AVG 9 Internet Security

Podrecznik uzytkownika

Wersja dokumentu 90.21 (3.2.2010)

Spis tresci

1. Wprowadzenie

Ten podrecznik uzytkownika zawiera kompleksowa dokumentacje systemu **AVG 9 Internet Security**.

Gratulujemy zakupu systemu AVG 9 Internet Security!

System **AVG 9 Internet Security** nalezy do linii uznanych i nagradzanych produktów AVG, które zapewniaja uzytkownikom spokój ducha, a ich komputerom — pelne bezpieczenstwo. Podobnie jak pozostale produkty system **AVG 9 Internet Security** zaprojektowano od podstaw pod katem zapewnienia slynnego juz poziomu ochrony w nowy, bardziej przyjazny dla uzytkownika sposób.

Nowy produkt **AVG 9 Internet Security** laczy ulepszony interfejs z agresywniejszym i szybszym skanowaniem. Dla wygody uzytkownika zautomatyzowano najczesciej uzywane funkcje i dodano nowe, „inteligentne" opcje, które pozwalaja precyzyjnie dostosowac funkcje ochronne programu do swoich potrzeb. Koniec z poswiecaniem wydajnosci na rzecz ochrony!

System AVG zaprojektowano i zbudowano tak, by chronil uzytkownika podczas pracy na komputerze i w sieci. Ciesz sie pelna ochrona AVG.

2. Wymagania instalacyjne AVG

2.1. Obslugiwane systemy operacyjne

System **AVG 9 Internet Security** sluzy do ochrony stacji roboczych dzialajacych pod nastepujacymi systemami operacyjnymi:

- Windows 2000 Professional z dodatkiem SP4 + pakiet zbiorczy aktualizacji 1
- Windows XP Home Edition z dodatkiem SP2
- Windows XP Professional z dodatkiem SP2
- Windows XP Professional x64 Edition z dodatkiem SP1
- Windows Vista (x86 i x64, wszystkie edycje)
- Windows 7 (x86 i x64, wszystkie edycje)

(a takze z nowszymi dodatkami SP dla niektórych systemów operacyjnych)

***Uwaga**: Skladnik ID Protection nie jest obslugiwany przez systemy Windows 2000 i XP x64. Dla tych systemów operacyjnych mozna zainstalowac systemAVG 9 Internet Security tylko bez skladnika IDP.*

2.2. Minimalne i zalecane wymagania sprzetowe

Minimalne wymagania sprzetowe dla systemu **AVG 9 Internet Security**:

- Procesor Intel Pentium 1,5 GHz
- 512 MB pamieci RAM.
- 390 MB wolnego miejsca na dysku twardym (w celu instalacji),

Zalecane wymagania sprzetowe dla systemu **AVG 9 Internet Security**:

- Procesor Intel Pentium 1,8 GHz
- 512 MB pamieci RAM.

- 510 MB wolnego miejsca na dysku twardym (w celu instalacji),

3. Opcje instalacji systemu AVG

System AVG mozna zainstalowac za pomoca instalatora znajdujacego sie na oryginalnym dysku CD lub pobranego z witryny firmy AVG (http://www.avg.com/).

Przed rozpoczeciem instalacji systemu AVG zalecamy odwiedzenie naszej witryny (http://www.avg.com/) w celu sprawdzenia, czy jest dostepny nowy plik instalacyjny. Dzieki temu mozesz miec pewnosc, ze instalujesz najnowsza dostepna wersje systemu AVG 9 Internet Security.

Polecamy wypróbowanie nowego programu AVG Download Manager — narzedzia, które pomoze skonfigurowac plik instalacyjny w zadanym jezyku.

Podczas samego procesu instalacji konieczne bedzie podanie numeru licencji/ sprzedazy. Nalezy wiec przygotowac go przed rozpoczeciem instalacji. Numer sprzedazy znajduje sie na opakowaniu dysku CD. W przypadku zakupienia pakietu AVG przez internet, numer licencji dostarczany jest poprzez e-mail.

4. AVG Download Manager

Program **AVG Download Manager** to proste narzedzie, które pomaga w wyborze odpowiedniego pliku instalacyjnego próbnej wersji danego produktu AVG. Na podstawie wprowadzonych przez uzytkownika informacji, menedzer wybierze odpowiedni produkt, typ licencji, zestaw skladników i jezyk. Na koniec program **AVG Download Manager** pobierze odpowiednie pliki i rozpocznie proces instalacji.

Ostrzezenie: *Program AVG Download Manager nie jest odpowiedni do pobierania wersji sieciowych oraz SBS i obsluguje tylko nastepujace systemy operacyjne: Windows 2000 (SP4 + pakiet zbiorczy SRP), Windows XP, Windows Vista i Windows 7.*

Program **AVG Download Manager** mozna pobrac ze strony internetowej firmy AVG dostepnej pod adresem http://www.avg.com/). Ponizej znajduje sie krótki opis kazdego wymaganego kroku w oknie programu **AVG Download Manager**:

4.1. Wybór jezyka

W pierwszym kroku wyswietlanym w programie **AVG Download Manager** nalezy z rozwijanego menu wybrac jezyk instalacji. Nalezy pamietac, ze wybór ten dotyczy tylko procesu instalacji; po jej zakonczeniu jezyk programu bedzie mozna zmienic bezposrednio w jego ustawieniach. Aby kontynuowac, kliknij przycisk ***Dalej***.

4.2. Test polaczenia

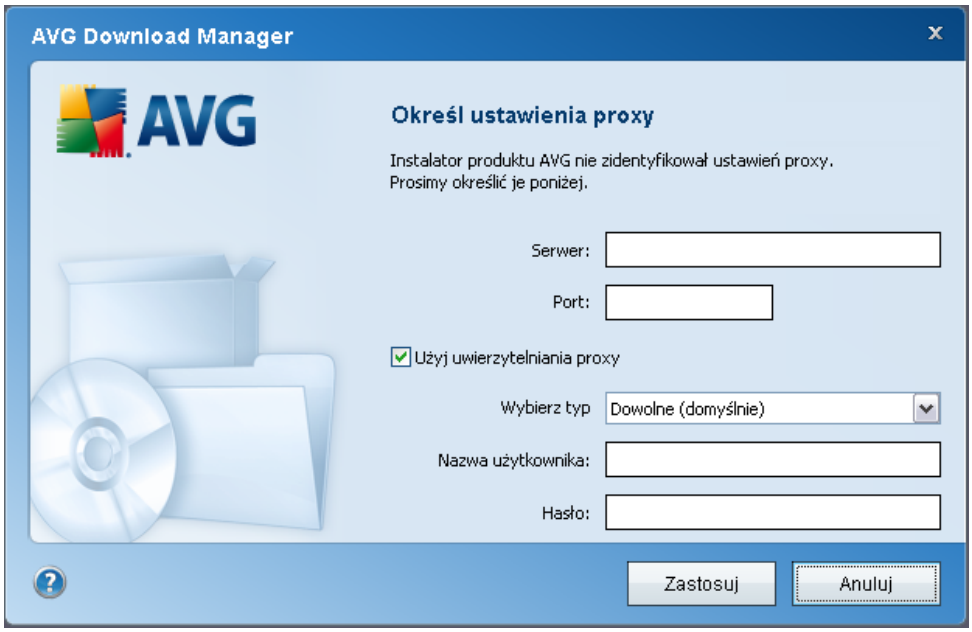
W nastepnym kroku program **AVG Download Manager** spróbuje nawiazac polaczenie internetowe, aby mozna bylo znalezc aktualizacje. Przejscie do procesu aktualizacji nie bedzie mozliwe, dopóki program **AVG Download Manager** nie zakonczy testu polaczenia.

- Jesli test wykaze brak lacznosci, nalezy upewnic sie, ze komputer jest faktycznie polaczony z internetem. Aby ponowic próbe, kliknij przycisk ***Powtórz***

- Jesli uzywasz serwera proxy, kliknij przycisk ***Ustawienia proxy*** i wprowadz wymagane informacje:

- Jesli test wypadl pomyslnie, kliknij przycisk ***Dalej***, aby kontynuowac.

4.3. Ustawienia proxy

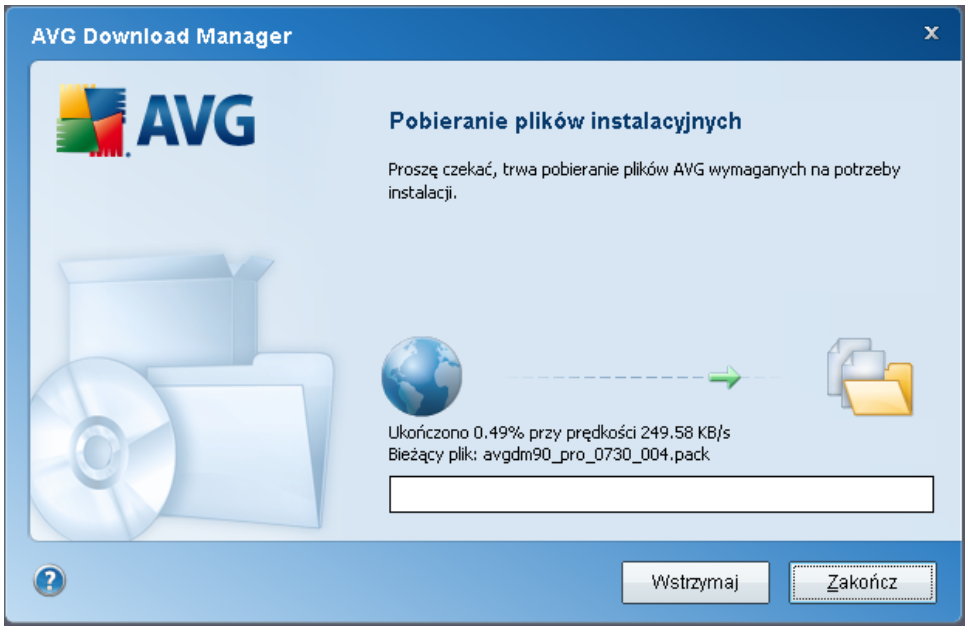


Jesli program **AVG Download Manager** nie moze zidentyfikowac ustawien proxy, trzeba okreslic je recznie. Podaj nastepujace informacje:

- ***Serwer*** — prawidlowa nazwa lub adres IP serwera proxy.
- ***Port*** — odpowiedni numer portu.
- ***Uzyj uwierzytelniania proxy*** — zaznacz to pole, jesli Twój serwer proxy wymaga uwierzytelniania.
- ***Wybierz typ uwierzytelniania*** — wybierz z listy rozwijanej typ uwierzytelniania. Stanowczo zalecamy, aby zachowac wartosc domyslna (*serwer sam poda swoje wymagania*). Doswiadczeni uzytkownicy moga jednak wybrac opcje "Podstawowe" (*wymagane przez niektóre serwery*) lub "NTLM" (*wymagane przez wszystkie serwery ISA*). Nastepnie podaj prawidlowa ***Nazwe uzytkownika*** i ***Haslo*** (opcjonalnie).

Po potwierdzeniu ustawien za pomoca przycisku ***Zastosuj*** program **AVG Download Manager** automatycznie przejdzie do nastepnego kroku.

4.4. Pobieranie plików instalacyjnych



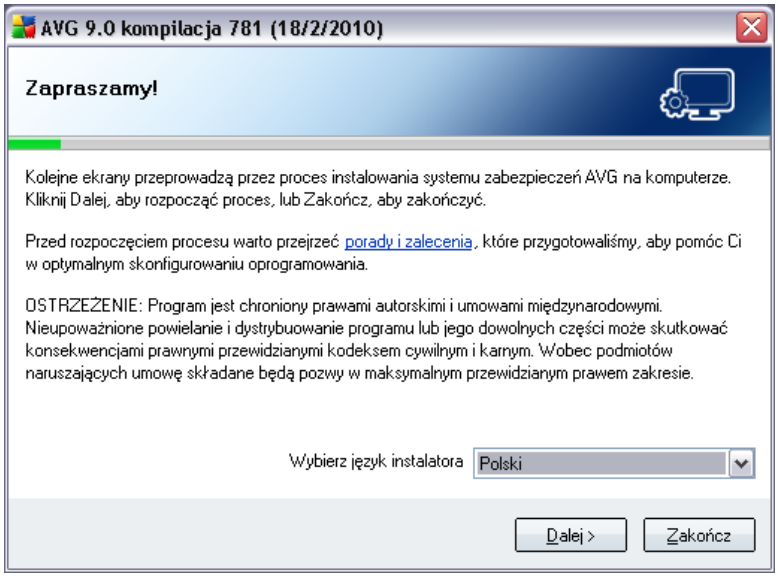
Podano juz wszystkie informacje, których program **AVG Download Manager** potrzebuje do pobrania pakietów instalacyjnych i uruchomienia instalacji. Teraz mozna rozpoczac instalacje systemu AVG.

5. Proces instalacji systemu AVG

Do zainstalowania systemu **AVG 9 Internet Security** na komputerze konieczny jest najnowszy plik instalacyjny. Mozna znalezc go na dysku CD bedacym czescia dystrybucyjnej edycji programu - istnieje jednak w tym wypadku ryzyko, ze bedzie on nieaktualny. Dlatego zaleca sie pobranie najnowszego pliku instalacyjnego z internetu. Mozna go pobrac na stronie internetowej firmy AVG (http://www.avg.com/) w sekcji ***Pomoc techniczna / Pobierz***. Mozna również uzyc nowego narzedzia ***AVG Download Manager***, które pomaga wybrac odpowiedni pakiet instalacyjny i automatycznie uruchamia proces instalacji.

Instalacja to sekwencja okien dialogowych zawierajacych krótkie opisy poszczególnych etapów. Ponizej znajduja sie objasnienia kazdego z nich:

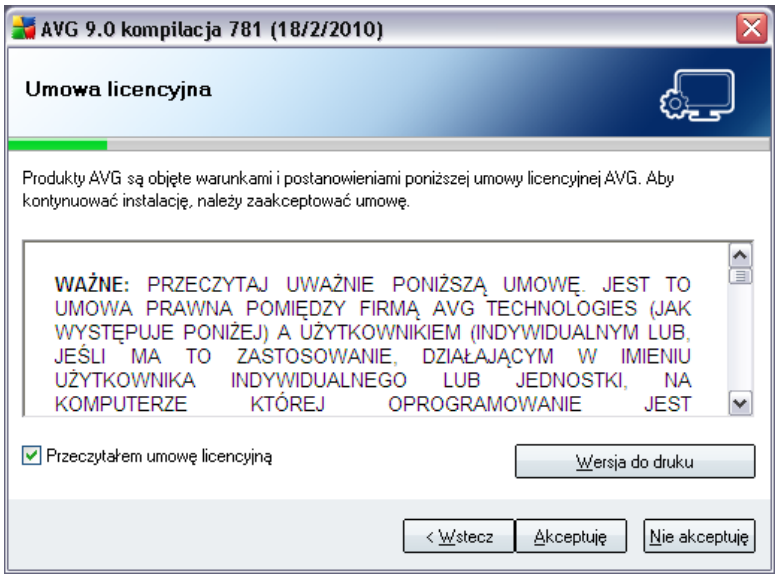
5.1. Uruchamianie instalacji



Proces instalacji rozpoczyna okno ***Witamy w instalatorze AVG***. Mozna w nim wskazac jezyk, który ma byc uzywany podczas instalacji. W dolnej czesci okna znajdziesz menu ***Wybierz jezyk instalatora***. Kliknij przycisk ***Dalej***, aby potwierdzic wybór i przejsc do kolejnego ekranu.

Uwaga: *W tym miejscu wybierany jest tylko jezyk instalatora. Nie jest to jezyk samego systemu AVG — ten zostanie wybrany na dalszym etapie instalacji.*

5.2. Umowa licencyjna



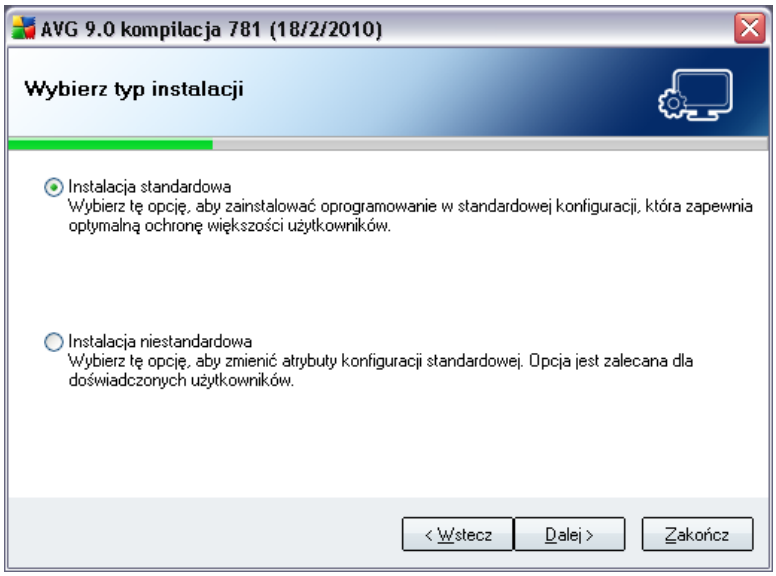
Okno dialogowe ***Umowa licencyjna*** zawiera pelna tresc umowy licencyjnej AVG. Przeczytaj ja uwaznie i potwierdz jej akceptacje, zaznaczajac pole ***Przeczytalem warunki umowy licencyjnej*** i wciskajac przycisk ***Dalej***.

Jesli nie zgadzasz sie na postanowienia umowy, kliknij przycisk ***Nie akceptuje***; instalacja zostanie natychmiast przerwana.

5.3. Sprawdzanie stanu systemu

Po potwierdzeniu umowy licencyjnej nastapi przekierowanie do okna ***Sprawdzanie stanu systemu***. W oknie tym nie trzeba wykonywac zadnych czynnosci; system jest sprawdzany przed rozpoczeciem instalacji AVG. Nalezy poczekac na ukonczenie procesu; przejscie do kolejnego okna nastapi automatycznie.

5.4. Wybieranie typu instalacji



Okno dialogowe·***Wybierz typ instalacji*** daje mozliwosc wybrania jednej z dwóch opcji instalacji: ***standardowej*** lub ***niestandardowej.***

Wiekszosc uzytkowników zdecydowanie powinna wybrac opcje ***instalacji standardowej***, która pozwala zainstalowac system AVG w calkowicie zautomatyzowany sposób, z ustawieniami zdefiniowanymi przez dostawce oprogramowania AVG. Taka konfiguracja zapewnia maksymalne bezpieczenstwo oraz optymalne wykorzystanie zasobów. Jesli w przyszlosci zajdzie potrzeba zmiany konfiguracji, mozna bedzie to zrobic bezposrednio z poziomu interfejsu AVG.

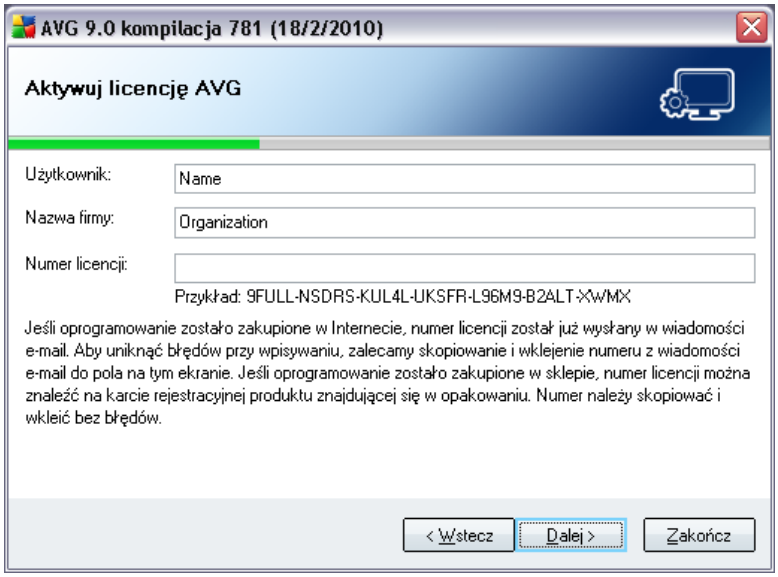
Instalacje niestandardowa powinni wybierac tylko doswiadczeni uzytkownicy, którzy maja uzasadnione powody, aby nie instalowac systemu AVG z domyslnymi ustawieniami, tj. na przyklad po to, aby dostosowac go do specyficznych wymagan systemowych.

5.5. Uaktywnienie licencji AVG

W oknie dialogowym ***Aktywacja licencji AVG*** nalezy wprowadzic swoje dane rejestracyjne. W polu ***Nazwa uzytkownika*** wprowadz swoje imie i nazwisko, a w polu ***Nazwa firmy*** — nazwe organizacji.

Nastepnie wprowadz numer licencji (lub numer sprzedazy) w polu tekstowym ***Numer licencji***. Numer sprzedazy mozna znalezc na opakowaniu dysku CD z

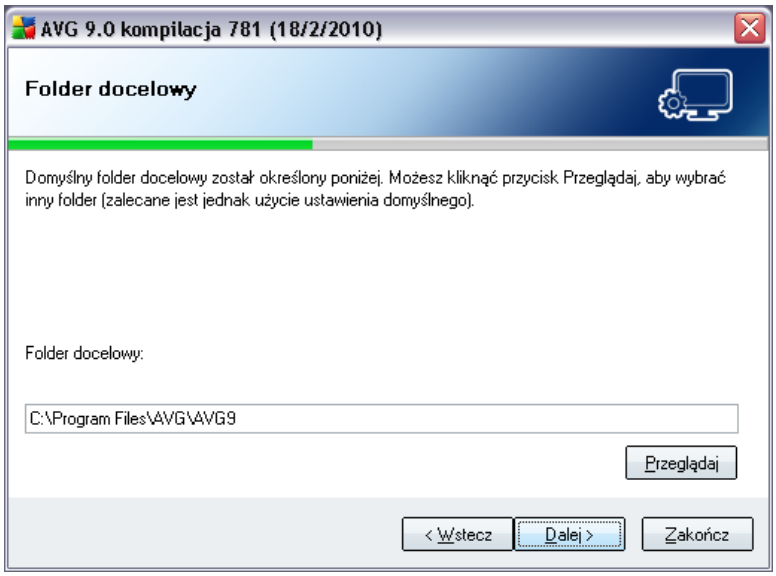
oprogramowaniem **AVG 9 Internet Security**. Numer licencji jest wysylany za posrednictwem poczty e-mail po dokonaniu zakupu oprogramowania **AVG 9 Internet Security**online. Wazne jest dokladne wprowadzenie wspomnianego numeru. Jesli numer jest dostepny w formie cyfrowej (*w wiadomosci e-mail*), zaleca sie skopiowanie go i wklejenie w odpowiednim polu.



Aby kontynuowac instalacje, kliknij przycisk ***Dalej***.

Jesli w poprzednim kroku zostala wybrana instalacja standardowa, nastapi przekierowanie bezposrednio do okna ***Pasek narzedzi AVG Security Toolbar***. Jesli zostala wybrana instalacja niestandardowa, zostanie wyswietlone okno ***Folder docelowy***.

5.6. Instalacja niestandardowa — Folder docelowy

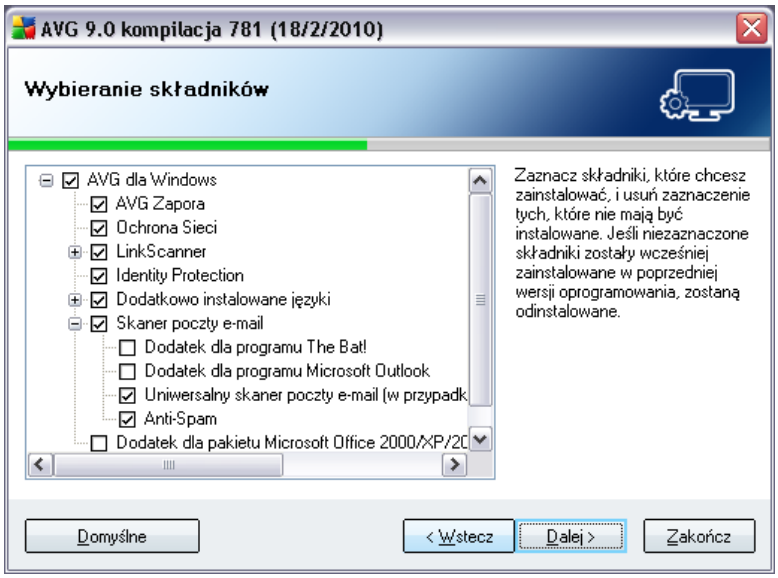


Okno dialogowe ***Folder docelowy*** umozliwia okreslenie lokalizacji, w której system **AVG 9 Internet Security** ma zostac zainstalowany. Domyslnie pakiet AVG jest instalowany w folderze "Program Files" na dysku C:. Jesli wybrany folder nie istnieje, zostanie wyswietlone nowe okno dialogowe z pytaniem o zgode na jego utworzenie.

Aby zmienic te lokalizacje, kliknij przycisk ***Przegladaj*** i w wyswietlonym oknie wybierz odpowiedni folder.

Kliknij przycisk ***Dalej***, aby potwierdzic wybór.

5.7. Instalacja niestandardowa — Wybór skladników



Okno dialogowe ***Wybór składników*** zawiera przeglad mozliwych do zainstalowania skladników systemu**AVG 9 Internet Security**. Jesli ustawienia domyslne nie sa dla Ciebie odpowiednie, mozesz dodac lub usunac zadane skladniki.

Wybierac mozna jednak tylko skladniki nalezace do zakupionej edycji systemu AVG. Tylko one beda widoczne w oknie dialogowym Wybór skladników!

- ***Wybór jezyka***

  Na tej samej liscie mozna takze zdefiniowac jezyk (lub jezyki) instalowanego systemu AVG. Nalezy w tym celu zaznaczyc opcje ***Dodatkowe zainstalowane jezyki*** i wybrac je z odpowiedniego menu.

- ***Pluginy skanera poczty e-mail***

  Wybranie pozycji ***Skaner poczty e-mail*** pozwala wskazac pluginy, które maja zostac zainstalowane w celu zapewnienia ochrony poczty elektronicznej. Domyslnie instalowany jest ***Plugin dla programu Microsoft Outlook***. Jesli zakupiona licencja uwzglednia skladnik ***Anti-Spam***, jego instalacja nastapi automatycznie.Inna opcja jest ***Dodatek dla programu The Bat!.*** W przypadku korzystania z innego klienta poczty e-mail (*MS Exchange, Qualcomm Eudora, ...*) nalezy wybrac ***Uniwersalny skaner poczty e-mail***, który chroni wiadomosci e-mail niezaleznie od uzywanego programu pocztowego.

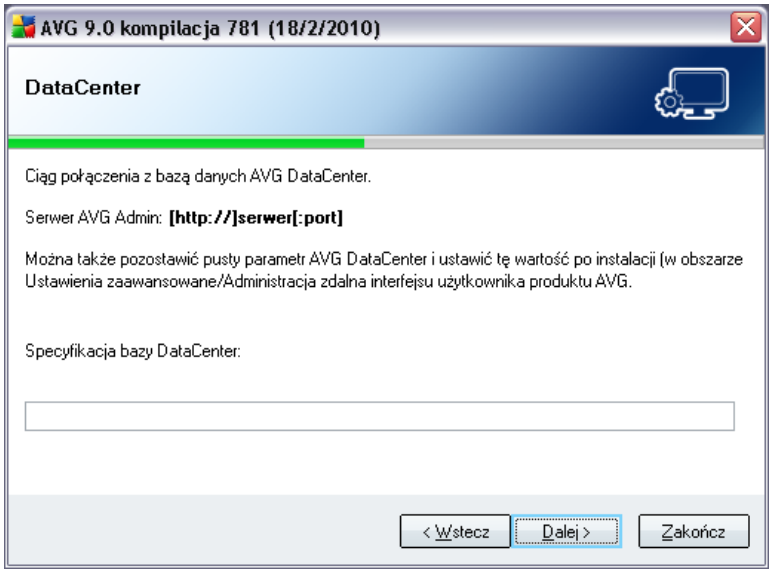
- ***Administracja zdalna***

  Jesli planujesz korzystac z Administracji zdalnej AVG, zaznacz takze odpowiednia pozycje na liscie.

Aby kontynuowac, kliknij przycisk ***Dalej***.

5.8. AVG DataCenter

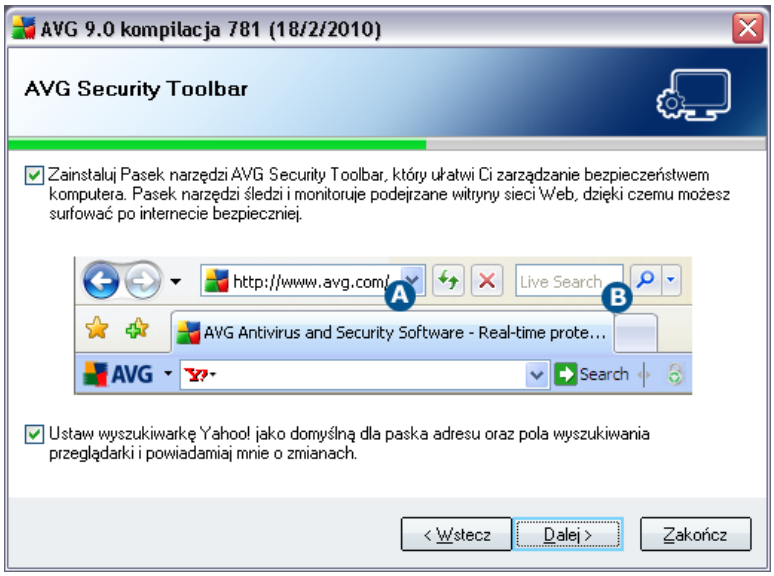
Jesli uzywasz sieciowej licencji systemu AVG i w poprzednim oknie dialogowym (***Instalacja niestandardowa — Wybór skladników***) wybrano do zainstalowania skladnik ***Administracja zdalna***, nalezy okreslic parametry bazy ***AVG DataCenter***:



W polu tekstowym ***Specyfikacja bazy AVG DataCenter*** podaj parametry polaczenia z baza ***AVG DataCenter*** (w formacie *serwer:port*). Jesli nie masz tych informacji, mozesz pozostawic to pole puste i dokonac konfiguracji później w oknie dialogowym ***Ustawienia zaawansowane / Administracja zdalna***.

Uwaga: *Szczególowe informacje dotyczace Administracji zdalnej systemu AVG mozna znalezc w podreczniku uzytkowania systemu AVG Network Edition; podrecznik mozna pobrac ze strony internetowej systemu AVG (http://www.avg.com/).*

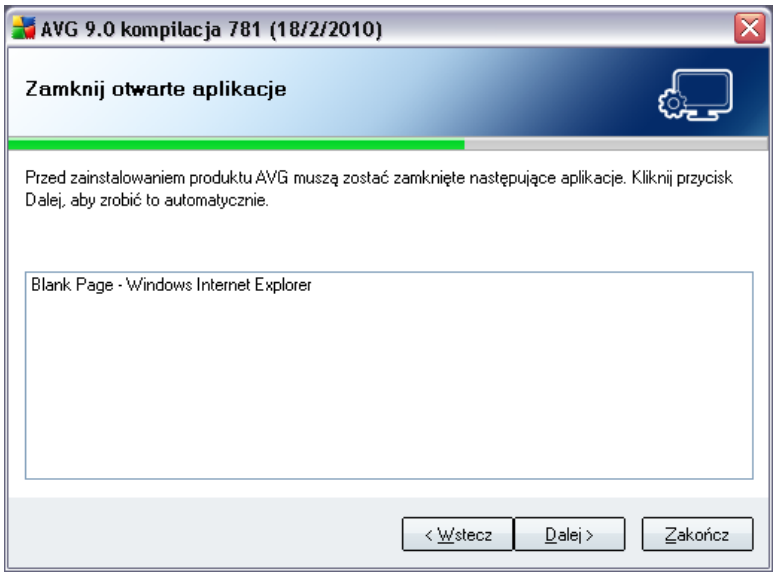
5.9. Pasek narzedzi AVG Security Toolbar



W oknie dialogowym ***Pasek narzedzi AVG Security Toolbar*** nalezy zdecydowac, czy ma zostac zainstalowany ***Pasek narzedzi AVG Security Toolbar*** (*sluzacy do weryfikacji wyników wyszukiwania zwracanych przez obslugiwane wyszukiwarki internetowe*). Jesli domyslne ustawienia nie zostana zmienione, skladnik zostanie automatycznie zainstalowany w przegladarce internetowej (*obecnie obslugiwane przegladarki to Microsoft Internet Explorer w wersji 6.0 i późniejszych i Mozilla Firefox w wersji 2.0 i późniejszych*), aby zapewnic kompleksowa ochrone podczas surfowania po internecie.

Mozna tam również zdecydowac, czy Yahoo! ma byc wyszukiwarka domyslna. Jesli tak, zaznacz odpowiednie pole wyboru.

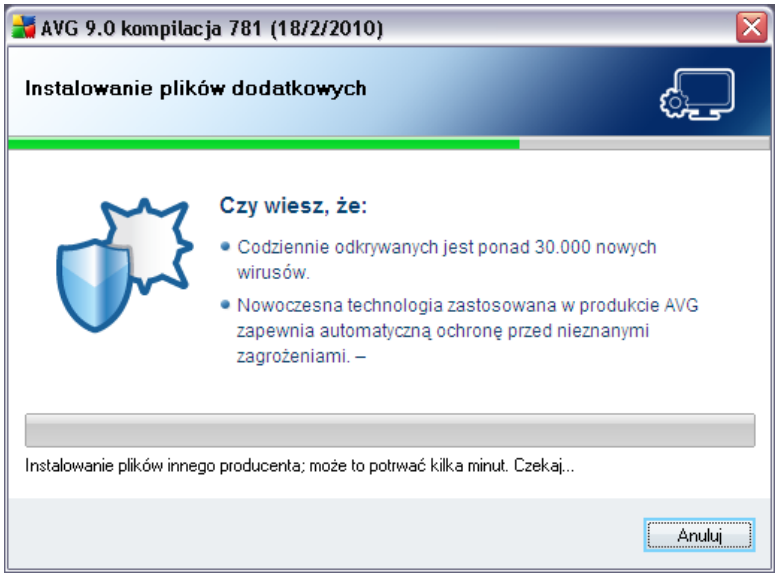
5.10. Zamknij otwarte aplikacje



Okno dialogowe ***Zamknij wszystkie otwarte aplikacje*** zostaje wyswietlone w trakcie procesu instalacji tylko wtedy, gdy na komputerze uruchomione sa równoczesnie inne programy, które moglyby zaklócac przebieg instalacji. Nastepnie zostaje wyswietlona lista programów, które musza zostac zamkniete, aby mozliwe bylo pomyslne zakonczenie procesu instalacji. Kliknij przycisk ***Dalej***, aby potwierdzic zamkniecie odpowiednich aplikacji i przejsc do nastepnego kroku.

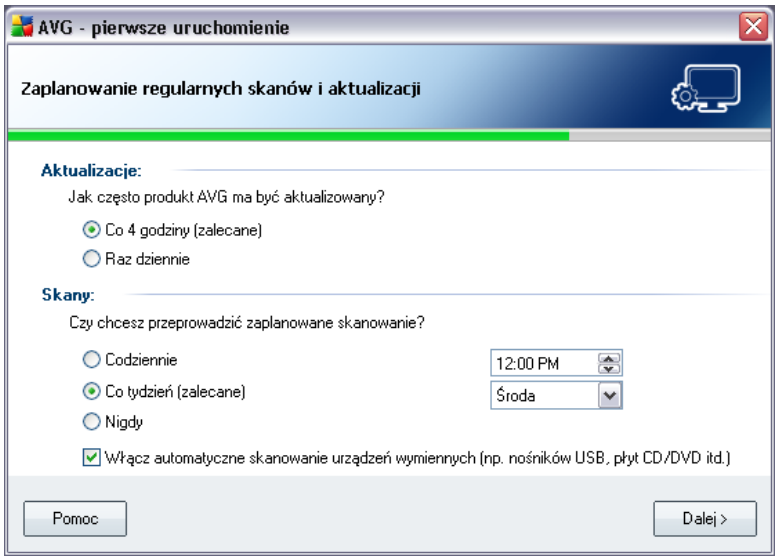
5.11. Instalowanie systemu AVG

Okno dialogowe ***Instalowanie systemu AVG*** zawiera informacje o postepie instalacji i nie wymaga dzialan ze strony uzytkownika:



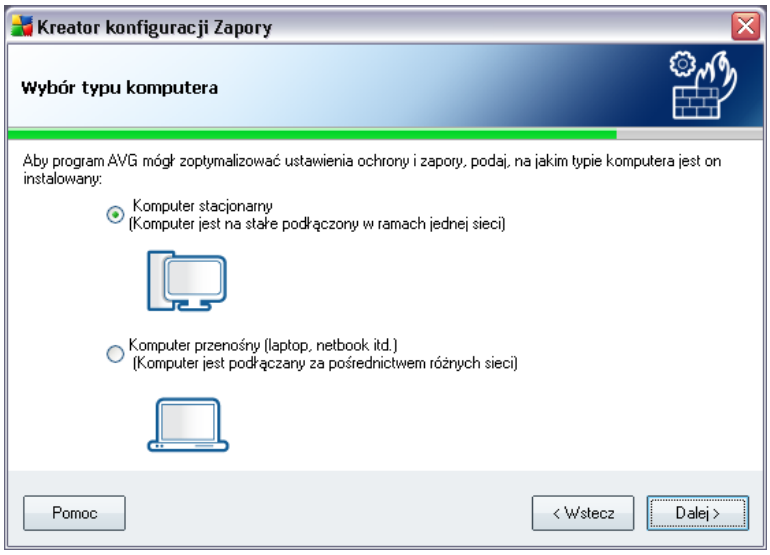
Po zakonczeniu instalacji automatycznie nastapi przekierowanie do nastepnego okna dialogowego.

5.12. Zaplanowanie regularnych skanów i aktualizacji



W oknie dialogowym ***Planowanie cyklicznych skanów i aktualizacji*** okreslic mozna czestotliwosc sprawdzania dostepnosci nowych plików aktualizacji i czasu, w którym nalezy uruchomic skan zaplanowany. Zaleca sie zachowanie wartosci domyslnych. Aby kontynuowac, kliknij przycisk ***Dalej***.

5.13. Wybór typu komputera



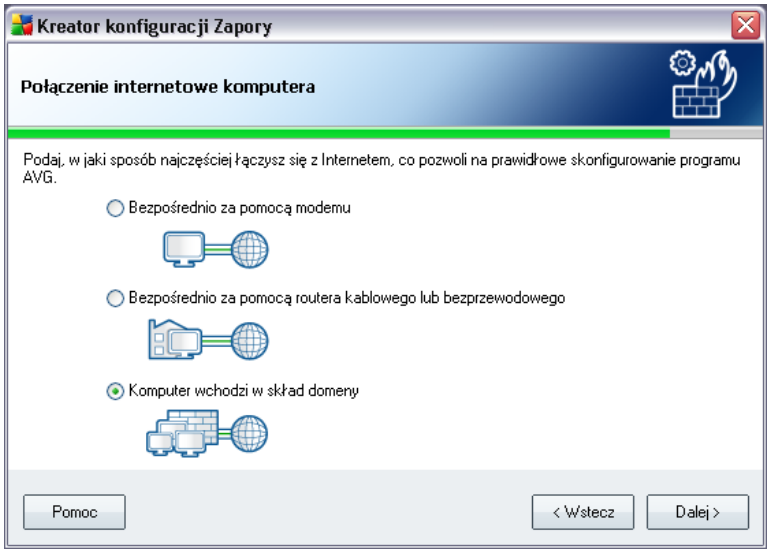
W tym oknie dialogowym ***Kreator konfiguracji skladnika Zapora*** zapyta o rodzaj uzywanego komputera. Na przyklad: notebook laczacy sie z internetem z wielu róznych lokalizacji (*lotniska, pokoje hotelowe itp.*) wymaga bardziej rygorystycznych regul zabezpieczen niz komputer pracujacy w domenie (*siec firmowa itp.*). Na podstawie wybranego sposobu uzytkowania komputera dobrany zostanie poziom bezpieczenstwa domyslnych regul ***Zapory.***

Dostepne sa tu dwie opcje:

- ***Komputer stacjonarny***
- ***Komputer przenosny***

Wybór nalezy potwierdzic kliknieciem przycisku ***Dalej***, co spowoduje przejscie do nastepnego okna dialogowego.

5.14. Polaczenie internetowe komputera



W tym oknie, ***Kreator konfiguracji Zapory*** wyswietla pytanie o sposób podlaczenia komputera do internetu. Domyslne reguly ***Zapory*** zostana dopasowane do poziomu zabezpieczen zapewnianych przez wybrany rodzaj polaczenia.

Dostepne sa tu trzy opcje:

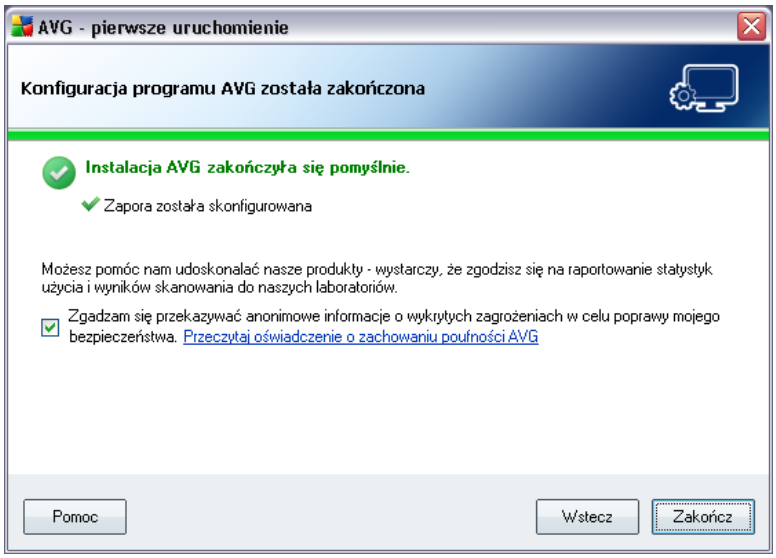
- ***Bezposrednio za pomoca modemu***

- ***Bezposrednio za pomoca routera kablowego lub bezprzewodowego***
- ***Komputer wchodzi w sklad domeny***

Wskaz, który typ polaczenia internetowego jest najbardziej zblizony do Twojego.

