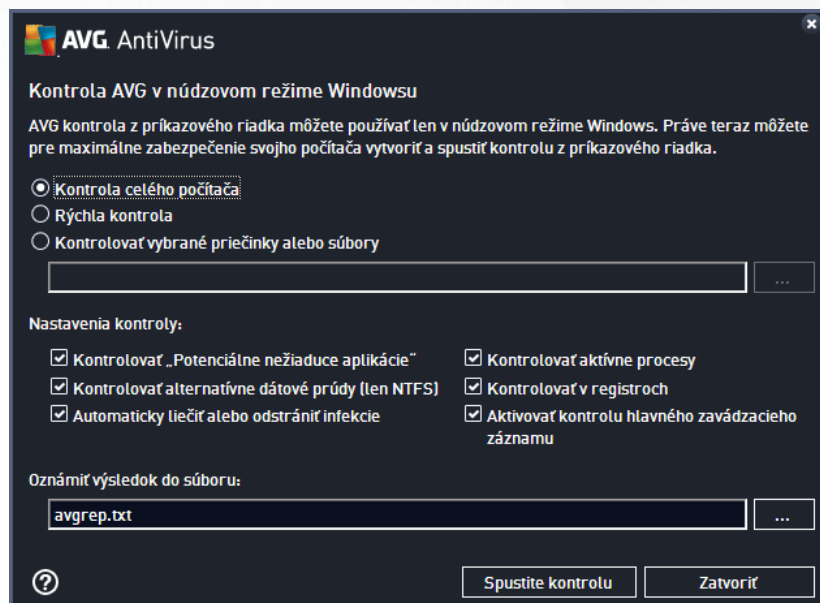
8.3.2. Parametre kontroly

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

Na spustenie kontroly stlačte kláves **Enter**. Počas kontrolovania môžete zastaviť tento proces pomocou kombinácie tlačidiel **Ctrl+C** alebo **Ctrl+Pause**.

8.3.3. Kontrola z príkazového riadka spustená z grafického rozhrania

Keď je počítač spustený v Núdzovom režime, máte možnosť spustiť kontrolu pomocou príkazového riadka z grafického používateľského rozhrania:





V Núdzovom režime sa samotná kontrola spustí z príkazového riadka. Toto dialógové okno vám len umožňuje špecifikovať parametre kontroly v pohodlnom grafickom rozhraní.

Najskôr vyberte oblasti vášho počítača, ktoré chcete skontrolovať. Môžete sa rozhodnúť buď pre vopred definovanú **Kontrolu celého počítača**, alebo pre možnosť **Skontrolovať vybrané priečinky**. Tretia možnosť, **Rýchla kontrola**, spustí špeciálnu kontrolu vytvorenú na použitie v Núdzovom režime, ktorá kontroluje všetky dôležité oblasti potrebné na spustenie vášho počítača.

Nastavenia kontroly v ďalšej časti vám umožňujú zadať podrobné parametre kontroly. V predvolenom nastavení sú všetky zaškrtnuté. Odporúčame vám ponechať ich takto označené a začiarknutie konkrétneho parametra zrušiť len v prípade, že na to máte konkrétny dôvod:

- **Kontrolovať „Potenciálne nežiaduce aplikácie“** – kontroluje spyware okrem vírusov
- **Kontrolovať alternatívne dátové prúdy (len pre NTFS)** – kontrola alternatívnych dátových prúdov NTFS, tzn. funkciu Windowsu, ktorú môžu zneužiť hackeri na skrývanie údajov, najmä škodlivého kódu
- **Automaticky liečiť alebo odstrániť infekcie** – všetky možné detekcie budú automaticky vyliečené alebo odstránené z vášho počítača
- **Kontrolovať aktívne procesy** – kontrola procesov a aplikácií načítaných do pamäte vášho počítača
- **Kontrolovať register** – kontrola registra Windows
- **Aktivovať kontrolu hlavného zavádzacieho záznamu** – kontrola tabuľky oblastí a zavádzacieho sektora

A nakoniec, v spodnej časti tohto dialógového okna môžete určiť názov a typ súboru správy o kontrole.

8.3.4. Parametre kontroly z príkazového riadka

Nasleduje zoznam všetkých dostupných parametrov pre kontrolu z príkazového riadka:

- | | |
|---------------|--|
| • /? | Zobraziť pomoc k tejto téme |
| • /@ | Súbor s príkazmi /názov súboru/ |
| • /ADS | Kontrolovať alternatívne dátové prúdy (len NTFS) |
| • /ARC | Kontrolovať archívy |
| • /ARCBOMBSW | Hlásiť opakovane komprimované archívne súbory |
| • /ARCBOMBSW | Hlásiť archívne bomby (opakovane komprimované archívy) |
| • /BOOT | Povoliť kontrolu MBR/BOOT |
| • /BOOTPATH | Spustiť rýchlu kontrolu |
| • /CLEAN | Automaticky vyčistiť |
| • /CLOUDCHECK | Kontrola nesprávnych pozitívnych detekcií |



- /COMP [Kontrola celého počítača](#)
- /COO Kontrolovať súbory cookies
- /EXCLUDE Cesty alebo súbory, ktoré sa majú vynechať z kontroly
- /EXT Kontrolovať tieto prípony (*napríklad EXT=EXE,DLL*)
- /FORCESHUTDOWN Vypnúť počítač po dokončení kontroly
- /HELP Zobrazit' pomocníka pre túto tému
- /HEUR Použiť heuristickú analýzu
- /HIDDEN Hlásiť súbory so skrytými príponami
- /IGNLOCKED Ignorovať zamknuté súbory
- /INFECTABLEONLY Kontrolovať len súbory s infikovateľnými príponami
- /LOG Generovať súbor s výsledkami kontroly
- /MACROW Hlásiť makrá
- /NOBREAK Nepovolit' prerušenie klávesmi CTRL-BREAK
- /NOEXT Nekontrolovať tieto prípony (*napríklad NOEXT=JPG*)
- /PRIORITY Nastaviť prioritu kontroly (*nízka, automatická, vysoká – pozrite časť [Rozšírené nastavenia/Kontroly](#)*)
- /PROC Kontrolovať aktívne procesy
- /PUP Hlásiť potenciálne nežiaduce aplikácie
- /PUPEXT Hlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií
- /PWDW Hlásiť súbory chránené heslom
- /QT Rýchly test
- /REG Kontrolovať register
- /REPAPPEND Pripojiť k súboru s hlásením
- /REPOK Hlásiť neinfikované súbory so značkou OK
- /REPORT Hlásiť do súboru (*názov súboru*)
- /SCAN [Kontrola súborov/priečinkov](#) (SCAN=cesta;cesta – *napr. /SCAN=C:\;D:*)
- /SHUTDOWN Vypnúť počítač po dokončení kontroly

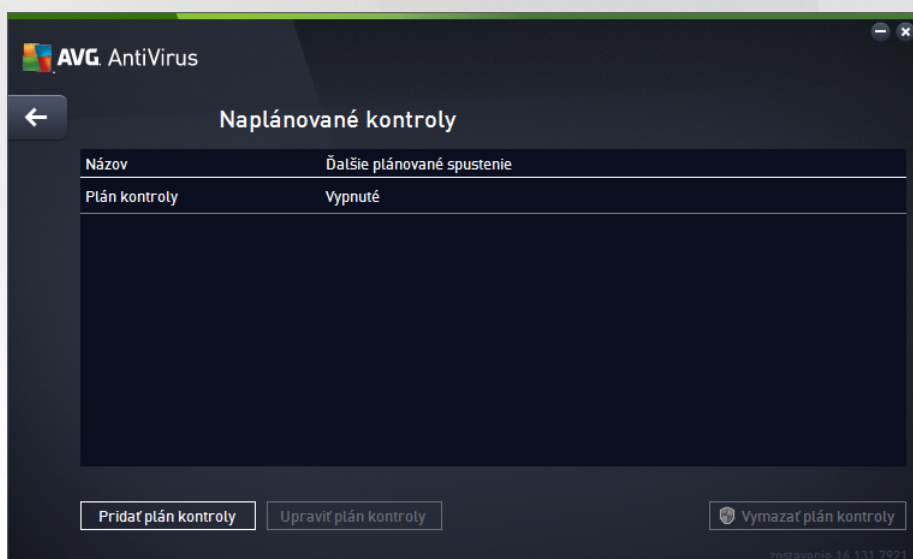


- /THOROUGHSCAN Zapnúť dôkladnú kontrolu
- /TRASH Presunúť infikované súbory do [Vírusového trezora](#)

8.4. Plánovanie kontrol

Pomocou **AVG AntiVirus** môžete spustiť kontrolu na požiadanie (*napríklad, keď máte podozrenie, že sa do počítača dostala infekcia*) alebo na základe vytvoreného plánu. Odporúča sa spúšťať kontroly na základe plánov: týmto spôsobom môžete zabezpečiť, že je váš počítač chránený pred možnosťou infekcie 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 kontrolu celého počítača spúšťajte každý deň v predvolenej konfigurácii plánu kontroly. Ak je počítač „stále zapnutý“, môžete naplánovať kontrolu na čas, keď sa počítač nepoužíva. Ak je počítač v tomto čase vypnutý, potom sa zmeškané naplánované kontroly spustia [pri spustení počítača](#).