Wybór nalezy potwierdzic klknieciem przycisku ***Dalej***, co spowoduje przejscie do nastepnego okna dialogowego.

5.15. Zakonczenie konfiguracji ochrony produktu AVG



System**AVG 9 Internet Security** zostal skonfigurowany.

W tym oknie dialogowym nalezy wskazac, czy informacje o znalezionych zagrozeniach szkodliwych witrynach maja byc anonimowo przesylane do laboratorium wirusów AVG. Jesli tak, nalezy zaznaczyc opcje ***Zgadzam sie dostarczac ANONIMOWE informacje o wykrytych zagrozeniach, aby podniesc swój poziom ochrony***.

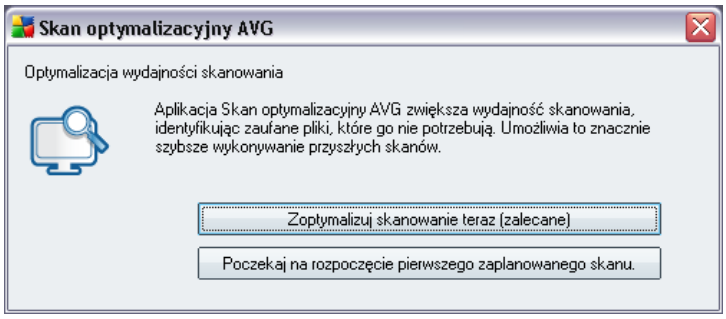
Na koniec nalezy wcisnac przycisk ***Zakoncz.*** Rozpoczecie pracy z systemem AVG moze wymagac ponownego uruchomienia komputera.

6. Po instalacji

6.1. Optymalizacja skanowania

Funkcja optymalizacji skanowania przeszukuje foldery *Windows* i *Program Files*w poszukiwaniu odpowiednich plików (*obecnie sa to pliki *.exe, *.dll i *.sys*) i zapisuje informacje o nich. Przy kolejnych próbach uzyskania dostepu do tych plików, nie beda one wiecej skanowane, dzieki czemu czasu skanowania ulegnie znacznemu skróceniu.

Po zakonczeniu procesu instalacji zostanie wyswietlone nowe okno dialogowe z opcja optymalizacji skanowania:



Zalecamy skorzystanie z tej opcji i uruchomienie procesu optymalizacji skanowania. W tym celu nalezy kliknac przycisk ***Optymalizuj skanowanie teraz***.

6.2. Rejestracja produktu

Po ukonczeniu instalacji systemu **AVG 9 Internet Security** nalezy zarejestrowac produkt online na stronie internetowej AVG (http://www.avg.com/) w sekcji ***Rejestracja*** (*postepujac zgodnie z wyswietlanymi tam instrukcjami*). Rejestracja umozliwia pelny dostep do konta uzytkownika AVG, biuletynu aktualizacji AVG i innych uslug oferowanych wylacznie zarejestrowanym klientom.

6.3. Dostep do Interfejsu uzytkownika

Dostep do ***interfejsu uzytkownika AVG*** mozna uzyskac na kilka sposobów:

- klikajac dwukrotnie ikone AVG na pasku zadan,
- klikajac dwukrotnie ikone AVG na pulpicie,

- z poziomu menu ***Start/Programy/AVG 9.0/Interfejs uzytkownika AVG.***

6.4. Skanowanie calego komputera

Istnieje pewne ryzyko, ze wirus dostal sie do komputera przed zainstalowaniem systemu **AVG 9 Internet Security**. Z tego powodu nalezy uruchomic test ***Skan calego komputera***, aby upewnic sie, ze jest on w pelni bezpieczny.

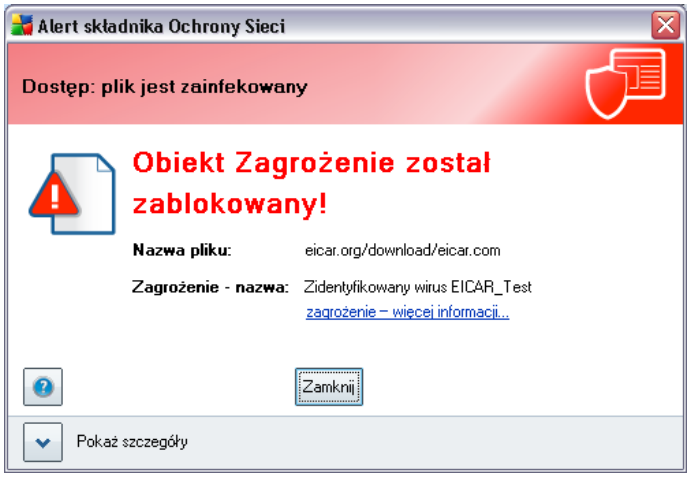
Instrukcje dotyczace uruchamiania testu ***Skan calego komputera*** zawiera rozdzial ***Skanowanie AVG***.

6.5. Test Eicar

Aby potwierdzic, ze system **AVG 9 Internet Security** zostal zainstalowany poprawnie, mozna przeprowadzic test EICAR.

Test EICAR jest standardowa i calkowicie bezpieczna metoda sluzaca do sprawdzania prawidlowosci dzialania systemu antywirusowego. Mozna go bezpiecznie rozpowszechniac, poniewaz nie jest prawdziwym wirusem i nie zawiera zadnych fragmentów zlosliwego kodu. Wiekszosc produktów rozpoznaje go jako wirusa (*chociaz zwykle zglasza go pod jednoznaczna nazwa, np. „EICAR-AV-Test”*). Wirusa EICAR mozna pobrac z witryny stowarzyszenia EICAR, dostepnej pod adresem www.eicar.com . Mozna tam równiez znalezc wszystkie niezbedne informacje na temat testu EICAR.

Spróbuj pobrac plik ***eicar.com*** i zapisac go na dysku twardym komputera. Natychmiast po rozpoczeciu pobierania pliku testowego, skladnik ***Ochrona Sieci*** zareaguje wyswietleniem ostrzezenia. Pojawienie sie komunikatu potwierdza, ze oprogramowanie AVG jest prawidlowo zainstalowane na komputerze.



Ze strony internetowej http://www.eicar.com mozna równiez pobrac skompresowana wersje "wirusa" EICAR (*w formie pliku eicar_com.zip*). ***Ochrona Sieci*** pozwoli pobrac ten plik i zapisac go na dysku, ale juz ***Ochrona rezydentna*** wykryje tego "wirusa" w chwili rozpakowywania go. **Jesli system AVG nie rozpozna pliku testowego EICAR jako wirusa, nalezy ponownie sprawdzic jego konfiguracje!**

6.6. Konfiguracja domyslna AVG

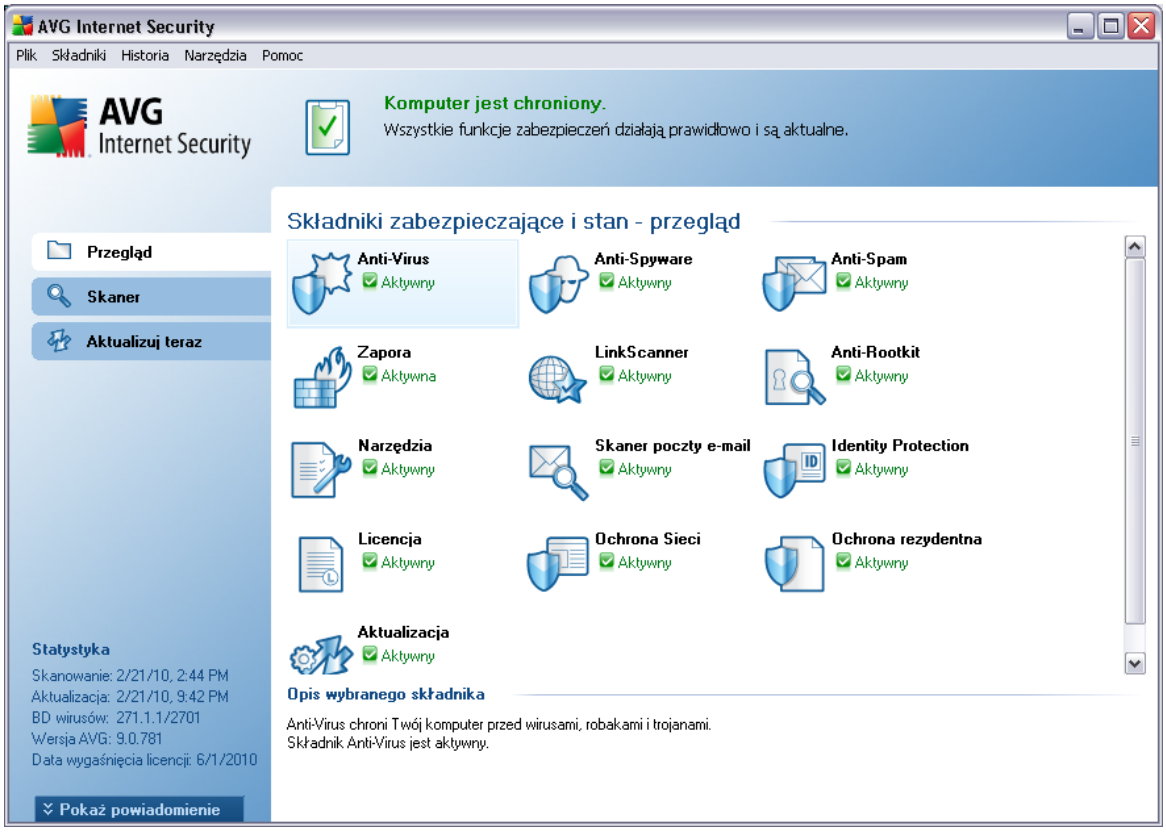
Konfiguracja domyslna (*ustawienia stosowane zaraz po instalacji*) systemu **AVG 9 Internet Security** jest wstepnie definiowana przez dostawce oprogramowania i ma na celu zapewnienie optymalnej wydajnosci wszystkich skladników i funkcji.

Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach! Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników.

Mniejsze zmiany ustawien skladników AVG mozna wprowadzac bezposrednio z ich interfejsu uzytkownika. Jesli konfiguracja systemu AVG powinna zostac lepiej dopasowana do potrzeb uzytkownika, nalezy przejsc do ***zaawansowanych ustawien systemu AVG***, wybierajac z menu systemowego pozycje ***Narzedzia/Ustawienia zaawansowane*** i edytujac opcje w otwartym oknie dialogowym ***Zaawansowane ustawienia AVG***.

7. Interfejs uzytkownika AVG

Otwarcie systemu **AVG 9 Internet Security** nastepuje w jego oknie głównym:



Okno główne jest podzielone na kilka sekcji:

- ***Menu główne*** *(górny wiersz okna)* to standardowe narzedzie nawigacyjne umozliwiajace dostep do wszystkich skladników, uslug i funkcji programu AVG — szczegóły >>
- ***Informacje o stanie bezpieczenstwa*** *(prawa czesc górnej sekcji okna)* zawiera informacje dotyczace biezacego stanu programu AVG — szczegóły >>
- ***Szybkie lacza*** *(lewa kolumna)* umozliwiaja uzyskanie szybkiego dostepu do najwazniejszych i najczesciej uzywanych funkcji programu AVG — szczegóły >>
- ***Przeglad skladników*** *(centralna czesc okna)* zawiera przeglad

zainstalowanych skladników programu AVG — szczegóły >>

- ***Statystyka*** *(lewa dolna sekcja okna)* zawiera najwazniejsze dane statystyczne dotyczace dzialania programu — szczegóły >>

- ***Ikona na pasku zadan*** *(prawy dolny róg ekranu, na pasku systemowym)* sygnalizuje biezacy stan programu AVG — szczegóły >>

7.1. Menu systemowe

Menu systemowe to standardowa metoda nawigacji we wszystkich aplikacjach w systemie Windows. Jest zlokalizowane horyzontalnie w górnej czesci glównego okna systemu **AVG 9 Internet Security**. Menu systemowe zapewnia dostep do poszczególnych skladników AVG, funkcji i uslug.

Menu systemowe jest podzielone na piec sekcji:

7.1.1. Plik

- ***Zakoncz*** — powoduje zamkniecie **AVG 9 Internet Security**interfejsu uzytkownika. System AVG dziala jednak w tle, a komputer jest nadal chroniony!

7.1.2. Skladniki

Pozycja ***Skladniki*** w menu glównym zawiera lacza do wszystkich zainstalowanych skladników systemu AVG; kliknieciе któregos z nich powoduje otwarcie domyslnego okna interfejsu odpowiedniego skladnika:

- ***Przeglad systemu*** — pozwala przelaczyc widok do domyslnego okna interfejsu uzytkownika systemu AVG, zawierajacego przeglad zainstalowanych skladników i ich stanu.

- ***Anti-Virus*** — otwiera domyslne okno interfejsu skladnika ***Anti-Virus***.

- ***Anti-Rootkit*** — otwiera domyslne okno interfejsu skladnika ***Anti-Rootkit***.

- ***Anti-Spyware*** — otwiera domyslne okno interfejsu skladnika ***Anti-Spyware***.

- ***Zapora*** — otwiera domyslne okno interfejsu skladnika ***Zapora***.

- ***Link Scanner —*** otwiera domyslne okno interfejsu skladnika ***Link Scanner***.

- ***Narzedzia systemowe —*** otwiera domyslne okno interfejsu skladnika ***Narzedzia systemowe.***

- ***Anti-Spam*** — otwiera domyslne okno interfejsu skladnika ***Anti-Spam***.
- ***Skaner poczty e-mail*** — otwiera domyslne okno interfejsu skladnika ***Skaner poczty e-mail***.
- ***ID Protection*** — otwiera domyslne okno interfejsu skladnika ***ID Protection*** .
- ***Licencja*** — otwiera domyslne okno interfejsu skladnika ***Licencja***.
- ***Ochrona Sieci*** — otwiera domyslne okno interfejsu skladnika ***Ochrona Sieci***.
- ***Ochrona rezydentna*** — otwiera domyslne okno interfejsu skladnika ***Ochrona rezydentna***.
- ***Menedzer aktualizacji*** — otwiera domyslne okno interfejsu ***Menedzera aktualizacji***.

7.1.3. Historia

- ***Wyniki skanowania*** — przelacza do interfejsu skanera AVG, konkretnie do okna dialogowego ***Przeglad wyników skanowania***
- ***Zagrozenia wykryte przez Ochrone rezydentna*** — powoduje otwarcie okna dialogowego zawierajacego przeglad zagrozen wykrytych przez skladnik ***Ochrona rezydentna***
- ***Zagrozenia wykryte przez Skaner poczty e-mail*** — otwiera okno dialogowe zawierajacego przeglad zalaczników e-mail uznanych za niebezpieczne przez skladnik ***Skaner poczty e-mail***.
- ***Zagrozenia wykryte przez Ochrone Sieci*** — otwiera okno dialogowe zawierajace przeglad zagrozen wykrytych przez skladnik ***Ochrone Sieci***
- ***Przechowalnia wirusów*** — powoduje otwarcie interfejsu ***Przechowalni wirusów***, do której program AVG przenosi wszystkie niemozliwe do wyleczenia infekcje. W czasie tej kwarantanny zainfekowane pliki sa izolowane i nie zagrazaja bezpieczenstwu komputera, a jednoczesnie istnieje mozliwosc ich naprawy w przyszlosci.
- ***Dziennik historii zdarzen*** — powoduje otwarcie interfejsu dziennika historii z przegladem wszystkich zarejestrowanych akcji **AVG 9 Internet Security** .
- ***Zapora*** — powoduje otwarcie karty ***Dzienniki*** (dostepnej równiez w Konfiguracji Zapory), która zawiera szczegółowy przeglad wszystkich dzialan tego skladnika

7.1.4. Narzedzia

- ***Skanuj komputer*** — przelacza do Interfejsu skanera AVGi uruchamia skanowanie calego komputera
- ***Skanuj wybrany folder*** — przelacza do Interfejsu skanera AVGi umozliwia zdefiniowanie (w ramach struktury katalogów i dysków) plików oraz folderów, które maja byc przeskanowane
- ***Skanuj plik*** □ umozliwia uruchomienie na zadanie testu pojedynczego pliku wybranego z drzewa katalogów.
- ***Aktualizuj*** □ automatycznie uruchamia proces aktualizacji systemu **AVG 9 Internet Security**
- ***Aktualizuj z katalogu*** — uruchamia proces aktualizacji korzystajac z pliku zlokalizowanego w okreslonym folderze na dysku lokalnym. Jednak ta opcja jest zalecana do uzytku jedynie w sytuacjach awaryjnych, np. gdy nie ma polaczenia z internetem (*komputer zostal zainfekowany i odlaczony od internetu, komputer jest podlaczony do sieci bez dostepu do internetu itp.*). W nowo otwartym oknie nalezy wskazac folder, w którym zostal wczesniej umieszczony plik aktualizacyjny i uruchomic proces.
- ***Ustawienia zaawansowane*** □ otwiera okno dialogowe ***Ustawienia zaawansowane systemu AVG***, w którym mozna edytowac konfiguracje systemu **AVG 9 Internet Security**. Na ogól zaleca sie zachowanie domyslnych ustawien zdefiniowanych przez producenta oprogramowania AVG.
- ***Ustawienia Zapory*** — otwiera okno zaawansowanej konfiguracji skladnika ***Zapora AVG***.

7.1.5. Pomoc

- ***Spis tresci*** — otwiera pliki pomocy systemu AVG.
- ***Uzyskaj pomoc online*** — otwiera witryne firmy AVG (http://www.avg.com/) na stronie centrum pomocy technicznej dla klientów.
- ***Strona Mój AVG*** — otwiera witryne systemu AVG (http://www.avg.com/).
- ***Informacje o wirusach i zagrozeniach*** — powoduje otwarcie ***Encyklopedii Wirusów*** online, w której znalezc mozna szczególowe informacje na temat znanych wirusów.
- ***Aktywuj ponownie*** — otwiera okno ***Aktywacja programu AVG*** zawierajace

dane wprowadzone na etapie ***personalizacja programu AVG*** (podczas procesu instalacji). W oknie tym mozna wprowadzic numer licencji w celu zastapienia numeru sprzedazy (*uzytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przyklad podczas uaktualnienia do nowego produktu AVG*).

- ***Zarejestruj teraz*** — laczy sie ze strona rejestracji w witrynie systemu AVG (http://www.avg.com/). Nalezy tam podac swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysluguje bezplatna pomoc techniczna.

Uwaga**: W przypadku korzystania z próbnej wersji systemu* **AVG 9 Internet Security**, *ostatnie dwie wyswietlone pozycje to* ***Kup teraz *i* ***Aktywuj***. *Umozliwiaja one uaktualnienie programu do jego pelnej wersji. W przypadku systemu* **AVG 9 Internet Security** *zainstalowanego z numerem sprzedazy, te pozycje to* ***Zarejestruj*** *i* ***Aktywuj***. *Wiecej informacji mozna znalezc sekcji Licencja niniejszej dokumentacji.*

- ***AVG — informacje*** — otwiera okno dialogowe ***Informacje***. Okno to sklada sie z pieciu kart zawierajacych informacje na temat nazwy programu, wersji silnika antywirusowego i jego bazy danych, systemu, umowy licencyjnej oraz danych kontaktowych firmy ***AVG Technologies CZ***.

7.2. Status bezpieczenstwa

Sekcja ***Informacje o stanie bezpieczenstwa*** znajduje sie w górnej czesci Interfejsu uzytkownika AVG. Znajdziesz tam informacje o biezacym stanie bezpieczenstwa systemu **AVG 9 Internet Security**. W obszarze tym moga byc wyswietlane nastepujace ikony:


Ikona zielona oznacza, ze system AVG jest w pelni funkcjonalny. Komputer jest calkowicie chroniony, bazy danych sa aktualne, a wszystkie zainstalowane skladniki dzialaja prawidlowo.


Ikona pomaranczowa oznacza, ze co najmniej jeden skladnik jest nieprawidlowo skonfigurowany; nalezy sprawdzic jego wlasciwosci i ustawienia. W systemie AVG nie wystapil jednak zaden problem krytyczny, a uzytkownik prawdopodobnie wylaczyl tylko z jakiegos powodu jeden lub wiecej skladników. System AVG nadal chroni komputer, nalezy jednak sprawdzic ustawienia skladnika, który zglasza problem. Jego nazwa jest wyswietlana w sekcji ***Informacje o stanie bezpieczenstwa***.

Ikona ta jest takze wyswietlana, gdy z jakiegos powodu stan bledu skladników ma byc ignorowany (*opcja "Ignoruj stan skladnika" jest dostepna po kliknieciu prawym przyciskiem ikony odpowiedniego skladnika w głównej sekcji okna AVG*). Uzycie tej opcji moze byc wskazane w okreslonych sytuacjach, ale stanowczo zaleca sie jak najszybsze ponowne wylaczenie opcji ***Ignoruj stan skladnika***.

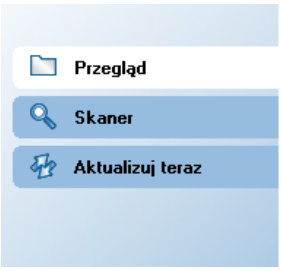

Ikona czerwona oznacza, ze stan systemu AVG jest krytyczny! Jeden lub wiecej skladników nie dziala, a system AVG nie moze chronic komputera. Nalezy natychmiast usunac zgloszony problem. Jesli nie jest to mozliwe, nalezy skontaktowac sie z zespolem Pomocy Technicznej AVG.

Stanowczo zaleca sie reagowanie na zmiany ***Statusu Bezpieczenstwa*** i natychmiastowe rozwiazywanie ewentualnych problemów. Brak reakcji naraza komputer na powazne zagrozenia!

Uwaga: *Dostep do informacji o stanie systemu AVG zapewnia przez caly czas również ikona na pasku zadan.*

7.3. Linki

Szybkie linki *(z lewej strony interfejsu uzytkownika AVG)* pozwalaja natychmiast uzyskiwac dostep do najwazniejszych i najczesciej uzywanych funkcji systemu AVG:



- ***Przeglad*** — pozwala przelaczac miedzy biezacym interfejsem AVG a interfejsem domyslnym, zawierajacym przeglad wszystkich zainstalowanych skladników - zobacz rozdzial ***Przeglad skladników >>***
- ***Skaner*** — otwiera interfejs skanowania AVG, w którym mozna uruchamiac test, planowac skany i edytowac ich parametry (zobacz rozdzial ***Skanowanie AVG >>***
- ***Aktualizuj teraz*** — otwiera odpowiedni interfejs i uruchamia proces aktualizacji systemu AVG (zobacz rozdzial ***Aktualizacje AVG >>***

Linki te sa dostepne przez caly czas. Klikniecie jednego z nich w celu uruchomienia okreslonego procesu powoduje wyswietlenie innego okna dialogowego, ale sama sekcja linków nie ulegnie zmianie. Uruchomiony proces zostal dodatkowo przedstawiony w formie graficznej.

7.4. Przeglad skladników

Sekcja ***Przeglad skladników*** znajduje sie w srodkowej czesci interfejsu uzytkownika AVG. Obszar ten podzielony jest na dwie czesci:

- Przeglad wszystkich zainstalowanych skladników (panel z odpowiednimi ikonami oraz informacjami o tym, czy dany skladnik jest aktywny, czy nie)
- Opis wybranego skladnika.

Sekcja **Przeglad skladników** systemu ***AVG 9 Internet Security*** zawiera informacje o nastepujacych skladnikach:

- ***Anti-Virus*** — zapewnia ochrone przed wirusami, które moga zainfekowac komputer — szczegóły >>
- ***Anti-Spyware*** — skanuje uruchamiane aplikacje w tle — szczegóły >>
- ***Anti-Spam*** — sprawdza wszystkie przychodzace wiadomosci e-mail i oznacza niepozadana poczte jako SPAM — szczegóły >>
- ***Zapora*** — kontroluje wymiane danych z innymi komputerami w internecie lub sieci lokalnej — szczegóły >>
- ***LinkScanner*** — sprawdza wyniki wyszukiwania wyswietlane przez serwisy internetowe — szczegóły >>
- ***Anti-Rootkit*** — wykrywa programy i technologie próbujace ukryc w systemie szkodliwe oprogramowanie — szczegóły >>
- ***Narzedzia systemowe*** — oferuje szczególowe podsumowanie srodowiska AVG i informacji o systemie operacyjnym — szczegóły >>
- ***Skaner poczty e-mail*** — sprawdza wszystkie przychodzace i wychodzace wiadomosci e-mail w poszukiwaniu wirusów — szczegóły >>
- ***ID Protection*** — skladnik chroniacy przed zlosliwym oprogramowaniem wyspecjalizowany w zapobieganiu kradziezy cennych danych osobistych — szczegóły >>

- ***Licencja*** — wyswietla numer, typ i date wygasniecia licencji —szczegól >>
- ***Ochrona Sieci*** — skanuje wszystkie dane pobierane przez przegladarke internetowa — szczegóły >>
- ***Ochrona rezydentna*** — dziala w tle; skanuje pliki przy ich kopiowaniu, otwieraniu i zapisywaniu — szczegóły >>
- ***Menedzer aktualizacji*** — kontroluje wszystkie aktualizacje systemu AVG — szczegóły >>

Pojedyncze klikniecie ikony dowolnego skladnika powoduje podswietlenie go w sekcji przegladu. Jednoczesnie u dolu interfejsu uzytkownika pojawia sie opis funkcji wybranego skladnika. Dwukrotne klikniecie ikony powoduje otwarcie interfejsu konkretnego skladnika (z jego opcjami i statystykami).

Klikniecie prawym przyciskiem ikony skladnika powoduje otwarcie menu kontekstowego. Mozna w nim nie tylko otworzyc graficzny interfejs skladnika, ale takze wybrac opcje ***ignorowania stanu skladnika***. Opcje te nalezy wybrac, jesli stan bledu skladnika jest znany, ale z dowolnego powodu system AVG ma byc nadal uzywany, a uzytkownik nie ma byc ostrzegany za pomoca ikony na pasku zadan.

7.5. Statystyki

Obszar·***Statystyki*** znajduje sie w lewym dolnym rogu Interfejsu uzytkownika AVG. Sekcja ta zawiera szereg informacji o dzialaniu programu:

- ***Skanowanie*** — data ostatniego przeprowadzonego testu.
- ***Aktualizacja*** — data uruchomienia ostatniej aktualizacji.
- ***BD wirusów*** — aktualnie uzywana wersja bazy wirusów.
- ***Wersja AVG*** — zainstalowana wersja systemu AVG *(numer w formacie 9.0.xx, gdzie 9.0 to wersja linii produktów, a xx — numer kompilacji).*
- ***Data wygasniecia licencji*** — data wygasniecia licencji systemu AVG.

7.6. Ikona na pasku zadan

Ikona na pasku zadan (*na pasku zadan systemu Windows*) wskazuje obecny stan systemu **AVG 9 Internet Security**. Ikona ta jest zawsze widoczna, niezaleznie od tego, czy Interfejs uzytkownika AVG jest otwarty, czy tez nie.

Jesli ***ikona na pasku zadan*** jest kolorowa, wszystkie skladniki systemu AVG sa aktywne i w pelni funkcjonalne. Moze ona byc kolorowa takze wtedy, gdy system AVG zasygnalizowal bledy, ale uzytkownik akceptuje je i celowo ***ignoruje stan skladników*** .

Ikona z wykrzyknikiem wskazuje problem (*nieaktywny skladnik, stan bledu itp.*). W takim przypadku nalezy dwukrotnie kliknac ***ikone AVG***, aby otworzyc Interfejs uzytkownika i sprawdzic stan skladników.

Ikona na pasku zadan informuje równiez o biezacych aktywnosciach systemu AVG i mozliwych zmianach stanu programów (*np. automatyczne uruchomienie zaplanowanego skanowania lub aktualizacji, przelaczanie profilu Zapory, zmiane stanu skladnika, wystapienie stanu bledu, ...*) dzieki wyskakujacym okienkom wyswietlanym nad ikona AVG:

Dwukrotne klikniecie ***ikony na pasku zadan*** pozwala takze szybko, w dowolnym momencie uzyskac dostep do Interfejsu uzytkownika systemu AVG. Kliknięcie ***ikony na pasku zadan*** prawym przyciskiem myszy otwiera menu kontekstowe zawierajace nastepujace opcje:

- ***Otwórz Interfejs uzytkownika AVG*** — otwiera Interfejs uzytkownika.
- ***Aktualizuj*** — uruchamia natychmiastowa aktualizacje

8. Skladniki AVG

8.1. Anti-Virus

8.1.1. Zasady dzialania skladnika Anti-Virus

Silnik skanujacy programu antywirusowego skanuje wszystkie pliki i wykonywane na nich operacje (otwieranie, zamykanie itd.) w poszukiwaniu znanych wirusów. Kazdy wykryty wirus jest blokowany (aby nie mógl wykonywac zadnych szkodliwych dzialan), a nastepnie usuwany lub izolowany. Wiekszosc programów antywirusowych korzysta takze z analizy heurystycznej — pliki sa skanowane w poszukiwaniu charakterystycznych cech wirusów - tak zwanych sygnatur. Oznacza to, ze skaner antywirusowy moze wykryc nowe, nieznane dotad wirusy, jesli posiadaja one pewne popularne wlasciwosci.

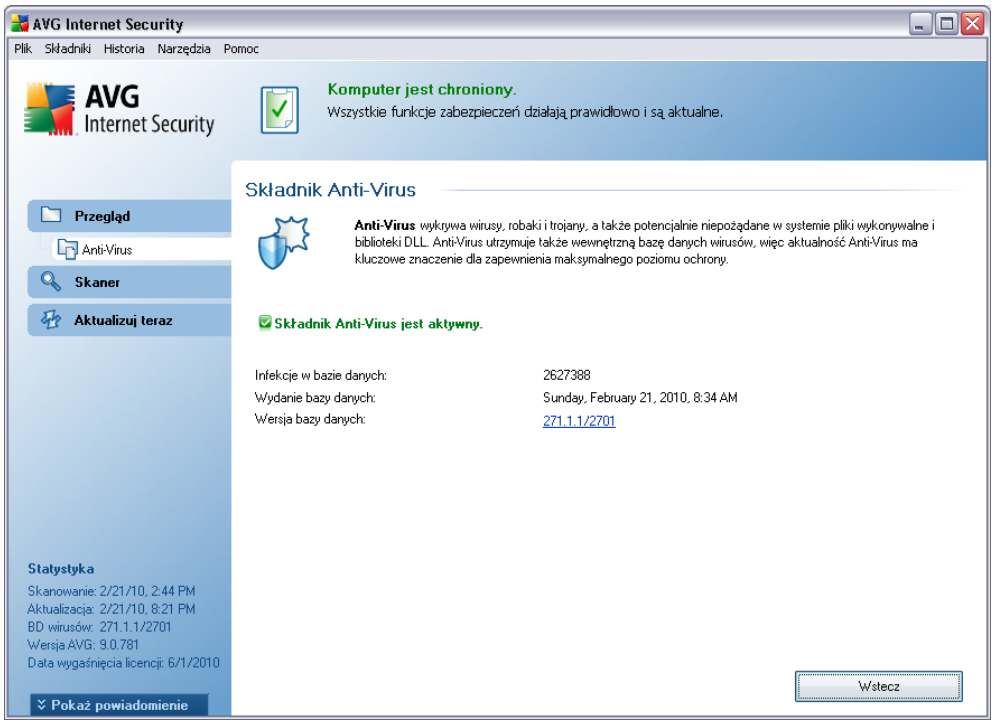
Wazna zaleta ochrony antywirusowej jest fakt, ze nie pozwala ona na uruchomienie zadnych znanych wirusów na komputerze!

Korzystanie z tylko jednej technologii nie zapewnia stuprocentowej skutecznosci wykrywania wirusów, dlatego skladnik ***Anti-Virus*** wykorzystuje jednoczesnie kilka metod:

- Skanowanie — wyszukiwanie ciagów znaków typowych dla danego wirusa.
- Analiza heurystyczna — dynamiczna emulacja instrukcji skanowanego obiektuw srodowisku maszyny wirtualnej.
- Wykrywanie generyczne — wykrywanie instrukcji typowych dla danego wirusa lub grupy wirusów.

Program AVG jest równiez w stanie analizowac i wykrywac wykonywalne aplikacje i biblioteki DLL, które moga byc potencjalne niepozadane w Twoim systemie. Takie zagrozenia (rózne rodzaje oprogramowania szpiegujacego, reklamowego itp.) nazywane sa równiez Potencjalnie Niechcianymi Programami. Ponadto program AVG skanuje rejestr systemu w poszukiwaniu podejrzanych wpisów, a takze monitoruje tymczasowe pliki internetowe i sledzace pliki cookie. Umozliwia to traktowanie wszystkich potencjalnie szkodliwych obiektów w ten sam sposób jak infekcji.

8.1.2. Interfejs skladnika Anti-Virus



Interfejs skladnika ***Anti-Virus*** zawiera krótki opis jego funkcji, informacje o biezacym stanie (Skladnik *Anti-Virus jest aktywny.*), a takze krótki przeglad statystyk:

- ***Infekcje w bazie danych*** — liczba wirusów zdefiniowanych w najnowszej wersji bazy danych.
- ***Ostatnia aktualizacja bazy danych*** — data i godzina ostatniej aktualizacji bazy wirusów.
- ***Wersja bazy danych*** — numer ostatniej wersji bazy danych; numer ten rosnie przy kazdej aktualizacji.

Interfejs tego skladnika zawiera tylko jeden przycisk (***Wstecz***) — klikniecie go powoduje powrót do domyslnego interfejsu uzytkownika systemu AVG (przegladu skladników).

Uwaga: *Dostawca oprogramowania AVG skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu*

*AVG, nalezy wybrac z menu głównego**Narzedzia / Ustawienia zaawansowane** i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

8.2. Anti-Spyware

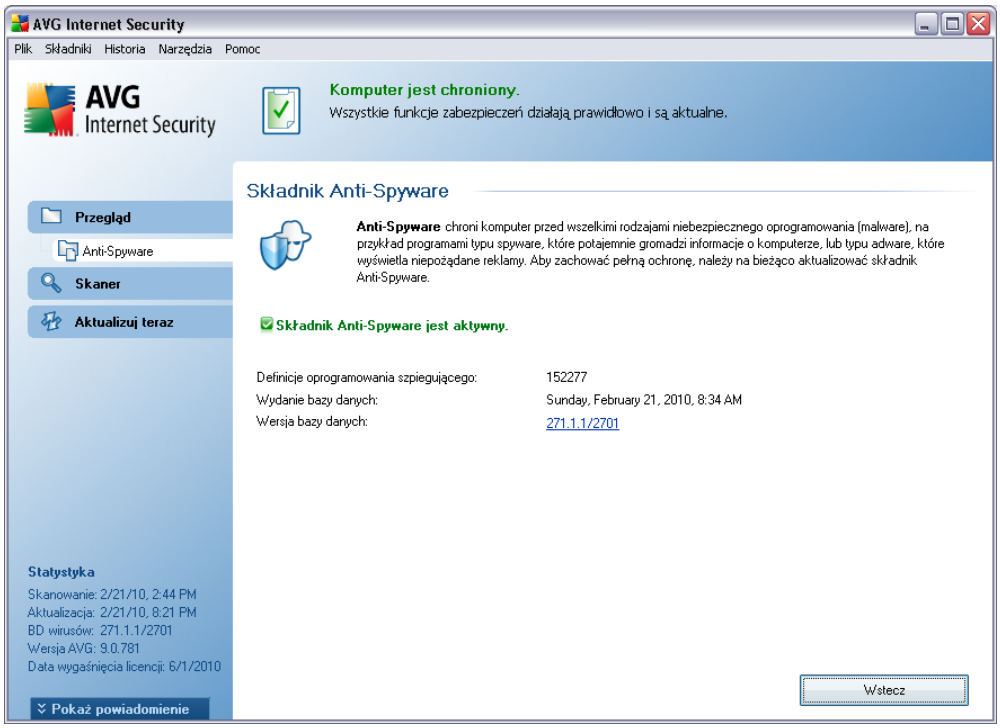
8.2.1. Zasady dzialania skladnika Anti-Spyware

Oprogramowanie szpiegujace (spyware) jest zazwyczaj definiowane jako pewien rodzaj szkodliwego oprogramowania, które gromadzi informacje z komputera uzytkownika bez jego wiedzy i pozwolenia. Niektóre aplikacje szpiegujace moga byc instalowane celowo i czesto zawieraja reklamy, wyskakujace okna i inne nieprzyjemne elementy.

Obecnie zródlem wiekszosci infekcji sa potencjalnie niebezpieczne witryny internetowe. Powszechne sa równiez inne metody rozprzestrzeniania, na przyklad poprzez e-mail lub w efekcie dzialalnosci robaków i wirusów. Najskuteczniejsza ochrona jest stosowanie stale pracujacego w tle skladnika ***Anti-Spyware***, który dziala jak ochrona rezydentna i skanuje aplikacje podczas ich uruchamiania.

Istnieje jednak ryzyko, ze szkodliwe oprogramowanie znalazlo sie na komputerze przed zainstalowaniem systemu **AVG 9 Internet Security** lub ze uzytkownik zaniedbal jego aktualizacje, nie korzystajac z aktualnych baz wirusów i nowych wersji programu. Z tego powodu AVG umozliwia pelne przeskanowanie komputera pod katem obecnosci oprogramowania szpiegujacego (za pomoca interfejsu skanera). Wykrywa on równiez szkodliwe oprogramowanie, które jest uspione lub nie stwarza zagrozenia, czyli takie, które zostalo pobrane, ale nie aktywowane.

8.2.2. Interfejs skladnika Anti-Spyware



Interfejs skladnika ***Anti-Spyware*** zawiera krótki opis jego funkcji, informacje o biezacym stanie (Skladnik *Anti-Spyware jest aktywny.*), oraz statystyki:

- ***Definicje oprogramowania szpiegujacego*** — liczba sygnatur programów typu spyware zdefiniowanych w najnowszej wersji bazy danych.
- ***Ostatnia aktualizacja bazy danych*** — data i godzina ostatniej aktualizacji.
- ***Wersja bazy danych*** — numer ostatniej wersji bazy danych; numer ten rosnie przy kazdej aktualizacji.

Interfejs tego skladnika zawiera tylko jeden przycisk (***Wstecz***) — kliknięcie go powoduje powrót do domyslnego interfejsu uzytkownika systemu AVG (przegladu skladników).

Uwaga: Dostawca oprogramowania AVG *skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu głównego****Narzedzia / Ustawienia zaawansowane*** *i*

skorzystac z interfejsu Zaawansowane ustawienia AVG.

8.3. Anti-Spam

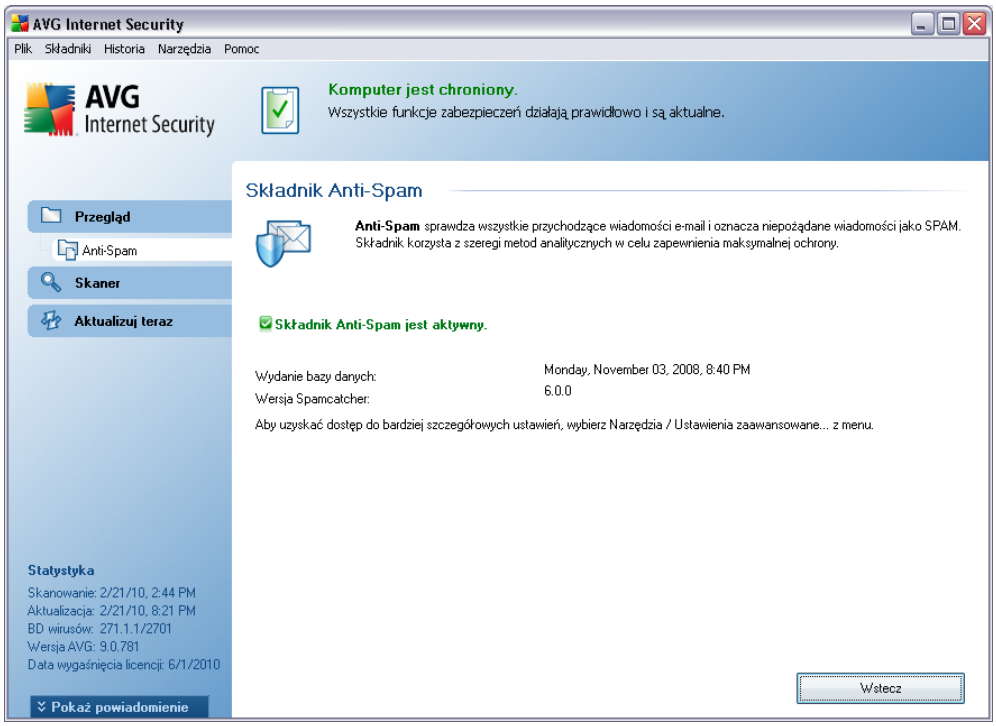
Mianem „spam" okresla sie niechciana poczte e-mail (głównie reklamy produktów lub uslug, które sa hurtowo rozsylane do wielkiej liczby odbiorców jednoczesnie, zapelniajac ich skrzynki pocztowe). Spamem nie jest korespondencja seryjna rozsylana do odbiorców po wyrazeniu przez nich zgody. Spam jest nie tylko irytujacy, ale moze byc równiez zródlem oszustw, wirusów i obrazliwych tresci.

8.3.1. Zasady dzialania skladnika Anti-Spam

Skladnik AVG Anti-Spam sprawdza wszystkie przychodzace wiadomosci e-mail i oznacza te niepozadane jako SPAM.***Skladnik AVG Anti-Spam*** moze modyfikowac temat wiadomosci e-mail (*wykrytej jako SPAM*), dodajac do niego specjalny ciag tekstowy. Dzieki temu mozliwe jest latwe filtrowanie wiadomosci e-mail w programie pocztowym.

Skladnik AVG Anti-Spam podczas przetwarzania kazdej wiadomosci wykorzystuje kilka metod analizy, oferujac maksymalnie skuteczna ochrone przeciwko niepozadanym wiadomosciom e-mail. Skladnik ***AVG Anti-Spam*** do wykrywania spamu korzysta z regularnie aktualizowanej bazy danych. Mozna takze uzyc serwerów RBL (*publicznych baz adresów znanych nadawców spamu*) lub recznie dodac adresy do bialej listy (*wiadomosci pochodzace z tych adresów nie sa nigdy oznaczane jako spam*) lub czarnej listy (*wiadomosci pochodzace z tych adresów sa zawsze oznaczane jako spam*).

8.3.2. Interfejs skladnika Anti-Spam



Okno dialogowe skladnika ***Anti-Spam*** zawiera krótki opis jego funkcji, informacje o biezacym stanie (Skladnik *Anti-Spam jest aktywny.*) oraz nastepujace statystyki:

- ***Wersja bazy danych*** — okresla, czy i kiedy baza sygnatur spamu zostala zaktualizowana i opublikowana.
- ***Wersja silnika Spamcatcher*** — numer ostatniej wersji silnika antyspamowego.

Interfejs uzytkownika tego skladnika zawiera tylko jeden przycisk (***Wstecz***) — kliknięcie tego przycisku powoduje powrót do domyslnego interfejsu uzytkownika systemu AVG (*przegladu skladników*).

Uwaga: *Dostawca oprogramowania AVG skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu glównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

8.4. Anti-Rootkit

Program typu rootkit to aplikacja zaprojektowana w celu przejecia calkowitej kontroli nad systemem komputerowym bez zgody jego wlascicieli czy upowaznionych administratorów. Bezposredni dostep do sprzetu jest rzadko wymagany, poniewaz programy typu rootkit w pelni zdalnie kontroluja system operacyjny komputera. Zwykle ukrywaja one swoja obecnosc mylac lub unikajac standardowych mechanizmów bezpieczenstwa systemu operacyjnego. Wiele z nich jest jednoczesnie konmi trojanskimi, które dodatkowo staraja sie przekonac uzytkowników, ze ich systemy sa bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorujacymi) oraz plików lub danych przed samym systemem operacyjnym.

8.4.1. Zasady dzialania skladnika Anti-Rootkit

AVG Anti-Rootkit to specjalistyczne narzedzie do wykrywania i skutecznego usuwania niebezpiecznych programów typu rootkit, wykorzystujacych technologie, które moga kamuflowac obecnosc innego szkodliwego oprogramowania na komputerze. Skladnik ***AVG Anti-Rootkit*** umozliwia wykrywanie programów typu rootkit na podstawie wstepnie zdefiniowanego zestawu regul. Nalezy zwrócic uwage na fakt, ze wykrywane sa wszystkie programy typu rootkit (*nie tylko te szkodliwe*). Jesli skladnik ***AVG Anti-Rootkit*** wykrywa program typu rootkit, nie znaczy to jeszcze, ze ten program jest szkodliwy. Niekiedy programy typu rootkit sa uzywane jako sterowniki lub jako komponenty innych, pozytecznych aplikacji.

8.4.2. Interfejs skladnika Anti-Rootkit

Interfejs skladnika ***Anti-Rootkit*** zawiera krótki opis jego funkcji, informacje o biezacym stanie (*Skladnik Anti-Rootkit jest aktywny*) oraz date ostatniego uruchomienia testu ***Anti-Rootkit***.

W dolnej czesci okna znajduje sie sekcja ***ustawien skladnika Anti-Rootkit***, w której skonfigurowac mozna podstawowe funkcje skanowania w poszukiwaniu programów typu rootkit. Po pierwsze: nalezy zaznaczyc odpowiednie pola, aby okreslic obiekty, które maja byc skanowane:

- ***Skanuj aplikacje***
- ***Skanuj biblioteki DLL***
- ***Skanuj sterowniki***

Nastepnie nalezy wybrac tryb skanowania w poszukiwaniu programów typu rootkit:

- ***Szybkie skanowanie w poszukiwaniu programów typu rootkit*** — skanuje wszystkie uruchomione procesy, zaladowane sterowniki i folder systemowy (*zazwyczaj c:\Windows*)

- ***Pelne skanowanie w poszukiwaniu programów typu rootkit*** — skanuje wszystkie uruchomione procesy, zaladowane sterowniki i folder systemowy (*zazwyczaj c:\Windows*) oraz wszystkie dyski lokalne (*w tym dyski flash, ale bez uwzglednienia napedów dyskietek/plyt CD*)

Dostepne sa nastepujace przyciski kontrolne:

- ***Szukaj programów typu rootkit*** — poniewaz to skanowanie nie jest czescia testu ***Skan calego komputera***, mozna je uruchomic bezposrednio z interfejsu skladnika ***Anti-Rootkit***, klikajac ten przycisk.

- ***Zapisz zmiany*** — pozwala zapisac wszystkie zmiany wprowadzone w danym oknie i powrócic do domyslnego ***interfejsu uzytkownika AVG*** (przegladu skladników).

- ***Anuluj*** — pozwala powrócic do domyslnego ***interfejsu uzytkownika AVG*** (przegladu skladników) bez zapisywania wprowadzonych zmian.

8.5. Narzedzia systemowe

Narzedzia systemowe odnosza sie do narzedzi udostepniajacych szczególowe podsumowanie srodowiska systemu **AVG 9 Internet Security** oraz systemu operacyjnego. Wyswietlany jest tam przeglad:

- Procesy — lista procesów (czyli dzialajacych aplikacji) aktualnie aktywnych na komputerze.

- Polaczenia sieciowe — lista aktualnie aktywnych polaczen

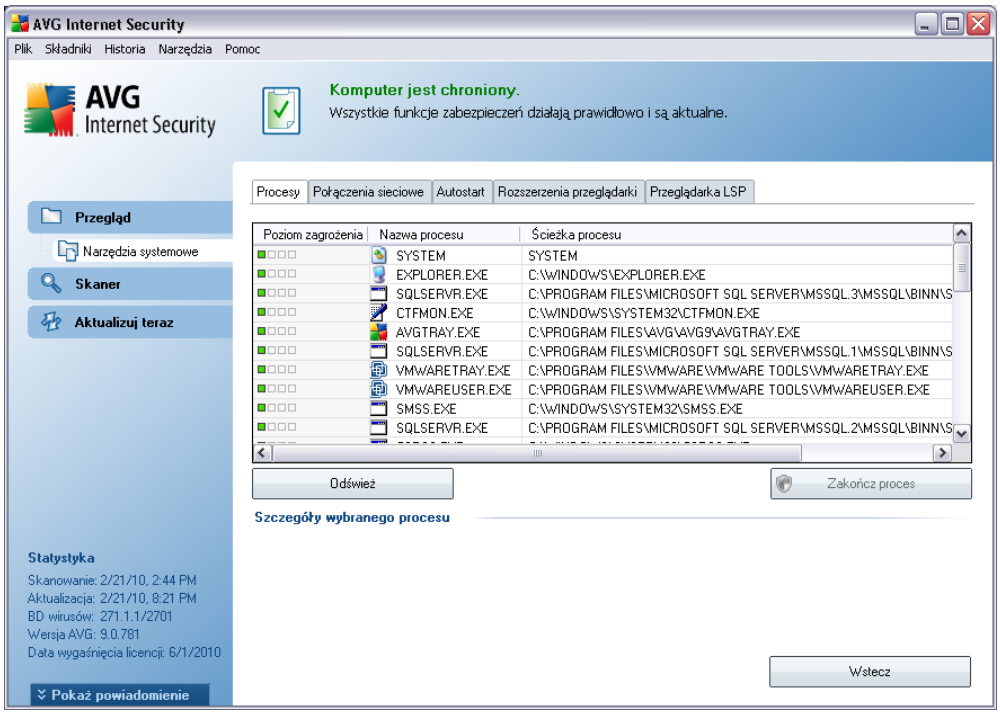
- Autostart — lista wszystkich aplikacji uruchamianych podczas startu systemu Windows

- Rozszerzenia przegladarki — lista pluginów, tzn. aplikacji zainstalowanych w przegladarce internetowej.

- Przegladarka LSP — lista dostawców uslug warstwowych (LSP)

Niektóre listy mozna tez edytowac, ale powinni to robic wylacznie bardzo doswiadczeni uzytkownicy!

8.5.1. Procesy



Okno ***Procesy*** zawiera liste procesów (*czyli dzialajacych aplikacji*) aktualnie aktywnych na komputerze. Lista ta podzielona jest na nastepujace kolumny:

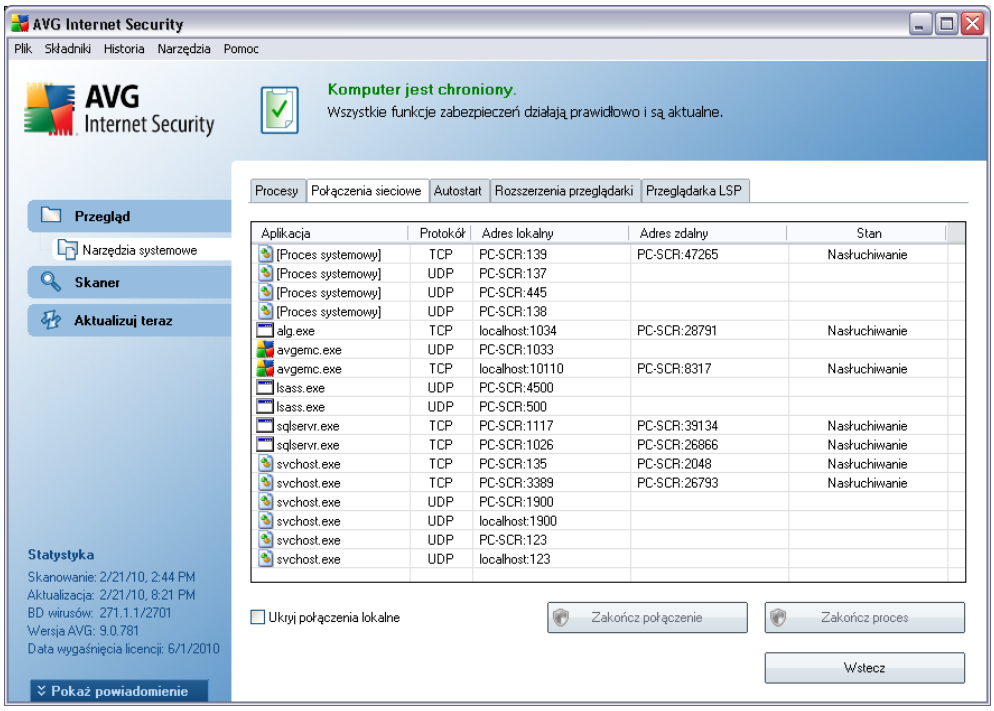
- ***Poziom ryzyka*** — graficzna reprezentacja ryzyka stwarzanego przez okreslone procesy, przedstawiana na czterostopniowej skali od najmniej istotnego (■□□□) do krytycznego (■■■■).
- ***Nazwa procesu*** — nazwa dzialajacego procesu.
- ***Sciezka*** — fizyczna sciezka do uruchomionego pliku.
- ***Okno*** — jesli to mozliwe, podaje nazwe okna aplikacji.
- ***Internet*** — wskazuje, czy dzialajacy proces laczy sie takze z internetem (*Tak/Nie*).
- ***Usluga*** — wskazuje, czy dzialajacy proces jest usluga (*Tak/Nie*).
- ***PID*** — numer identyfikacyjny procesu - unikatowy, wewnetrzny numer procesu w systemie Windows.

Przyciski kontrolne

W interfejsie ***narzedzi systemowych*** dostepne sa nastepujace przyciski sterujace:

- ***Odswiez*** — aktualizuje liste procesów zgodnie z obecnym stanem.
- ***Zakoncz procesy*** — mozna wybrac jedna lub kilka aplikacji i zakonczyc je, klikajac ten przycisk. ***Stanowczo zaleca sie, aby nie zamykac zadnych procesów, jesli nie ma absolutnej pewnosci, ze stanowia one rzeczywiste zagrozenie!***
- ***Wstecz*** — przelacza z powrotem do domyslnego ***Interfejsu uzytkownika systemu AVG*** (przegladu skladników).

8.5.2. Polaczenia sieciowe



Okno ***Polaczenia sieciowe*** zawiera liste aktywnych polaczen. Lista ta podzielona jest na nastepujace kolumny:

- ***Aplikacja*** — nazwa aplikacji powiazanej z polaczeniem (*wyjatek stanowi system Windows 2000, w którym informacje te nie sa dostepne*)

- ***Protokól*** — protokól transmisyjny uzywany do polaczenia:
    - TCP — protokól wspólpracujacy z protokolem IP (Internet Protocol) przy transmisji danych w internecie.
    - UDP — protokól alternatywny do TCP.
- ***Adres lokalny*** — uzywany adres IP komputera lokalnego (i numer portu).
- ***Adres zdalny*** — Adres IP komputera zdalnego (i numer portu). Jesli jest to mozliwe, znaleziona zostanie równiez nazwa hosta komputera zdalnego.
- ***Stan*** — okresla najbardziej prawdopodobny stan polaczenia (*Polaczony, Serwer powinien zamknac, Nasluchiwanie, Ukonczono zamykanie aktywne, Zamykanie pasywne, Zamykanie aktywne*).

Aby stworzyc liste tylko zewnetrznych polaczen, nalezy zaznaczyc pole wyboru ***Ukryj polaczenia lokalne*** w dolnej sekcji okna dialogowego.

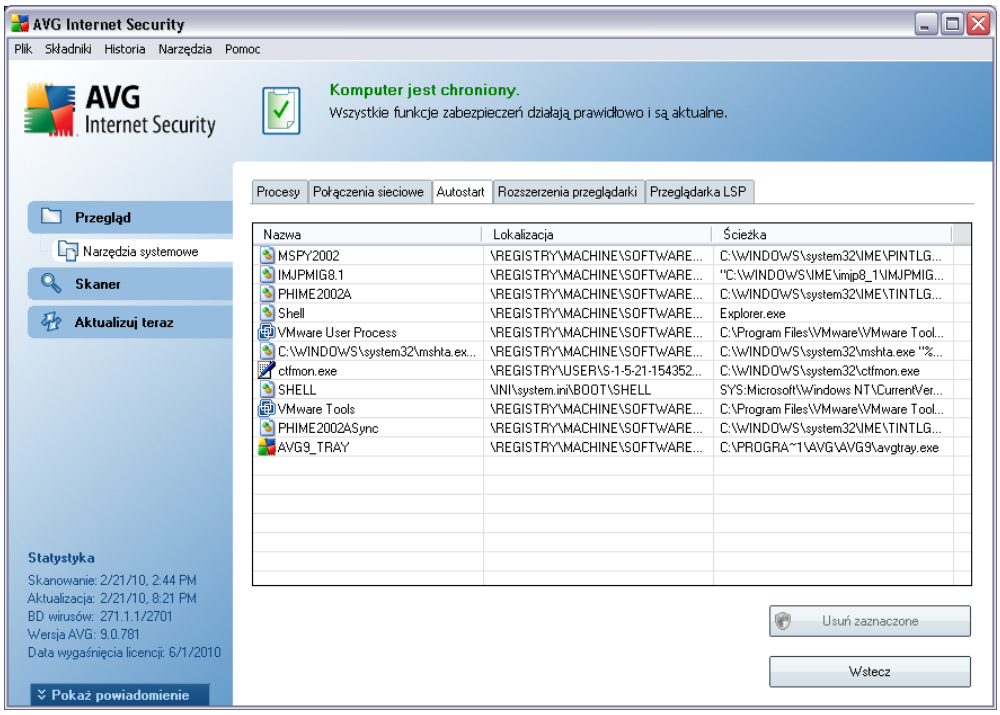
Przyciski kontrolne

Dostepne przyciski sterujace to:

- ***Zakoncz polaczenie*** — zamyka wybrane polaczenia.
- ***Przerwij proces*** — zamyka jedna lub wiecej aplikacji powiazanych z polaczeniami zaznaczonymi na liscie
- ***Wstecz*** — wraca do domyslnego ***Interfejsu uzytkownika AVG*** (przegladu skladników).

Uwaga: Czasami mozliwe jest konczenie tylko tych aplikacji, które sa w stanie ''Polaczony''. Stanowczo zaleca sie, aby nie zamykac zadnych polaczen, jesli nie ma absolutnej pewnosci, ze stanowia one rzeczywiste zagrozenie!

8.5.3. Autostart

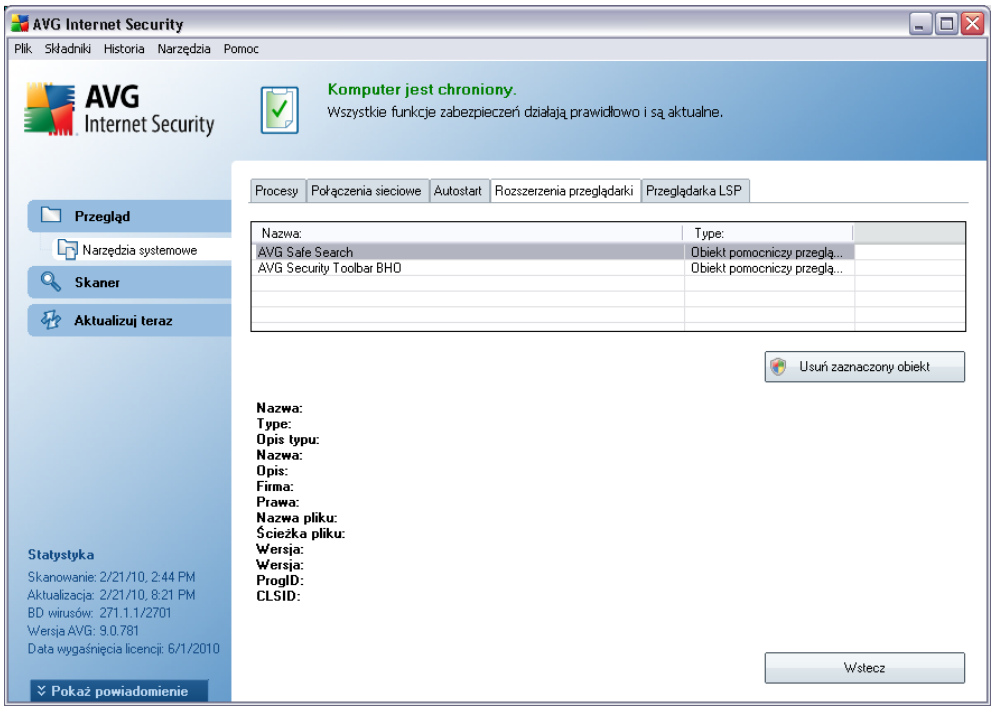


Okno ***Autostart*** zawiera liste wszystkich aplikacji uruchamianych w czasie rozruchu systemu Windows. Bardzo czesto szkodliwe aplikacje dodaja sie automatycznie do listy autostartu zlokalizowanej w rejestrze.

Mozna usunac jeden lub wiecej wpisów, zaznaczajac je i klikajac przycisk ***Usun zaznaczone elementy.*** Przycisk ***Wstecz*** przelacza z powrotem do domyslnego okna ***Interfejsu uzytkownika systemu AVG*** (przegladu skladników).

Zaleca sie, aby nie usuwac zadnych aplikacji z tej listy, jesli nie ma absolutnej pewnosci, ze stanowia one rzeczywiste zagrozenie!

8.5.4. Rozszerzenia przegladarki



Okno ***Rozszerzenia przegladarki*** zawiera liste pluginów, *tj. aplikacji* zintegrowanych z przegladarka internetowa. Lista ta moze zawierac zarówno uzyteczne dodatki, jak i potencjalnie szkodliwe programy. Kliknij obiekt z listy, aby otrzymac szczególowe informacje o wybranym pluginie. Zostana one wyswietlone w dolnej sekcji okna dialogowego.

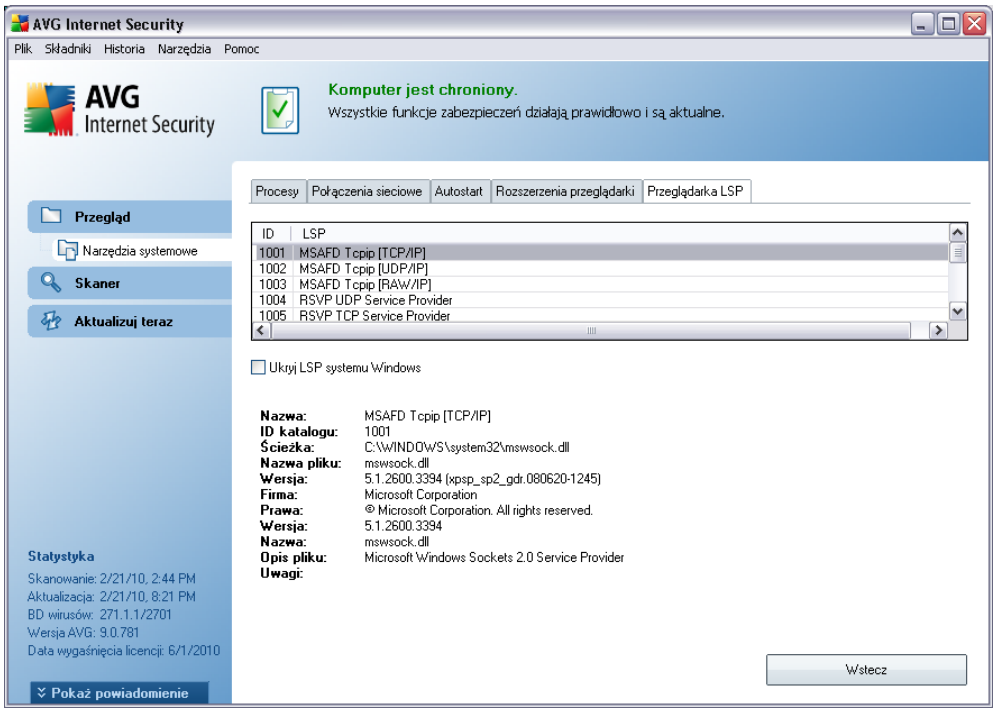
Przyciski kontrolne

Na karcie ***Rozszerzenia przegladarki*** dostepne sa nastepujace przyciski kontrolne:

- ***Usun zaznaczony obiekt*** — usuwa plugin w danej chwili zaznaczony na liscie. ***Stanowczo zaleca sie, aby nie usuwac z listy zadnych pluginów, jesli nie ma absolutnej pewnosci, ze stanowia one rzeczywiste zagrozenie!***

- ***Wstecz***— przelacza z powrotem do domyslnego ***interfejsu uzytkownika systemu AVG*** (przegladu skladników)

8.5.5. Przegladarka LSP



Okno ***Przegladarka LSP*** zawiera pelna liste dostawców uslug warstwowych (LSP).

Dostawca uslug warstwowych (LSP) jest sterownikiem systemowym odpowiedzialnym za uslugi sieciowe systemu operacyjnego Windows. Ma on dostep do wszystkich danych przychodzacych i wychodzacych z komputera, a takze moze je modyfikowac. Niektóre sterowniki LSP sa niezbedne, aby system Windows mógl laczyc sie z innymi komputerami (w tym równiez z internetem). Jednak pewne szkodliwe aplikacje potrafia zarejestrowac sie w systemie jako LSP, uzyskujac w ten sposób dostep do wszystkich transmitowanych danych. Dlatego tez przeglad ten moze byc pomocny w sprawdzaniu wszystkich mozliwych zagrozen zwiazanych LSP.

W pewnych okolicznosciach mozliwa jest takze naprawa uszkodzonych sterowników LSP (*np. gdy plik zostal usuniety, ale pozostaly wpisy w rejestrze*). W przypadku wykrycia sterownika LSP kwalifikujacego sie do naprawy zostanie wyswietlony przycisk umozliwiajacy jej dokonanie.

Aby uwzglednic na liscie sterowniki LSP nalezace bezposrednio do systemu Windows, usun zaznaczenie pola ***Ukryj sterowniki LSP systemu Windows.*** Przycisk ***Wstecz*** przelacza z powrotem do domyslnego okna ***interfejsu uzytkownika AVG*** *(przegladu skladników*).

8.6. Zapora

Zapora internetowa to system, który wymusza stosowanie zasad kontroli dostepu miedzy dwoma lub wieksza liczba sieci, blokujac lub umozliwiajac przeplyw danych. Zapora sklada sie z zestawu regul, które steruja komunikacja na kazdym indywidualnym porcie sieciowym, chroniac w ten sposób siec lokalna przed atakami, których zródlo znajduje sie na zewnatrz (zazwyczaj w internecie). Komunikacja jest oceniana (w oparciu o zdefiniowane reguly), a nastepnie akceptowana lub blokowana. Jesli zapora wykryje próbe ataku, blokuje ja i nie pozwala intruzowi przejac kontroli nad komputerem.

Konfiguracja Zapory pozwala blokowac lub dopuszczac komunikacje wewnetrzna lub zewnetrzna (zarówno wychodzaca, jak i przychodzaca) na konkretnych portach i dla zdefiniowanych programów. Zapora moze np. akceptowac tylko ruch WWW, z którego korzysta program Microsoft Internet Explorer. Próba transmisji danych WWW przez jakakolwiek inna przegladarke bedzie w takim przypadku blokowana.

Zapora chroni równiez Twoje dane osobowe - nikt nie uzyska ich z Twojego komputera bez wyraznej zgody. Decyduje tez o tym, jak wymieniane sa dane z innymi komputerami w sieci lokalnej lub internecie. Zapora w srodowisku komercyjnym chroni równiez pojedyncze komputery przed atakami przeprowadzanymi z wnetrza tej samej sieci.

Sugestia: *Generalnie nie zaleca sie uzywania wiecej niz jednej zapory internetowej na tym samym komputerze. Zainstalowanie dodatkowych zapór nie zwiekszy bezpieczenstwa komputera. Zwiekszy sie natomiast prawdopodobienstwo, ze wystapia konflikty miedzy tymi dwiema aplikacjami. Dlatego tez zalecamy uzywanie tylko jednej zapory i wylaczenie wszystkich innych. Pozwala to wyeliminowac ryzyko konfliktów i wszelkich problemów z tym zwiazanych.*

8.6.1. Zasady dzialania Zapory

W systemie AVG ***Zapora*** kontroluje caly ruch na kazdym porcie sieciowym komputera. Na podstawie zdefiniowanych regul ***Zapora*** ocenia uruchomione aplikacje (chcace nawiazac polaczenie z siecia lokalna lub internetem) oraz programy usilujace z zewnatrz polaczyc sie z Twoim komputerem. ***Zapora*** dopuszcza lub blokuje komunikacje tych aplikacji na okreslonych portach sieciowych. Domyslnie, jesli aplikacja jest nieznana (tj. nie posiada zdefiniowanych regul ***Zapory***), wyswietlone bedzie pytanie, czy jej komunikacja ma zostac zaakceptowana.

Uwaga: *Zapora AVG nie jest przeznaczona do współpracy z serwerami!*

Zapora moze wykonac nastepujace czynnosci:

- Automatycznie zablokowac lub zezwolic na komunikacje znanych aplikacji, albo poprosic uzytkownika o potwierdzenie
- Korzystaj z kompletnych profili zawierajacych wstepnie zdefiniowane reguly (zgodnie z Twoimi potrzebami)
- Automatycznie przelaczaj profile przy laczeniu sie z róznymi sieciami lub przy uzywaniu róznych kart sieciowych

8.6.2. Profile Zapory

Zapora umozliwia definiowanie okreslonych regul bezpieczenstwa w oparciu o srodowisko i tryb pracy komputera. *** Kazda z opcji wymaga innego poziomu zabezpieczen, a ich dostosowywanie odbywa sie za pomoca odpowiednich profili. Krótko mówiac, ***profil Zapory*** to okreslona konfiguracja tego skladnika. Dostepna jest pewna liczba wstepnie zdefiniowanych profili.***

Dostepne profile

- ***Odblokuj wszystko***to profil systemowy skladnika ***Zapora*** wstepnie skonfigurowany przez producenta; jest zawsze dostepny. Gdy profil ten jest aktywny, cala komunikacja sieciowa jest akceptowana, bez stosowania jakichkolwiek regul zabezpieczen - tak, jakby skladnik ***Zapora*** byl wylaczony *(tj. wszystkie programy moga wymieniac dane, ale pakiety wciaz obslugiwane sa przez sterownik filtra AVG - aby tego uniknac, calkowicie wylacz Zapore)*. Tego profilu systemowego nie mozna powielic ani usunac, a jego ustawien nie da sie modyfikowac.
- ***Blokuj wszystko***to profil systemowy skladnika ***Zapora*** wstepnie skonfigurowany przez producenta; jest zawsze dostepny. Gdy zostanie on aktywowany, wszystkie próby komunikacji z siecia beda blokowane. Komputer nie bedzie ani dostepny z sieci zewnetrznej, ani nie bedzie mógl sie z nia polaczyc. Tego profilu systemowego nie mozna powielic ani usunac, a jego ustawien nie da sie modyfikowac.
- ***Profile niestandardowe***:
  - ***Podlaczony bezposrednio do internetu*** — odpowiedni dla typowych komputerów stacjonarnych polaczonych bezposrednio z internetem lub dla notebooków laczacych sie z internetem poza bezpieczna siecia firmowa. Opcje te nalezy wybrac, jesli laczysz sie z siecia w domu malej sieci firmowej (bez centralnej administracji). Opcje te nalezy wybrac równiez podczas podrózowania z notebookiem i laczenia sie z siecia z

nieznanych i potencjalnie niebezpiecznych miejsc (*kawiarnie internetowe, pokoje hotelowe itp.*). Zostana w tym wypadku utworzone bardziej restrykcyjne reguly, poniewaz zaklada sie, ze komputer taki nie ma zapewnionej zadnej dodatkowej ochrony, dlatego tez wymaga maksymalnej troski o bezpieczenstwo.

- ***Komputer w domenie*** — odpowiedni dla komputerów pracujacych w sieci lokalnej, np. w szkolach lub sieci firmowej. Zaklada sie, ze wspomniana siec chroniona jest przy uzyciu pewnych dodatkowych srodków, wiec poziom bezpieczenstwa moze byc nizszy niz dla pojedynczego komputera.

- ***Siec w domu lub malym biurze*** — odpowiedni dla komputerów w mniejszej sieci, np. w domu lub w malej firmie (zazwyczaj tylko kilka komputerów polaczonych ze soba, bez „centralnego" administratora).

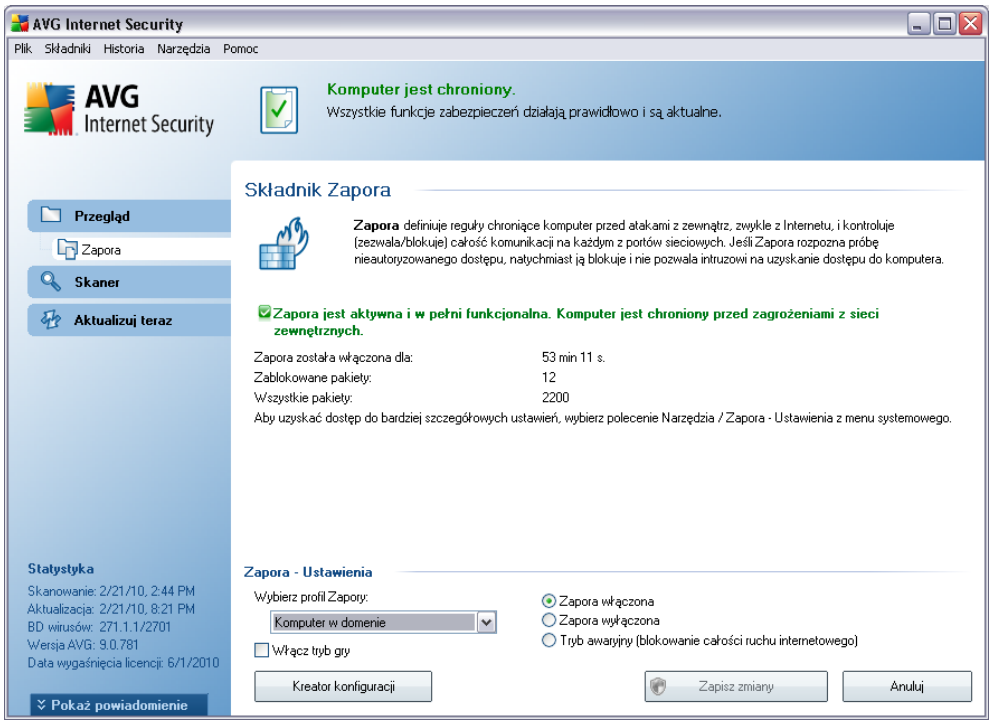
Przelaczanie profili

Funkcja przelaczania profili umozliwia skladnikowi ***Zapora*** automatyczne przelaczenie sie na zdefiniowany wczesniej profil w przypadku uzycia okreslonej karty sieciowej lub polaczenia z okreslonym typem sieci. Jesli do obszaru sieciowego nie zostal jeszcze przypisany zaden profil, przy najblizszym polaczeniu z tym obszarem ***Zapora*** wyswietli okno dialogowe z prosba o przypisanie profilu.

Profile mozna tworzyc dla dowolnych interfejsów sieciowych lub obszarów. Ich dalsze ustawienia dostepne sa w oknie ***Profile kart sieciowych i obszarów***, w którym mozna równiez w razie potrzeby wylaczyc te funkcje (*w takim przypadku dla kazdego rodzaju polaczenia bedzie uzywany profil domyslny*).

Zazwyczaj funkcja ta bedzie przydatna dla uzytkowników laptopów, korzystajacych z róznych typów polaczen. W przypadku komputera stacjonarnego korzystajacego tylko z jednego typu polaczenia (*tj. kablowego polaczenia z internetem*) funkcja przelaczania profili prawdopodobnie nigdy nie bedzie uzywana.

8.6.3. Interfejs Zapory



Interfejs skladnika ***Zapora*** udostepnia niektóre podstawowe informacje na temat funkcji oraz krótkie omówienie statystyk ***Zapory***:

- ***Zapora jest aktywna od*** — czas, jaki uplynal od jej ostatniego uruchomienia.
- ***Zablokowane pakiety*** — liczba zablokowanych pakietów (ze wszystkich sprawdzonych).
- ***Wszystkie pakiety*** — liczba wszystkich pakietów sprawdzonych przez Zapore.

Podstawowa konfiguracja skladnika

- ***Wybierz profil Zapory*** — z menu rozwijanego wybierz jeden ze zdefiniowanych profili — dwa profile sa dostepne przez caly czas (*domyslne profile o nazwach* ***Odblokuj wszystko*** *oraz* ***Blokuj wszystko***). Inne profile zostaly dodane recznie w wyniku edycji ustawien w oknie ***Profile*** w ***Ustawieniach Zapory***.

- ***Wlacz tryb gry —*** Zaznaczenie tego pola daje pewnosc, ze podczas dzialania aplikacji pelnoekranowych (gier, prezentacji programu PowerPoint itp.) ***Zapora*** nie bedzie wyswietlala okien dialogowych z pytaniami, czy komunikacja dla nieznanej aplikacji ma zostac odblokowana. Jesli w tym czasie nowa aplikacja spróbuje polaczyc sie z siecia, ***Zapora*** automatycznie odblokuje lub zablokuje te próbe (zgodnie z ustawieniami biezacego profilu).

- ***Stan Zapory***:

    - ***Zapora wlaczona —*** nalezy zaznaczyc te opcje, aby zezwalac na komunikacje wszystkim aplikacjom, którym w zbiorze regul zdefiniowanych dla wybranego profilu ***Zapory*** przypisano akcje Odblokuj.

    - ***Zapora wylaczona —*** ta opcja calkowicie wylacza ***Zapore***. Ruch sieciowy nie bedzie blokowany ani monitorowany!

    - ***Tryb awaryjny (blokowanie calosci ruchu internetowego)*** — nalezy zaznaczyc te opcje, aby blokowac caly ruch na wszystkich portach. ***Zapora*** wciaz dziala, lecz komunikacja z siecia jest zablokowana.

Uwaga: *Dostawca oprogramowania AVG skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana ustawien Zapory, nalezy wybrac z menu glównego pozycje* ***Narzedzia / Ustawienia Zapory*** *i edytowac konfiguracje w nowo otwartym oknie dialogowym* ***Ustawienia Zapory****.*

Przyciski kontrolne

- ***Kreator konfiguracji*** — przycisk ten pozwala przejsc do okna *Wybór typu komputera* (***uzywanego podczas instalacji***), w którym mozna skonfigurowac dzialanie ***Zapory***.

- ***Zapisz zmiany*** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.

- ***Anuluj*** — klikniecie tego przycisku powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (*przegladu skladników*).

8.7. Skaner poczty e-mail

Poczta e-mail to od dawna czeste zródlo wirusów i koni trojanskich. Wyludzenia danych i spam powoduja, ze stala sie ona jeszcze wiekszym zagrozeniem. Darmowe konta pocztowe sa szczególnie narazone na otrzymywanie szkodliwych wiadomosci e-mail, *gdyz rzadko korzystaja z technologii antyspamowych*, a domowi uzytkownicy najczesciej uzywaja wlasnie takich kont. Dodatkowo odwiedzaja oni nieznane witryny i wpisuja w formularzach dane osobowe (*takie jak adres e-mail*), co powoduje, ze w jeszcze wiekszym stopniu narazaja sie na ataki za posrednictwem poczty e-mail. Firmy uzywaja na ogól komercyjnych kont pocztowych, które w celu ograniczenia ryzyka korzystaja z filtrów antyspamowych i innych srodków bezpieczenstwa.

8.7.1. Zasady dzialania Skanera poczty e-mail

Skladnik ***Skaner poczty e-mail*** automatycznie skanuje poczte przychodzaca i wychodzaca. Mozna z niego korzystac przy programach pocztowych, dla których nie powstaly pluginy AVG (*np. Outlook Express, Mozilla, Incredimail itd.*).

Podczas instalacji systemu AVG tworzone sa automatyczne serwery kontrolujace poczte e-mail: jeden do sprawdzania wiadomosci przychodzacych, drugi do wychodzacych. Przy pomocy tych serwerów wiadomosci e-mail sa automatycznie sprawdzane na portach 110 i 25 (*standardowe porty dla wysylania/odbierania poczty e-mail*).

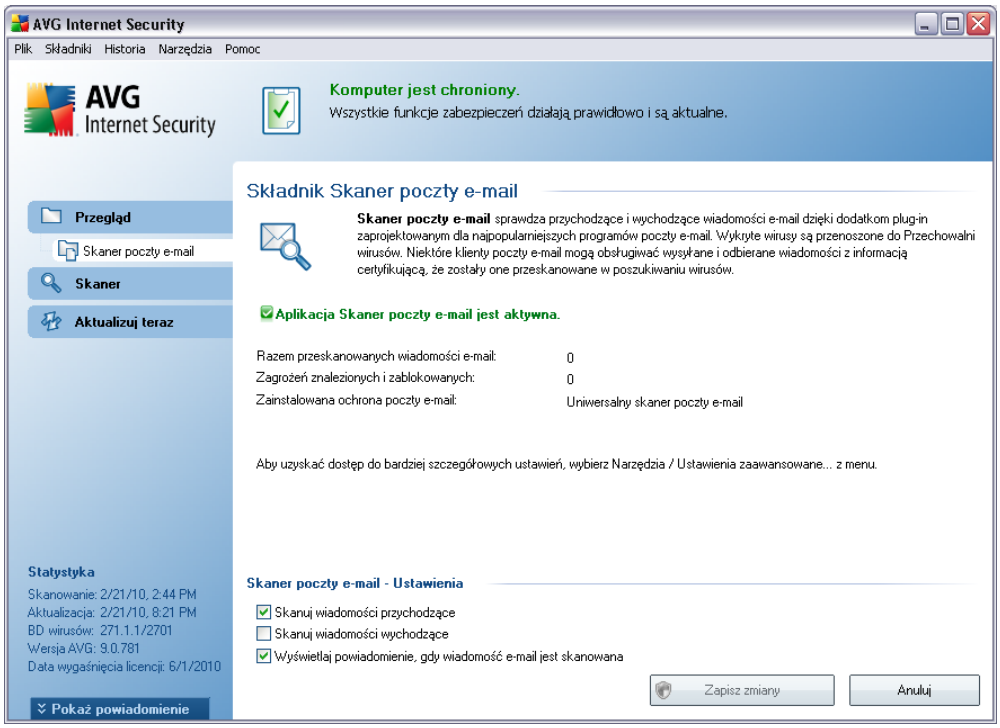
Skaner poczty e-mail posredniczy miedzy programem pocztowym a zewnetrznymi serwerami pocztowymi.

- ***Poczta przychodzaca:*** Podczas otrzymywania wiadomosci z serwera, ***Skaner poczty e-mail*** sprawdza ja w poszukiwaniu wirusów, usuwa zainfekowane zalaczniki i dolacza certyfikat. Wykryte wirusy sa natychmiast poddawane kwarantannie w ***Przechowalni wirusów***. Wiadomosc jest pózniej przekazywana do programu pocztowego.

- ***Poczta wychodzaca:*** Wiadomosc jest wysylana z programu pocztowego do skladnika Skaner poczty e-mail, gdzie jest sprawdzana wraz z zalacznikami w poszukiwaniu wirusów. Nastepnie wiadomosc jest wysylana do serwera SMTP (*skanowanie wychodzacych wiadomosci e-mail jest domyslnie wylaczone i mozna je skonfigurowac recznie*).

Uwaga: *Skaner poczty e-mail nie jest przeznaczony dla platform serwerowych!*

8.7.2. Interfejs Skanera poczty e-mail



Interfejs skladnika ***Skaner poczty e-mail*** zawiera krótki opis jego funkcji, informacje o stanie (Skladnik *Skaner poczty e-mail jest aktywny.*) oraz nastepujace statystyki:

- ***Razem przeskanowanych wiadomosci e-mail*** — liczba wiadomosci e-mail przeskanowanych od czasu ostatniego uruchomienia skladnika ***Skaner poczty e-mail*** (*w razie potrzeby ta wartosc moze zostac zresetowana, np. dla celów statystycznych — Resetuj wartosc*)
- ***Zagrozen znalezionych i zablokowanych*** — liczba zainfekowanych wiadomosci wykrytych od czasu ostatniego uruchomienia ***Skanera poczty e-mail***.
- ***Zainstalowany plugin poczty e-mail*** — informacje o pluginie odpowiednim dla Twojego domyslnego klienta poczty

Podstawowa konfiguracja skladnika

W dolnej czesci okna znajduje sie sekcja ***Skaner poczty e-mail - Ustawienia*** , w

której mozna skonfigurowac podstawowe funkcje skladnika:

- ***Skanuj wiadomosci przychodzace*** — pozycje te nalezy zaznaczyc, aby wszystkie wiadomosci e-mail przychodzace na dane konto pocztowe byly skanowane w poszukiwaniu wirusów. Domyslnie ta opcja jest wlaczona i nie zaleca sie zmian w tych ustawieniach!