Plán kontroly môžete vytvoriť/upraviť v dialógovom okne **Plán kontroly**, ktoré zobrazíte tlačidlom **Správa plánu kontroly** v dialógovom okne [Možnosti kontroly](#). V novom dialógovom okne **Plán kontroly** môžete zobrazit' prehľad všetkých naplánovaných kontrol:

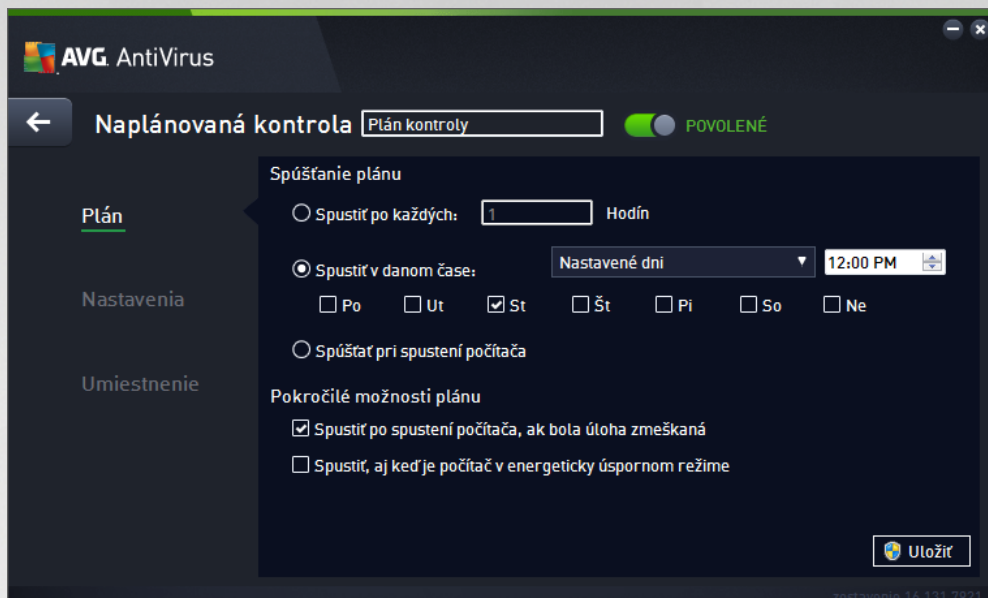


V dialógovom okne môžete zadať svoje vlastné kontroly. Pomocou tlačidla **Pridať plán kontroly** si môžete vytvoriť nový plán kontroly. Parametre plánu kontroly sa dajú upraviť (*alebo sa dá nastaviť nový plán*) v troch kartách:

- [Plán](#)
- [Nastavenia](#)
- [Umiestnenie](#)

Na každej karte môžete jednoducho zapnúť tlačidlo „semafor“ , aby ste dočasne deaktivovali naplánovaný test a znovu ho podľa potreby zapli.

8.4.1. Plán



V hornej časti záložky **Plán** sa nachádza textové pole, do ktorého môžete zadať názov modulu kontroly, ktorý sa aktuálne definuje. Pokúste sa použiť stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom odlíšiť. Príklad: Nie je vhodné nazývať kontrolu „Nová kontrola“ alebo „Moja kontrola“, pretože tieto názvy sa nevzťahujú na to, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod.

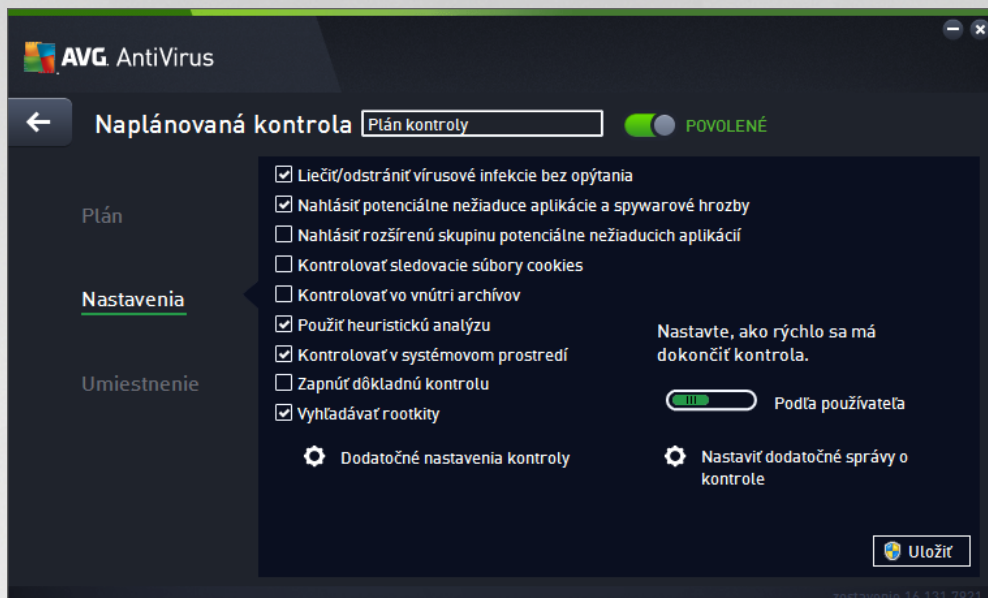
Toto dialógové okno umožňuje ďalej definovať tieto parametre kontroly:

- **Naplánovať spúšťanie** – tu môžete nastaviť časové intervaly pre spustenie novo naplánovanej kontroly. Čas spúšťania sa definuje ako opakované spúšťanie kontroly po uplynutí určitého času (*Spustiť po každých ...*), definovaním presného dátumu a času (*Spustiť v konkrétnom čase*), prípadne definovaním udalosti, s ktorou sa bude spájať spustenie kontroly (*Spustiť pri spustení počítača*).
- **Možnosti pokročilého plánu** – táto časť vám umožňuje zadefinovať, za akých podmienok by sa kontrola mala/nemala spustiť, ak je počítač v úspornom režime alebo celkom vypnutý. Keď sa spustí plán kontroly vo vami zadanom čase, o tejto skutočnosti budete informovaní pomocou kontextového okna, ktoré sa otvorí nad [ikonou AVG v paneli úloh](#). Potom sa zobrazí nová [ikona AVG v paneli úloh](#) (farebná s blikajúcim svetlom), ktorá informuje o tom, že prebieha naplánovaná kontrola. Kliknutím pravým tlačidlom myši na ikonu AVG prebiehajúcej kontroly otvoríte kontextovú ponuku, ktorá vám umožní pozastaviť alebo dokonca úplne zastaviť prebiehajúcu kontrolu a zároveň zmeniť prioritu práve spustenej kontroly.

Ovládacie prvky dialógového okna

- **Uložiť** – uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu [Plánu kontrol](#). Preto, ak chcete konfigurovať parametre testu vo všetkých kartách, stlačte toto tlačidlo pre uloženie parametrov až po zadaní všetkých svojich požiadaviek.
- **←** – Zelenou šípkou v ľavej hornej časti okna sa dostanete naspäť do prehľadu [Plánu kontrol](#).

8.4.2. Nastavenia



V hornej časti záložky **Nastavenia** sa nachádza textové pole, do ktorého môžete zadať názov modulu kontroly, ktorý sa aktuálne definuje. Pokúste sa použiť stručné, opisné a výstižné názvy pre kontroly, aby sa dali neskôr ľahšie navzájom odlíšiť. Príklad: Nie je vhodné nazývať kontrolu „Nová kontrola“ alebo „Moja kontrola“, pretože tieto názvy sa nevzťahujú na to, čo kontrola vlastne preveruje. Na druhej strane, príkladom dobrého opisného názvu je „Kontrola systémových oblastí“ a pod.