- ***Skanuj wiadomosci wychodzace*** — zaznaczenie tej opcji pozwala okreslic, czy powinny byc skanowane wszystkie wiadomosci e-mail wysylane z konta pocztowego. Opcja ta jest domyslnie wylaczona.

- ***Wyswietlaj ikone powiadomienia, gdy wiadomosc e-mail jest skanowana*** — pozycje nalezy zaznaczyc, jesli nad ikona AVG na pasku zadan ma byc wyswietlane odpowiednie okno powiadomienia w chwili, gdy poczta jest skanowana przez skladnik ***Skaner poczty e-mail***. Domyslnie ta opcja jest wlaczona i nie zaleca sie zmian w tych ustawieniach!

Dostep do zaawansowanej konfiguracji ***Skanera poczty e-mail*** mozna uzyskac z poziomu menu ***Narzedzia / Ustawienia zaawansowane***. Wszelkie zmiany w konfiguracji powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników!

Uwaga: *Dostawca oprogramowania AVG skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu glównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

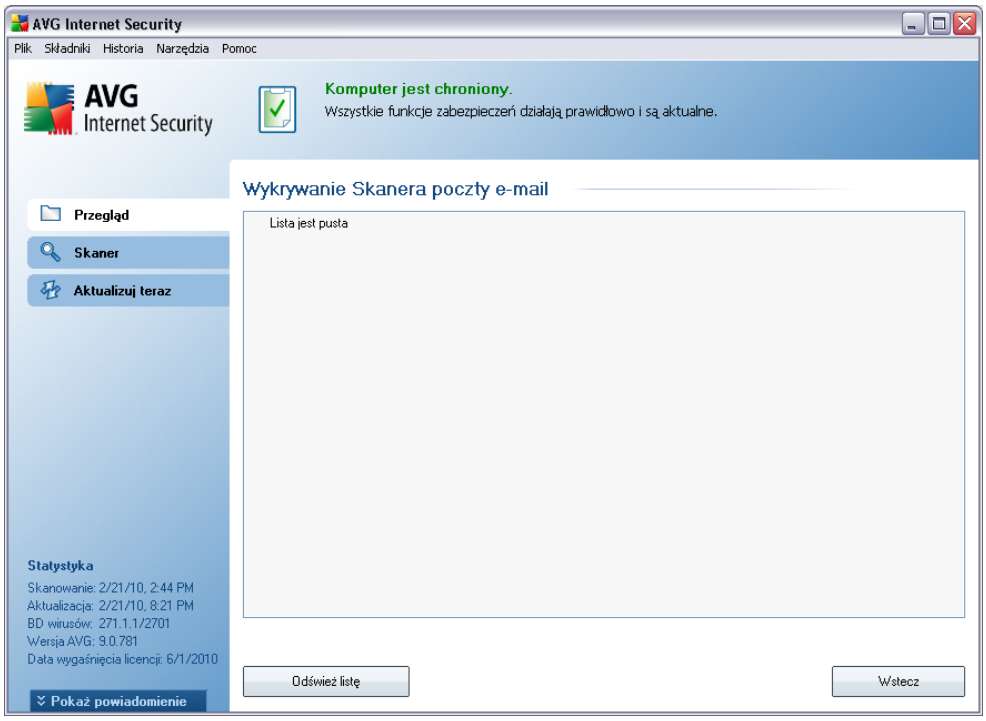
Przyciski kontrolne

W interfejsie ***Skanera poczty e-mail*** dostepne sa nastepujace przyciski kontrolne:

- ***Zapisz zmiany*** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.

- ***Anuluj*** — klikniecie tego przycisku powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (przegladu skladników).

8.7.3. Zagrozenia wykryte przez Skaner poczty e-mail



W oknie ***Zagrozenia wykryte przez Skaner poczty e-mail*** (*dostepnym po wybraniu odpowiedniej opcji z menu Historia*) wyswietlana jest lista wszystkich obiektów wykrytych przez skladnik ***Skaner poczty e-mail***. Podawane sa tam nastepujace informacje:

- ***Infekcja***— opis (ewentualnie nazwa) wykrytego zagrozenia.
- ***Obiekt*** — lokalizacja obiektu.
- ***Wynik*** — dzialanie podjete w zwiazku z wykryciem.
- ***Czas wykrycia*** — data i godzina wykrycia podejrzanego obiektu.
- ***Typ obiektu*** — typ wykrytego obiektu.

U dolu okna znajduja sie informacje na temat lacznej liczby wykrytych infekcji. Ponadto, mozna wyeksportowac cala liste obiektów do pliku, (***Eksportuj liste do pliku***) lub usunac wszystkie jej pozycje (***Opróznij liste***).

Przyciski kontrolne

W interfejsie skladnika ***Skaner poczty e-mail*** dostepne sa nastepujace przyciski sterujace:

- ***Odswiez liste*** — aktualizuje liste wykrytych zagrozen.
- ***Wstecz***— przelacza z powrotem do domyslnego ***Interfejsu uzytkownika systemu AVG*** (przegladu skladników).

8.8. Skladnik ID Protection

AVG Identity Protection to program chroniacy przed szkodliwym oprogramowaniem; jego głównym zadaniem jest zapobieganie kradziezom hasel, rachunków bankowych, numerów kart kredytowych i innych cennych danych przez oprogramowanie typu *malware*. Gwarantuje on, ze wszystkie programy uruchomione na komputerze dzialaja prawidlowo. ***AVG Identity Protection*** wykrywa i blokuje podejrzane zachowanie (dzieki stalemu nadzorowi), a takze chroni komputer przed nowym szkodliwym oprogramowaniem.

8.8.1. Podstawy dzialania ID Protection

Skladnik AVG Identity Protection sluzy do ochrony przed szkodliwym oprogramowaniem, zapewniajac ochrone przed wszystkimi jego rodzajami (*jak np. programami szpiegujacymi, botami, kradziezami tozsamosci itp.*), uzywajac technologii behawioralnych. Poniewaz szkodliwe oprogramowanie jest coraz bardziej zaawansowane i przybiera postac zwyklych programów, które moga jednak narazic komputer na zdalny atak w celu kradziezy tozsamosci, skladnik ***AVG Identity Protection*** zapewnia ochrone przed wszystkimi podejrzanymi aplikacjami. Aplikacja dopelnia ochrone zapewniana przez skladnik ***AVG Anti-Virus***, który zabezpiecza przed znanymi wirusami, korzystajac z mechanizmu skanowania i analizy sygnatur.

Stanowczo zalecamy zainstalowanie zarówno skladnika AVG Anti-Virus, jak i AVG Identity Protection. Razem zapewniaja one kompleksowa ochrone komputera.

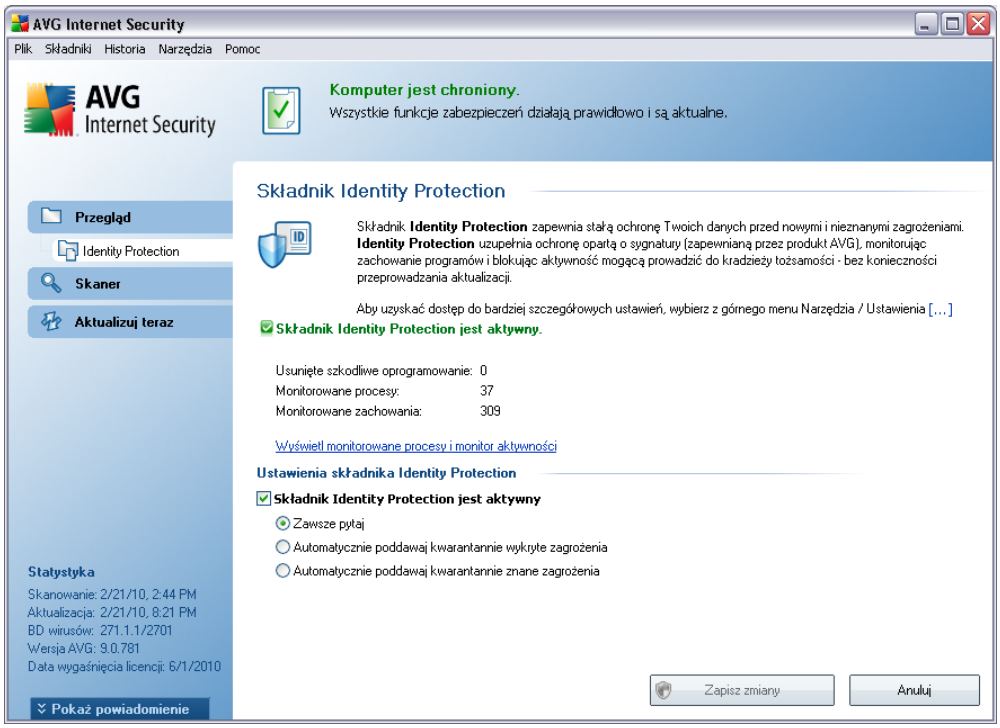
8.8.2. Interfejs skladnika ID Protection

Interfejs skladnika ***Identity Protection***zawiera krótki opis jego podstawowych funkcji, stanu (*Skladnik AVG Identity Protection jest aktywny i dziala poprawnie.*) i niektórych danych statystycznych:

- ***Usuniete szkodliwe oprogramowanie*** — zawiera liczbe aplikacji wykrytych

jako szkodliwe oprogramowanie (a nastepnie usunietych)

- ***Monitorowane procesy*** — liczba obecnie uruchomionych aplikacji, które sa monitorowane przez skladnik IDP
- ***Monitorowane zachowania*** — liczba okreslonych czynnosci uruchomionych w monitorowanych aplikacjach



Podstawowa konfiguracja skladnika

W dolnej czesci okna dialogowego znajduje sie sekcja ***Ustawienia skladnika Identity Protection***, w której mozna skonfigurowac jego podstawowe funkcje:

- ***Skladnik Identity Protection jest aktywny*** — (*domyslnie wlaczone*) nalezy zaznaczyc to pole, aby aktywowac skladnik IDP i otworzyc dalsze opcje edycji.

W pewnych przypadkach program ***Identity Protection*** moze zglosic, ze plik pochodzacy z zaufanego zródla jest podejrzany lub niebezpieczny. Poniewaz program ***Identity Protection*** wykrywa zagrozenia na podstawie zachowania, takie zdarzenie ma zazwyczaj miejsce, gdy jakis program próbuje przechwytywac sekwencje klawiszy, instalowac inne programy lub gdy na komputerze

instalowany jest nowy sterownik.

Dlatego tez nalezy wybrac jedna z ponizszych opcji, aby okreslic zachowanie skladnika ***Identity Protection*** w przypadku wykrycia podejrzanej aktywnosci:

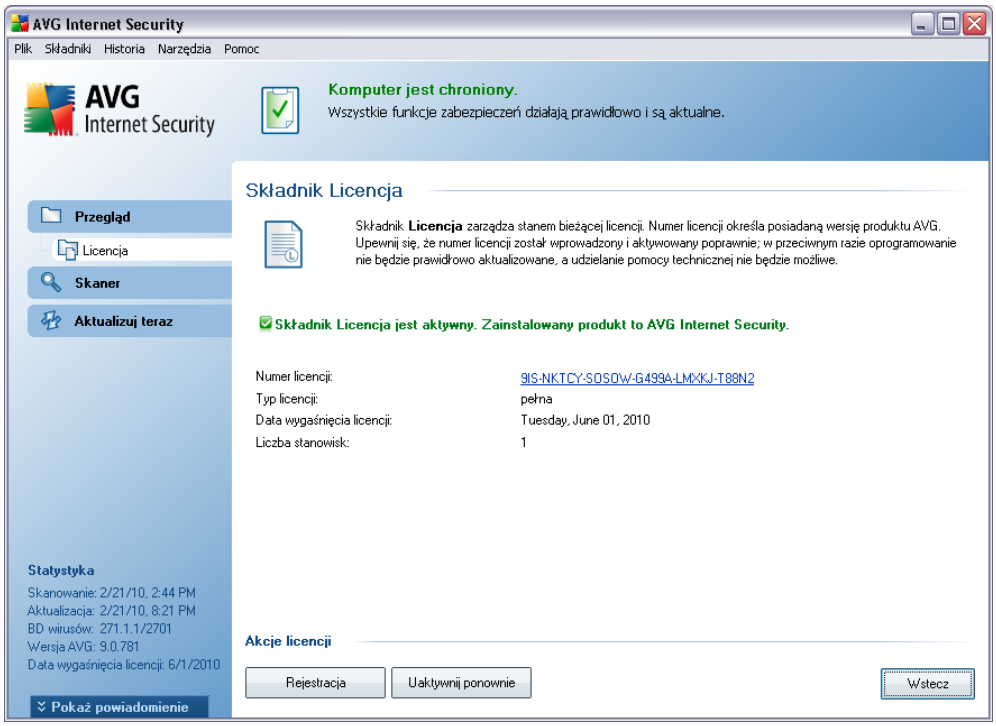
- ***Zawsze monituj*** — jesli aplikacja zostanie wykryta jako szkodliwe oprogramowanie, uzytkownik zostanie zapytany, czy ma ona zostac zablokowana (*ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego bez waznego powodu*)
- ***Automatycznie poddawaj kwarantannie wykryte zagrozenia*** — wszystkie aplikacje uznane za szkodliwe beda automatycznie blokowane
- ***Automatycznie poddawaj kwarantannie znane zagrozenia*** — tylko aplikacje, które z cala pewnoscia zostaly wykryte jako szkodliwe oprogramowanie, beda blokowane

Przyciski kontrolne

W interfejsie skladnika ***Identity Protection*** sa dostepne nastepujace przyciski sterujace:

- ***Zapisz zmiany*** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- ***Anuluj*** — klikniecie tego przycisku powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (przegladu skladników).

8.9. Licencja



Okno dialogowe skladnika ***Licencja*** zawiera krótki opis jego funkcji, informacje o jego biezacym stanie (Skladnik Licencja *jest aktywny.*), a takze nastepujace informacje:

- ***Numer licencji*** — dokladny numer licencji. Jezeli kiedykolwiek bedziesz proszony o podanie swojego numeru licencji, uzyj go w tej samej formie. Dlatego tez zdecydowanie zalecamy korzystanie z metody kopiuj-wklej w przypadku jakiejkolwiek manipulacji numerem licencji.

- ***Typ licencji*** — okresla typ zainstalowanego produktu.

- ***Data wygasniecia licencji*** — data okreslajaca okres waznosci licencji. Aby korzystac z systemu **AVG 9 Internet Security** po tej dacie, nalezy odnowic licencje. Licencje mozna odnowic online za posrednictwem witryny firmy AVG (http://www.avg.com/).

- ***Liczba stanowisk*** — liczba stacji roboczych, na których mozna zainstalowac system **AVG 9 Internet Security**.

Przyciski kontrolne

- ***Zarejestruj*** — laczy sie ze strona rejestracji w witrynie internetowej systemu AVG (http://www.avg.com/). Nalezy tam podac swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysluguje bezplatna pomoc techniczna.

- ***Uaktywnij ponownie*** — otwiera okno dialogowe ***Aktywacja programu AVG*** zawierajace dane wprowadzone na etapie ***Personalizacji programu AVG*** podczas Instalacji. W oknie tym mozna wprowadzic numer licencji w celu zastapienia numeru sprzedazy (*uzytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przyklad podczas uaktualnienia do nowego produktu AVG*).

Uwaga: W przypadku korzystania z próbnej wersji systemu *AVG 9 Internet Security*, **dostepne przyciski to** *Kup teraz* ***i*** *Aktywuj. Umozliwiaja one uaktualnienie programu do jego pelnej wersji. W przypadku systemu* **AVG 9 Internet Security** *zainstalowanego z numerem sprzedazy, te przyciski to* ***Zarejestruj*** *i* ***Aktywuj****.*

- ***Wstecz*** — klikniecie tego przycisku powoduje powrót do domyslnego Interfejsu uzytkownika systemu AVG (przegladu skladników).

8.10. LinkScanner

8.10.1. Zasady dzialania technologii LinkScanner

Skladnik ***LinkScanner®*** zapewnia darmowa ochrone przed witrynami internetowymi, które zdolne sa do instalowania na komputerze szkodliwego oprogramowania za posrednictwem przegladarki internetowej lub jej pluginów. Technologia skladnika ***LinkScanner*** sklada sie z dwóch funkcji: ***AVG Search-Shield*** i ***AVG Active Surf-Shield*** :

- ***Skladnik*** AçΓ Σεαρχη Σηιελδ zawiera liste witryn sieci Web (*adresów URL*), które uznane zostaly za niebezpieczne. Wszystkie wyniki wyszukiwania serwisów Google, Yahoo!, Bing, Baidu, Yandex i Altavista sa sprawdzane na podstawie tej listy, a nastepnie obok kazdego z nich wyswietlana jest odpowiednia ikona klasyfikacji bezpieczenstwa. (*w przypadku wyników wyszukiwania serwisu Yahoo! wyswietlane sa tylko ikony „niebezpieczna witryna”*). Jesli bezposrednio w przegladarce wprowadzony zostanie jakikolwiek adres, klikniety zostanie link na stronie WWW lub np. w wiadomosci e-mail, AVG automatycznie go

przeskanuje i — w razie potrzeby — adres zostanie zablokowany.

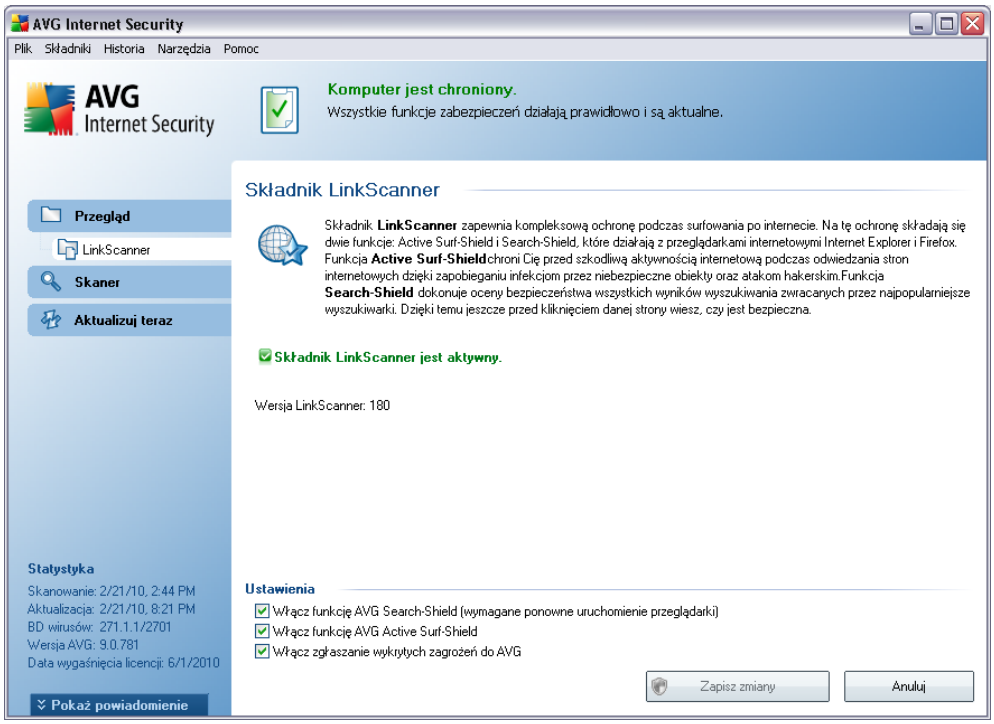
- ***Skladnik AVG Active Surf-Shield***skanuje zawartosc odwiedzanych witryn internetowych bez wzgledu na ich adres. Nawet jesli jakas witryna nie zostanie wykryta przez skladnik ***AVG Search Shield*** (*np. gdy utworzono nowa szkodliwa witryne sieci Web lub witryna wczesniej uznana za nieszkodliwa zawiera aktualnie niebezpieczny kod*), przy próbie jej odwiedzenia zostanie ona przeskanowana (a w razie podejrzen zablokowana) przez skladnik ***AVG Active Surf-Shield***.

Uwaga: *Technologia AVG LinkScanner nie jest przeznaczona dla platform serwerowych!*

8.10.2. Interfejs LinkScanner

Skladnik ***LinkScanner*** sklada sie z dwóch funkcji, które mozna wlaczyc lub wylaczyc w jego interfejsie:

Interfejs skladnika ***LinkScanner*** zawiera krótki opis jego funkcji oraz informacje na temat jego biezacego stanu (*Skladnik LinkScanner jest aktywny*). Co wiecej, mozna tam znalezc informacje o numerze wersji najnowszej bazy danych skladnika ***LinkScanner*** (*Wersja skladnika LinkScanner*).



W dolnej czesci okna dialogowego mozliwa jest edycja nastepujacych opcji:

- ***Wlacz skladnik AVG Search-Shield*** (*opcja domyslnie wlaczona*) — skanuje wszystkie lacza pojawiajace sie w wynikach wyszukiwania serwisów Google, Yahoo!, Bing, Baidu, Yandex i Altavista, a nastepnie obok kazdego z nich wyswietla odpowiednia klasyfikacje bezpieczenstwa.

- ***Wlacz funkcje AVG Active Surf-Shield*** — (*domyslnie wlaczona*): aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (*w czasie rzeczywistym*). Znane zlosliwe witryny i ich niebezpieczna zawartosc blokowane sa juz w momencie otwarcia ich przez uzytkownika za pomoca przegladarki (*lub jakiejkolwiek innej aplikacji korzystajacej z protokolu HTTP*).

- ***Wlacz zglaszanie wykrytych zagrozen do firmy AVG*** — nalezy zaznaczyc to pole, aby wlaczyc raportowanie exploitów oraz niebezpiecznych witryn znalezionych przy uzyciu funkcji ***Safe Surf*** lub ***Safe Search***. Informacje te sa przekazywane do naszej bazy danych.

8.10.3. AVG Search-Shield

Podczas surfowania po internecie z wlaczonym skladnikiem ***AVG Search-Shield*** wszystkie wyniki zwracane przez najbardziej popularne wyszukiwarki internetowe, np. Yahoo!, Google, Bing, Altavista, Yandex itd. sa oceniane pod katem obecnosci niebezpiecznego lub podejrzanego kodu. Sprawdzajac te lacza i oznaczajac niebezpieczne, skladnik ***AVG Link Scanner*** ostrzega przed przejsciem na niebezpieczna lub podejrzana strone. Dzieki temu mozna miec pewnosc, ze odwiedza sie tylko bezpieczne witryny internetowe.

Obok ocenianego aktualnie wyniku wyszukiwania wyswietlany jest symbol informujacy o trwajacym sprawdzaniu lacza. Po zakonczeniu skanowania wyswietlana jest ikona informujaca o jego wynikach:

 Strona, do której prowadzi lacze, jest bezpieczna (*w wyszukiwarce Yahoo! ta ikona nie jest wyswietlana na pasku narzedzi AVG Security Toolbar!*).

 Strona, do której prowadzi lacze, nie zawiera zagrozen, ale jest podejrzana (*watpliwosci budzi jej pochodzenie lub przeznaczenie, wiec nie zaleca sie dokonywania na niej zakupów itp.*).

 Strona, do której prowadzi lacze, jest bezpieczna, ale zawiera lacza do potencjalnie niebezpiecznych stron lub podejrzany kod (który jednak nie stanowi bezposredniego zagrozenia).

Strona, do której prowadzi lacze, zawiera aktywne zagrozenia! Dla bezpieczenstwa uzytkownika dostep do tej strony zostanie zablokowany.

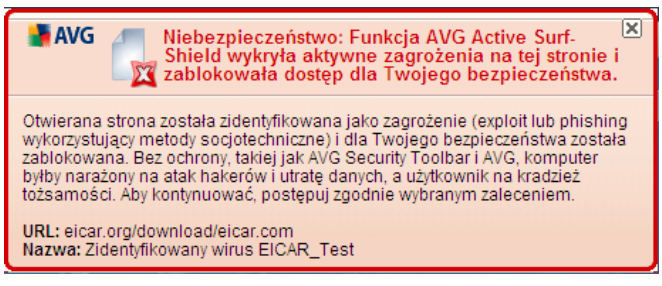
Strona, do której prowadzi lacze, nie jest dostepna i nie udalo sie jej przeskanowac.

Umieszczenie kursora na wybranej ikonie wyników sprawdzania powoduje wyswietlenie szczególowych informacji o danym laczu. Informacje te obejmuja dodatkowe szczegóły dotyczace zagrozenia (jesli sa dostepne), adres IP serwera docelowego, oraz czas skanowania strony przez produkt AVG:

8.10.4. AVG Active Surf-Shield

Ta zaawansowana funkcja ochrony blokuje szkodliwa zawartosc dowolnej otwieranej witryny internetowej, zapobiegajac pobraniu jej na dysk twardy. Gdy funkcja ta jest wlaczona, klikniecie linku lub wpisanie adresu URL prowadzacego do niebezpiecznej witryny powoduje automatycznie zablokowanie jej otwarcia, dzieki czemu komputer nie zostanie nieswiadomie zainfekowany. Nalezy pamietac, ze nawet samo wyswietlenie niebezpiecznej witryny internetowej moze zainfekowac komputer. Dlatego tez, gdy zostanie wywolana strona zawierajaca kod wykorzystujacy luki zabezpieczen lub inne powazne zagrozenia, skladnik ***AVG Link Scanner*** nie pozwoli na jej wyswietlenia w przegladarce.

Jesli kiedykolwiek trafisz na szkodliwa strone internetowa, ***skladnik Link Scanner*** wyswietli w przegladarce ostrzezenie podobne do tego:



Odwiedzanie takiej witryny jest bardzo ryzykowne i nalezy tego unikac!

8.11. Ochrona Sieci

8.11.1. Zasady dzialania skladnika Ochrona Sieci

Ochrona Sieci to rodzaj programu rezydentnego, zapewniajacego ochrone w czasie rzeczywistym. Skanuje on zawartosc odwiedzanych stron internetowych (oraz znajdujacych sie na nich plików) jeszcze zanim zostana wyswietlone w przegladarce lub pobrane na dysk twardy.

Ochrona Sieci wykrywa strony zawierajace niebezpieczny kod javascript i blokuje ich ladowanie. Ponadto, identyfikuje szkodliwe oprogramowanie zawarte na stronach WWW i w razie podejrzen zatrzymuje pobieranie, aby nie dopuscic do infekcji komputera.

Uwaga: *Ochrona Sieci nie jest przeznaczona dla platform serwerowych!*

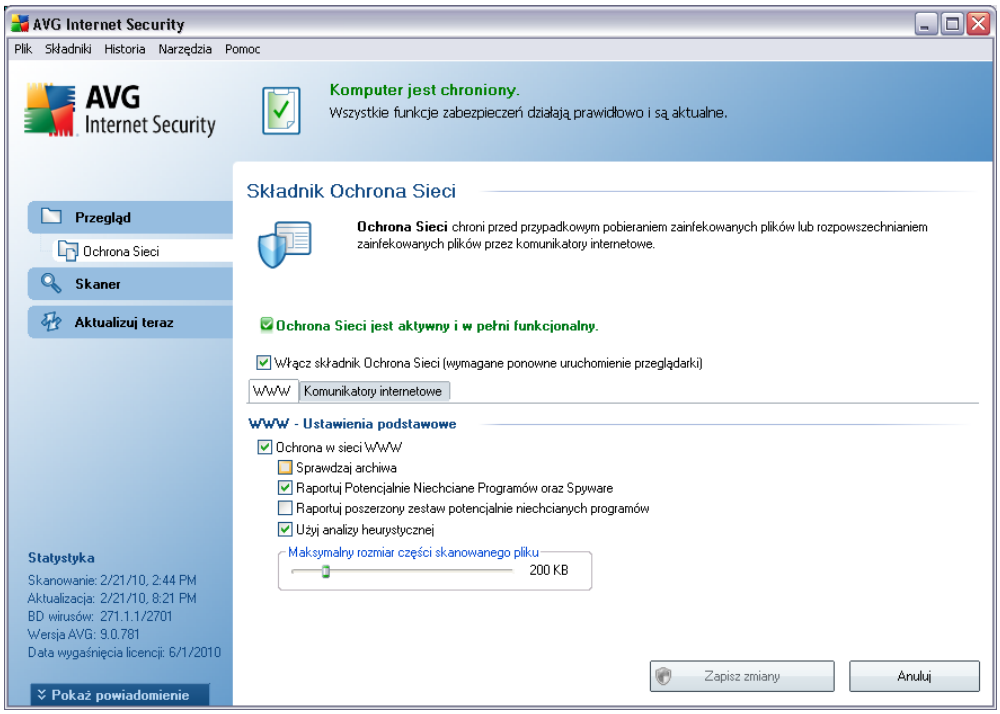
8.11.2. Interfejs skladnika Ochrona Sieci

Interfejs skladnika ***Ochrona Sieci*** opisuje dzialanie tego rodzaju ochrony. Znajduja sie tam informacje na temat jej biezacego stanu (*Skladnik Ochrona Sieci jest aktywny i w pelni funkcjonalny.*). W dolnej czesci okna widoczne sa podstawowe opcje Ochrony sieci WWW.

Podstawowa konfiguracja skladnika

Najistotniejsza opcja umozliwia natychmiastowe wlaczenie lub wylaczenie skladnika ***Ochrona Sieci*** (mozna to zrobic, zaznaczajac lub usuwajac zaznaczenie pola ***Wlacz Ochrone Sieci***). Opcja ta jest domyslnie wlaczona, a skladnik ***Ochrona Sieci*** aktywny. Jednak jesli nie istnieja wazne powody do zmiany tego ustawienia, zaleca sie pozostawienie skladnika aktywnego. Jesli to pole jest zaznaczone, a skladnik ***Ochrona Sieci*** jest wlaczony, na dwóch kolejnych kartach znajduja sie dalsze opcje konfiguracji:

- ***WWW*** — karta odpowiadajaca za skanowanie zawartosci witryny internetowych. Interfejs pozwala modyfikowac nastepujace ustawienia:



- ***Ochrona sieci WWW*** — potwierdza, ze skladnik ***Ochrona Sieci*** ma skanowac zawartosc stron internetowych. Jesli ta opcja jest aktywna (*domyslnie*), mozna wlaczyc lub wylaczyc nastepujace funkcje:

  - ***Skanuj wewnatrz archiwów*** — skanowanie ma obejmowac takze archiwa dostepne na odwiedzanych stronach WWW.

  - ***Raportuj zagrozenia potencjalnie niechcianymi programami i oprogramowaniem szpiegujacym*** (*opcja domyslnie wlaczona*) — zaznaczenie tego pola powoduje wlaczenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegujacego (a nie tylko wirusów). Oprogramowanie szpiegujace nalezy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrozenie dla bezpieczenstwa, ale niektóre z takich programów moga zostac zainstalowane umyslnie. Nie zaleca sie wylaczania tej opcji — znaczaco zwieksza ona poziom ochrony komputera

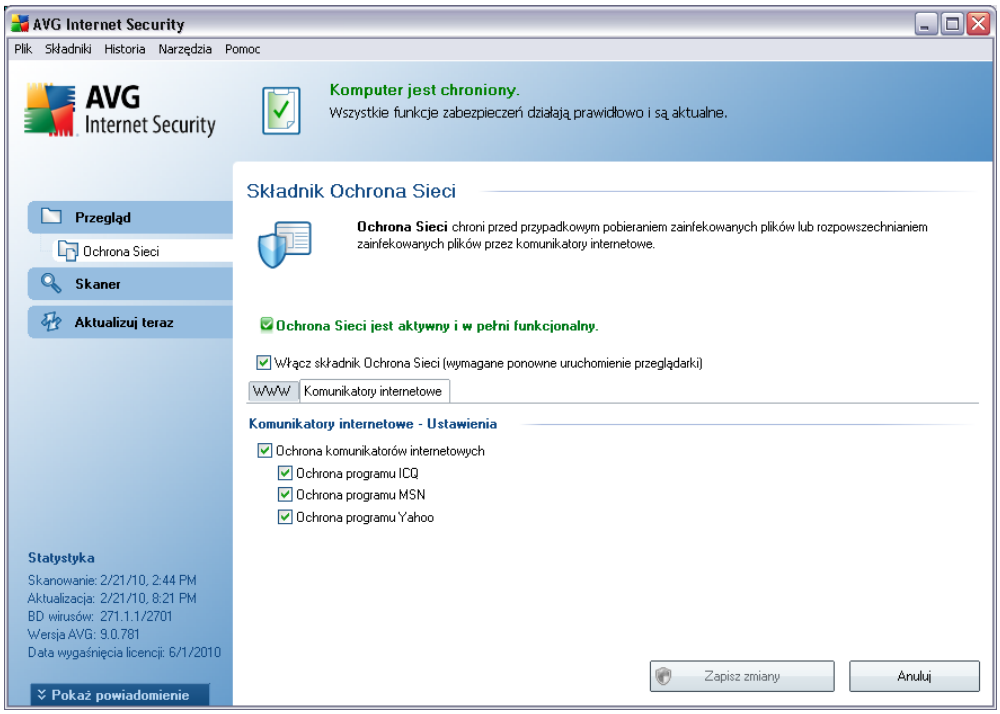
  - ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** — jesli poprzednia opcja jest aktywna, mozna równiez zaznaczyc to pole, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie

bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona.

- ***Uzyj heurystyki*** — skanowanie zawartosci wyswietlanych stron ma wykorzystywac analize heurystyczna, czyli dynamiczna symulacje i ocene instrukcji skanowanego obiektu w wirtualnym srodowisku. Dlatego tez metoda ta pozwala wykryc nawet taki szkodliwy kod, który nie zostal jeszcze opisany w bazie danych wirusów *(patrz rozdzial Zasady dzialania skladnika Anti-Virus)*.

- ***Maksymalny rozmiar skanowanych plików*** — jesli wyswietlana strona zawiera pliki, mozna skanowac ich zawartosc jeszcze przed pobraniem na twardy dysk. Poniewaz jednak skanowanie obszernych plików zajmuje dluzszy czas, otwieranie stron WWW moze zostac znacznie spowolnione. Za pomoca tego suwaka mozna okreslic maksymalny rozmiar plików, które maja byc skanowane przez skladnik ***Ochrona Sieci*** . Nawet jesli pobierany plik jest wiekszy od wybranego limitu i nie zostanie przeskanowany przez ***Ochrone Sieci***, nie zmniejsza to Twojego bezpieczenstwa: jesli plik jest zainfekowany, skladnik ***Ochrona rezydentna*** natychmiast to wykryje.

- ***Komunikatory internetowe*** — karta umozliwiajaca edycje ustawien monitorowania komunikatorów internetowych (*np. ICQ, MSN Messenger, Yahoo itp.*).



- Ochrona komunikatorów internetowych — zaznacz to pole, jesli chcesz, aby Ochrona Sieci zapewniala bezpieczenstwo komunikacji online. O ile opcja ta jest zaznaczona, mozna dodatkowo okreslic, które komunikatory internetowe maja byc kontrolowane — aktualnie program AVG**AVG 9 Internet Security** obsluguje aplikacje ICQ, MSN oraz Yahoo.

Uwaga: Dostawca oprogramowania AVG *skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu głównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

Przyciski kontrolne

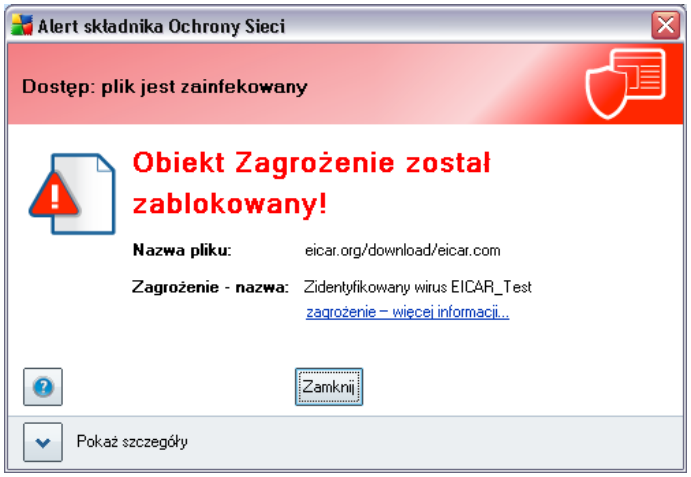
W interfejsie skladnika ***Ochrona rezydentna*** dostepne sa nastepujace przyciski kontrolne:

- ***Zapisz zmiany*** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.

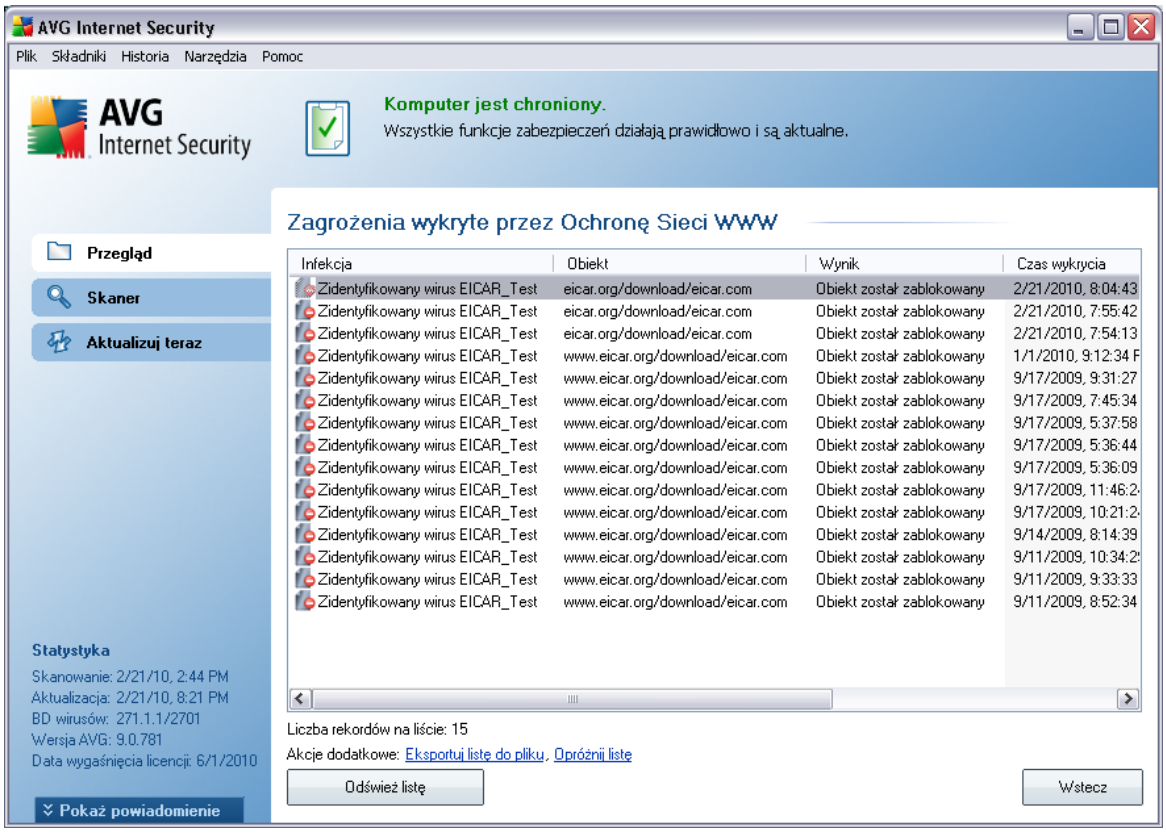
- ***Anuluj*** — powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (*przegladu skladników*).

8.11.3. Obiekt wykryty przez skladnik Ochrona Sieci

Ochrona Sieci skanuje zawartosc odwiedzanych stron internetowych (oraz znajdujacych sie na nich plików) jeszcze zanim zostana wyswietlone w przegladarce lub pobrane na dysk twardy. Wykrycie jakiegokolwiek zagrozenia powoduje natychmiastowe wyswietlenie nastepujacego okna:



Podejrzana strona nie zostanie otwarta, a wykryty obiekt zostanie zapisany na liscie ***zagrozen wykrytych przez Ochrone Sieci*** (ten przeglad wykrytych zagrozen jest dostepny z menu systemowego po wybraniu opcji ***Historia / Zagrozenia wykryte przez Ochrone Sieci***.



Podawane sa tam nastepujace informacje:

- ***Infekcja***— opis (*ewentualnie nazwa*) wykrytego zagrozenia.
- ***Obiekt*** — zródlo obiektu (*strona WWW*)
- ***Wynik*** — dzialanie podjete w zwiazku z wykryciem.
- ***Czas wykrycia*** — data i godzina wykrycia i zablokowania zagrozenia
- ***Typ obiektu*** — typ wykrytego obiektu.
- ***Proces*** — akcja wykonana w celu wywolania potencjalnie niebezpiecznego obiektu (co umozliwilo jego wykrycie).

U dolu okna znajduja sie informacje na temat lacznej liczby wykrytych infekcji. Ponadto, mozna wyeksportowac cala liste obiektów do pliku, (***Eksportuj liste do pliku***) lub usunac wszystkie jej pozycje (***Opróznij liste***). Przycisk ***Odswiez liste*** pozwala

zaktualizowac liste obiektów wykrytych przez skladnik ***Ochrona Sieci***. Przycisk ***Wstecz*** przelacza z powrotem do domyslnego okna ***Interfejsu uzytkownika systemu AVG*** (przegladu skladników).

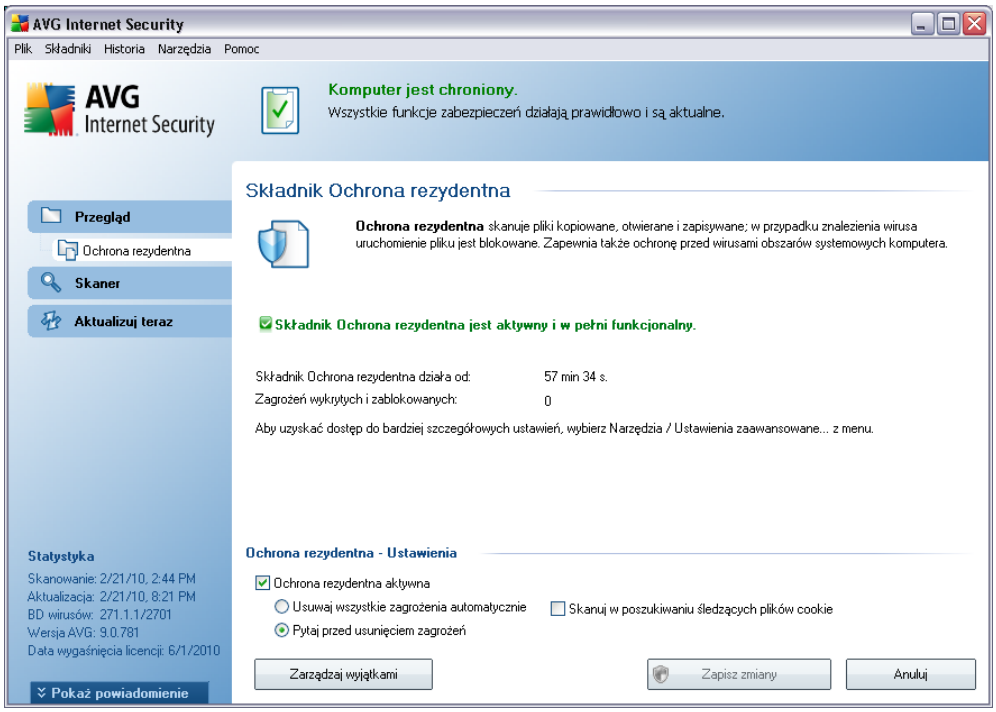
8.12. Ochrona rezydentna

8.12.1. Zasady dzialania Ochrony rezydentnej

Skladnik ***Ochrona rezydentna*** zapewnia stala ochrone komputera. Skladnik ten skanuje kazdy otwierany, zapisywany lub kopiowany plik, oraz chroni obszary systemowe komputera. Po wykryciu wirusa w przetwarzanym pliku, ***Ochrona rezydentna*** zatrzymuje aktualnie wykonywane operacje i uniemozliwia uaktywnienie sie wirusa. Uzytkownik zwykle nie zauwaza dzialania tego skladnika, poniewaz funkcjonuje ona „w tle" i wyswietla powiadomienia tylko w przypadku, gdy wykryje zagrozenie. Domyslna reakcja ***Ochrony rezydentnej*** jest zablokowanie dostepu do niebezpiecznego pliku. Skladnik ***Ochrona rezydentna*** jest ladowany do pamieci komputera podczas uruchamiania systemu.

Ostrzezenie: Ochrona rezydentna ladowana jest do pamieci komputera podczas uruchamiania systemu i musi pozostac wlaczona przez caly czas!

8.12.2. Interfejs skladnika Ochrona rezydentna



Oprócz przegladu najwazniejszych statystyk oraz informacji na temat stanu skladnika (*skladnik Ochrona rezydentna jest aktywny i w pelni funkcjonalny*), interfejs ***Ochrony rezydentnej*** oferuje takze kilka elementarnych opcji konfiguracyjnych. Wyswietlane sa nastepujace statystyki:

- ***Ochrona Rezydenta dziala od*** — okresla czas, jaki uplynal od ostatniego uruchomienia skladnika.
- ***Zagrozenia wykryte i zablokowane*** — liczba wykrytych infekcji, do których uruchomienia/otwarcia nie dopuszczono (*w razie potrzeby ta wartosc moze zostac zresetowana, np. do celów statystycznych — Resetuj wartosc*)

Podstawowa konfiguracja skladnika

W dolnej czesci okna dialogowego znajduje sie sekcja o nazwie ***Ochrona rezydentna — Ustawienia*** , w której mozna edytowac niektóre jej podstawowe funkcje (*szczególowa konfiguracja, podobnie jak w wypadku innych skladników, dostepna jest za posrednictwem menu Narzedzia/Ustawienia zaawansowane*).

Pole ***Ochrona rezydentna aktywna*** umozliwia latwe wlaczanie/wylaczanie Ochrony rezydentnej. Domyslnie funkcja ta jest wlaczona. Gdy Ochrona rezydentna jest wlaczona, mozna okreslic w jaki sposób ma reagowac na wykryte infekcje:

- automatycznie (***Usuwaj wszystkie zagrozenia automatycznie***)
- lub tylko za zgoda uzytkownika (***Pytaj przed usunieciem zagrozen***).

Wybór te nie ma wplywu na poziom bezpieczenstwa — umozliwia on jedynie podjecie kazdorazowej decyzji o usunieciu lub pozostawieniu wykrytych infekcji.

W obu przypadkach mozna okreslic, czy pliki maja byc ***skanowane w poszukiwaniu sledzacych plików cookie***. W konkretnych wypadkach mozna wlaczyc te opcje, aby osiagnac najwyzszy poziom ochrony, ale domyslnie jest ona wylaczona. (*pliki cookie to dane tekstowe wysylane przez serwer do przegladarki, która przy nastepnych odwiedzinach na danej stronie udostepni je serwerowi w celach identyfikacyjnych. Pliki cookie sa uzywane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach — np. preferencji dotyczacych wygladu witryny lub zawartosci koszyka w sklepach internetowych*).

Uwaga: Dostawca oprogramowania AVG *skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu głównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

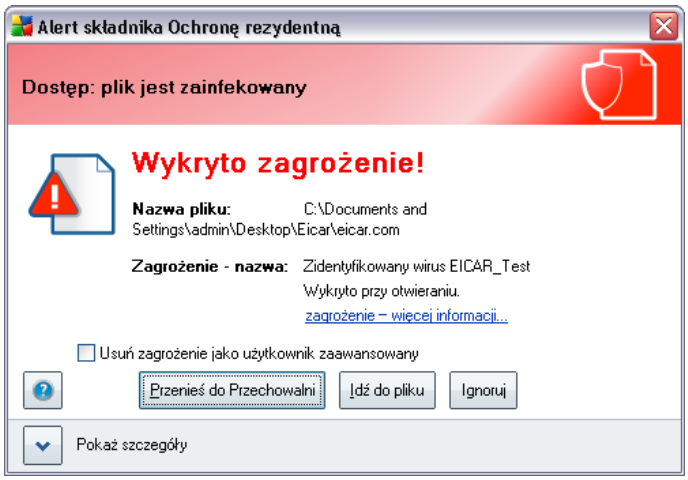
Przyciski kontrolne

W interfejsie skladnika ***Ochrona rezydentna*** dostepne sa nastepujace przyciski kontrolne:

- ***Zarzadzaj wyjatkami*** otwiera okno dialogowe ***Ochrona rezydentna — Wykluczone foldery***, w którym mozna zdefiniowac foldery pomijane przy skanowaniu przez skladnik ***Ochrona rezydentna***.
- ***Zapisz zmiany*** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- ***Anuluj*** — klikniecie tego przycisku powoduje powrót do domyslnego okna ***Interfejsu uzytkownika AVG*** (przegladu skladników).

8.12.3. Zagrozenia wykryte przez Ochrone rezydentna

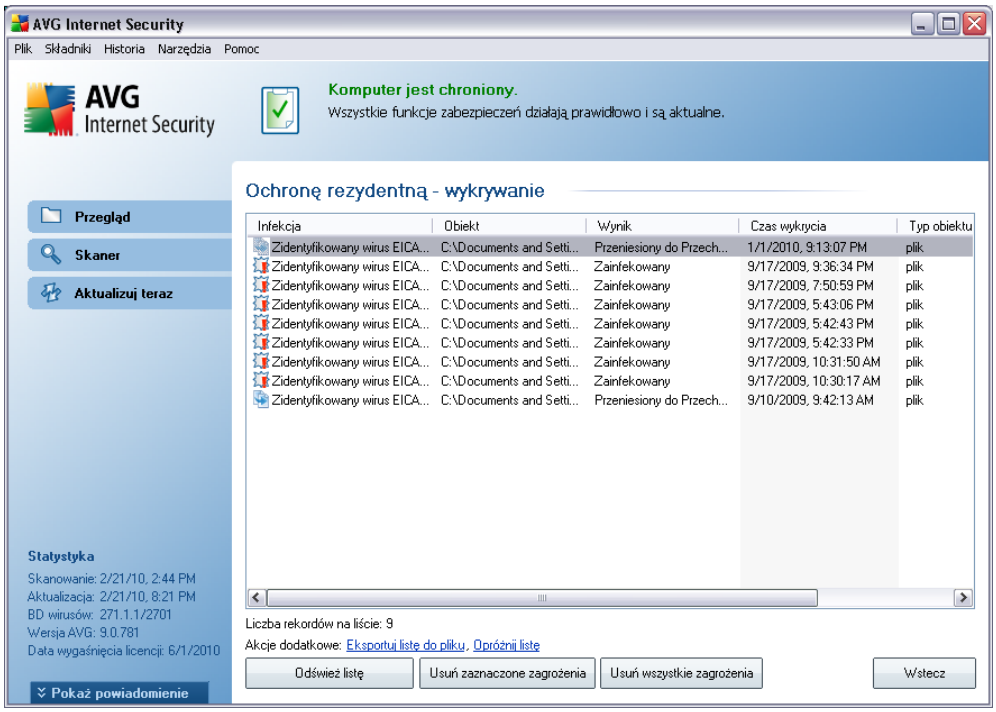
Ochrona rezydentna to skladnik sluzacy do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrozenia powoduje natychmiastowe wyswietlenie nastepujacego ostrzezenia:



Okno to zawiera informacje dotyczace wykrytej infekcji i pozwala wybrac czynnosc, która ma zostac wykonana:

- ***Wylecz*** — jesli mozliwe jest wyleczenie pliku, system AVG zrobi to automatycznie (opcja zalecana).
- ***Przenies do Przechowalni*** — wirus zostanie przeniesiony do ***Przechowalni wirusów AVG***
- ***Przejdz do pliku*** — pozwala przejsc do lokalizacji podejrzanego obiektu (*w nowym oknie Eksploratora Windows*)
- ***Ignoruj*** — tej opcji NIE nalezy uzywac bez uzasadnionego powodu!

Przeglad wszystkich zagrozen wykrytych przez skladnik ***Ochrona rezydentna*** mozna znalezc w oknie dialogowym ***Zagrozenia wykryte przez Ochrone rezydentna*** dostepnym poprzez menu ***Historia / Zagrozenia wykryte przez Ochrone rezydentna***:



Okno ***Zagrozenia wykryte przez Ochrone rezydentna*** zawiera przeglad obiektów wykrytych i uznanych przez ten skladnik ***za niebezpieczne (które nastepnie wyleczono lub przeniesiono do ***Przechowalni wirusów***). Podawane sa tam nastepujace informacje:

- ***Infekcja***— opis (ewentualnie nazwa) wykrytego zagrozenia.
- ***Obiekt*** — lokalizacja obiektu.
- ***Wynik*** — dzialanie podjete w zwiazku z wykryciem.
- ***Czas wykrycia*** — data i godzina wykrycia obiektu.
- ***Typ obiektu*** — typ wykrytego obiektu.
- ***Proces*** — akcja wykonana w celu wywolania potencjalnie niebezpiecznego obiektu (co umozliwilo jego wykrycie).

U dolu okna znajduja sie informacje na temat lacznej liczby wykrytych infekcji. Ponadto, mozna wyeksportowac cala liste obiektów do pliku, (***Eksportuj liste do pliku***) lub usunac wszystkie jej pozycje (***Opróznij liste***). Przycisk ***Odswiez liste*** pozwala zaktualizowac liste obiektów wykrytych przez ***Ochrone rezydentna***. Przycisk ***Wstecz***

przelacza z powrotem do domyslnego okna ***Interfejsu uzytkownika systemu AVG*** (przegladu skladników).

8.13. Menedzer aktualizacji

8.13.1. Zasady dzialania Menedzera aktualizacji

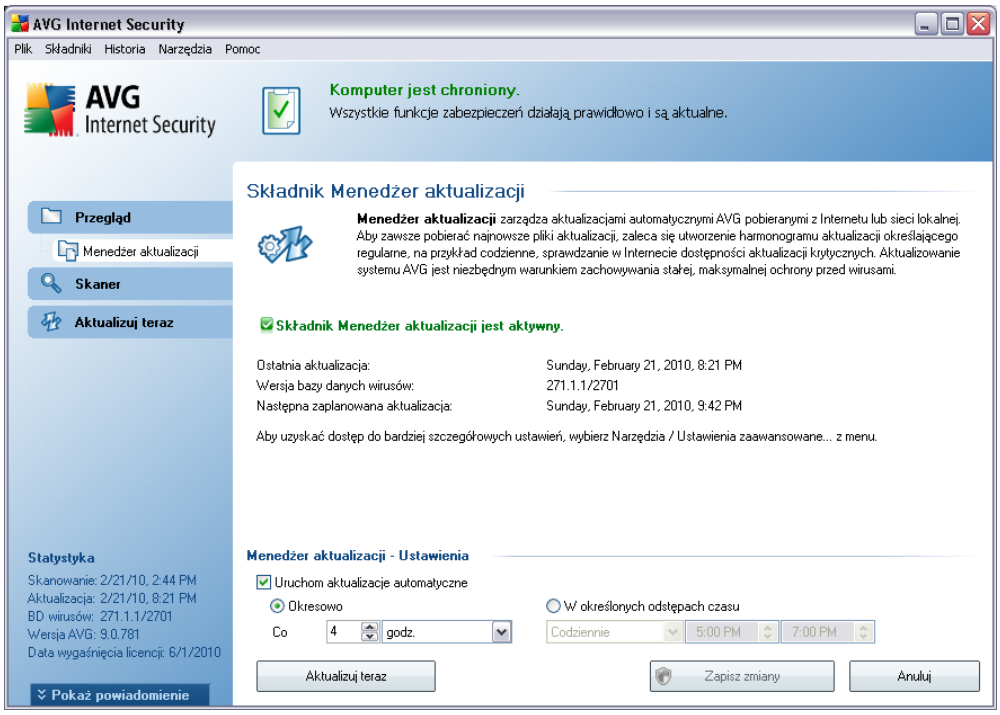
Zadne oprogramowanie zabezpieczajace nie moze zapewnic realnej ochrony przed róznymi typami zagrozen bez regularnych aktualizacji! Twórcy wirusów nieustannie szukaja nowych luk w programach i systemach operacyjnych, które mogliby wykorzystac. Nowe wirusy, szkodliwe oprogramowanie i metody ataków pojawiaja sie kazdego dnia. Z tego powodu dostawcy oprogramowania na biezaco wydaja aktualizacje i poprawki zabezpieczen, które maja usuwac wykryte luki.

Regularne aktualizacje systemu AVG sa kluczowe dla Twojego bezpieczenstwa!

Pomaga w tym skladnik ***Menedzer aktualizacji***. Za jego pomoca mozna zaplanowac automatyczne pobieranie aktualizacji (z internetu lub sieci lokalnej). Jesli jest to mozliwe, definicje wirusów nalezy pobierac codziennie. Mniej istotne aktualizacje programu mozna pobierac co tydzien.

Uwaga: *Wiecej informacji na temat typów i poziomów aktualizacji zawiera rozdzial Aktualizacje AVG.*

8.13.2. Interfejs Menedzera aktualizacji



Interfejs skladnika·***Menedzer aktualizacji*** zawiera informacje o jego funkcjach i biezacym stanie (Skladnik *Menedzer aktualizacji jest aktywny.*), a takze istotne statystyki:

- ***Ostatnia aktualizacja*** — data i godzina ostatniej aktualizacji bazy danych.
- ***Wersja bazy danych wirusów*** — numer ostatniej wersji bazy danych wirusów; numer ten jest zwiekszany przy kazdej aktualizacji bazy danych.
- ***Nastepna zaplanowana aktualizacja*** — godzina i data kolejnej zaplanowanej aktualizacji.

Podstawowa konfiguracja skladnika

W dolnej czesci okna dialogowego znajduje sie sekcja ***ustawien Menedzera aktualizacji***, w której mozna wprowadzac zmiany regul uruchamiania procesu aktualizacji. Mozna okreslic tam, czy pliki aktualizacyjne maja byc pobierane automatycznie (***Uruchom aktualizacje automatyczne***), czy tylko na zadanie. Opcja ***Uruchom aktualizacje automatyczne*** jest wlaczona i zaleca sie pozostawienie jej w

tym stanie. Regularne pobieranie najnowszych aktualizacji ma kluczowe znaczenie dla prawidlowego funkcjonowania kazdego oprogramowania zabezpieczajacego!

Ponadto, mozna okreslic, kiedy aktualizacje maja byc uruchamiane:

- ***Okresowo*** — nalezy zdefiniowac interwal aktualizacji.
- ***O okreslonej godzinie*** — nalezy zdefiniowac dokladna date i godzine.

Domyslny interwal aktualizacji to 4 godziny. Stanowczo nie zaleca sie zmiany tych opcji bez uzasadnionej przyczyny!

Uwaga: Dostawca oprogramowania AVG *skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu głównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

Przyciski kontrolne

W interfejsie skladnika ***Menedzer aktualizacji*** dostepne sa nastepujace przyciski kontrolne:

- ***Aktualizuj teraz*** — klikniecie przycisku uruchamia natychmiastowa aktualizacje na zadanie.
- ***Zapisz zmiany*** — klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- ***Anuluj*** — klikniecie tego przycisku powoduje powrót do domyslnego okna ***Interfejsu uzytkownika AVG*** (przegladu skladników).

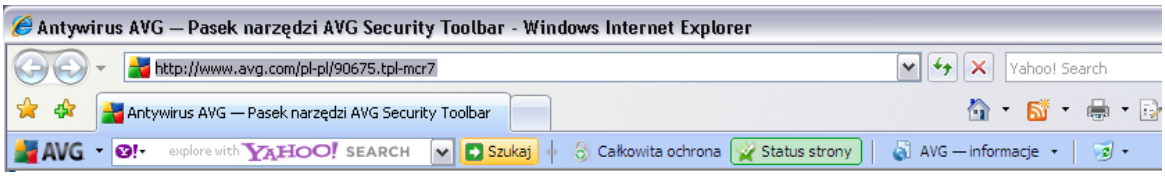
9. Pasek narzedzi AVG Security Toolbar

Pasek narzedzi AVG Security Toolbar to nowy plugin współpracujacy ze skladnikiem ***AVG Link Scanner***. Zadaniem paska jest sprawdzanie wyników zwracanych przez obslugiwane wyszukiwarki internetowe (*Yahoo!, Google, Bing, Altavista, Baidu*). ***Pasek narzedzi AVG Security Toolbar*** pozwala na kontrolowanie funkcji skladnika ***AVG Link Scanner*** i dostosowywanie jego zachowania.

Jesli w czasie instalacji systemu **AVG 9 Internet Security** zostanie wybrana instalacja paska narzedzi, automatycznie nastapi jego dodanie do przegladarki internetowej. Uwaga: W przypadku korzystania z alternatywnej przegladarki internetowej (*np. Avant Browser*) moga wystapic nieoczekiwane zachowania.

9.1. Interfejs paska narzedzi AVG Security Toolbar

Pasek narzedzi ***AVG Security Toolbar*** jest zgodny z przegladarkami ***MS Internet Explorer*** (*wersja 6.0 lub nowsza*) i ***Mozilla Firefox*** (*wersja 2.0 lub nowsza*). Po podjeciu decyzji o zainstalowaniu paska narzedzi ***AVG Security Toolbar*** (*w czasie procesu instalacji systemu AVG pojawilo sie pytanie o zainstalowanie tego skladnika*), pasek umieszczany jest pod paskiem adresu w oknie przegladarki:



Uwaga: *AVG Security Toolbar nie jest przeznaczony dla platform serwerowych!*

AVG Security Toolbar sklada sie z nastepujacych elementów:

- ***Logo AVG*** — pozwala uzyskac dostep do głównych elementów paska. Klikniecie go spowoduje przejscie do witryny systemu AVG (http://www.avg.com/). Klikniecie strzalki obok ikony AVG powoduje otwarcie menu z nastepujacymi opcjami:
    - ***Informacje o pasku narzedzi*** — link do strony głównej ***AVG Security Toolbar, zawierajacej szczegółowe informacje o dzialaniu paska.***
    - ***Uruchom AVG 9 Internet Security*** — powoduje otwarcie interfejsu uzytkownika systemu **AVG 9 Internet Security**
    - ***Opcje*** — powoduje otwarcie okna dialogowego, w którym mozna modyfikowac ustawienia paska narzedzi ***AVG Security Toolbar*** — patrz

rozdzial ***Opcje paska narzedzi AVG Security Toolbar***

- ***Usun historie*** — daje dostep do polecen·*Usun cala historie*, *Usun historie wyszukiwania, Usun historie przegladania, Usun historie pobierania* i *Usun pliki cookie* w Pasku narzedzi AVG Security Toolbar.

- ***Aktualizacja*** — pozwala sprawdzic dostepnosc nowych aktualizacji ***dotyczacych Paska narzedzi AVG***

- ***Pomoc*** — pomaga znalezc odpowiednie pliki pomocy, wyslac opinie na temat produktu lub wyswietlic szczegóły dotyczace biezacej wersji paska narzedzi

- ***Pole wyszukiwania*** — w polu wyszukiwania nalezy wprowadzic slowo lub fraze. Nastepnie nalezy kliknac przycisk ***Wyszukaj***, aby rozpoczac wyszukiwanie przy uzyciu okreslonej wyszukiwarki (*wyszukiwarke, która ma byc uzywana, mozna okreslic w zaawansowanych opcjach paska narzedzi AVG Security Toolbar; dostepne opcje to: Yahoo!, Wikipedia, Baidu, WebHledani i Yandex*) niezaleznie od wyswietlanej w danej chwili strony. Wspomniane pole zawiera takze historie poprzednich wyszukiwan. Wszystkie wyniki wyszukiwania sa sprawdzane za pomoca funkcji ***AVG Search-Shield***.

- ***Calkowita ochrona*** — ten przycisk wyswietlany jest jako ***Calkowita ochrona*** / ***Ograniczona ochrona*** / ***Brak ochrony*** w zaleznosci od wybranej **AVG 9 Internet Security**konfiguracji.

- ***Stan strony*** — ten przycisk wyswietla ocene ladowanej w danej chwili strony internetowej bezposrednio na pasku narzedzi. Podstawa oceny sa kryteria skladnika ***AVG Search-Shield*** (*mozliwe oceny strony to: bezpieczna / podejrzana / niebezpieczna / zawiera zagrozenia /nie mogla zostac przeskanowana*). Kliknij przycisk, aby otworzyc panel zawierajacy szczególowe informacje dotyczace okreslonej strony internetowej.

- ***Informacje o programie AVG*** — zawiera lacza do waznych informacji dotyczacych bezpieczenstwa, znajdujacych sie w witrynie AVG (http://www.avg.com/).

  - ***Informacje o pasku narzedzi*** — link do strony glównej ***AVG Security Toolbar, zawierajacej szczególowe informacje o dzialaniu paska.***

  - ***Zagrozenia — informacje*** — otwiera strone internetowa firmy AVG zawierajaca informacje na temat najnowszych wirusów i zagrozen internetowych.

- ***Nowosci AVG*** — otwiera strone internetowa zawierajaca najnowsze informacje prasowe dotyczace systemu AVG.

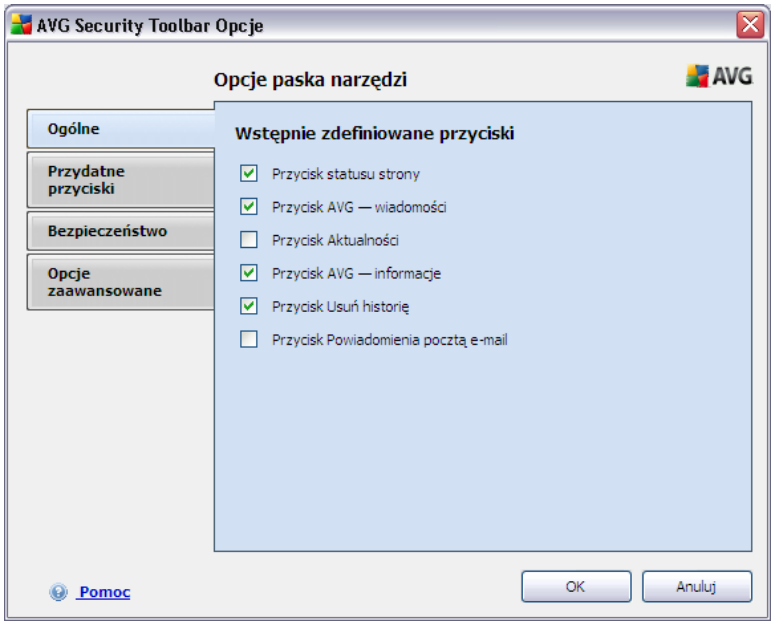
- ***Obecny poziom zagrozenia*** — otwiera strone internetowa laboratorium wirusów, która zawiera graficzna reprezentacje obecnego poziomu zagrozen w sieci.

- ***Encyklopedia wirusów*** — otwiera strone encyklopedii wirusów, w której mozna wyszukac okreslone wirusy na podstawie ich nazw i uzyskac szczególowe informacje na ich temat.

9.2. Opcje Paska narzedzi AVG Security Toolbar

Opcje konfiguracji wszystkich parametrów ***Paska narzedzi AVG Security Toolbar*** dostepne sa bezposrednio z poziomu panelu ***AVG Security Toolbar***. Interfejs edycji dostepny jest po wybraniu opcji *AVG / Opcje* z menu paska. Jego otwarcie nastepuje w nowym oknie dialogowym (***Opcje paska narzedzi***), które jest podzielone na cztery sekcje:

9.2.1. Karta Ogólne

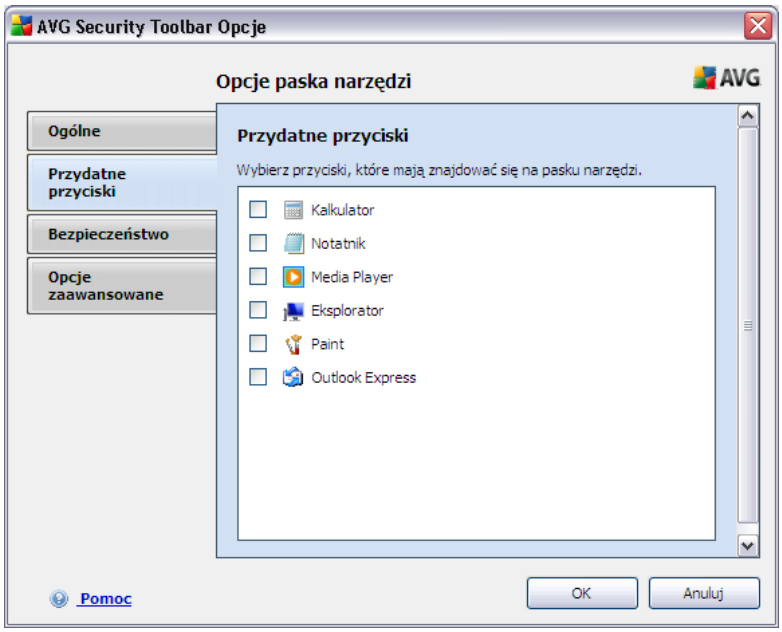


Na tej karcie mozliwe jest okreslenie, które przyciski kontrolne paska narzedzi maja byc wyswietlane / ukryte na panelu ***Paska narzedzi AVG Security Toolbar***. Nalezy zaznaczyc opcje wszystkich przycisków, które maja byc wyswietlane. Ponizej znajduje

sie opis funkcji wszystkich przycisków paska narzedzi:

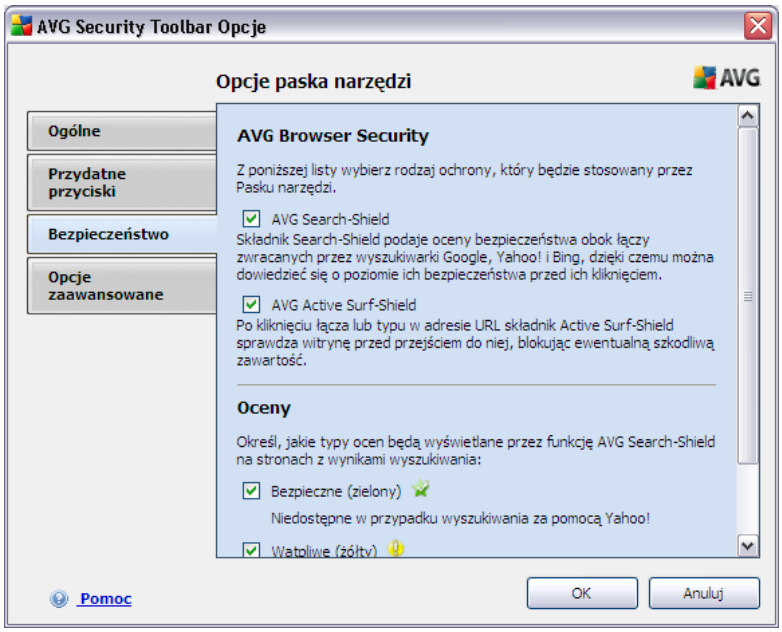
- ***Nowosci AVG*** — przycisk otwiera strone internetowa zawierajaca najnowsze informacje prasowe dotyczace systemu AVG.
- ***Wiadomosci*** — przycisk udostepnia ustrukturalizowany przeglad biezacych wiadomosci z codziennej prasy.
- ***System AVG — informacje*** — przycisk powoduje wyswietlanie na pasku narzedzi AVG informacji dotyczacych biezacych zagrozen i poziomu zagrozenia internetowego, umozliwia otwarcie encyklopedii wirusów i udostepnia dodatkowe wiadomosci dotyczace produktów AVG.
- ***Przycisk Usun historie*** — przycisk ten pozwala usunac cala historie, lub usunac historie wyszukiwania, przegladania i pobierania lub tylko usunac ciasteczka bezposrednio z panelu Paska narzedzi AVG Security Toolbar.

9.2.2. Karta Uzyteczne przyciski



Karta ***Uzyteczne przyciski*** umozliwia wybór aplikacji z listy i wyswietlanie ich ikon w interfejsie paska narzedzi. Ikona sluzy wówczas jako szybkie lacze umozliwiajace natychmiastowe uruchomienie odpowiedniej aplikacji.

9.2.3. Karta Bezpieczenstwo

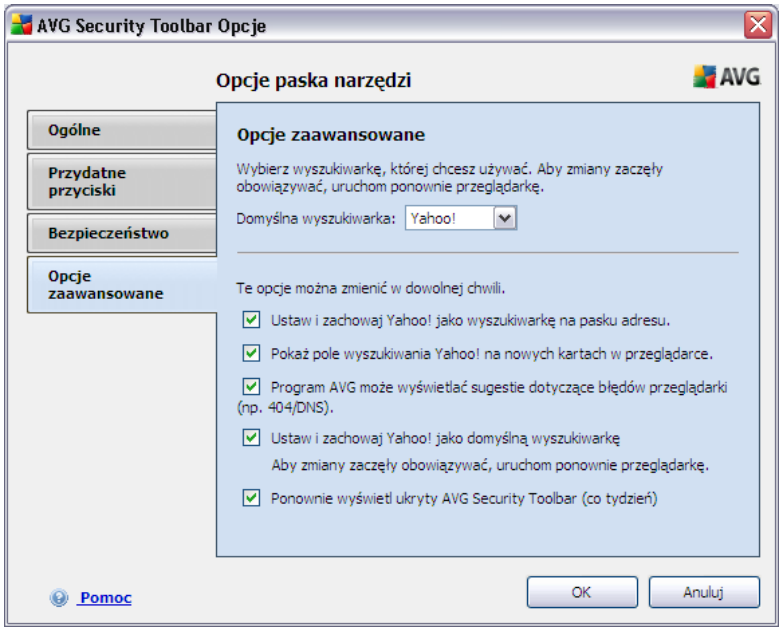


Karta ***Bezpieczenstwo*** jest podzielona na dwie sekcje (***Bezpieczenstwo przegladarki*** i ***Oceny***), w których mozna zaznaczyc okreslone pola, aby skonfigurowac nastepujace funkcje:

- ***Bezpieczenstwo przegladarki*** — te pozycje nalezy zaznaczyc, aby aktywowac lub wylaczyc ***funkcje AVG Search-Shield*** i/lub ***funkcje AVG Surf-Shield***
- ***Oceny*** — nalezy wybrac symbole graficzne, które maja byc uzywane przy klasyfikacji wyników wyszukiwania przez funkcje ***AVG Search-Shield***:
  - strona jest bezpieczna
  - strona jest podejrzana
  - strona zawiera linki do niebezpiecznych stron
  - strona zawiera aktywne zagrozenia
  - strona nie jest dostepna i nie mozna jej przeskanowac

Nalezy zaznaczyc odpowiednia opcje, aby potwierdzic, ze informacje o okreslonym poziomie zagrozenia maja byc wyswietlane. Nie mozna jednak wylaczyc wyswietlania czerwonego symbolu przypisanego stronom zawierajacym realne zagrozenie. ***Jesli nie istnieje wazny powód, zeby modyfikowac domyslna konfiguracje zdefiniowana przez twórców programu, stanowczo zaleca sie jej zachowanie.***

9.2.4. Karta Opcje zaawansowane



Na karcie ***Opcje zaawansowane*** nalezy najpierw okreslic, która wyszukiwarka ma byc uzywana jako domyslna. Dostepne opcje to: *Yahoo!, Baidu, WebHledani* i *Yandex*. Po zmienieniu domyslnej wyszukiwarki nalezy ponownie uruchomic przegladarke internetowa, aby zmiany zostaly zachowane.

Nastepnie mozna aktywowac lub wylaczyc szczególowe ustawienia paska narzedzi ***AVG Security Toolbar***:

- ***Ustaw i zachowaj Yahoo! jako wyszukiwarke na pasku adresu*** — (*domyslnie wlaczone*) — jesli ta opcja jest zaznaczona, mozliwe jest wprowadzanie slowa kluczowego wyszukiwania bezposrednio w pasku adresu przegladarki internetowej, dzieki czemu wyszukiwarka Yahoo! zostanie automatycznie uzyta do wyszukania odpowiednich stron internetowych.

- ***Zezwalaj systemowi AVG na sugestie dotyczace bledów nawigacji***

przegladarki (404/DNS) (*opcja domyslnie wlaczona*) — jesli podczas przegladania sieci zostanie wybrana strona nieistniejaca lub niedostepna (blad 404), automatycznie zostanie zaproponowany przeglad alternatywnych stron o podobnej tematyce.

- ***Ustaw i zachowaj Yahoo! jako domyslna wyszukiwarke*** — (*domyslnie wylaczone*) — Yahoo! jest domyslna wyszukiwarka internetowa Paska narzedzi AVG Security Toolbar, a aktywowanie tej opcji powoduje, ze staje sie również domyslna wyszukiwarka przegladarki internetowej.

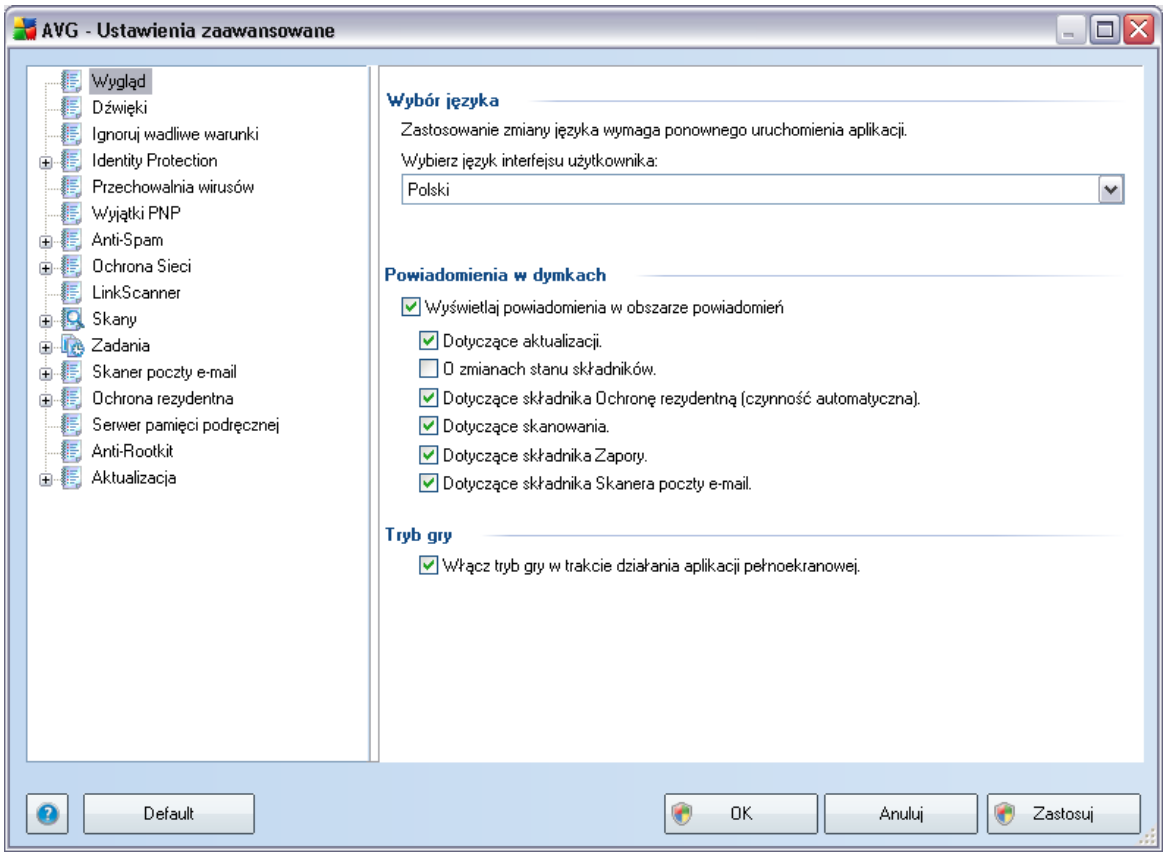
- ***Ponownie wyswietlaj Pasek narzedzi AVG Security Toolbar, jesli zostal ukryty (po tygodniu)*** — (*domyslnie wlaczone*) — ta opcja jest domyslnie aktywna i w przypadku przypadkowego ukrycia ***Paska narzedzi AVG Security Toolbar*** zostanie on ponownie wyswietlony po uplywie tygodnia.

10. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG 9 Internet Security** zostaja otwarte w nowym oknie o nazwie ***Zaawansowane ustawienia systemu AVG***. Okno to podzielone jest na dwa obszary: lewy zawiera drzewo nawigacyjne, a prawy — opcje konfiguracji programu. Wybranie skladnika, którego (*lub czesci którego*) konfiguracja ma zostac zmieniona, powoduje przejscie do odpowiedniego okna z prawej strony.

10.1. Wyglad

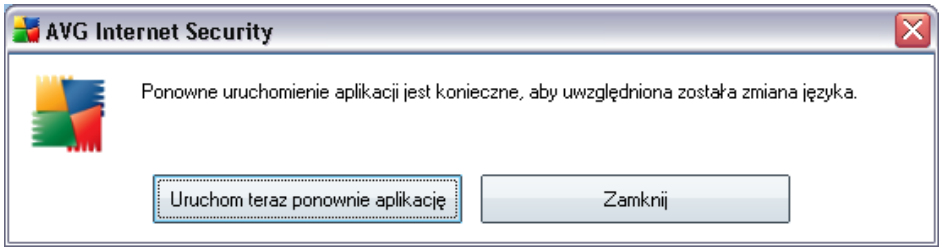
Pierwszy element w drzewie nawigacyjnym, ***Wyglad***, odnosi sie do ogólnych ustawien interfejsu uzytkownika AVG oraz kilku podstawowych opcji sterujacych zachowaniem aplikacji:



Wybór jezyka

W sekcji ***Wybór jezyka*** mozna wybrac zadany jezyk z listy rozwijanej; jezyk ten bedzie uzywany w calym interfejsie uzytkownika AVG. Menu rozwijane zawiera tylko jezyki wybrane podczas instalacji (zobacz rozdzial Instalacja niestandardowa — Wybieranie skladników). Przelaczenie aplikacji na inny jezyk wymaga ponownego uruchomienia interfejsu uzytkownika. W tym celu nalezy wykonac nastepujace kroki:

- Wybierz zadany jezyk aplikacji i potwierdz wybór, klikajac przycisk ***Zastosuj*** (widoczny w prawym dolnym rogu).
- Wcisnij przycisk ***OK***, aby potwierdzic.
- W nowym oknie dialogowym pojawi sie informacja, ze zmiana jezyka interfejsu systemu AVG wymaga ponownego uruchomienia programu:



Powiadomienia w dymkach

W tym obszarze mozna wylaczyc wyswietlane w dymkach powiadomienia dotyczace stanu aplikacji. Domyslnie wszystkie powiadomienia sa wyswietlane i nie zaleca sie zmiany tych ustawien. Zwykle informuja one o zmianach stanu skladników AVG i w zadnym wypadku nie wolno ich ignorowac!