V karte **Nastavenia** nájdete zoznam parametrov kontrolovania, ktoré sa dajú voliteľne zapnúť/vypnúť. **Ak nemáte závažný dôvod meniť tieto nastavenia, odporúčame vám ponechať vopred definovanú konfiguráciu:**

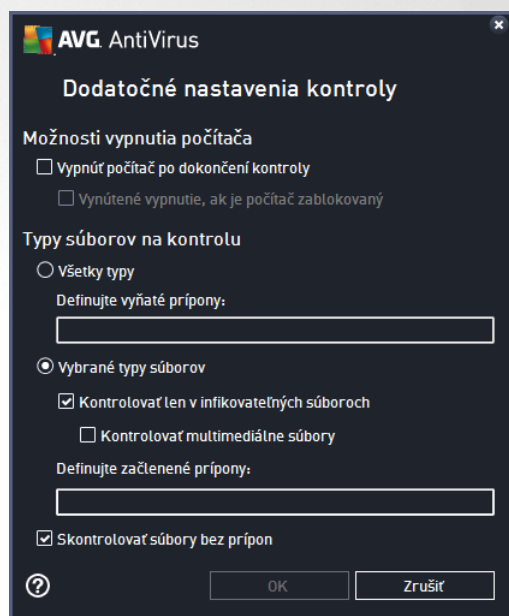
- **Liečiť/odstrániť vírusové infekcie bez opýtania** (predvolene zapnuté): ak sa počas kontroly identifikuje vírus, môže sa automaticky vyliečiť, ak je dostupná liečba. Ak nie je možné infikovaný súbor vyliečiť automaticky, premiestni sa do [Vírusového trezora](#).
- **Nahlásiť potenciálne nežiaduce aplikácie a spywarové hrozby** (predvolene zapnuté): začiarňte toto políčko, ak chcete aktivovať kontrolu spyware a vírusov. Spyware predstavuje pochybnú kategóriu malware: 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.
- **Nahlásiť rozšírenú skupinu potenciálne nežiaducich aplikácií** (predvolene vypnuté): začiarňte toto políčko, 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 predvolene vypnutá.
- **Kontrolovať sledovacie súbory cookies** (predvolene vypnuté): tento parameter súčasť zapína funkciu na detekciu súborov cookies počas kontroly; (súbory 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 vo vnútri archívov** (predvolene vypnuté): tento parameter určuje, že sa majú počas kontroly preverovať všetky súbory, aj keď sú uložené vo vnútri archívu, napr. ZIP, RAR, atď.
- **Použiť heuristickú analýzu** (predvolene zapnuté): heuristická analýza (dynamická emulácia inštrukcií kontrolovaného objektu vo virtuálnom počítačovom prostredí) bude jednou z metód, ktoré sa použijú na detekciu vírusov počas kontroly.
- **Kontrolovať v systémovom prostredí** (predvolene zapnuté): počas kontroly sa budú overovať aj systémové oblasti počítača.
- **Zapnúť dôkladnú kontrolu** (predvolene vypnuté): v určitých situáciách (podozrenie na infikovanie počítača) môžete touto možnosťou aktivovať najdôkladnejšie kontrolné algoritmy, ktoré pre istotu skontrolujú aj tie oblasti počítača, ktoré sa obvyčajne vôbec neinfikujú. Upozorňujeme však, že tento spôsob je náročný na čas.
- **Kontrolovať rootkity** (predvolene zapnuté): Kontrola Anti-Rootkit kontroluje počítač a zisťuje prítomnosť potenciálnych rootkitov (programov a technológií, ktoré dokážu zakryť činnosť malwaru 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.

Ďalšie nastavenia kontroly

Odkaz otvorí nové dialógové okno **Dodatočné nastavenia kontroly**, ktoré sa používa na nastavenie nasledujúcich parametrov:



- **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 zablokovaný (*Vynútené vypnutie, ak je počítač zablokovaný*).
- **Typy súborov na kontrolu** – mali by ste tiež určiť, čo chcete kontrolovať:



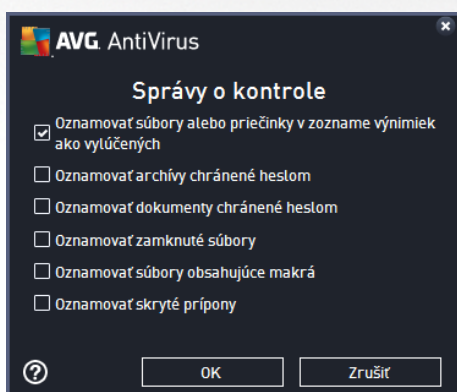
- o **Všetky typy súborov** s možnosťou definovať výnimky z kontroly vytvorením zoznamu čiarkou oddelených prípon súborov, ktoré sa nemajú kontrolovať.
- o **Vybrané typy súborov** – môžete nastaviť, aby sa kontrolovali len súbory, pri ktorých existuje pravdepodobnosť infikovania (súbory, ktoré nemôžu byť napadnuté infekciou, napríklad niektoré jednoduché textové súbory alebo niektoré nespustiteľné súbory) vrátane mediálnych súborov (video, audio súborov – ak necháte toto políčko nezačiarknuté, potom sa čas kontroly skráti ešte viac, pretože tieto súbory sú často veľmi veľké, pričom pravdepodobnosť napadnutia vírusom je veľmi malá). Znova môžete definovať, podľa prípony, ktoré súbory sa majú kontrolovať vždy.
- o Alternatívne môžete rozhodnúť, že chcete **kontrolovať súbory bez prípony** – táto možnosť je predvolene 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 tejto časti môžete ďalej špecifikovať želanú rýchlosť kontroly v závislosti od využívania systémových zdrojov. V predvolenom nastavení je úroveň automatického využívania zdrojov nastavená *Podľa používateľa*. Ak chcete, aby kontrola prebiehala rýchlejšie, potom bude trvať kratšie, ale výrazne sa zvýši využívanie systémových zdrojov a spomalia 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 systémových zdrojov predĺžením doby trvania kontroly.

Vytvoriť ďalšie správy o kontrole

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



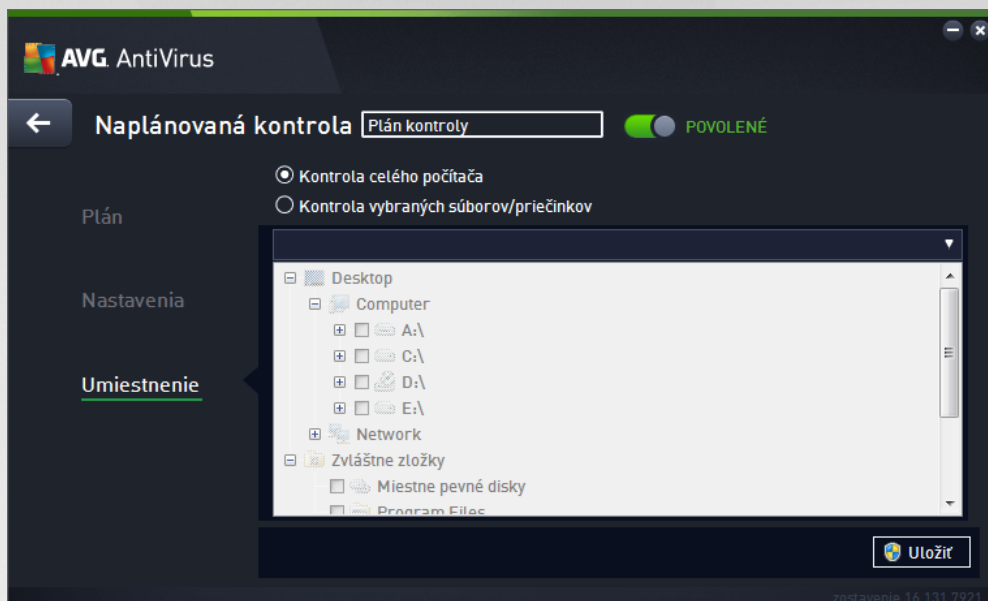
Ovládacie prvky dialógového okna

- **Uložiť** – uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu [Plánu kontrol](#). Preto, ak chcete konfigurovať parametre testu vo všetkých kartách, stlačte toto tlačidlo pre uloženie parametrov až po zadaní všetkých svojich požiadaviek.



- – Zelenou šípkou v ľavej hornej časti okna sa dostanete naspäť do prehľadu [Plánu kontrol](#).