Jesli jednak z jakiegos powodu powiadomienia te nie maja byc wcale wyswietlane lub maja dotyczyc tylko okreslonych skladników AVG, mozna zdefiniowac wlasne preferencje, zaznaczajac lub usuwajac zaznaczenie odpowiednich opcji:

- ***Wyswietlaj powiadomienia w obszarze powiadomien*** — pole jest domyslnie zaznaczone (*opcja wlaczona*), a powiadomienia sa wyswietlane. Usuniecie zaznaczenia opcji powoduje calkowite wylaczenie wyswietlania powiadomien w dymkach. Po wlaczeniu tej opcji mozna bardziej szczegółowo okreslic, jakie powiadomienia maja byc wyswietlane:
  - ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace aktualizacji*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace rozpoczecia, postepu i zakonczenia aktualizacji systemu AVG;

- ***Wyswietlaj powiadomienia o zmianach stanu skladników*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace aktywnosci lub nieaktywnosci skladników badz mozliwych problemów ich dotyczacych. W przypadku zglaszania stanu bledu skladnika, opcja ta okresla funkcje informacyjna ikony na pasku zadan (zmiany koloru), która wskazuje na problemy z dowolnym skladnikiem systemu AVG;

- ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace Ochrony rezydentnej*** — nalezy okreslic, czy informacje dotyczace zapisywania, kopiowania i otwierania procesów maja byc wyswietlane czy ukrywane (*ta konfiguracja jest dostepna tylko, jesli opcja automatycznego leczenia Ochrony rezydentnej jest wlaczona*);

- ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace skanowania*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace automatycznego rozpoczecia, postepu i zakonczenia zaplanowanego skanowania;

- ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace Zapory*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace stanu i procesów Zapory, np. ostrzezenia o wlaczeniu/wylaczeniu skladnika, mozliwym blokowaniu ruchu sieciowego itp.;

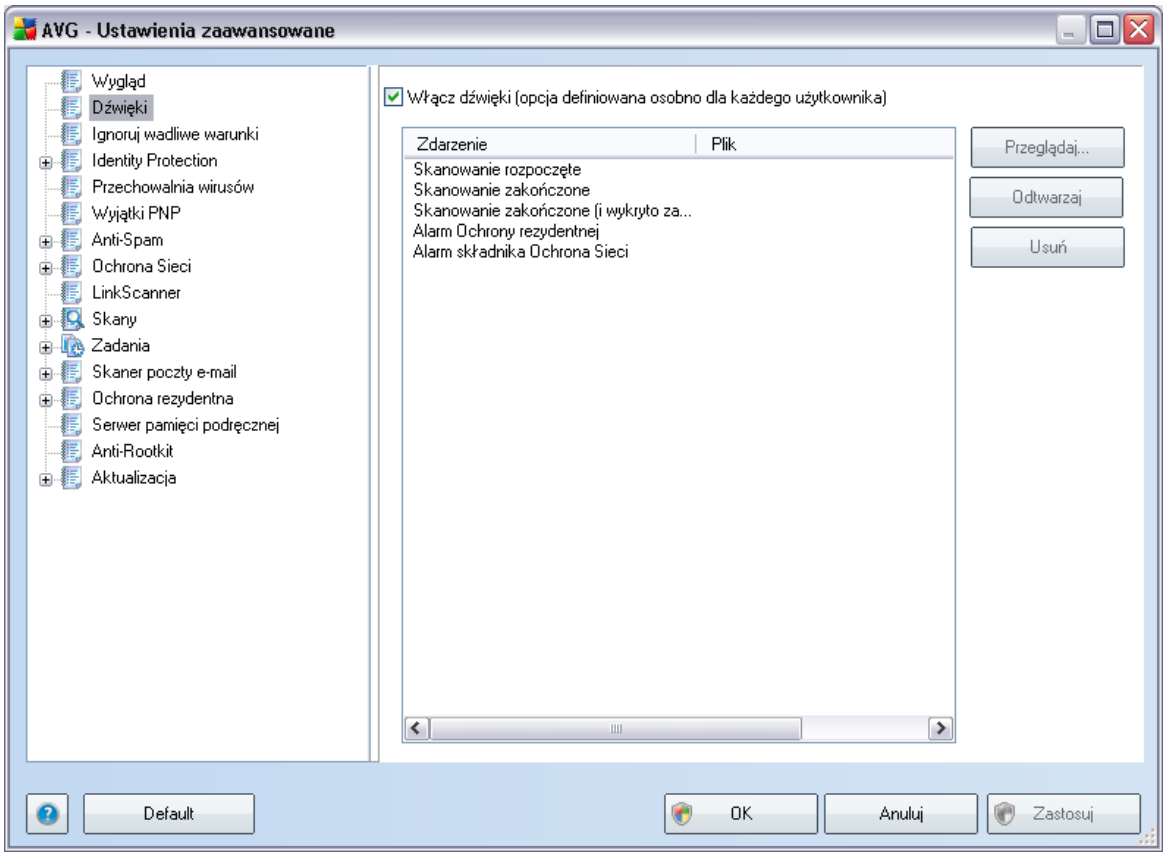
- ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace skladnika Skaner poczty e-mail*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace skanowania wszystkich przychodzacych i wychodzacych wiadomosci e-mail.

Tryb gry

Ta funkcja jest przeznaczona dla aplikacji pelnoekranowych, w dzialaniu których moglyby przeszkadzac (*np. minimalizowac lub zaklócac wyswietlanie grafiki*) powiadomienia systemu AVG (*wyswietlane np. w chwili uruchomienia zaplanowanego skanowania*). Aby tego uniknac, nalezy pozostawic pole wyboru ***Wlacz tryb gry w trakcie dzialania aplikacji pelnoekranowej*** zaznaczone (*ustawienie domyslne*).

10.2. Dzwieki

W oknie dialogowym ***Dzwieki*** mozna okreslic, czy system AVG ma informowac o okreslonych czynnosciach za pomoca dzwieków. Jesli tak, nalezy zaznaczyc pole wyboru ***Wlacz efekty dzwiekowe*** (*domyslnie wylaczone*), aby wlaczyc liste czynnosci systemu AVG:

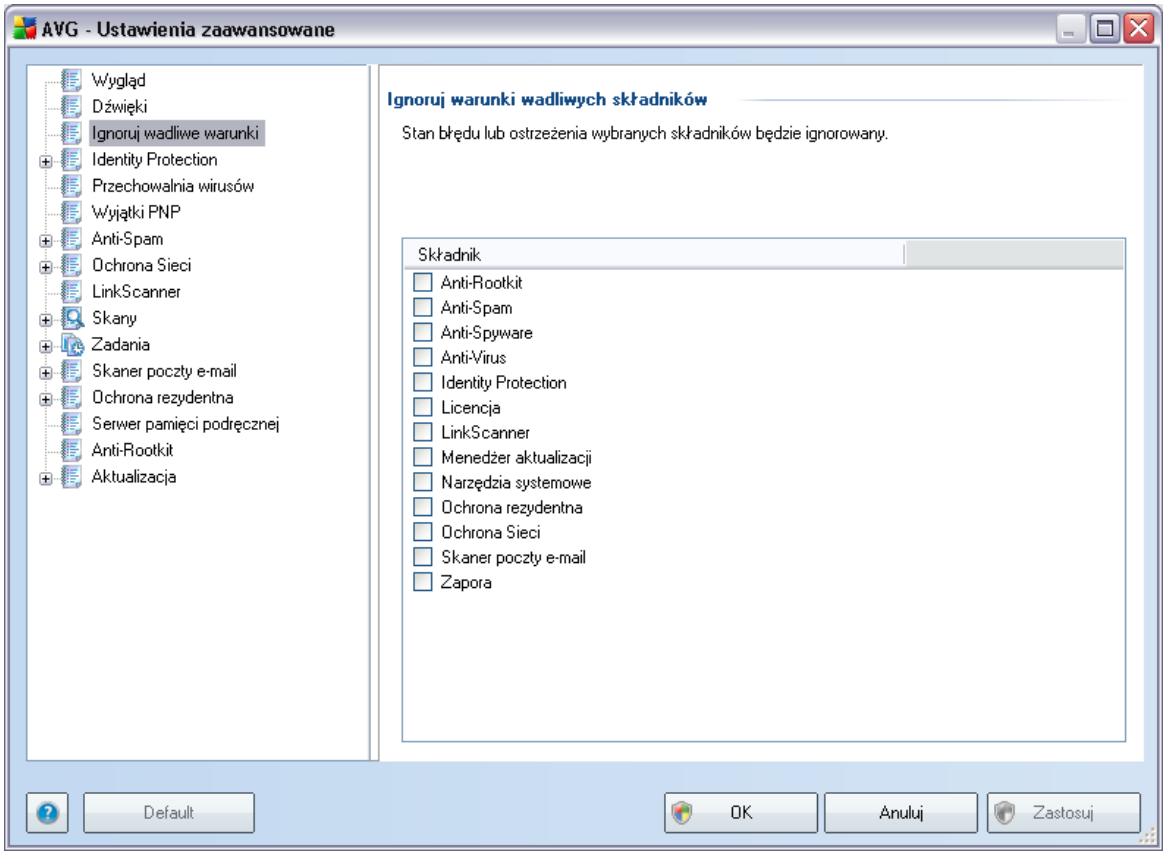


Nastepnie nalezy wybrac odpowiednie zdarzenie z listy i wskazac plik dzwiekowy, który ma zostac do niego przypisany (***Przegladaj***). Aby odtworzyc wybrany dzwiek, nalezy zaznaczyc go na liscie i nacisnac przycisk ***Odtwórz***. Aby usunac dzwiek przypisany do okreslonego zdarzenia, nalezy uzyc przycisku ***Usun***.

Uwaga: *Obslugiwane sa tylko pliki *.wav!*

10.3. Ignoruj bledny stan skladników

W oknie dialogowym ***Ignoruj wadliwy stan skladników*** mozna wskazac skladniki, które maja byc pomijane w powiadomieniach o stanie:



Domyslnie zaden skladnik nie jest zaznaczony. Oznacza to, ze jesli dowolny skladnik znajdzie sie w stanie bledu, natychmiast wygenerowane zostanie powiadomienie:

- ***ikona na pasku zadan*** — gdy wszystkie skladniki systemu AVG dzialaja prawidlowo, wyswietlana ikona jest czterokolorowa; w przypadku bledu wyswietlany jest zólty wykrzyknik,
- tekstowy opis problemu jest widoczny w sekcji ***Informacje o stanie bezpieczenstwa*** okna glównego AVG

Moze wystapic sytuacja, w której skladnik powinien zostac tymczasowo wylaczony (*nie jest to zalecane; wszystkie skladniki powinny byc zawsze wlaczone i dzialac w*

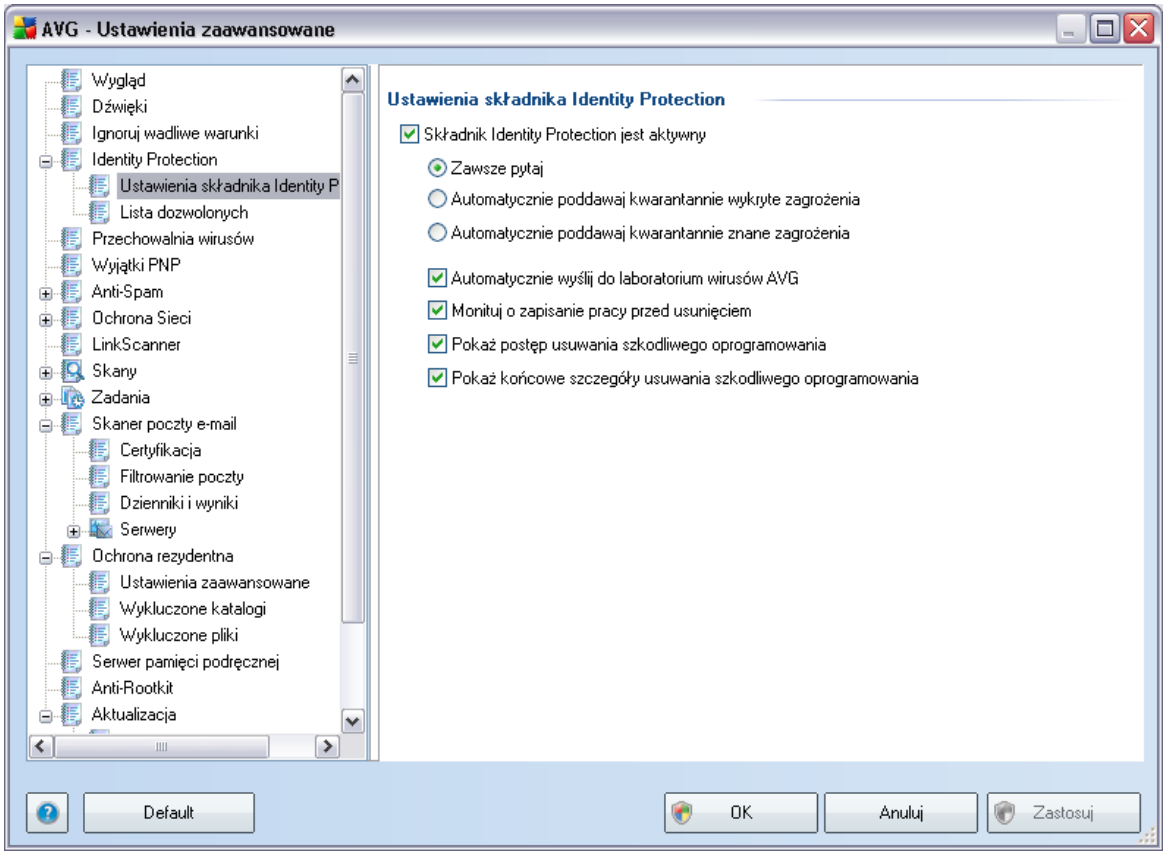
trybie domyslnym, ale niekiedy moze byc wymagane odstepstwo od tej reguly). W takim przypadku ikona na pasku zadan automatycznie informuje o stanie bledu skladnika. W takiej sytuacji nie ma jednak faktycznego bledu, poniewaz wylaczenie skladnika bylo celowe, a ryzyko z tym zwiazane jest znane. Ponadto, gdy ikona jest szara, nie moze juz informowac o ewentualnych realnych bledach.

W takim przypadku nalezy w powyzszym oknie dialogowym zaznaczyc skladniki, które moga byc w stanie bledu (*lub wylaczone*) bez wyswietlania odpowiednich powiadomien. Opcja ***ignorowania stanu skladnika*** jest takze dostepna dla okreslonych skladników bezposrednio w sekcji przegladu skladników okna glównego AVG.

10.4. AVG Identity Protection

10.4.1. Ustawienia skladnika Identity Protection

Okno dialogowe ***Ustawienia skladnika Identity Protection***umozliwia wlaczenie/ wylaczenie podstawowych funkcji skladnika ***Identity Protection***:



Skladnik Identity Protection jest aktywny (*opcja domyslnie wlaczona*) — zaznaczenie tej opcji nalezy usunac, aby wylaczyc skladnik ***Identity Protection***.

Stanowczo odradza sie wylaczanie tej funkcji bez uzasadnionej przyczyny!

Jesli skladnik ***Identity Protection*** jest aktywny, mozna okreslic jego zachowanie w przypadku wykrycia zagrozenia:

- ***Zawsze monituj*** (*opcja domyslnie wlaczona*) — w przypadku wykrycia zagrozenia uzytkownik zostanie zapytany, czy dany proces ma zostac przeniesiony do kwarantanny. Dzieki temu aplikacje, które maja pozostac uruchomione, nie zostana usuniete.

- ***Automatycznie poddawaj kwarantannie wykryte zagrozenia*** — nalezy zaznaczyc to pole wyboru, aby okreslic, ze wszystkie wykryte zagrozenia beda natychmiast przenoszone w bezpieczne miejsce (do ***Przechowalnie wirusów***). Jesli ustawienia domyslne zostana zachowane, w przypadku wykrycia zagrozenia uzytkownik zostanie zapytany, czy dany proces ma zostac przeniesiony do kwarantanny. Dzieki temu aplikacje, które maja pozostac uruchomione, nie zostana usuniete.

- ***Automatycznie poddawaj kwarantannie znane zagrozenia*** — jesli ta pozycja jest zaznaczona, wszystkie aplikacje wykryte jako potencjalnie szkodliwe oprogramowanie beda natychmiast przenoszone do ***Przechowalni wirusów***.

Nastepnie do wybranych pozycji mozna opcjonalnie przypisac dodatkowe funkcje skladnika ***Identity Protection***:

- ***Automatycznie przeslij do laboratoriów firmy AVG*** — (*domyslnie wlaczone*) — zaleca sie zachowanie tego ustawienia, aby uzupelnic baze danych o zlosliwej aktywnosci w sieci. Pomoze nam to identyfikowac nowe zagrozenia.

- ***Monituj o zapisanie pracy przed usunieciem*** (*opcja domyslnie wylaczona*) — zaznaczenie tej pozycji aktywuje ostrzezenia przed przeniesieniem do kwarantanny aplikacji wykrytej jako potencjalnie szkodliwe oprogramowanie. Jesli aplikacja jest w danym momencie uzywana, praca moze zostac utracona - nalezy ja wiec najpierw zapisac. Domyslnie ta opcja jest wlaczona i stanowczo zalecamy niewylaczanie jej.

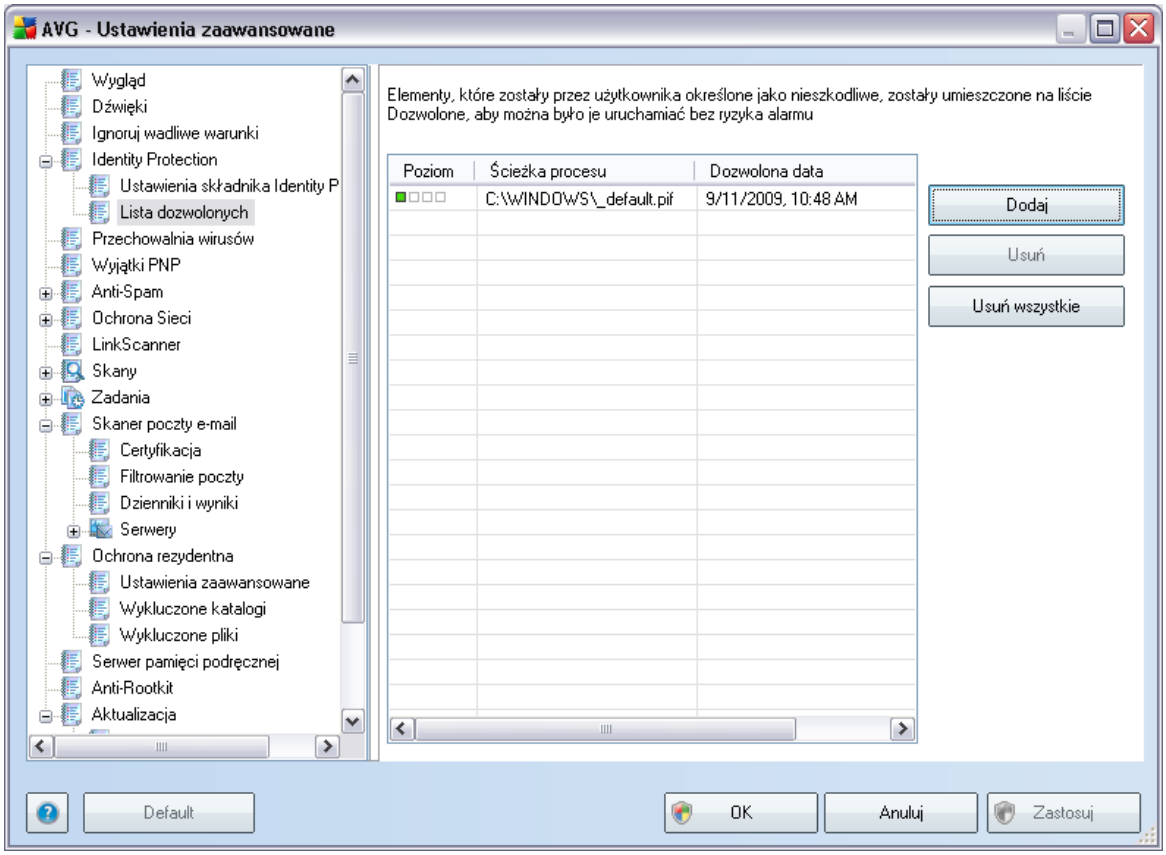
- ***Pokaz postep usuwania szkodliwego oprogramowania*** - (*domyslnie wlaczone*) - jesli ta opcja jest wlaczona, wykrycie potencjalnie szkodliwego oprogramowania spowoduje otwarcie okna dialogowego wyswietlajacego postep przenoszenia szkodliwego oprogramowania do kwarantanny.

- ***Pokaz koncowe szczegóły usuwania szkodliwego oprogramowania*** (*opcja domyslnie wlaczona*) — jesli ta opcja jest wlaczona, skladnik ***Identity Protection*** wyswietla szczegółowe informacje o kazdym obiekcie przeniesionym do kwarantanny (*poziom zagrozenia, lokalizacja itp.*).

10.4.2. Lista dozwolonych

Jesli znajdujace sie w oknie dialogowym ***Ustawienia programu Identity Protection*** pole wyboru ***Automatycznie przenos wykryte zagrozenia do kwarantanny*** pozostalo niezaznaczone, system bedzie pytal o potwierdzenie usuniecia kazdego potencjalnego szkodliwego oprogramowania, które wykryje. Jesli taki podejrzany

program (*wykryty na podstawie zachowania*) zostanie uznany za bezpieczny, nastapi dodanie go do tak zwanej ***listy Dozwolone*** i nie bedzie ponownie zglaszany jako niebezpieczny:



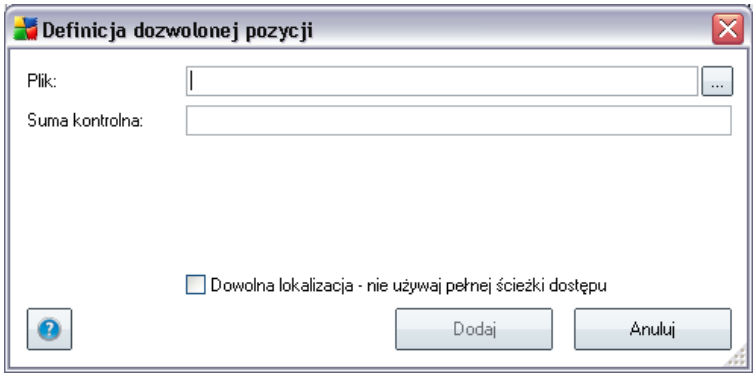
Lista Dozwolonezawiera nastepujace informacje o kazdej aplikacji:

- ***Poziom*** — graficzna reprezentacja ryzyka stwarzanego przez okreslone procesy, przedstawiana na czterostopniowej skali od najmniej istotnego (■□□□) do krytycznego (■■■■)
- ***Sciezka procesu*** — sciezka dostepu do lokalizacji pliku wykonywalnego aplikacji (*procesu*)
- ***Data odblokowania*** — data recznego okreslenia aplikacji jako bezpiecznej

Przyciski kontrolne

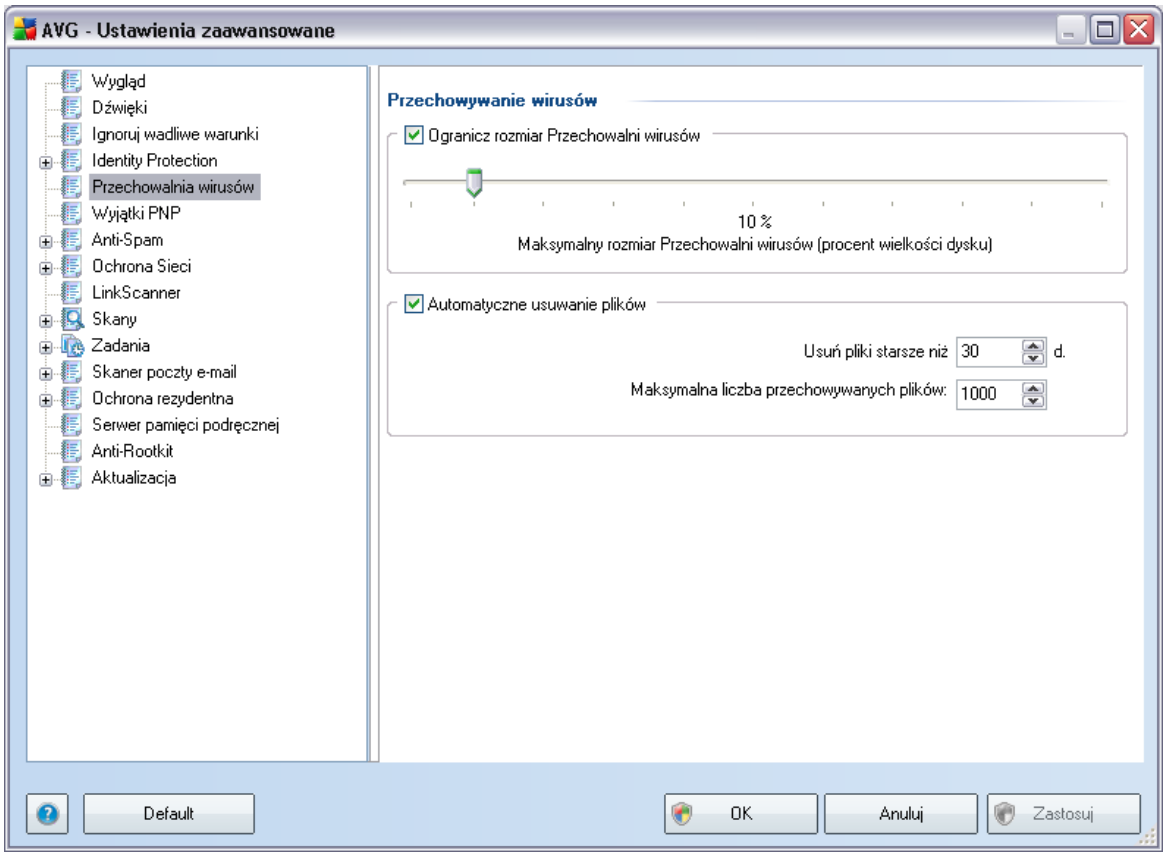
W oknie dialogowym ***Lista Dozwolone*** dostepne sa nastepujace przyciski kontrolne:

- ***Dodaj*** — nacisnij ten przycisk, aby dodac nowa aplikacje do listy programów dozwolonych. Zostanie wyswietlone ponizsze okno dialogowe:



  - ***Plik*** — nalezy podac pelna sciezke dostepu do pliku (*aplikacji*), który ma zostac oznaczony jako wyjatek
  - ***Suma kontrolna*** — wyswietla unikatowa „sygnature" wybranego pliku. Suma ta jest generowanym automatycznie ciagiem znaków, który pozwala programowi AVG jednoznacznie odrózniac wybrany plik od innych. Jest ona generowana i wyswietlana po pomyslnym dodaniu pliku.
  - ***Dowolna lokalizacja*** — nie uzywaj pelnej sciezki dostepu — jesli plik ma zostac zdefiniowany jako wyjatek jedynie dla konkretnej lokalizacji, wówczas nalezy pozostawic to pole niezaznaczone.
- ***Usun*** — wcisnij ten przycisk, aby usunac z listy zaznaczone aplikacje.
- ***Usun wszystkie*** — wcisnij ten przycisk, aby usunac wszystkie aplikacje z listy.

10.5. Przechowalnia wirusów

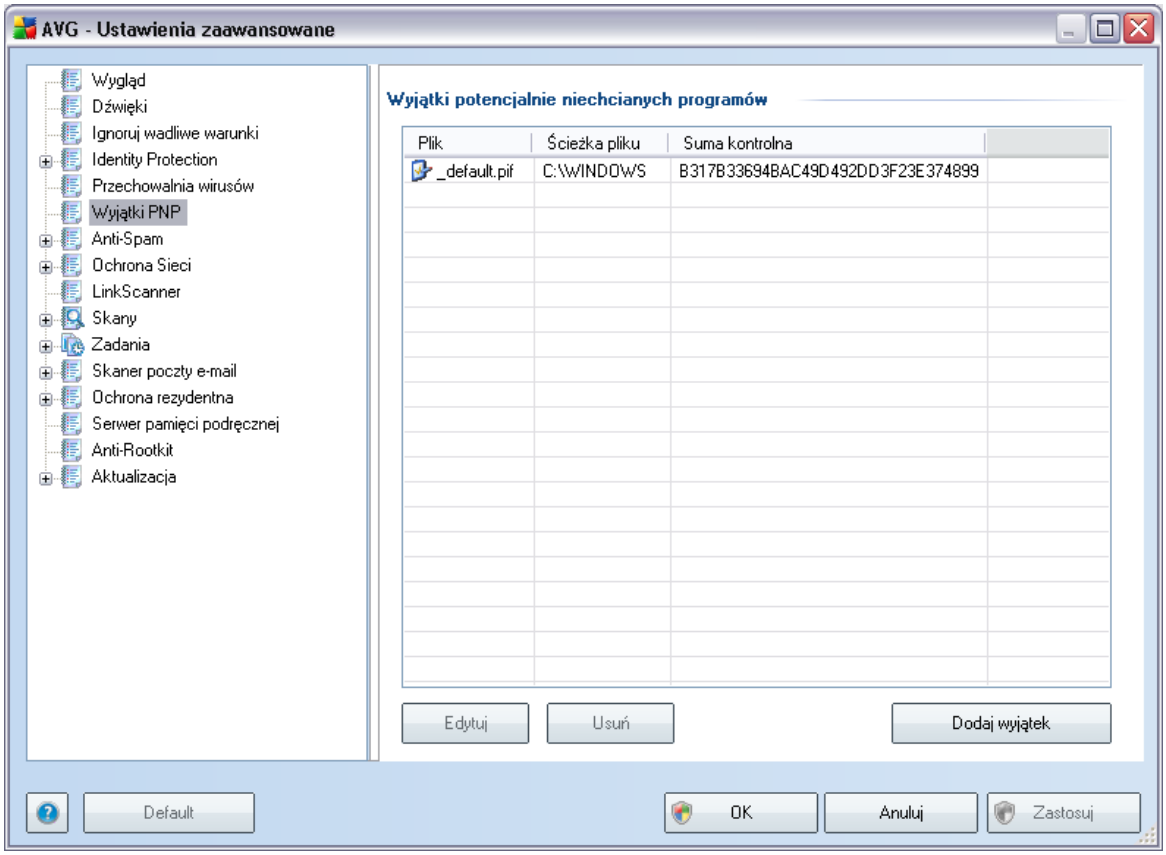


W oknie ***Przechowalnia wirusów*** mozna zdefiniowac kilka parametrów dotyczacych administrowania obiektami znajdujacymi sie w ***Przechowalni***:

- ***Ogranicz rozmiar Przechowalni wirusów*** — za pomoca suwaka nalezy okreslic maksymalny rozmiar ***Przechowalni wirusów***. Rozmiar jest okreslany w stosunku do rozmiaru dysku lokalnego.
- ***Automatyczne usuwanie plików*** — w tym obszarze mozna zdefiniowac maksymalny okres przetrzymywania obiektów w ***Przechowalni wirusów*** (***Usun pliki starsze niz ... dni***) oraz maksymalna liczbe plików, które moga znajdowac sie w ***Przechowalni*** (***Maksymalna liczba przechowywanych plików***).

10.6. Wyjatki PNP

System **AVG 9 Internet Security** potrafi analizowac i wykrywac pliki wykonywalne i biblioteki DLL, których obecnosc w systemie operacyjnym moze byc niepozadana. W niektórych przypadkach uzytkownik moze chciec zachowac na komputerze okreslone potencjalnie niechciane programy (*jesli zostaly zainstalowane celowo*). Niektóre aplikacje, zwlaszcza bezplatne, zawieraja oprogramowanie reklamowe. Moze ono zostac wykryte i zgloszone przez system AVG jako ***potencjalnie niechciany program***. Jesli chcesz zachowac taki program na komputerze, mozesz zdefiniowac go jako wyjatek potencjalnie niechcianych programów:



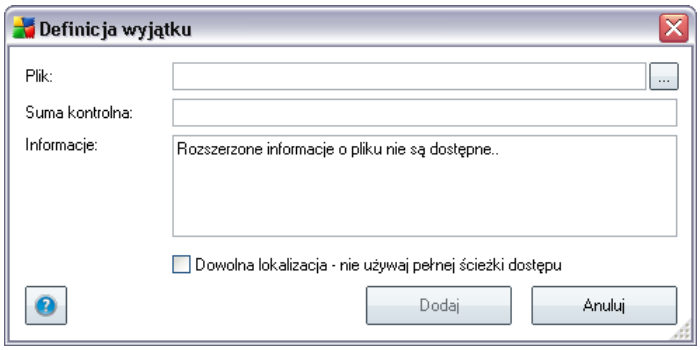
Okno ***Wyjatki potencjalnie niechcianych programów*** zawiera liste juz zdefiniowanych i aktualnie obowiazujacych wyjatków potencjalnie niechcianych programów. Liste te mozna edytowac, usuwac istniejace pozycje lub dodawac nowe wyjatki. Dla kazdego wyjatku na liscie dostepne sa nastepujace informacje:

- ***Plik*** — zawiera nazwe odpowiedniej aplikacji.

- ***Sciezka pliku*** — wyswietla sciezke dostepu do aplikacji.
- ***Suma kontrolna*** — wyswietla unikatowa „sygnature" wybranego pliku. Suma ta jest generowanym automatycznie ciagiem znaków, który pozwala programowi AVG jednoznacznie odrózniac wybrany plik od innych. Jest ona generowana i wyswietlana po pomyslnym dodaniu pliku.

Przyciski kontrolne

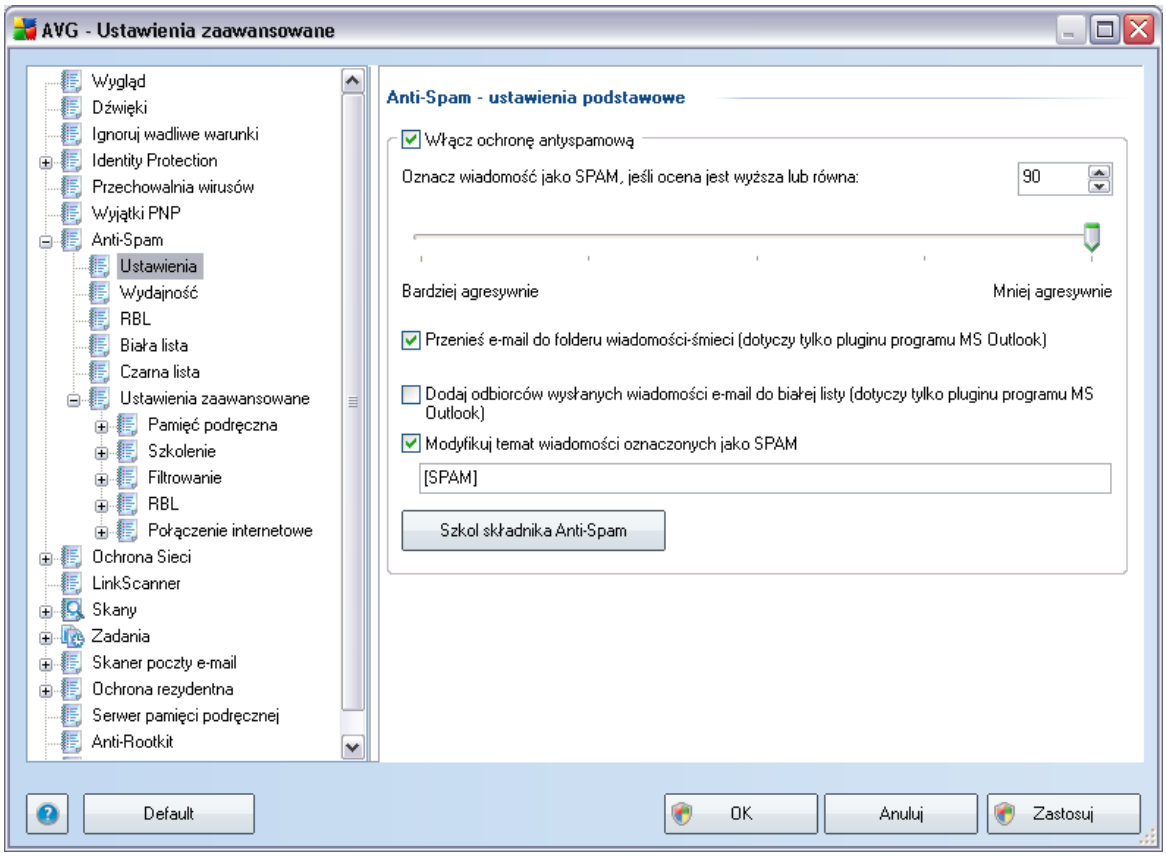
- ***Edytuj —*** otwiera okno edycji (*identyczne jak okno definiowania nowego wyjatku, patrz nizej*), w którym mozna zmienic parametry istniejacego wyjatku.
- ***Usun*** — usuwa wybrany element z listy wyjatków.
- ***Dodaj wyjatek —*** otwiera okno edycji, w którym mozna zdefiniowac parametry nowego wyjatku:



  - ***Plik*** — nalezy podac pelna sciezke do pliku, który ma byc oznaczony jako wyjatek.
  - ***Suma kontrolna*** — wyswietla unikatowa „sygnature" wybranego pliku. Suma ta jest generowanym automatycznie ciagiem znaków, który pozwala programowi AVG jednoznacznie odrózniac wybrany plik od innych. Jest ona generowana i wyswietlana po pomyslnym dodaniu pliku.
  - ***Informacje o pliku*** — wyswietla wszelkie dodatkowe dostepne informacje na temat pliku (*licencja/wersja itp.*).
  - ***Dowolna lokalizacja — nie uzywaj pelnej sciezki dostepu*** — jesli plik ma byc zdefiniowany jako wyjatek jedynie dla konkretnej lokalizacji, wówczas nalezy pozostawic to pole niezaznaczone.

10.7. Anti-Spam

10.7.1. Ustawienia



W oknie ***Podstawowe ustawienia skladnika Anti-Spam*** mozna zaznaczyc pole ***Wlacz ochrone antyspamowa***, aby wlaczyc/wylaczyc skanowanie wiadomosci e-mail. Ta opcja jest domyslnie wlaczona i jak zwykle nie zaleca sie zmiany jej konfiguracji bez waznego powodu.

W tym samym oknie mozna takze wybrac mniej lub bardziej agresywne metody oceny. Filtr ***Anti-Spam*** przypisuje kazdej wiadomosci ocene (*tj. wskaznik informujacy, jak bardzo jej tresc przypomina SPAM*) na podstawie kilku dynamicznych technik skanowania. Wartosc opcji ***Oznacz wiadomosc jako spam, jesli ocena jest wyzsza niz*** mozna dostosowac, wpisujac odpowiednia liczbe (*od 0 do 100*) badz·przesuwajac suwak w lewo lub w prawo (*tylko od 50 do 90*).

Zwykle zaleca sie stosowanie progu z przedzialu od 50 do 90, a jesli nie ma pewnosci co do wlasciwego ustawienia — równego 90. Ponizej przedstawiono opis progów oceny:

- ***Wartosc 90–99*** — wiekszosc przychodzacych wiadomosci e-mail jest normalnie dostarczana (bez oznaczania jako spam). Spam, który latwo zidentyfikowac, jest odfiltrowywany, ale znaczna jego czesc ***moze nadal trafiac do Twojej skrzynki odbiorczej.
- ***Wartosc 80–89*** — wiadomosci e-mail, które stanowia potencjalny spam, sa poprawnie odfiltrowywane. Niektóre z pozadanych wiadomosci (niebedacych spamem) moga zostac blednie zablokowane.
- ***Wartosc 60–79*** — umiarkowanie agresywna konfiguracja. Wiadomosci e-mail, które moga stanowic spam, sa poprawnie odfiltrowywane. Pozadane wiadomosci (niebedace spamem) moga zostac blednie zablokowane.
- ***Wartosc 1–59*** — bardzo agresywna konfiguracja. Pozadane wiadomosci e-mail sa odfiltrowywane w równym stopniu, jak wiadomosci stanowiace spam. Nie zalecamy stosowania tego progu podczas normalnej pracy.
- ***Wartosc 0*** — w tym trybie dostarczane sa tylko wiadomosci od nadawców z ***bialej listy***. Wszystkie pozostale wiadomosci e-mail sa uznawane za spam. ***Nie zalecamy stosowania tego progu podczas normalnej pracy.***

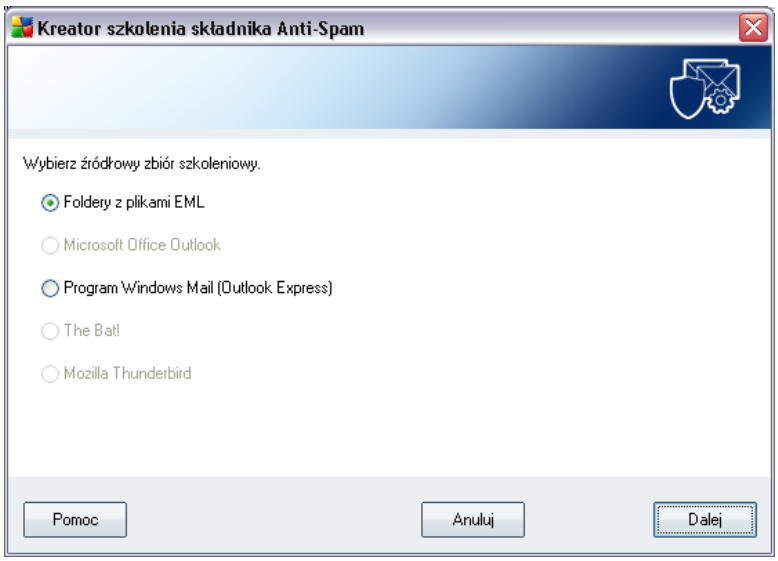
W oknie ***Podstawowe ustawienia skladnika Anti-Spam*** mozna dokladniej zdefiniowac sposób traktowania spamu wykrytego w wiadomosciach e-mail:

- ***Przenies wiadomosc do folderu wiadomosci-smieci*** — jesli opcja jest zaznaczona, wykryty spam bedzie automatycznie przenoszony do wskazanego folderu wiadomosci-smieci w kliencie poczty.
- ***Dodaj odbiorców wyslanych wiadomosci e-mail do bialej listy*** — zaznacz to pole, aby potwierdzic, ze masz zaufanie do odbiorców wyslanych przez Ciebie wiadomosci e-mail, a wiec poczta przychodzace z ich kont ma zawsze byc dostarczana.
- ***Zmodyfikuj temat wiadomosci oznaczonych jako spam*** — jesli opcja ta jest zaznaczona, wszystkie wykryte wiadomosci zawierajace spam beda oznaczane (w temacie) wskazana fraza lub znakiem; zadany tekst mozna wpisac w polu znajdujacym sie ponizej.

Przyciski kontrolne

Przycisk "Rozpocznij szkolenie skladnika Anti-Spam" pozwala uruchomic ***Kreator szkolenia skladnika Anti-Spam*** opisany szczegółowo w nastepnym rozdziale.

W pierwszym oknie dialogowym***kreatora szkolenia skladnika Anti-Spam*** nalezy wybrac zródlo wiadomosci e-mail, które zostana uzyte do szkolenia. Na ogól uzywa sie do tego celu niechcianych wiadomosci reklamowych, oraz e-maili blednie oznaczonych jako spam.



Dostepne sa nastepujace opcje:

- ***Konkretny klient poczty e-mail***— jesli uzywasz jednego z wymienionych klientów poczty e-mail (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), po prostu wskaz go na wyswietlonej liscie.

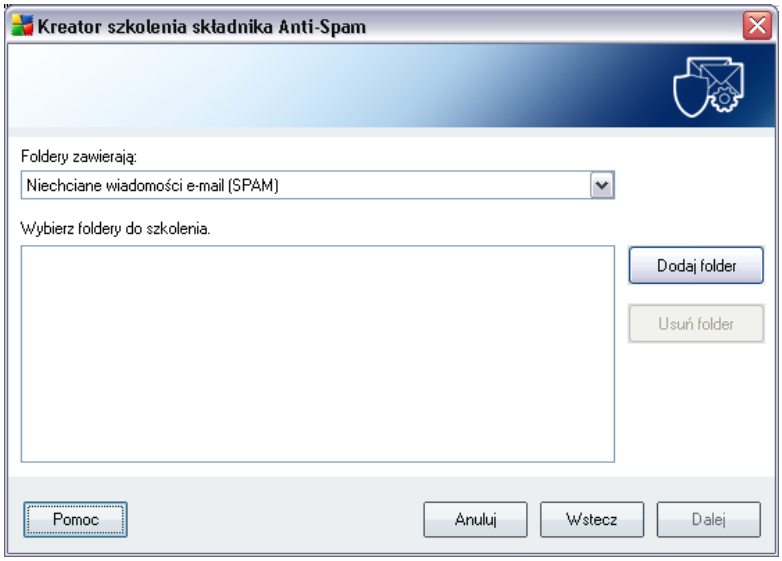
- ***Folder z plikami EML*** — jesli jest uzywany jakikolwiek inny program pocztowy, nalezy zgromadzic wszystkie wiadomosci w jednym folderze (*w formacie .eml*) lub upewnic sie, ze znasz lokalizacje folderu, w którym program pocztowy domyslnie przechowuje wiadomosci. Nastepnie nalezy zaznaczyc opcje ***Folder z plikami EML***, oraz wskazac odpowiedni folder w nastepnym kroku.

Aby proces szkolenia byl prostszy i przebiegal szybciej, warto juz wczesniej tak posortowac e-maile, aby folder uzywany w szkoleniu zawieral jedynie wiadomosci szkoleniowe (albo spam, albo ham). Nie jest to jednak konieczne, gdyz wiadomosci mozna przefiltrowac recznie w późniejszym czasie.

Aby kontynuowac, zaznacz odpowiednia opcje i kliknij przycisk ***Dalej*** .

Okno wyswietlane w tym kroku zalezy od poprzedniego wyboru.

Foldery z plikami EML



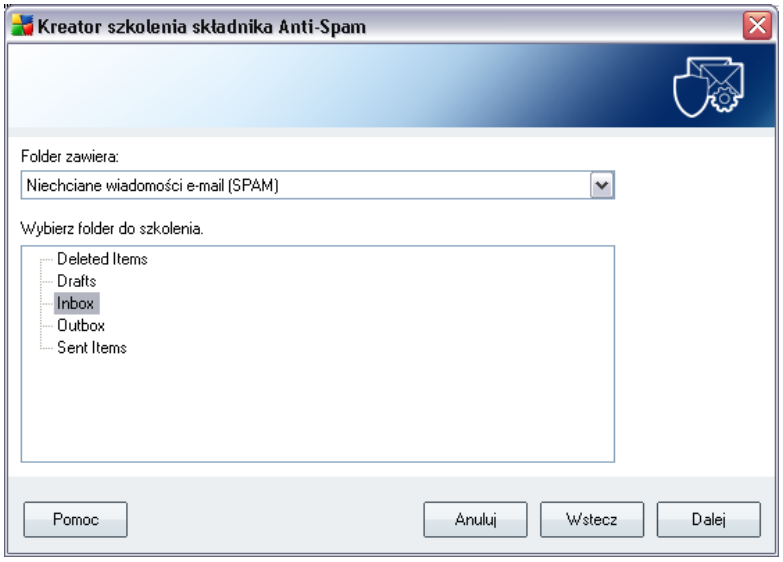
W oknie tym nalezy wybrac folder z wiadomosciami, które maja zostac uzyte do szkolenia. Kliknij przycisk ***Dodaj folder***, aby zlokalizowac folder z plikami .eml (*zapisanymi wiadomosciami e-mail*). Wybrany folder zostanie wyswietlony w biezacym oknie.

Z menu rozwijanego ***Foldery zawieraja*** wybierz jedna z dwóch opcji — czy folder zawiera pozadane wiadomosci (*HAM*), czy niechciane reklamy (*SPAM*). Nalezy pamietac, ze w nastepnym kroku bedzie mozliwa szczególowa selekcja plików, wiec folder nie musi zawierac tylko szkoleniowych wiadomosci e-mail. Mozna tez usunac z listy niechciane foldery, klikajac przycisk ***Usun folder***.

Po zakonczeniu ustawien nalezy kliknac przycisk ***Dalej*** i przejsc do ***Opcji filtrowania wiadomosci***.

Okreslony klient poczty e-mail

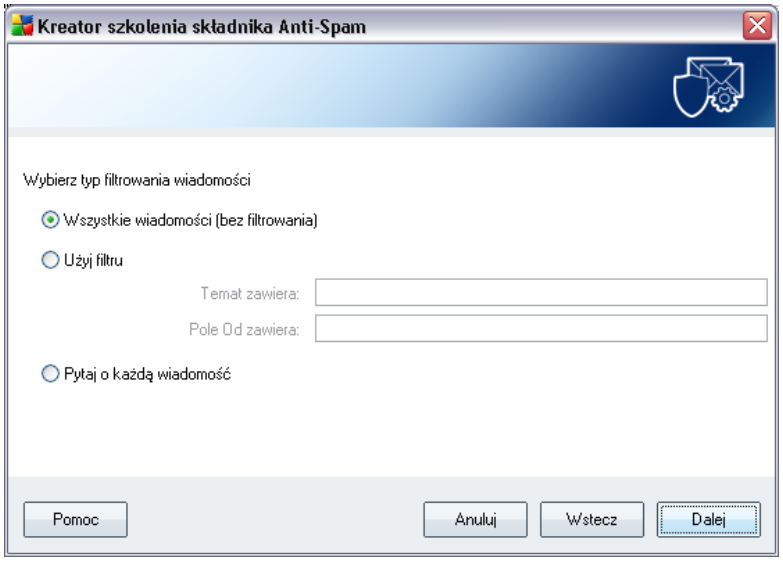
Po potwierdzeniu jednej z opcji pojawi sie nowe okno dialogowe.



Uwaga: *W wypadku programu Microsoft Office Outlook pojawi sie najpierw monit proszacy o wybranie profilu programu MS Office Outlook.*

Z menu rozwijanego ***Foldery zawieraja*** wybierz jedna z dwóch opcji — czy folder zawiera pozadane wiadomosci (*HAM*), czy niechciane reklamy (*SPAM*). Nalezy pamietac, ze w nastepnym kroku bedzie mozliwa szczególowa selekcja plików, wiec folder nie musi zawierac tylko szkoleniowych wiadomosci e-mail. W głównej czesci okna pojawi sie drzewo nawigacyjne wybranego klienta poczty e-mail. Zlokalizuj zadany folder i podswietl go za pomoca myszy.

Po zakonczeniu ustawien nalezy kliknac przycisk ***Dalej*** i przejsc do ***Opcji filtrowania wiadomosci***.



W tym oknie mozna ustawic filtrowanie wiadomosci e-mail.

Jesli wybrany folder na pewno zawiera tylko wiadomosci, które maja zostac uzyte do szkolenia, nalezy wybrac opcje ***Wszystkie wiadomosci (bez filtrowania)***.

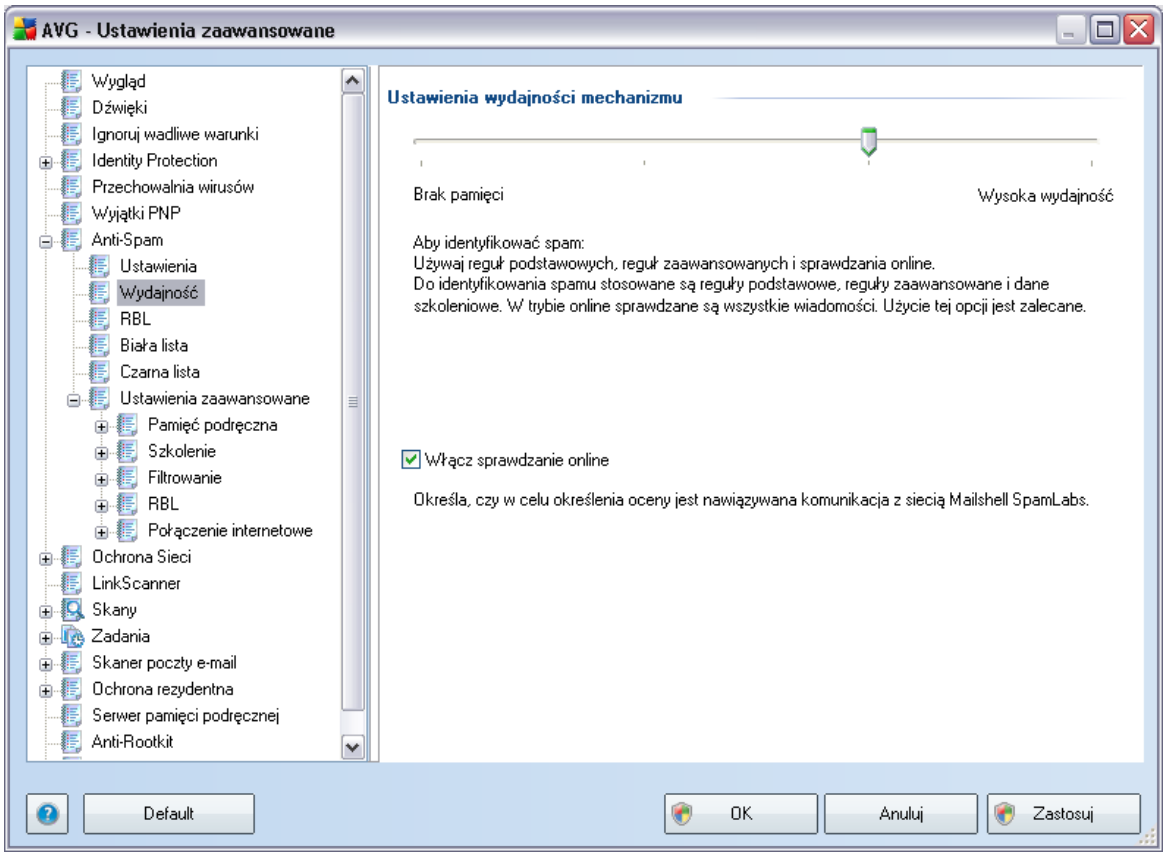
Jesli nie ma pewnosci co do charakteru wiadomosci znajdujacych sie w folderze i kreator powinien pytac o kazda z nich (dajac mozliwosc okreslenia, czy ma zostac uzyta w szkoleniu), nalezy wybrac opcje ***Pytaj o kazda wiadomosc***.

Aby zastosowac bardziej zaawansowane filtrowanie, nalezy wybrac opcje ***Uzyj filtru***. Mozna bedzie wówczas podac wyraz (*nazwe*), czesc wyrazu lub fraze, która ma byc wyszukiwana w tematach i/lub adresach nadawców wiadomosci. Wszystkie wiadomosci dokladnie spelniajace kryteria wyszukiwania zostana uzyte do szkolenia, bez dalszych monitów.

Uwaga: *W przypadku wypelnienia obu pól tekstowych zostana uzyte takze adresy spelniajace tylko jeden z dwóch warunków!*

Gdy juz zdecydujesz sie na jedna z opcji, kliknij przycisk ***Dalej***. Kolejne okno dialogowe ma charakter informacyjny i sygnalizuje, ze kreator jest gotowy do przetwarzania wiadomosci. Aby rozpoczac szkolenie, nalezy ponownie kliknac przycisk ***Dalej*** Szkolenie rozpocznie sie zgodnie z wybranymi wczesniej parametrami.

10.7.2. Wydajnosc



Okno ***Ustawienia wydajnosci mechanizmu*** (*otwierane po kliknieciu pozycji* ***Wydajnosc*** *w lewym panelu nawigacyjnym*) daje dostep do ustawien wydajnosci skladnika ***Anti-Spam***. Przesuwajac suwak w lewo lub w prawo, mozna zmienic wydajnosc skanowania na skali miedzy trybami ***Brak pamieci*** i ***Wysoka wydajnosc***.

- ***Brak pamieci*** — w czasie skanowania w poszukiwaniu spamu nie beda stosowane zadne reguly. Do identyfikacji beda uzywane tylko dane szkoleniowe. Ten tryb nie jest zalecany do czestego stosowania - chyba ze konfiguracja sprzetowa komputera jest bardzo slaba.

- ***Wysoka wydajnosc*** — wymaga duzej ilosci pamieci. W czasie skanowania w poszukiwaniu spamu stosowane beda nastepujace funkcje: pamiec podreczna dla regul i definicji spamu, reguly podstawowe i zaawansowane, adresy IP spamerów i inne bazy danych.

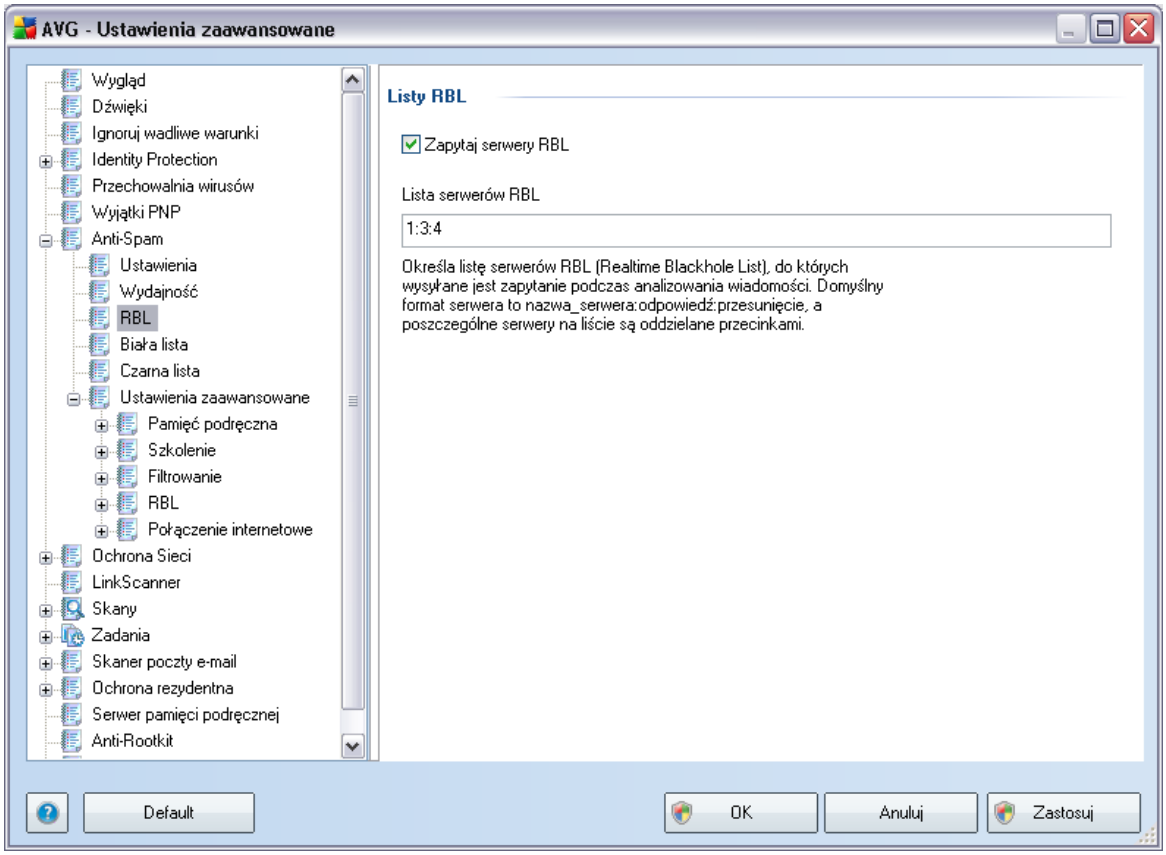
Opcja ***Wlacz sprawdzanie online*** jest domyslnie wlaczona. Pozwala ona skuteczniej

wykrywac spamdzieki komunikacji z serwerami Mailshell: skanowane dane sa porównywane z bazami danych online firmy Mailshell.

Zwykle zaleca sie zachowanie ustawien domyslnych i zmienianie ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny byc wprowadzane wylacznie przez zaawansowanych uzytkowników, którzy doskonale wiedza, co robia!

10.7.3. RBL

Kliknięcie pozycji ***RBL*** otwiera okno o nazwie ***Listy RBL***:



W oknie tym mozna wlaczyc/wylaczyc funkcje ***Zapytaj serwery RBL***.

Serwer RBL (*Realtime Blackhole List*) to specjalny serwer DNS z obszerna baza danych znanych nadawców spamu. Jezeli funkcja ta jest wlaczona, wszystkie wiadomosci e-mail zostana sprawdzone przy uzyciu bazy serwera RBL i oznaczone jako spam, w

przypadku gdy okaza sie identyczne z którymkolwiek wzorem w bazie danych. Bazy danych serwerów RBL zawieraja zawsze aktualne sygnatury spamu, co zapewnia najskuteczniejsze i najdokladniejsze wykrywanie niechcianych wiadomosci. Funkcja ta jest szczególnie przydatna dla uzytkowników otrzymujacych duze ilosci spamu, który zazwyczaj nie jest wykrywany przez silnik AVG Anti-Spam.

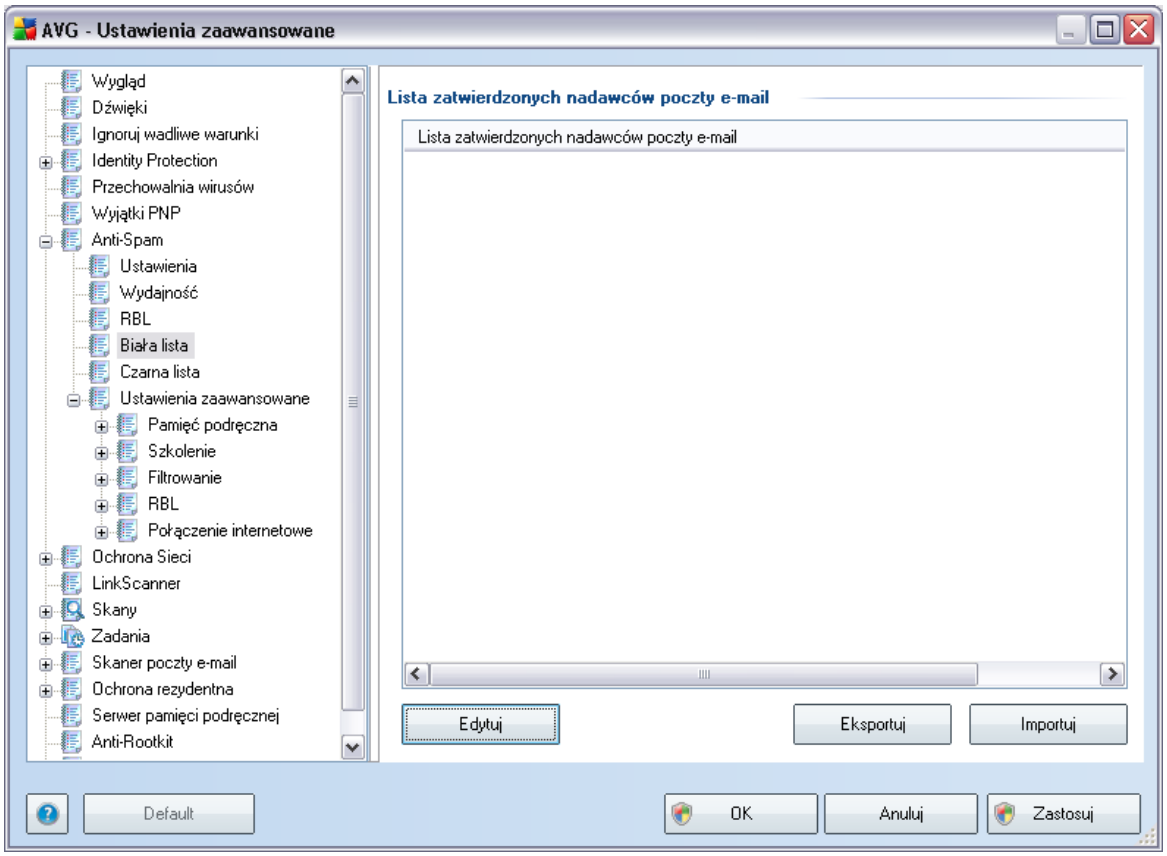
Lista serwerów RBL pozwala okreslic lokalizacje wybranych serwerów RBL.

Uwaga: *Wlaczenie tej funkcji moze w niektórych systemach i konfiguracjach spowolnic proces odbierania poczty e-mail, poniewaz kazda wiadomosc musi byc zweryfikowana przy uzyciu bazy danych serwera RBL.*

Do serwera nie sa wysylane zadne dane osobiste!

10.7.4. Biala lista

Kliknięcie elementu ***Biala lista*** pozwala otworzyc okno dialogowe ***Lista zatwierdzonych nadawców poczty e-mail***·zawierajace liste akceptowanych adresów nadawców i nazw domen, z których wysylane wiadomosci nigdy nie sa oznaczane jako spam.



W interfejsie tym mozna utworzyc liste nadawców, którzy nigdy nie wysylaja niepozadanych wiadomosci (spamu). Mozna takze utworzyc liste nazw calych domen (np. *avg.com*), które nie wysylaja spamu.

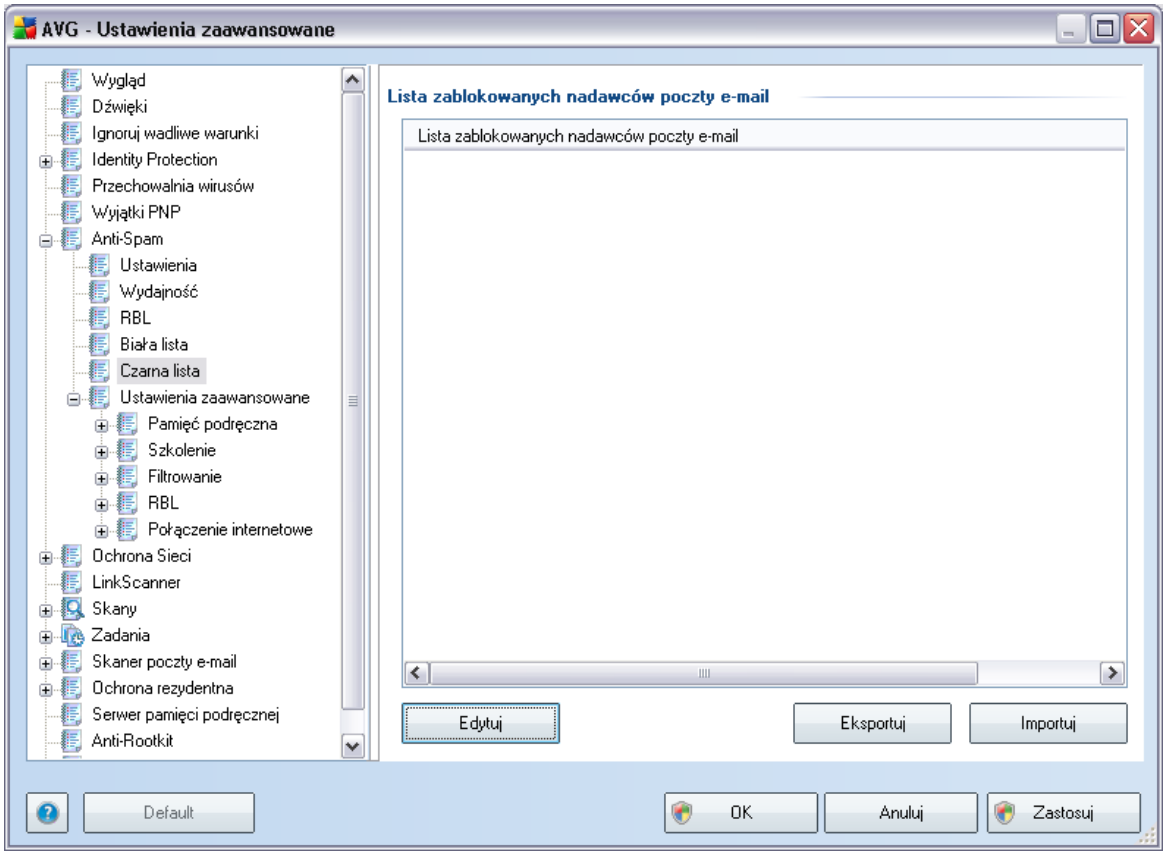
Po przygotowaniu listy adresów i domen, jej elementy mozna wprowadzic pojedynczo lub zaimportowac wszystkie na raz. Dostepne sa nastepujace przyciski kontrolne:

- ***Edytuj*** — przycisk ten sluzy do otwarcia okna dialogowego, w którym mozna recznie wprowadzic liste adresów (*równiez za pomoca metody kopiuj-wklej*). Kazda pozycje (*nadawce lub nazwe domeny*) nalezy wprowadzic w osobnym wierszu.
- ***Eksportuj*** — jezeli z jakiegos powodu chcesz wyeksportowac wpisy, mozna uzyc przycisku Eksportuj. Wszystkie wpisy zastana zapisane w zwyklym pliku tekstowym.
- ***Importuj*** — jezeli posiadasz plik tekstowy z adresami e-mail lub nazwami

domen, mozna go zaimportowac za pomoca tego przycisku. Wprowadzany plik musi byc w zwyklym formacie tekstowym i zawierac kazdy element (*adres lub nazwe domeny*) w osobnym wierszu.

10.7.5. Czarna lista

Kliknięcie pozycji ***Czarna lista*** pozwala otworzyc globalna liste zablokowanych adresów indywidualnych nadawców i domen, z których wiadomosci zawsze sa oznaczane jako spam.



W interfejsie tym mozna utworzyc liste nadawców, którzy wysylaja lub prawdopodobnie beda wysylali niepozadane wiadomosci (spam). Mozna takze utworzyc liste pelnych nazw domen (*np. spammingcompany.com*), z których otrzymujesz (lub spodziewasz sie otrzymywac) spam. Wszystkie wiadomosci e-mail wyslane z tych adresów/domen beda identyfikowane jako spam.

Po przygotowaniu listy adresów i domen, jej elementy mozna wprowadzic pojedynczo

lub zaimportowac wszystkie na raz. Dostepne sa nastepujace przyciski kontrolne:

- ***Edytuj*** — przycisk ten sluzy do otwarcia okna dialogowego, w którym mozna recznie wprowadzic liste adresów (*równiez za pomoca metody kopiuj-wklej*). Kazda pozycje (*nadawce lub nazwe domeny*) nalezy wprowadzic w osobnym wierszu.

- ***Eksportuj*** — jezeli z jakiegos powodu chcesz wyeksportowac wpisy, mozna uzyc przycisku Eksportuj. Wszystkie wpisy zastana zapisane w zwyklym pliku tekstowym.

- ***Importuj*** — jezeli posiadasz plik tekstowy z adresami e-mail lub nazwami domen, mozna go zaimportowac za pomoca tego przycisku. Wprowadzany plik musi byc w zwyklym formacie tekstowym i zawierac kazdy element (*adres lub nazwe domeny*) w osobnym wierszu.

10.7.6. Ustawienia zaawansowane

Galaz Ustawienia zaawansowane zawiera wiele dodatkowych opcji ustawien skladnika Anti-Spam. Ustawienia te sa przeznaczone dla doswiadczonych uzytkowników (zwykle administratorów sieci), którzy chca szczególowo skonfigurowac filtry antyspamowe w celu uzyskania optymalnej ochrony serwerów poczty. Z tego wzgledu nie istnieja tematy pomocy dla poszczególnych okien dialogowych, a jedynie krótkie opisy odpowiednich opcji, dostepne bezposrednio w interfejsie uzytkownika.

Stanowczo zalecamy pozostawienie tych ustawien bez zmian, jesli nie posiadasz pelnej wiedzy na temat zaawansowanych ustawien silnika antyspamowego Spamcatcher (MailShell Inc.). Nieodpowiednie zmiany moga skutkowac obnizona wydajnoscia lub nieprawidlowym dzialaniem skladnika.

Aby mimo wszystko zmienic zaawansowana konfiguracje skladnika ***Anti-Spam***, nalezy postepowac zgodnie z instrukcjami wyswietlanymi w interfejsie uzytkownika. Okna dialogowe najczesciej odpowiadaja tylko jednej edytowalnej funkcji, której opis jest zawsze dostepny w tym samym oknie:

- ***Pamiec podreczna*** — sygnatury, reputacja domen, LegitRepute

- ***Szkolenie*** -— maksymalna liczba wpisów slów, próg automatycznego szkolenia, waga

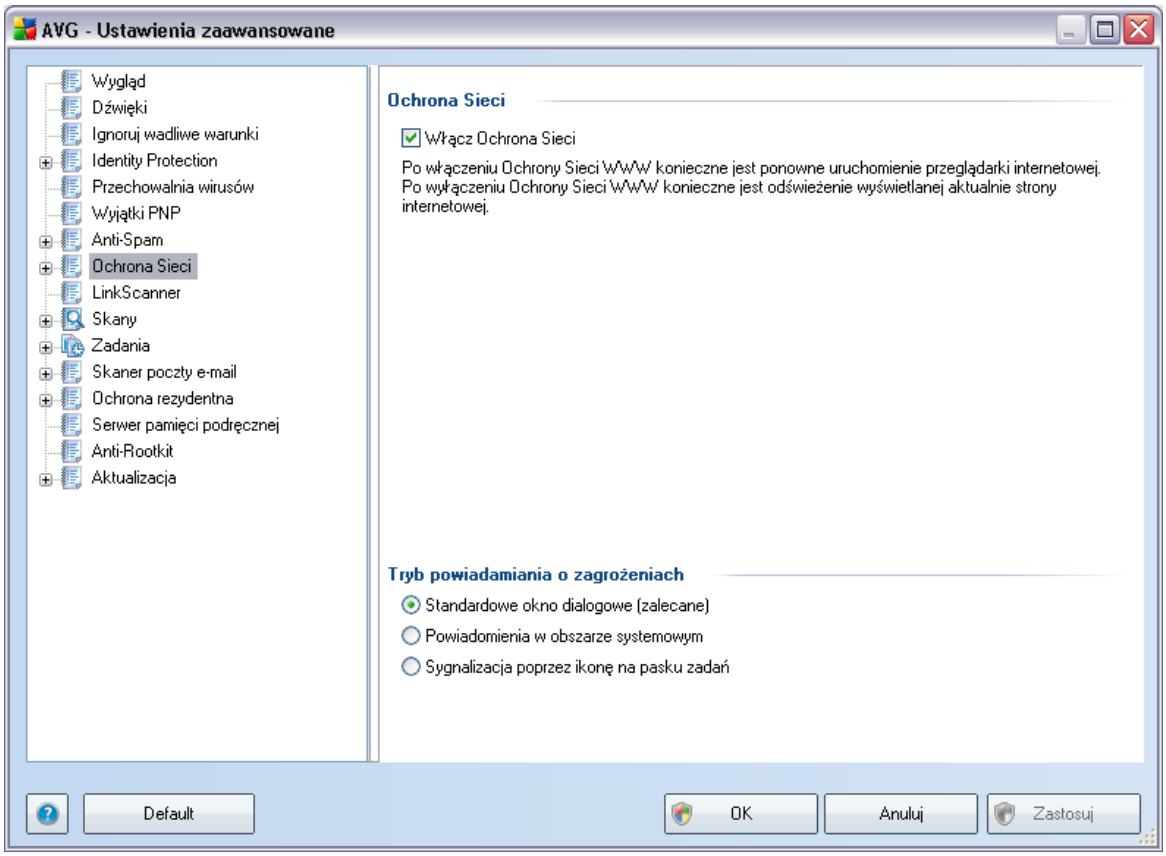
- ***Filtry*** — lista jezyków, lista krajów, akceptowane adresy IP, zablokowane adresy IP, zablokowane kraje, zablokowane zestawy znaków, falszywi nadawcy

- ***RBL*** — serwery RBL, trafienia wielokrotne, próg, limit czasu, maksymalna liczba

adresów IP

- ***Polaczenie internetowe*** — limit czasu, serwer proxy, uwierzytelnianie na serwerze proxy

10.8. Ochrona Sieci



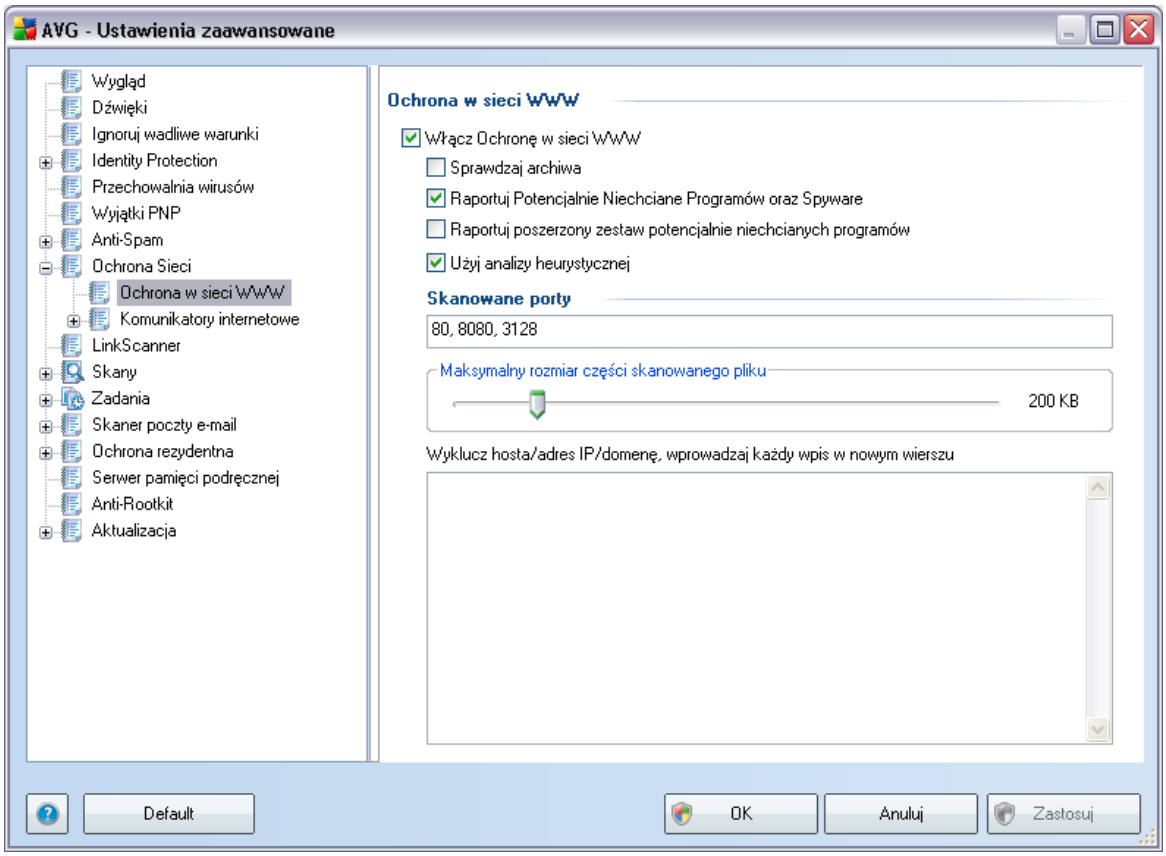
W oknie dialogowym·***Ochrona sieci WWW*** mozna wlaczyc lub wylaczyc caly skladnik ***Ochrona Sieci*** za pomoca opcji ***Wlacz Ochrone Sieci*** (*domyslnie opcja jest wlaczona*). Szczególowe ustawienia tego skladnika dostepne sa w kolejnych oknach dialogowych dostepnych z poziomu drzewa nawigacyjnego:

- ***Ochrona WWW***
- ***Komunikatory internetowe***

Tryb powiadamiania o zagrozeniach

W dolnej czesci okna mozna wybrac sposób informowania o wykrytych zagrozeniach: za pomoca zwyklych okien dialogowych, powiadomien w dymkach lub ikony na pasku zadan.

10.8.1. Ochrona WWW



W oknie dialogowym ***Ochrona w sieci WWW*** mozna edytowac konfiguracje dotyczaca skanowania zawartosci witryn internetowych. Interfejs pozwala modyfikowac nastepujace ustawienia:

- ***Wlacz Ochrone sieci WWW*** — potwierdza, ze skladnik ***Ochrona Sieci*** ma skanowac zawartosc stron WWW. Jesli ta opcja jest aktywna (*domyslnie*), mozna wlaczyc lub wylaczyc nastepujace funkcje:

- ***Skanuj wewnatrz archiwów*** — skanowanie ma obejmowac takze archiwa zawarte na wyswietlanych stronach WWW.

- ***Raportuj zagrozenia potencjalnie niechcianymi programami i oprogramowaniem szpiegujacym*** (*opcja domyslnie wlaczona*) — zaznaczenie tego pola powoduje wlaczenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegujacego (a nie tylko wirusów). Oprogramowanie szpiegujace nalezy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrozenie dla bezpieczenstwa, ale niektóre z takich programów moga zostac zainstalowane umyslnie. Nie zaleca sie wylaczania tej opcji — znaczaco zwieksza ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** — jesli poprzednia opcja jest aktywna, mozna równiez zaznaczyc to pole, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona.

- ***Uzyj heurystyki*** — skanowanie zawartosci wyswietlanych stron ma wykorzystywac analize heurystyczna (*dynamiczna emulacje instrukcji skanowanego obiektu w wirtualnym srodowisku*).

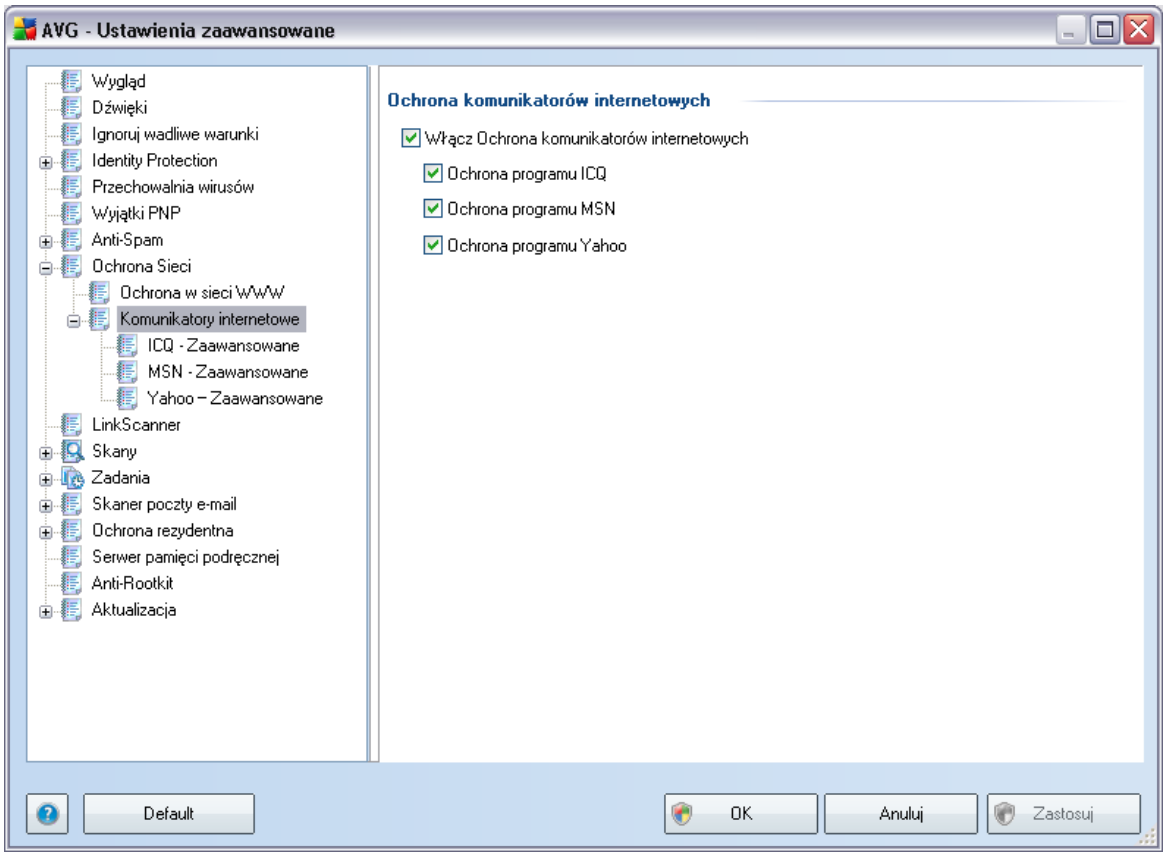
- ***Skanowane porty*** — to pole zawiera liste standardowych numerów portów http. Jesli konfiguracja komputera rózni sie od standardowej, mozna zmienic numery portów zgodnie z potrzebami.

- ***Maksymalny rozmiar czesci skanowanego pliku*** — jesli wyswietlana strona zawiera pliki, mozna skanowac ich zawartosc jeszcze przed pobraniem na dysk twardy. Poniewaz jednak skanowanie obszernych plików zajmuje dluzszy czas, otwieranie stron WWW moze zostac znacznie spowolnione. Za pomoca tego suwaka mozna okreslic maksymalny rozmiar plików, które maja byc skanowane przez skladnik ***Ochrona Sieci*** . Nawet jesli pobierany plik jest wiekszy od wybranego limitu i nie zostanie przeskanowany przez Ochrone Sieci, nie zmniejsza to Twojego bezpieczenstwa: jesli plik jest zainfekowany, skladnik ***Ochrona rezydentna*** natychmiast to wykryje.