8.4.3. Umiestnenie



Na karte **Umiestnenie** môžete nastaviť, či chcete naplánovať [kontrolu celého počítača](#) alebo [kontrolu súborov/priečinkov](#). Keď vyberiete kontrolu súborov/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 políчков môžete vybrať naraz niekoľko priečinkov. Vybrané priečinky sa zobrazia v textovom poli v hornej časti dialógového okna a do kontextovej 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**. Nasleduje zoznam umiestnení, ktoré sa skontrolujú po označení príslušného začiarkavacieho políčka:

- **Miestne pevné disky** – všetky pevné disky vášho počítača
- **Programové súbory**
 - o C:\Program Files\
 - o v 64-bitovej verzii C:\Program Files (x86)
- **Priečinok Moje dokumenty**
 - o vo Windows XP: C:\Dokumenty a nastavenia\Predvolený používateľ\Moje dokumenty\
 - o vo Windows Vista/7: C:\Používateľia\používateľ\Dokumenty\
- **Zdieľané dokumenty**
 - o vo Windows XP: C:\Dokumenty a nastavenia\Všetci používatelia\Dokumenty\



o vo Windows Vista/7: C:\Používateľia\Verejné\Dokumenty\

- **Priečink Windows** – C:\Windows\

- **Iné**

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

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

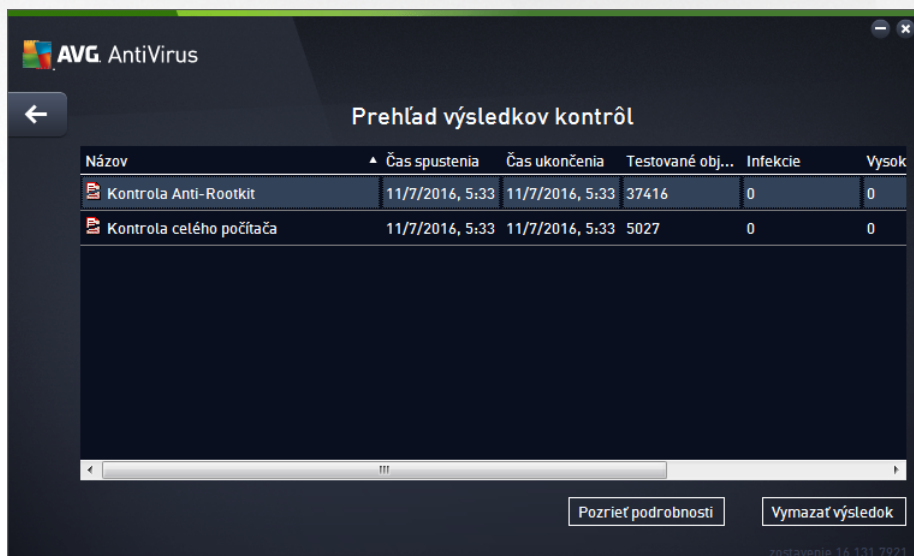
o **Priečinok Dočasné súbory** – C:\Dokumenty a nastavenia\Používateľ\Miestne\ (Windows XP) alebo C:\Používateľia\používateľ\AppData\Local\Temp\ (Windows Vista/7)

o **Dočasné internetové súbory** – C:\Dokumenty a nastavenia\Používateľ\Miestne nastavenia\Dočasné internetové súbory\ (Windows XP) alebo C:\Používateľia\používateľ\AppData\Local\Microsoft\Windows\Dočasné internetové súbory (Windows Vista/7)

Ovládacie prvky dialógového okna

- **Uložiť** – uloží všetky zmeny, ktoré ste vykonali v tejto karte alebo v inej karte tohto dialógového okna a prepne naspäť do prehľadu [Plánu kontrol](#). Preto, ak chcete konfigurovať parametre testu vo všetkých kartách, stlačte toto tlačidlo pre uloženie parametrov až po zadání všetkých svojich požiadaviek.
- – Zelenou šípkou v ľavej hornej časti okna sa dostanete naspäť do prehľadu [Plánu kontrol](#).

8.5. Výsledky kontrol



Dialógové okno **Prehľad výsledkov kontrol** obsahuje zoznam výsledkov všetkých doterajších kontrol. Tabuľka obsahuje pre každý výsledok kontroly tieto údaje:

- **Ikona** – v prvom stĺpci sa zobrazuje informačná ikona popisujúca stav kontroly:



- o  Nenašla sa žiadna infekcia, kontrola sa dokončila
 - o  Nenašla sa žiadna infekcia, kontrola sa prerušila pred dokončením
 - o  Našli sa infekcie, ktoré neboli vyliečené, kontrola sa dokončila
 - o  Našli sa infekcie, ktoré neboli vyliečené, kontrola sa prerušila pred dokončením
 - o  Našli sa infekcie a všetky boli vyliečené alebo odstránené, kontrola sa dokončila
 - o  Našli sa infekcie a všetky boli vyliečené alebo odstránené, kontrola sa prerušila pred dokončením
- **Názov** – v stĺpci sa nachádza názov príslušnej kontroly. Buď je to jedna z dvoch [vopred definovaných kontrol](#), alebo váš vlastný [plán kontroly](#).
 - **Čas spustenia** – uvádza presný dátum a čas, kedy bola kontrola spustená.
 - **Čas ukončenia** – uvádza presný dátum a čas ukončenia, pozastavenia alebo prerušenia kontroly.
 - **Testované objekty** – uvádza celkový počet skontrolovaných objektov.
 - **Infekcie** – uvádza počet odstránených/celkových nájdených infekcií.
 - **Vysoká/stredná/nízka** – v troch ďalších stĺpcoch je uvedený počet nájdených infekcií s vysokou, strednou a nízkou závažnosťou.
 - **Rootkity** – uvádza celkový počet [rootkitov](#) nájdených počas kontroly.

Ovládacie prvky dialógového okna

Pozrieť podrobnosti – kliknutím na tlačidlo zobrazíte [podrobné informácie o vybranej kontrole](#) (označenej v tabuľke vyššie).

Vymazať výsledky – kliknutím na tlačidlo odstránite údaje o vybranom výsledku kontroly z tabuľky.

 – Pomocou zelenej šípky v ľavej hornej časti dialógového okna sa vrátite naspäť do [hlavného používateľského rozhrania](#) s prehľadom súčastí.

8.6. Podrobnosti výsledkov kontrol

Ak chcete otvoriť prehľad s podrobnosťami o vybranom výsledku kontroly, kliknite na tlačidlo **Pozrieť podrobnosti** v dialógovom okne [Prehľad výsledkov kontrol](#). Budete presmerovaní na rovnaké rozhranie dialógového okna s podrobnými informáciami o príslušných výsledkoch kontroly. Informácie sú rozdelené na tri záložky:

- **Súhrn** – táto karta poskytuje základné informácie o kontrole: Či bola dokončená úspešne, či boli nájdené nejaké hrozby a čo sa s nimi stalo.



- **Podrobnosti** – táto karta zobrazuje všetky údaje o kontrole vrátane podrobností o akýchkoľvek detegovaných hrozbách. Exportovať prehľad do súboru umožňuje uložiť výsledky kontroly do súboru s príponou .csv.
- **Detekcie** – táto karta je zobrazená len v prípade, že boli počas kontroly detegované nejaké hrozby, a uvádza podrobné informácie o týchto hrozbách:

 **Informatívna závažnosť:** informácie alebo varovania, nie skutočné hrozby. Obvykle dokumenty obsahujúce makrá, dokumenty alebo archívy chránené heslom, uzamknuté súbory, atď.

 **Stredná závažnosť:** obvykle potenciálne nežiaduce aplikácie (ako napríklad adware) alebo sledovacie súbory cookies

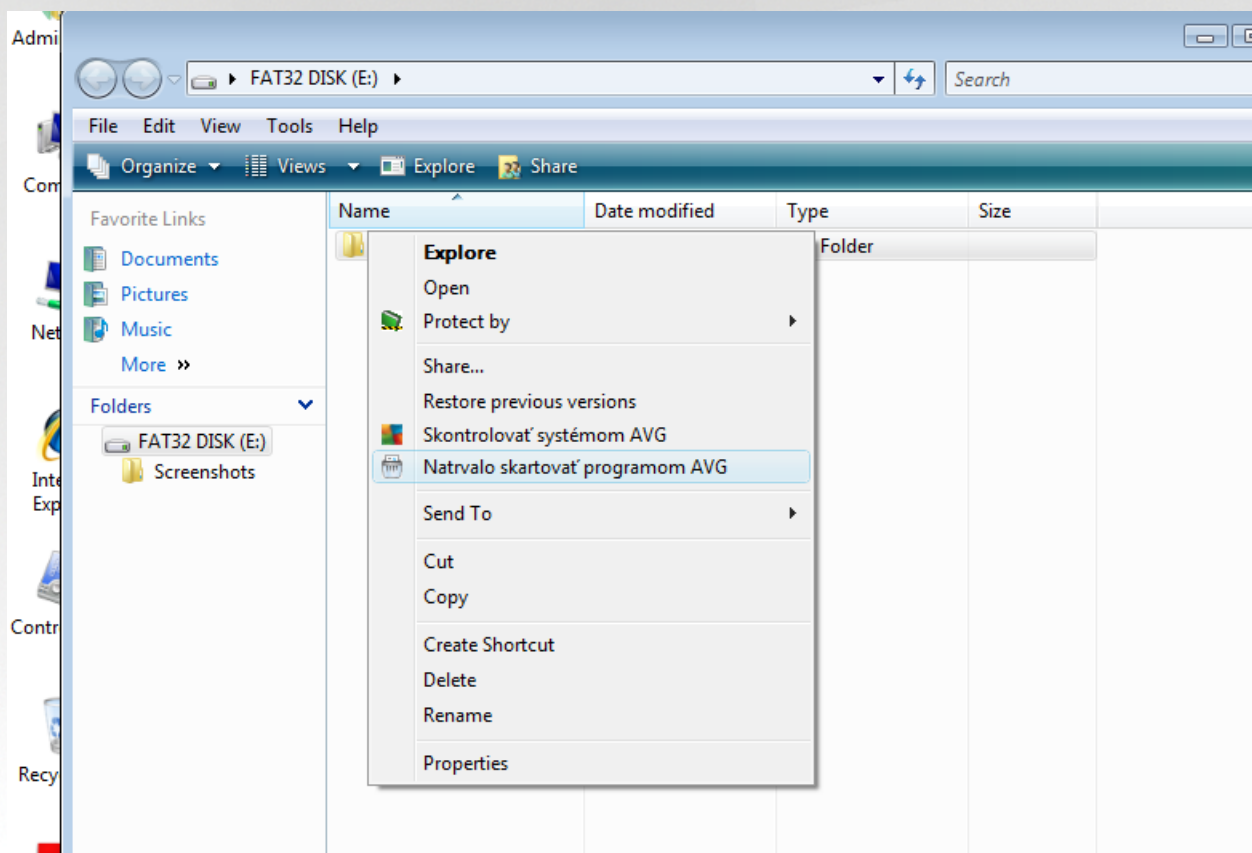
 **Vysoká závažnosť:** vážne hrozby, ako napríklad vírusy, trójske kone a zneužitia. Taktiež objekty detegované heuristickou metódou detekcie, teda hrozby, ktoré ešte nie sú popísané vo vírusovej databáze.



9. AVG File Shredder

AVG File Shredder bol navrhnutý na úplne bezpečné vymazávanie súborov, teda bez akejkoľvek možnosti ich obnovenia, dokonca ani s pokročilými softvérovými nástrojmi na to určenými.

Ak chcete skartovať súbor alebo priečinok, kliknite naň pravým tlačidlom myši v správcovi súborov (*Prieskumník Windows, Total Commander, atď.*) a z kontextovej ponuky vyberte možnosť **Natrvalo skartovať pomocou AVG**. Súbory v koši môžete takisto skartovať. Ak nebude možné určitý súbor v určitom umiestnení (napr. CD-ROM) spoľahlivo skartovať, zobrazí sa oznámenie alebo možnosť v kontextovej ponuke nebude vôbec dostupná.



Vždy pamätajte: hneď ako súbor skartujete, je navždy stratený.



10. Vírusový trezor

Vírusový trezor je bezpečné prostredie na správu podozrivých a infikovaných objektov detegovaných počas testov vykonaných AVG. Keď sa počas prehľadávania deteguje podozrivý objekt a AVG ho nedokáže automaticky vyliečiť, systém sa vás spýta, 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 nepotrebuje. Ak zistíte, že odstránenie súboru spôsobuje problémy, môžete ho poslať na analýzu alebo obnoviť do pôvodného umiestnenia.

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

- **Pridaný dňa** – uvádza dátum a čas, kedy bol podozrivý súbor detegovaný a presunutý do Vírusového trezora.
- **Hrozba** – ak sa rozhodnete nainštalovať súčasť [Software Analyzer](#) v rámci **AVG AntiVirus**, potom sa v tejto časti bude nachádzať grafické znázornenie úrovne závažnosti zisteného nálezu: od vyhovujúcej (tri zelené bodky) až po veľmi nebezpečnú (tri červené bodky). Taktiež zistíte informácie o type infekcie a jej pôvodnom umiestnení. Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#) uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Zdroj** – uvádza, ktorá súčasť **AVG AntiVirus** zistila príslušnú hrozbu.
- **Oznámenia** – veľmi výnimočne môžu byť v tomto stĺpci uvedené podrobné komentáre týkajúce sa príslušnej zistenej hrozby.

Ovládacie tlačidlá

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

- **Obnoviť** – odstráni infikovaný súbor naspäť na jeho pôvodné umiestnenie na vašom disku.
- **Obnoviť ako** – premiestni infikovaný súbor do vybraného priečinka.
- **Zaslať na analýzu** – toto tlačidlo je aktívne len v prípade, že v zozname detekcií vyššie označíte objekt. V takomto prípade máte možnosť zaslať vybranú detekciu do vírusových laboratórií spoločnosti AVG na ďalšiu podrobnú analýzu. Upozorňujeme, že táto funkcia by sa mala predovšetkým používať len na zasielanie súborov nesprávne detegovaných, t. j. súborov, ktoré program AVG označil ako infikované alebo podozrivé, ale o ktorých ste presvedčení, že sú neškodné.
- **Podrobnosti** – ak chcete zobrazit' podrobné informácie o konkrétnej hrozbe vlozenej do karantény vo **Vírusovom trezore**, označte vybranú položku v zozname a kliknutím na tlačidlo **Podrobnosti** otvoríte nové dialógové okno s popisom zistenej hrozby.
- **Vymazať** – dokonale a nenávratne odstráni infikovaný súbor z **Vírusového trezora**.
- **Vyprázdniť trezor** – vymaže celý obsah **Vírusového trezora**. Odstránením z **Vírusového trezora** sa súbory úplne a nenávratne odstránia z disku (nepremiestnia sa do Koša).

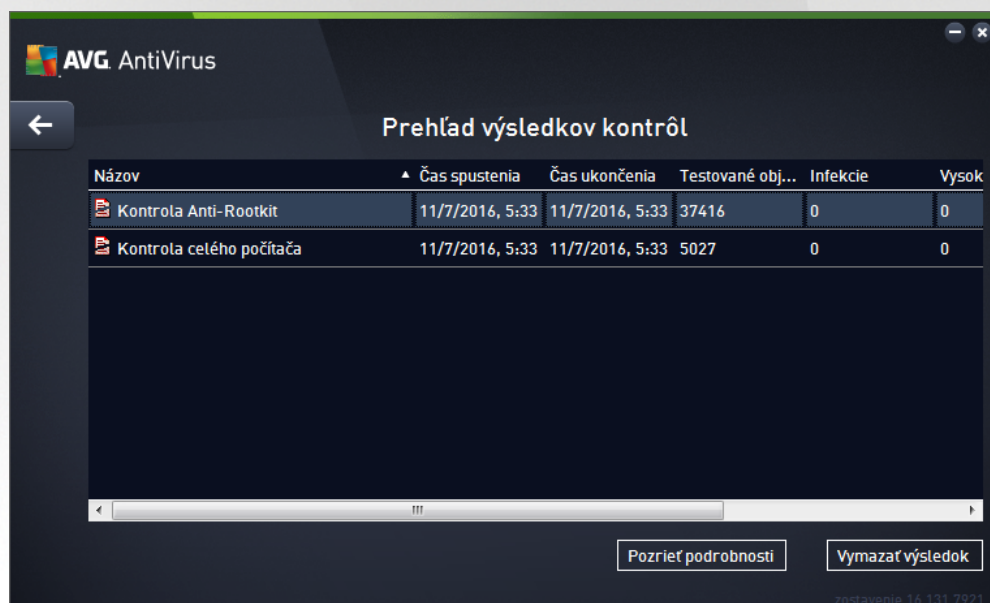


11. História

Časť **História** obsahuje informácie o všetkých udalostiach v minulosti (ako napríklad aktualizácie, kontroly, detekcie a pod.) a správy o týchto udalostiach. K tejto časti sa dostanete z [hlavného používateľského rozhrania](#) prostredníctvom položky **Možnosti/História**. História všetkých zaznamenaných udalostí je rozdelená do nasledujúcich častí:

- [Výsledky kontrol](#)
- [Nálezy súčasti Rezidentný štít](#)
- [Nálezy súčasti Ochrana e-mailu](#)
- [Nálezy súčasti Webový štít](#)
- [História udalostí](#)

11.1. Výsledky kontrol



Dialógové okno **Prehľad výsledkov kontrol** je prístupné prostredníctvom ponuky **Možnosti/História/Výsledky kontrol** v hornom navigačnom pruhu hlavného okna **AVG AntiVirus**. V dialógovom okne sa nachádza zoznam všetkých doposiaľ spustených kontrol a informácie o ich výsledkoch:

- **Názov** – označenie kontroly. Buď môže ísť o názov niektorého z [vopred definovaných kontrol](#), alebo o názov, ktorý ste priradili [vlastnej naplánovanej kontrole](#). Každý názov obsahuje ikonu s označením výsledku kontroly:

 – zelená ikona informuje, že počas kontroly nebola detegovaná žiadna infekcia.

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



 – červená ikona upozorňuje, že počas kontroly bola detegovaná infekcia, ktorá sa nedala vymazať!

Každá ikona môže byť buď plná, alebo rozdelená na polovicu – plné ikony predstavujú dokončené a správne ukončené kontroly, ikony rozdelené na polovicu predstavujú zrušené alebo prerušené kontroly.

Poznámka: Podrobné informácie o každej kontrole sa nachádzajú v dialógovom okne [Výsledky kontroly](#), ktoré sa otvára pomocou tlačidla *Pozrieť podrobnosti* (v spodnej časti tohto dialógového okna).

- **Čas spustenia** – dátum a čas, kedy bola kontrola spustená
- **Čas skončenia** – dátum a čas, kedy sa kontrola skončila
- **Testované objekty** – počet objektov, ktoré sa skontrolovali počas kontroly
- **Infekcie** – počet detegovaných/odstránených vírusových infekcií
- **Vysoká/stredná** – v týchto stĺpcoch sa uvádza číslo odstránených/celkových infekcií nájdených pre každú z úrovní závažnosti (vysokú a strednú)
- **Info** – informácie súvisiace s priebehom a výsledkami kontroly (*obvyčajne s jej dokončením alebo prerušením*)
- **Rootkity** – počet detegovaných [rootkitov](#)

Ovládacie tlačidlá

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

- **Pozrieť podrobnosti** – stlačením tohto tlačidla sa otvorí dialógové okno [Výsledky kontroly](#) s podrobnými informáciami o zvolenej kontrole
- **Vymazať výsledok** – stlačením tohto tlačidla sa zvolená položka odstráni z prehľadu výsledkov kontroly
-  – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (*prehľad súčasti*), použite šípku v ľavom hornom rohu tohto dialógového okna

11.2. Nálezy súčasti Rezidentný štít

Služba **Rezidentný štít** je časťou súčasti [Počítač](#) a kontroluje súbory, ktoré sa práve kopírujú, otvárajú alebo ukládajú. Pri detegovaní vírusu alebo akéhokoľvek druhu hrozby vás program ihneď upozorní zobrazením tohto dialógového okna:

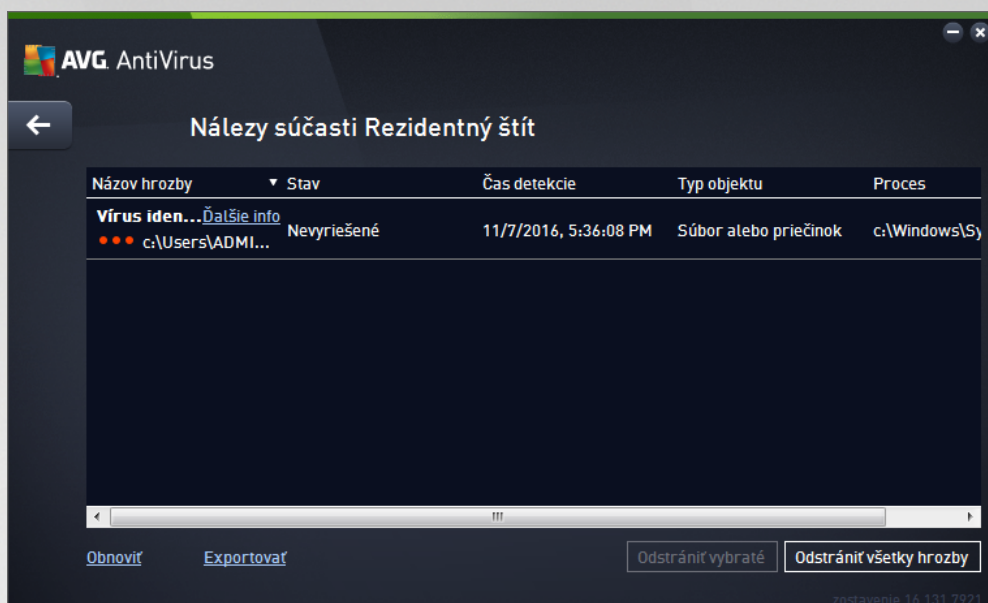


V tomto dialógovom okne s upozornením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Hrozba*), a kratší popis rozpoznanej infekcie (*Popis*). Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#), uvádzajúcu podrobné informácie o zistenej hrozbe, ak sú tieto známe. V tomto okne sa nachádza aj prehľad dostupných riešení zistenej hrozby. Jedna z možností bude označená ako odporúčaná: **Chrániť ma (odporúčané)**. *Ak je to možné, vždy by ste mali ponechať túto možnosť.*

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 objektu do Vírusového trezora. Veľkosť Vírusového trezora však môžete zmeniť. Je definovaná ako nastaviteľné percento skutočnej veľkosti vášho pevného disku. Na zväčšenie veľkosti Vírusového trezora otvorte dialógové okno [Vírusový trezor](#) v časti [Rozšírené nastavenia AVG](#) kliknutím na možnosť „Obmedziť veľkosť Vírusového trezora“.

V dolnej časti dialógového okna sa nachádza odkaz **Zobraziť podrobnosti**. Kliknutím naň otvoríte nové okno s podrobnosťami o procese, ktorý bol spustený pri zaznamenaní infekcie, a o identifikácii procesu.

Zoznam všetkých nálezov súčasti Rezidentný štít si môžete pozrieť v dialógovom okne **Nálezy súčasti Rezidentný štít**. Toto dialógové okno sa nachádza pod položkou ponuky **Možnosti/História/Nálezy súčasti Rezidentný štít** v hornom navigačnom pruhu [hlavného okna produktu AVG AntiVirus](#). Toto dialógové okno obsahuje prehľad objektov detegovaných súčastou Rezidentný štít vyhodnotených ako nebezpečné, ktoré boli buď vyliečené, alebo premiestnené do [Vírusového trezora](#).



Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho umiestnenie. Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#) uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Stav** – akcia vykonaná s detegovaným objektom
- **Čas detekcie** – dátum a čas detegovania a zablokovania hrozby
- **Typ objektu** – typ detegovaného objektu.
- **Proces** – aká akcia sa vykonala na zavolaní potenciálne nebezpečného objektu, aby sa mohol detegovať

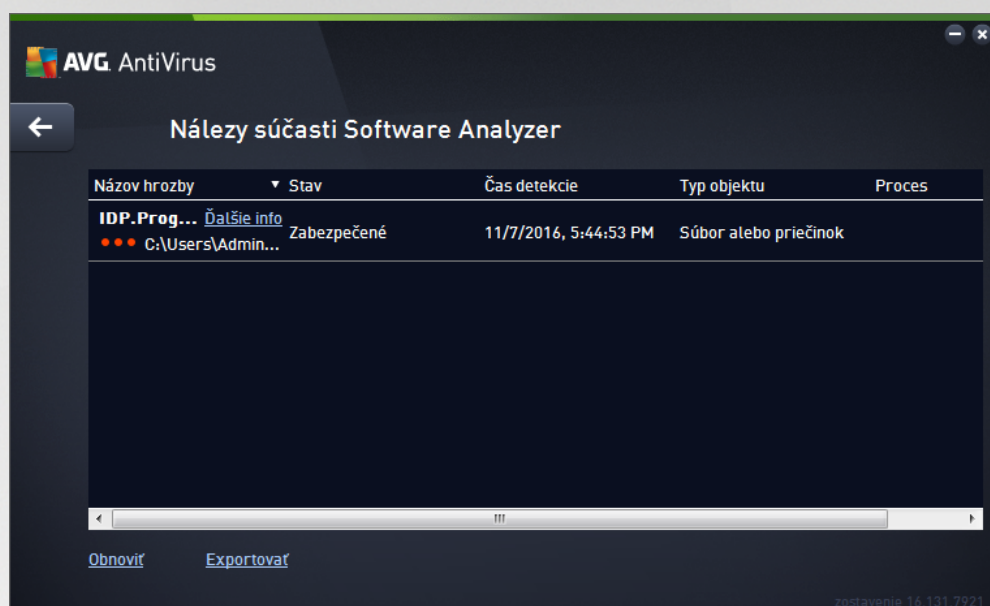
Ovládacie tlačidlá

- **Obnoviť** – aktualizuje sa zoznam nálezov zistených **Webovým štítom**
- **Exportovať** – exportuje celý zoznam zistených objektov do súboru
- **Odstrániť vybrané** – v zozname môžete označiť iba vybrané záznamy a týmto tlačidlom ich vymažete
- **Odstrániť všetky hrozby** – týmto tlačidlom vymažete všetky záznamy v tomto dialógovom okne
- – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčastí), použijete šípku v ľavom hornom rohu tohto dialógového okna



11.3. Nálezy súčasti Identity Protection

Dialógové okno **Nálezy súčasti Software Analyzer** je dostupné prostredníctvom ponuky **Možnosti /História/Nálezy súčasti Software Analyzer** v hornom navigačnom pruhu hlavného okna **AVG AntiVirus**.



Toto dialógové okno obsahuje zoznam všetkých nálezov detegovaných súčastou [Software Analyzer](#). Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho umiestnenie. Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#) uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Stav** – akcia vykonaná s detegovaným objektom
- **Čas detekcie** – dátum a čas detegovania a zablokovania hrozby
- **Typ objektu** – typ detegovaného objektu
- **Proces** – aká akcia sa vykonala na vyvolanie potenciálne nebezpečného objektu, aby sa mohol detegovať

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

Ovládacie tlačidlá

V rozhraní **Nálezov súčasti Software Analyzer** sa nachádzajú tieto ovládacie tlačidlá:

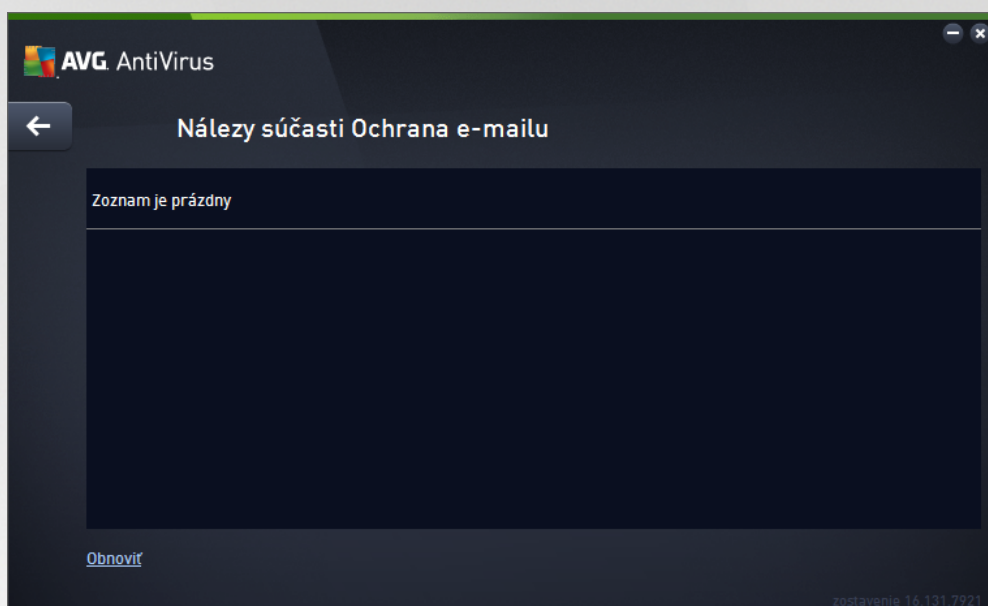
- **Obnoviť zoznam** – aktualizuje zoznam detegovaných hrozieb



-  – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčastí), použite šípku v ľavom hornom rohu tohto dialógového okna

11.4. Nálezy súčasti Ochrana e-mailu

Dialógové okno **Nálezy súčasti Ochrana e-mailu** je dostupné prostredníctvom ponuky **Možnosti/História/Nálezy súčasti Ochrana e-mailu** v hornom navigačnom pruhu hlavného okna produktu AVG AntiVirus.



Toto dialógové okno obsahuje zoznam všetkých nálezov detegovaných súčastou [Kontrola pošty](#). Pre každý detegovaný objekt sa zobrazia tieto informácie:

- **Názov detekcie** – popis (prípadne aj názov) detegovaného objektu a jeho zdroj
- **Výsledok** – akcia vykonaná na detegovanom objekte
- **Čas detekcie** – dátum a čas detekcie podozrivého objektu
- **Typ objektu** – typ detegovaného objektu
- **Proces** – aká akcia sa vykonala na vyvolanie potenciálne nebezpečného objektu, aby sa mohol detegovať

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

Ovládacie tlačidlá

V rozhraní **Nálezy súčasti Kontrola pošty** sa nachádzajú nasledujúce tlačidlá:

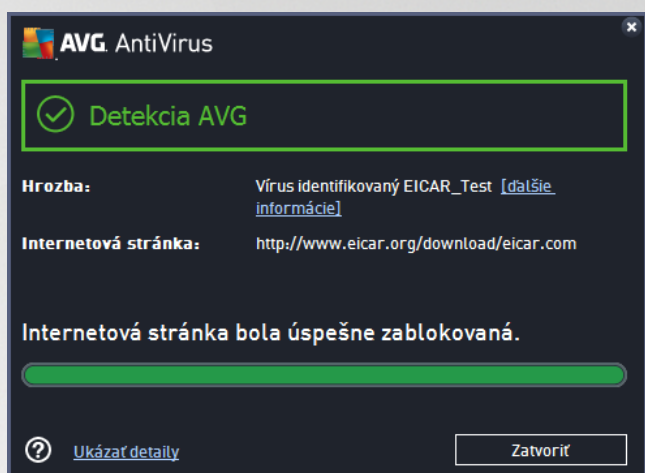
- **Obnoviť zoznam** – aktualizuje zoznam detegovaných hrozieb



-  – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (prehľad súčastí), použijete šípku v ľavom hornom rohu tohto dialógového okna

11.5. Nálezy súčasti Webový štít

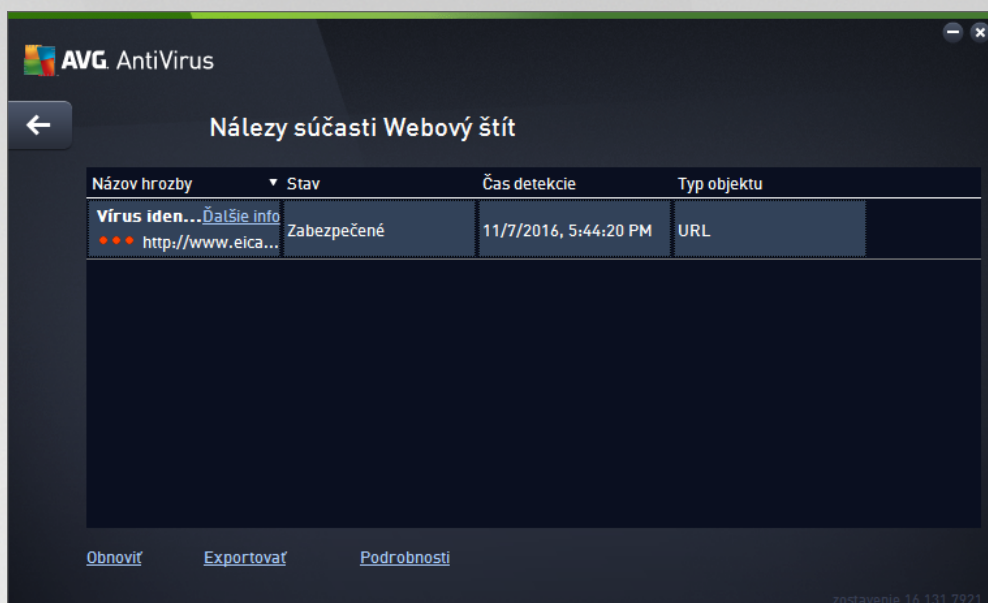
Webový štít kontroluje obsah navštívených internetových stránok a súborov, ktoré sa na nich môžu nachádzať, ešte predtým, než sa zobrazia v internetovom prehliadači alebo stiahnu do počítača. Pri detegovaní hrozby vás program ihneď upozorní otvorením tohto dialógového okna:



V tomto dialógovom okne s upozornením sa nachádzajú informácie o zistenom objekte, ktorý sa považuje za infikovaný (*Hrozba*), a kratší popis rozpoznanej infekcie (*Názov objektu*). Odkaz *Viac informácií* vás presmeruje na [online vírusovú encyklopédiu](#), kde nájdete podrobné informácie o zistenej infekcii, pokiaľ sú známe. V tomto dialógovom okne sa nachádzajú nasledujúce ovládacie prvky:

- **Zobraziť podrobnosti** – kliknutím na odkaz otvoríte nové kontextové okno s informáciami o procese, ktorý bol spustený v čase detegovania infekcie, a o identifikácii procesu.
- **Zatvoriť** – kliknutím na toto tlačidlo zatvorte dialógové okno s varovaním.

Podozrivá webová stránka sa neotvorí a detekcia hrozieb sa zapíše do zoznamu súčasti **Nálezy súčasti Webový štít**. Tento prehľad zistených hrozieb sa nachádza pod položkou ponuky **Možnosti/História/Nálezy súčasti Webový štít** v hornom navigačnom pruhu hlavného okna programu **AVG AntiVirus**.



Pre každý detegovaný objekt sa zobrazia tieto informácie:

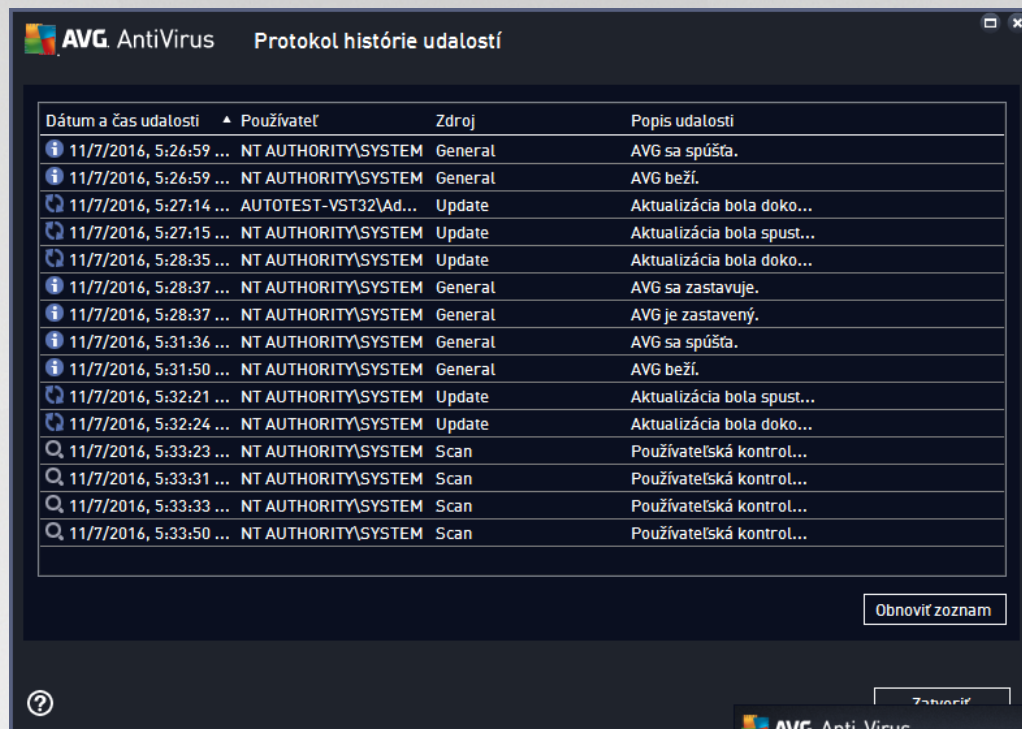
- **Názov hrozby** – popis (prípadne aj názov) zisteného objektu a jeho zdroj (webová stránka). Odkaz *Viac informácií* vás presmeruje na stránku v [online vírusovej encyklopédii](#), uvádzajúcu podrobné informácie o zistenej hrozbe.
- **Stav** – akcia vykonaná s detegovaným objektom
- **Čas detekcie** – dátum a čas detegovania a zablokovania hrozby
- **Typ objektu** – typ detegovaného objektu.

Ovládacie tlačidlá

- **Obnoviť** – aktualizuje sa zoznam nálezov zistených **Webovým štítom**.
- **Exportovať** – exportuje celý zoznam zistených objektov do súboru.
- – ak si želáte prepnúť naspäť na predvolené [hlavné dialógové okno AVG](#) (*prehľad súčasti*), použijete šípku v ľavom hornom rohu tohto dialógového okna



11.6. Protokol histórie udalostí



Dialógové okno **História udalostí** sa nachádza v ponuke **Možnosti/História/História udalostí** v hornom navigačnom pruhu hlavného okna programu **AVG AntiVirus**. V tejto časti nájdete zhrnutie významných udalostí, ktoré sa vyskytli počas **AVG AntiVirus** prevádzky. Toto okno obsahuje záznamy týchto typov udalostí: informácie o aktualizáciách aplikácie AVG; informácie o spustení, ukončení alebo zastavení kontroly (vrátane automaticky vykonávaných testov); informácie o udalostiach týkajúcich sa detekcie vírusov (či už *Rezidentným štítom* alebo kontrolou) vrátane miesta výskytu; a ďalšie dôležité udalosti.

Každá udalosť má uvedené tieto informácie:

- **Dátum a čas udalosti** informuje o presnom dátume a čase výskytu udalosti.
- **Používateľ** uvádza názov aktuálne prihláseného používateľa v čase výskytu udalosti.
- **Zdroj** poskytuje informácie o zdrojovej súčasti alebo inej časti systému AVG, ktorá spustila udalosť.
- **Popis udalosti** obsahuje stručný prehľad o tom, čo sa v skutočnosti udialo.

Ovládacie tlačidlá

- **Obnoviť zoznam** – stlačením tohto tlačidla aktualizujete všetky položky v zozname udalostí
- **Zatvoriť** – stlačením tohto tlačidla sa vrátite do hlavného okna **AVG AntiVirus**



12. Aktualizácie AVG

Žiadny bezpečnostný softvér nedokáže zaručiť skutočnú ochranu pred rôznymi typmi hrozieb, ak sa pravidelne neaktualizuje! Autori vírusov stále hľadajú nové trhlíny, 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. Vzhľadom na všetky nové počítačové hrozby a rýchlosť, akou sa šíria, je mimoriadne dôležité pravidelne aktualizovať **AVG AntiVirus**. Najlepším riešením je ponechať predvolené nastavenia programu, v ktorých sú nastavené automatické aktualizácie. Nezabudnite, že bez aktuálnej vírusovej databázy **AVG AntiVirus** nemôže program zistiť najnovšie hrozby!

Pravidelná aktualizácia AVG je nevyhnutná! Dôležité aktualizácie vírusových definícií by sa mali uskutočniť denne, ak to je možné. Menej naliehavé programové aktualizácie sa môžu uskutočniť raz za týždeň.

V záujme maximálneho využitia dostupného zabezpečenia je **AVG AntiVirus** predvolene nastavený tak, aby hľadal nové aktualizácie vírusovej databázy každé dve hodiny. Keďže sa aktualizácie AVG nezverejňujú podľa pevného harmonogramu, ale podľa počtu a závažnosti nových hrozieb, je táto kontrola veľmi dôležitá na zaistenie neustálej aktuálnosti vírusovej databázy AVG.

Ak chcete skontrolovať nové aktualizáčnne súbory okamžite, môžete tak urobiť pomocou rýchleho odkazu [Aktualizovať teraz](#) v hlavnom používateľskom rozhraní. Tento odkaz sa nachádza v každom dialógovom okne [používateľského rozhrania](#). Keď spustíte aktualizáciu, AVG najskôr overí, či sú dostupné nové aktualizáčnne súbory. Ak áno, **AVG AntiVirus** ich začne sťahovať a spustí samotný proces aktualizácie. O výsledkoch aktualizácie budete informovaní v oznámení nad ikonou AVG v paneli úloh.

Ak chcete znížiť počet spustení aktualizácie, môžete tak urobiť pomocou vlastných parametrov spúšťania aktualizácie. **Dôrazne sa však odporúča spúšťať aktualizáciu aspoň raz denne!** Konfiguráciu môžete upraviť v časti [Rozšírené nastavenia/Plány](#), konkrétne v nasledovných dialógových oknách:

- [Plán aktualizácie definícií](#)



13. Najčastejšie otázky a technická podpora

V prípade nákupných alebo technických problémov s aplikáciou **AVG AntiVirus** existuje niekoľko spôsobov, ako nájsť pomoc. Vyberte si z týchto možností:

- **Získajte podporu** – priamo v aplikácii AVG sa môžete dostať na špeciálnu webovú lokalitu zákazníckej podpory AVG (<http://www.avg.com/>). V hlavnej ponuke vyberte možnosť **Pomocník/Získajte podporu** a ocitnete sa na webovej lokalite AVG s miestami podpory. Ak chcete pokračovať, postupujte podľa pokynov na webovej lokalite.
- **Podpora** (odkaz v hlavnej ponuke) – ponuka aplikácie AVG (v hornej časti hlavného používateľského rozhrania) obsahuje prepojenie **Podpora**, pomocou ktorého otvoríte nové dialógové okno so všetkými typmi údajov, ktoré môžete pri hľadaní pomoci potrebovať. Dialógové okno obsahuje základné údaje o nainštalovanom programe AVG (verzia programu/databázy), podrobnosti o licencií a zoznam rýchlych prepojení podpory.
- **Riešenie problémov v súbore pomocníka** – nová časť **Riešenie problémov** je k dispozícii priamo v súbore pomocníka v produkte **AVG AntiVirus** (súbor pomocníka otvoríte stlačením klávesu **F1** v niektorom z dialógových okien aplikácie). V tejto časti nájdete zoznam najčastejších situácií, v ktorých používateľ potrebuje vyhľadať profesionálnu pomoc pre technický problém. Vyberte situáciu, ktorá najviac zodpovedá vášmu problému, a kliknutím zobrazte podrobné pokyny vedúce k riešeniu daného problému.
- **Webové stredisko podpory AVG** – riešenie problému môžete vyhľadať aj na webovej lokalite AVG (<http://www.avg.com/>). V časti **Podpora** nájdete prehľad tematických skupín zaoberajúcich sa predajom aj technickými otázkami, štruktúrovanú časť častých otázok a všetky dostupné kontakty.
- **AVG ThreatLabs** – osobitná webová stránka spojená s programom AVG (<http://www.avg.com/about-viruses>) venovaná problémom s vírusmi, ktorá poskytuje štruktúrovaný prehľad informácií súvisiacich s hrozbami on-line. Môžete tiež nájsť pokyny na odstraňovanie vírusov spyware a tipov na zachovanie ochrany.
- **Diskusné fórum** – môžete využiť aj diskusné fórum používateľov produktov AVG na adrese <http://community.avg.com/>.