- ***Wyklucz hosta/adres IP/domene*** — w polu mozna wpisac dokladna nazwe serwera (*host, adres IP, adres IP z maska lub adres URL*) lub

domene, które nie maja byc skanowane przez skladnik ***Ochrona Sieci***. Wykluczac nalezy tylko hosty, co do których istnieje absolutna pewnosc, ze nie stanowia zagrozenia.

10.8.2. Komunikatory internetowe



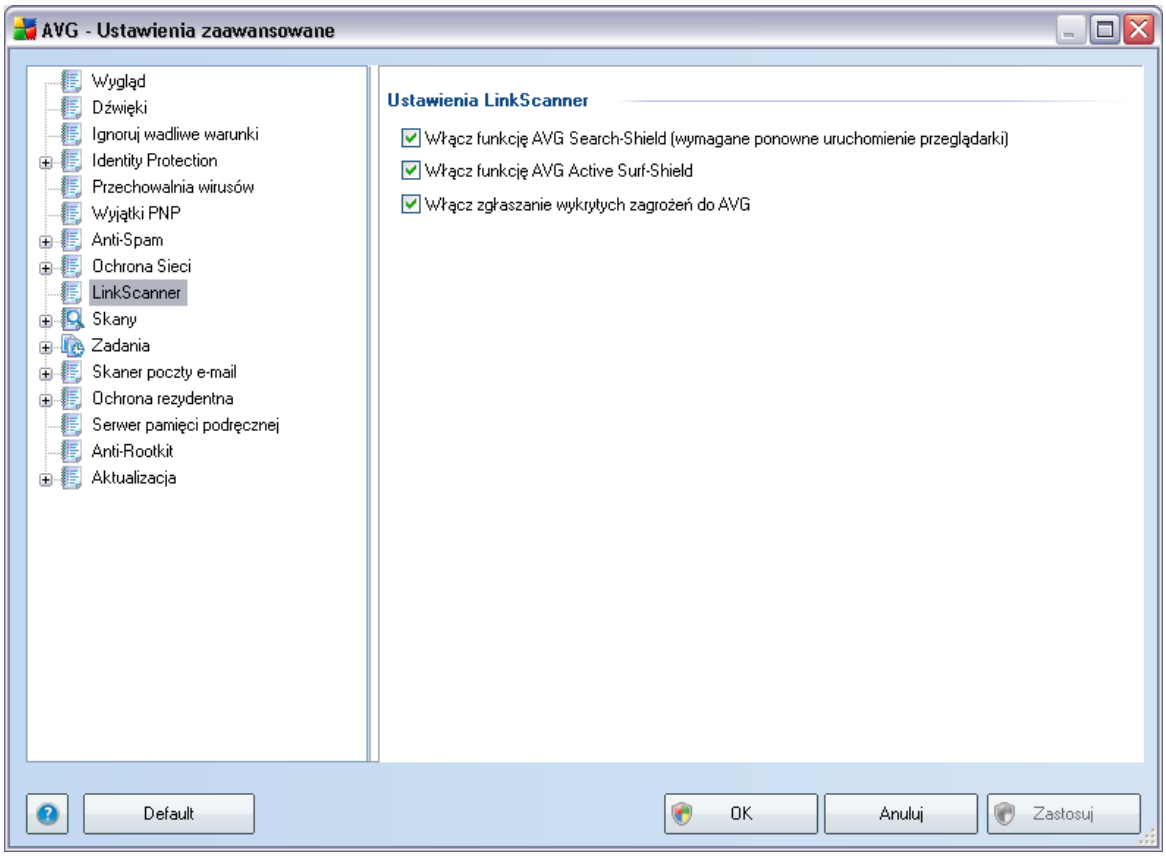
W oknie dialogowym ***Ochrona komunikatorów internetowych*** mozna edytowac ustawienia skladnika ***Ochrona Sieci*** dotyczace skanowania plików wymienianych za posrednictwem komunikatorów internetowych. Obecnie obslugiwane sa trzy komunikatory: ***ICQ***, ***MSN*** i ***Yahoo*** — jesli skladnik ***Ochrona Sieci*** ma sprawdzac, czy komunikacja danego komunikatora jest bezpieczna, nalezy zaznaczyc odpowiednie pole wyboru.

Aby szczególowo okreslic zaufane i blokowane kontakty, nalezy przejsc do odpowiedniego okna dialogowego (***ICQ — Zaawansowane***, ***MSN — Zaawansowane lub Yahoo — Zaawansowane***) i stworzyc ***biala liste*** (*liste uzytkowników, którzy beda mogli przesylac wiadomosci*) oraz ***czarna liste*** (*uzytkowników, którzy maja byc*

blokowani).

10.9. LinkScanner

Okno dialogowe ***Ustawienia skladnika LinkScanner*** umozliwia wlaczenie/wylaczenie podstawowych funkcji skladnika ***LinkScanner***:



- ***Wlacz skladnik AVG Search-Shield***(*opcja domyslnie wlaczona*) — umozliwia sprawdzanie zawartosc stron pojawiajacych sie w wynikach wyszukiwania serwisów Google, Yahoo, Bing, Yandex, Altavista i Baidu i wyswietlanie odpowiednich ikon powiadomien.

- ***Wlacz funkcje AVG Active Surf-Shield*** — (*domyslnie wlaczona*): aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (*w czasie rzeczywistym*). Znane zlosliwe witryny i ich niebezpieczna zawartosc blokowane sa juz w momencie otwarcia ich przez uzytkownika za pomoca przegladarki (*lub jakiejkolwiek innej aplikacji korzystajacej z protokolu HTTP*).

- ***Wlacz zglaszanie wykrytych zagrozen do firmy AVG*** — (*domyslnie wlaczone*): nalezy zaznaczyc to pole, aby wlaczyc raportowanie exploitów oraz niebezpiecznych witryn znalezionych przy uzyciu funkcji ***AVG Active Surf-Shield*** lub ***AVG Search-Shield***. Informacje te sa przekazywane do naszej bazy danych.

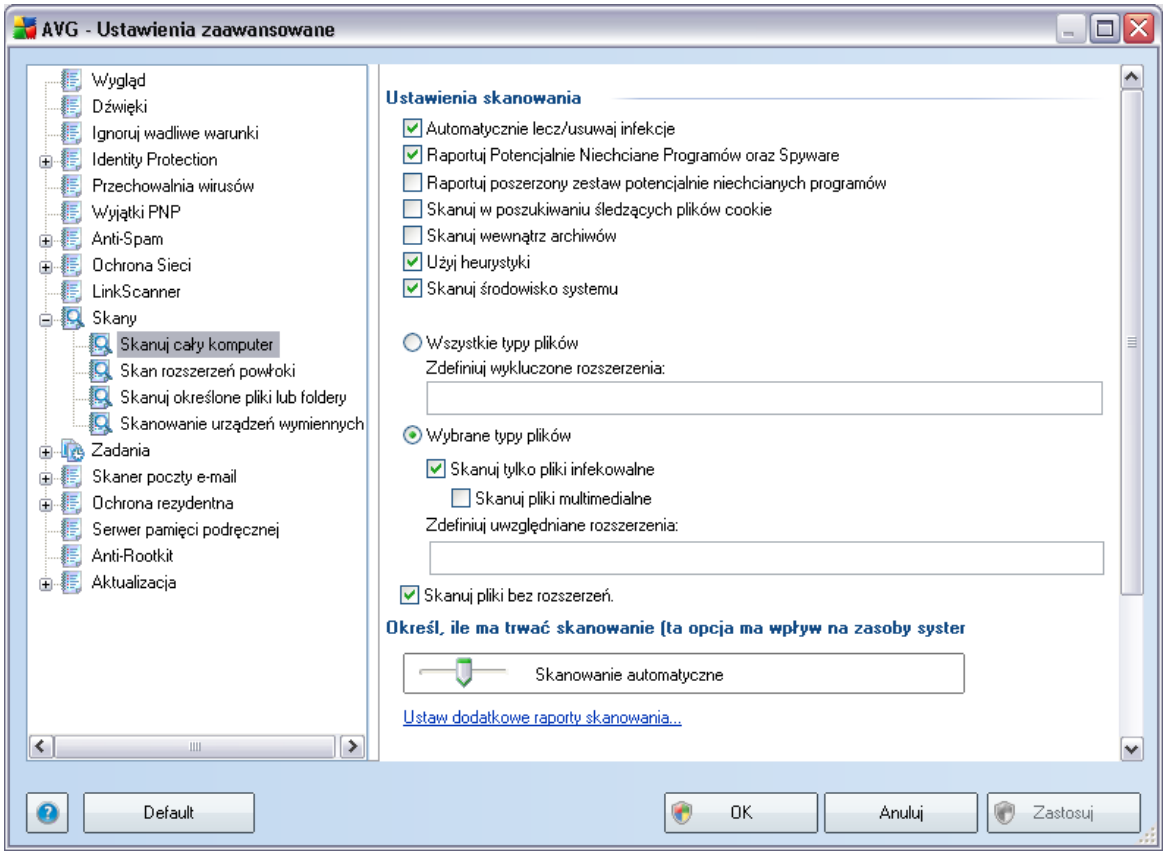
10.10. Skany

Zaawansowane ustawienia skanowania podzielone sa na trzy kategorie odnoszace sie do okreslonych typów testów zdefiniowanych przez producenta AVG:

- ***Skan calego komputera*** — standardowe, wstepnie zdefiniowane skanowanie calego komputera.
- ***Skan rozszerzenia powloki*** — skanowanie wybranych obiektów bezposrednio z interfejsu Eksploratora Windows.
- ***Skan okreslonych plików lub folderów*** — standardowe, wstepnie zdefiniowane skanowanie okreslonych obszarów komputera.
- ***Skan urzadzen wymiennych*** — skanowanie urzadzen wymiennych podlaczonych do komputera.

10.10.1. Skan calego komputera

Opcja ***Skanuj caly komputer*** umozliwia edycje parametrów jednego ze wstepnie zdefiniowanych testów: ***Skan calego komputera***:



Ustawienia skanowania

Sekcja ***Ustawienia skanowania*** zawiera liste parametrów silnika skanujacego:

- ***Automatycznie lecz/usuwaj infekcje*** — jezeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jesli zainfekowany plik nie moze zostac wyleczony automatycznie, obiekt zostanie przeniesiony do***Przechowalni wirusów***.
- ***Raportuj zagrozenia potencjalnie niechcianymi programami i oprogramowaniem szpiegujacym*** (*opcja domyslnie wlaczona*) —

zaznaczenie tego pola powoduje wlaczenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegujacego (a nie tylko wirusów). Oprogramowanie szpiegujace nalezy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrozenie dla bezpieczenstwa, ale niektóre z takich programów moga zostac zainstalowane umyslnie. Nie zaleca sie wylaczania tej opcji — znaczaco zwieksza ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** — jesli poprzednia opcja jest aktywna, mozna równiez zaznaczyc to pole, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona.

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** — ten parametr skladnika Anti-Spyware okresla, ze skanowanie ma wykrywac pliki cookie (*pliki cookie sa w protokole HTTP uzywane do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach, na przyklad preferencji wygladu witryny czy zawartosci koszyków w sklepach internetowych*).

- ***Skanuj wewnatrz archiwów*** — parametr ten okresla, czy skanowanie ma obejmowac wszystkie pliki — nawet te znajdujace sie wewnatrz niektórych typów archiwów, np. ZIP, RAR itd.

- ***Uzyj heurystyki*** — analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku wirtualnej maszyny*) jest jedna z metod wykrywania wirusów w czasie rzeczywistym.

- ***Skanuj srodowisko systemu*** — skanowanie obejmie takze obszary systemowe komputera.

Nastepnie nalezy zdecydowac, czy skanowane maja byc

- ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami (*po zapisaniu przecinki zostaja zamienione na sredniki*) rozszerzen plików, które maja nie byc skanowane;

- ***Wybrane typy plików*** — skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowanie skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa*

duze, a nie sa podatne na infekcje). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

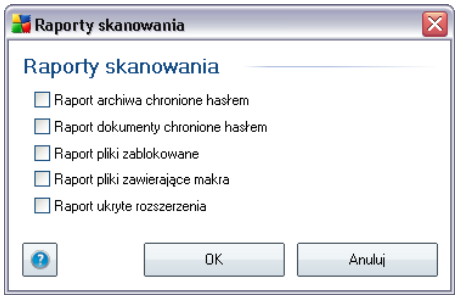
- Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

Priorytet procesu skanowania

W sekcji ***Priorytet procesu skanowania*** mozna szczególowo okreslic zadana predkosc skanowania, w zaleznosci od wykorzystania zasobów systemowych. Domyslnie wartosc tej opcji jest na srednim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jesli skanowanie ma przebiegac szybciej, poziom wykorzystania zasobów wzrosnie, co moze spowolnic dzialanie innych procesów i aplikacji (*opcji mozna smialo uzywac wtedy, gdy komputer jest wlaczony, ale nikt na nim nie pracuje*). Mozna takze obnizyc wykorzystanie zasobów, co przedluzy jednoczesnie czas skanowania.

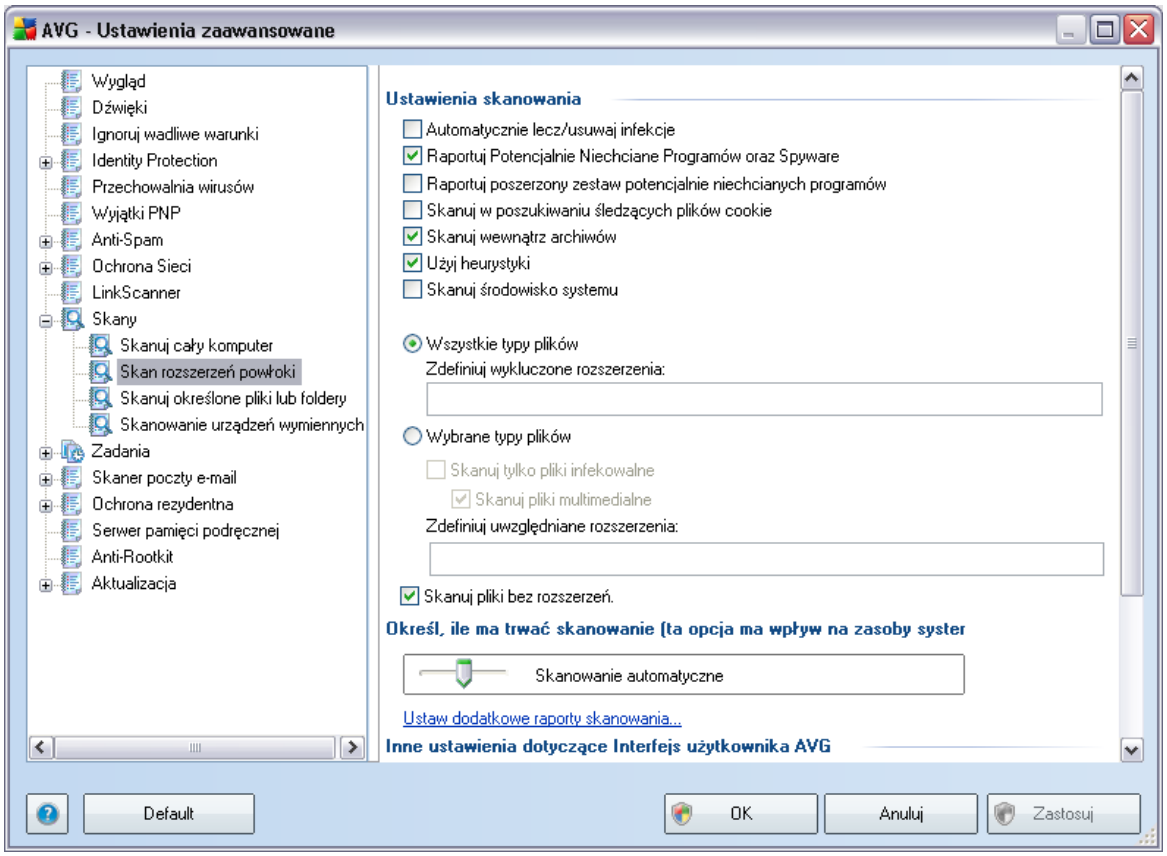
Ustaw dodatkowe raporty skanowania...

Klikniecie linku ***Ustaw dodatkowe raporty skanowania...*** powoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym mozna okreslic szczególowosc raportów, zaznaczajac zadane elementy:



10.10.2. Skan rozszerzenia powloki

Analogicznie do ***Skanu calego komputera***, test ***Skan rozszerzenia powloki*** takze oferuje szereg opcji silnika skanujacego, zdefiniowanych wstepnie przez dostawce oprogramowania AVG. W tym przypadku konfiguracja odnosi sie do skanowania okreslonych obiektów bezposrednio z interfejsu Eksploratora Windows (*rozszerzenie powloki*); zobacz rozdzial ***Skanowanie z poziomu Eksploratora Windows***:

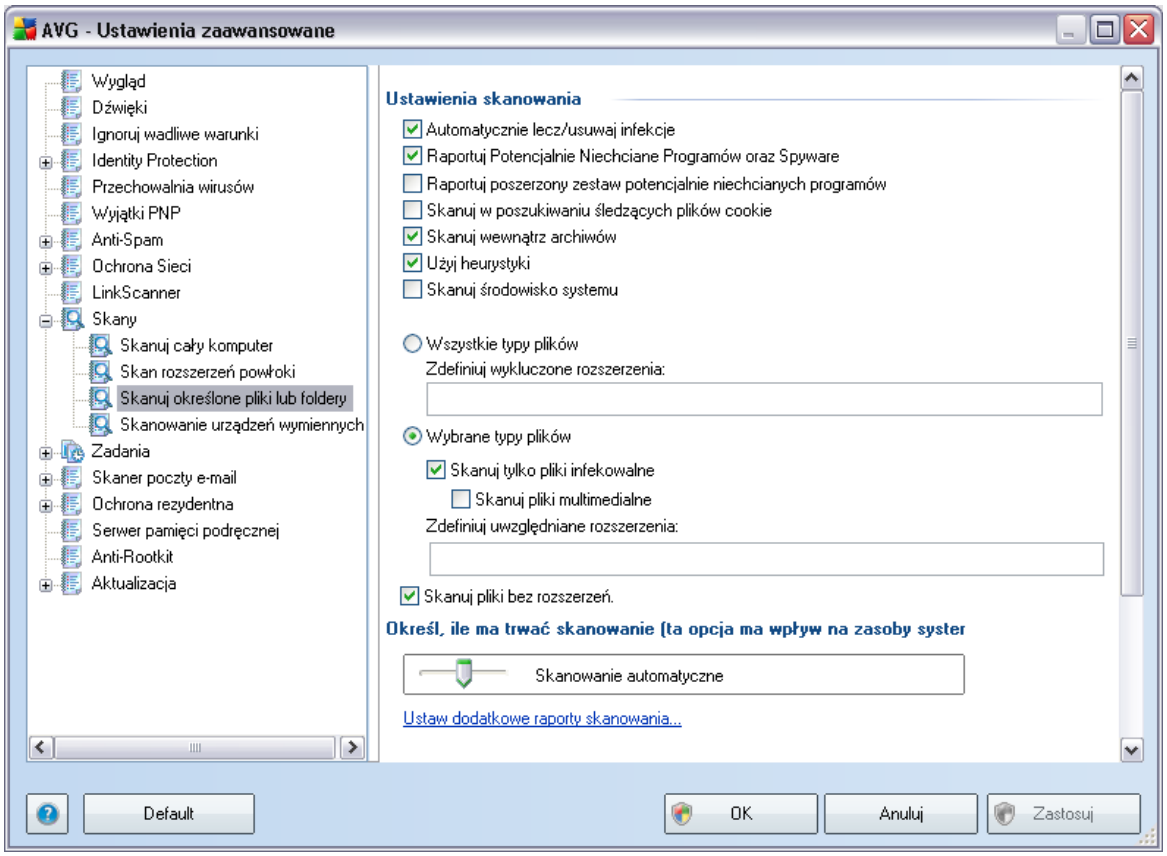


Lista parametrów jest identyczna jak dla testu ***Skan calego komputera***. Ustawienia domyslne sa jednak inne: wiekszosc opcji ***skanu calego komputera*** jest aktywna, natomiast w przypadku ***skanu rozszerzenia powloki*** (***Skanowanie z poziomu Eksploratora Windows***) wybrane sa tylko najistotniejsze parametry.

Uwaga: *Opis poszczególnych parametrów mozna znalezc w rozdziale* ***Zaawansowane ustawienia AVG / Skany / Skan calego komputera***.

10.10.3. Skan okreslonych plików lub folderów

Interfejs edycji testu ***Skan okreslonych plików lub folderów*** jest identyczny jak w przypadku ***Skanu calego komputera***. Wszystkie opcje konfiguracyjne sa takie same, jednak ustawienia domyslne dla ***skanu calego komputera***sa bardziej rygorystyczne:

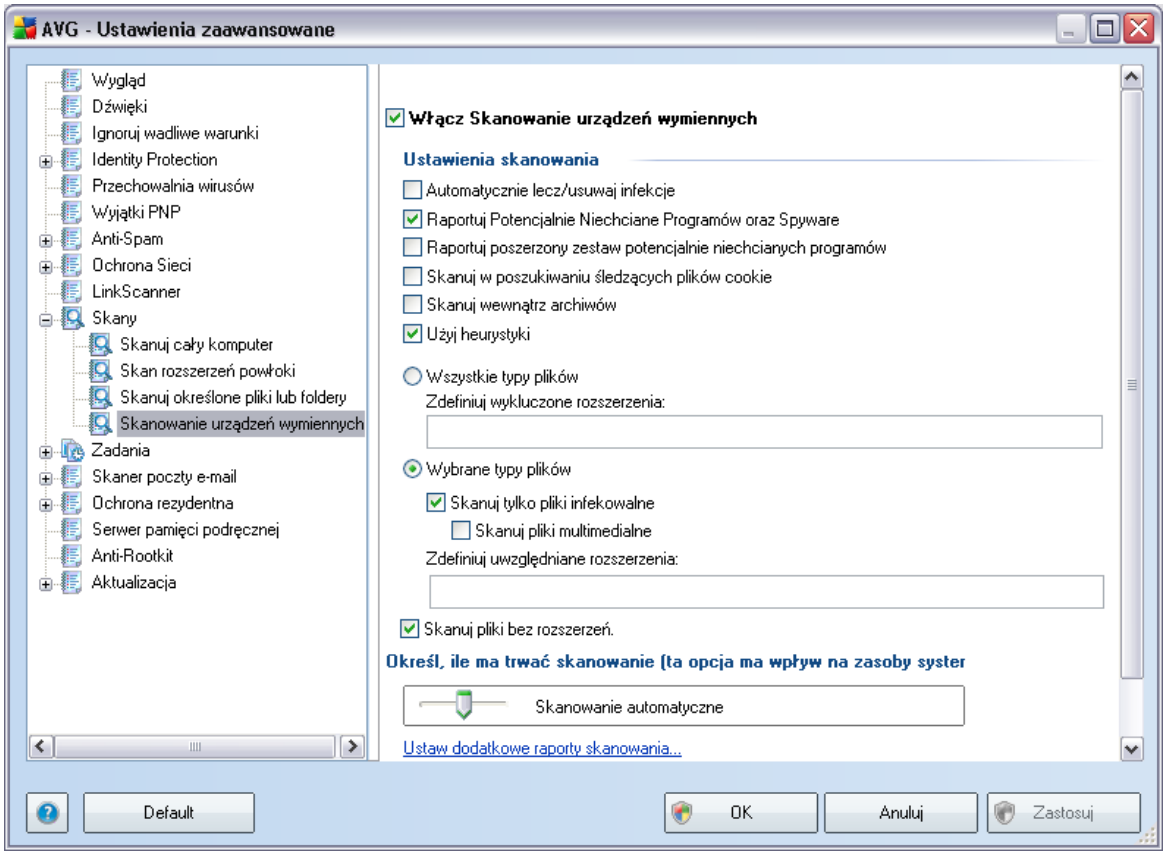


Wszystkie parametry ustawiane w tym oknie dialogowym odnosza sie tylko do obszarów wybranych do ***skanowania okreslonych plików lub folderów***!

Uwaga: *Opis poszczególnych parametrów mozna znalezc w rozdziale* ***Zaawansowane ustawienia AVG / Skany / Skan calego komputera***.

10.10.4. Skan urzadzen wymiennych

Okno z opcjami ***Skanu urzadzen wymiennych*** jest takze bardzo podobne do okna ***Skan calego komputera***:



Skan urzadzen wymiennych jest uruchamiany automatycznie po podlaczeniu do komputera dowolnego urzadzenia wymiennego. Domyslnie jest on wylaczony. Skanowanie urzadzen wymiennych w poszukiwaniu potencjalnych zagrozen jest jednak bardzo wazne, poniewaz sa one czestym zródlem infekcji. Jesli skan ma byc uruchamiany automatycznie, nalezy zaznaczyc opcje ***Wlacz skanowanie urzadzen wymiennych***.

Uwaga: *Opis poszczególnych parametrów mozna znalezc w rozdziale* ***Zaawansowane ustawienia AVG / Skany / Skan calego komputera***.

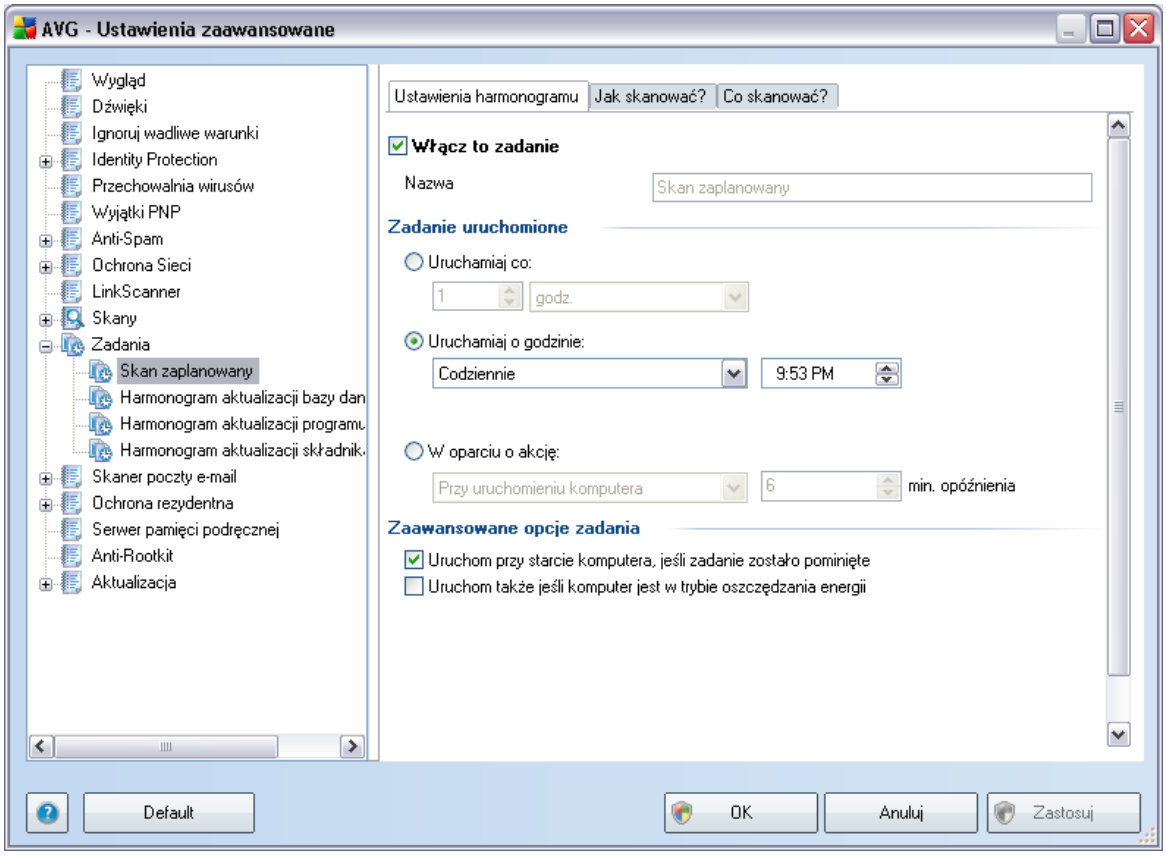
10.11. Zaplanowane zadania

W oknie ***Zadania*** mozna edytowac domyslne ustawienia nastepujacych pozycji:

- Skan zaplanowany
- Harmonogram aktualizacji bazy wirusów
- Harmonogram aktualizacji programu
- Harmonogram aktualizacji bazy Anti-Spam

10.11.1. Skan zaplanowany

Parametry skanowania zaplanowanego mozna edytowac (*albo utworzyc nowy harmonogram*) na trzech kartach:



Na karcie ***Ustawienia harmonogramu*** mozna zaznaczyc/odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowany test lub wlaczyc go ponownie, gdy zajdzie taka potrzeba.

W polu tekstowym ***Nazwa*** (*wylaczone dla harmonogramów domyslnych*) wyswietlana jest nazwa przypisana do danego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (*aby dodac harmonogram, nalezy kliknac prawym przyciskiem myszy element* ***Skan zaplanowany*** *w drzewie nawigacji po lewej*) mozna okreslic wlasna nazwe, a wspomniane pole tekstowe jest edytowalne. Nalezy uzywac krótkich, opisowych nazw, aby ulatwic rozpoznawanie ich przez innych uzytkowników w przyszlosci.

Przyklad: *Nazwy takie jak „Nowy skan” lub „Mój skan” nie sa odpowiednie, poniewaz nie informuja o tym, co jest przedmiotem skanowania. Przykladem dobrej, opisowej nazwy jest „Skan obszarów systemowych”. Ponadto, nie ma potrzeby okreslac w nazwie skanowania, czy skanowany jest caly komputer, czy tylko jego wybrane*

obszary — wlasne testy uzytkownika sa zawsze specyficznym skanowaniem okreslonych plików lub folderów.

W tym samym oknie mozna szczególowo okreslic nastepujace parametry skanowania:

Zadanie uruchomione

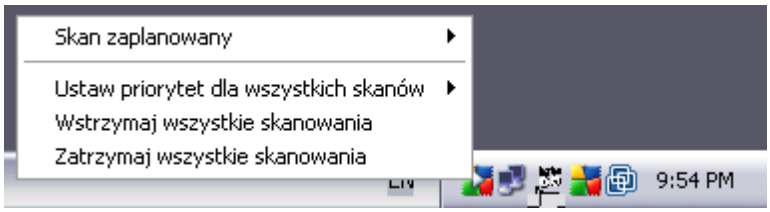
W tym miejscu mozna okreslic, jak czesto ma byc uruchamiane nowe skanowanie. Uruchamianie skanowania moze byc powtarzane w okreslonych odstepach czasu (***Uruchamiaj co***) lub w zadanych momentach (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia okreslonego zdarzenia (***akcja powiazana z uruchomieniem komputera***).

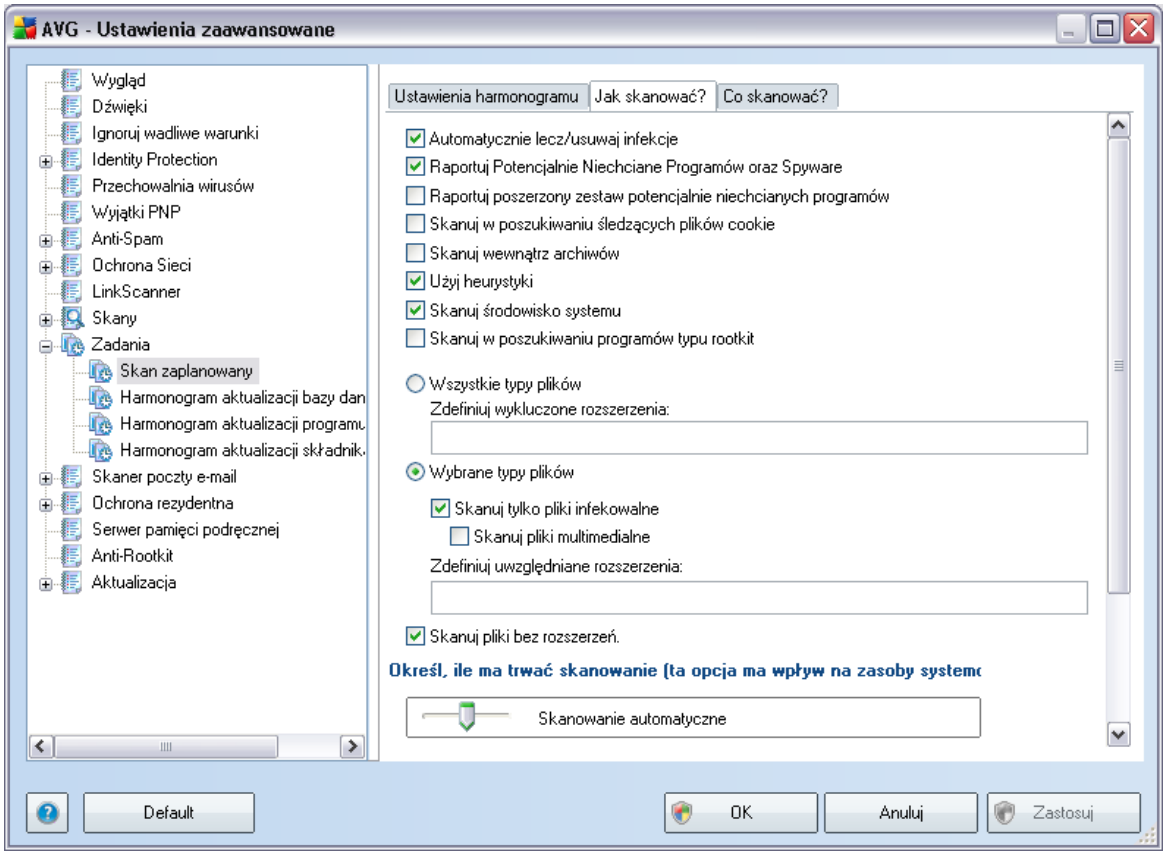
Zaawansowane opcje harmonogramu

Ta sekcja umozliwia zdefiniowanie warunków uruchamiania skanowania w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

Po rozpoczeciu zaplanowanego skanu, nad ikona AVG na pasku zadan wyswietlone zostanie odpowiednie powiadomienie:

Nastepnie pojawi sie tam nowa ikona AVG (*kolorowa, z biala strzalka — jak powyzej*), która informuje o uruchomieniu skanowania. Kliknieciu jej prawym przyciskiem myszy pozwala wyswietlic menu kontekstowe, dzieki któremu mozna wstrzymac lub anulowac skanowanie:





Karta ***Jak skanowac?*** zawiera liste parametrów testu, które mozna wlaczyc lub wylaczyc. Domyslnie wiekszosc funkcji jest wlaczona, a odpowiadajace im ustawienia sa stosowane podczas skanowania. Ustawienia te nalezy zmieniac tylko w uzasadnionych przypadkach, w pozostalych zachowujac wstepnie zdefiniowana konfiguracje:

- ***Automatycznie lecz/usuwaj infekcje*** — jezeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jesli zainfekowany plik nie moze zostac wyleczony automatycznie, obiekt zostanie przeniesiony do***Przechowalni wirusów***.

- ***Raportuj zagrozenia potencjalnie niechcianymi programami i oprogramowaniem szpiegujacym*** (*opcja domyslnie wlaczona*) — zaznaczenie tego pola powoduje wlaczenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegujacego (a nie tylko wirusów). Oprogramowanie szpiegujace nalezy do nietypowej

kategorii szkodliwych programów. Zazwyczaj stanowi zagrozenie dla bezpieczenstwa, ale niektóre z takich programów moga zostac zainstalowane umyslnie. Nie zaleca sie wylaczania tej opcji — znaczaco zwieksza ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** — jesli poprzednia opcja jest aktywna, mozna równiez zaznaczyc to pole, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona.

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** (*opcja domyslnie wlaczona*) — ten parametr skladnika ***Anti-Spyware*** okresla, czy wykrywane maja byc pliki cookie (*uzywane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach - np. preferencji wygladu witryny i zawartosc koszyków w sklepach internetowych*).

- ***Skanuj wewnatrz archiwów*** — (*domyslnie wlaczona*) parametr ten okresla, czy skanowanie ma obejmowac wszystkie pliki, nawet te znajdujace sie wewnatrz niektórych typów archiwów, np. ZIP, RAR itd.

- ***Uzyj heurystyki*** — (*domyslnie wlaczona*) analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku wirtualnej maszyny*) jest jedna z metod wykrywania wirusów w czasie rzeczywistym.

- ***Skanuj srodowisko systemu*** — (*domyslnie wlaczona*) skanowanie obejmie takze obszary systemowe komputera.

- ***Skanuj w poszukiwaniu programów typu rootkit*** — zaznaczenie tej pozycji pozwala dolaczyc wykrywanie programów typu rootkit do operacji skanowania calego komputera. Test Anti-Rootkit mozna takze uruchomic niezaleznie, dzieki interfejsowi skladnika ***Anti-Rootkit***

Nastepnie nalezy zdecydowac, czy skanowane maja byc

- ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami (*po zapisaniu przecinki zostaja zamienione na sredniki*) rozszerzen plików, które maja nie byc skanowane;

- ***Wybrane typy plików*** — skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików

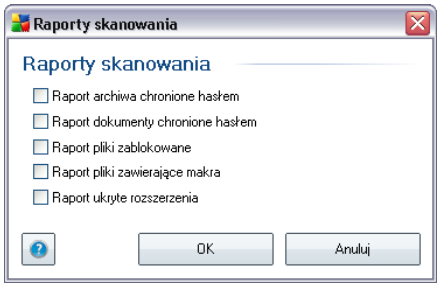
multimedialnych (*plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowanie skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

- Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

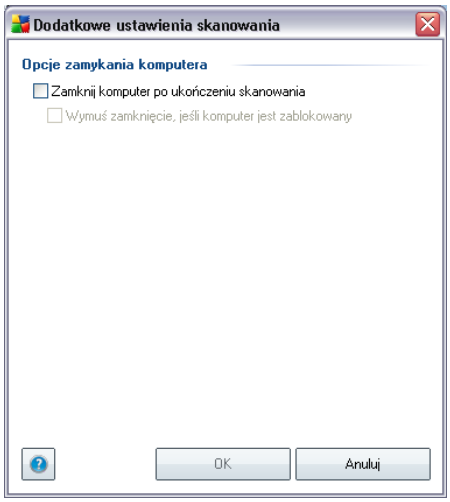
Priorytet procesu skanowania

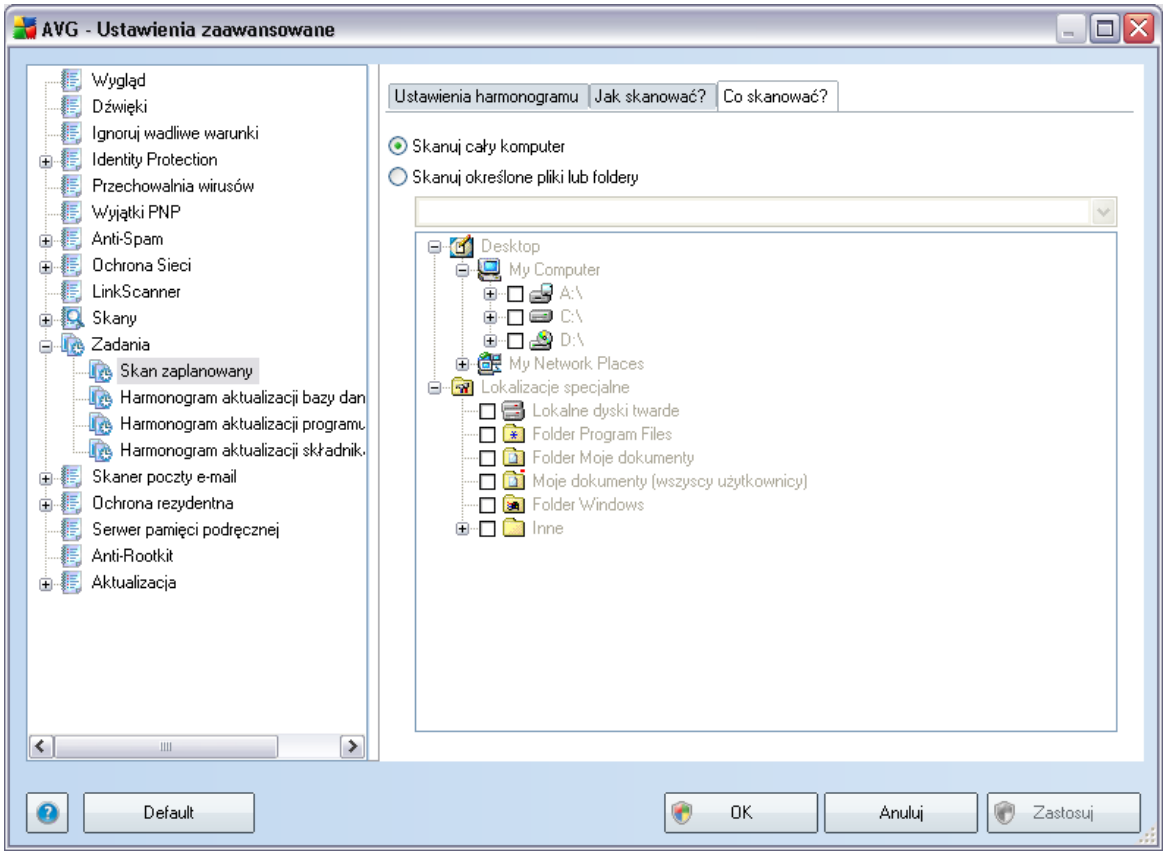
W sekcji ***Priorytet procesu skanowania*** mozna szczególowo okreslic zadana predkosc skanowania, w zaleznosci od wykorzystania zasobów systemowych. Domyslnie wartosc tej opcji jest na srednim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jesli skanowanie ma przebiegac szybciej, poziom wykorzystania zasobów wzrosnie, co moze spowolnic dzialanie innych procesów i aplikacji (*opcji mozna smialo uzywac wtedy, gdy komputer jest wlaczony, ale nikt na nim nie pracuje*). Mozna takze obnizyc wykorzystanie zasobów, co przedluzy jednoczesnie czas skanowania.

Klikniecie linku ***Ustaw dodatkowe raporty skanowania...*** powoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym mozna okreslic szczególowosc raportów, zaznaczajac zadane elementy:



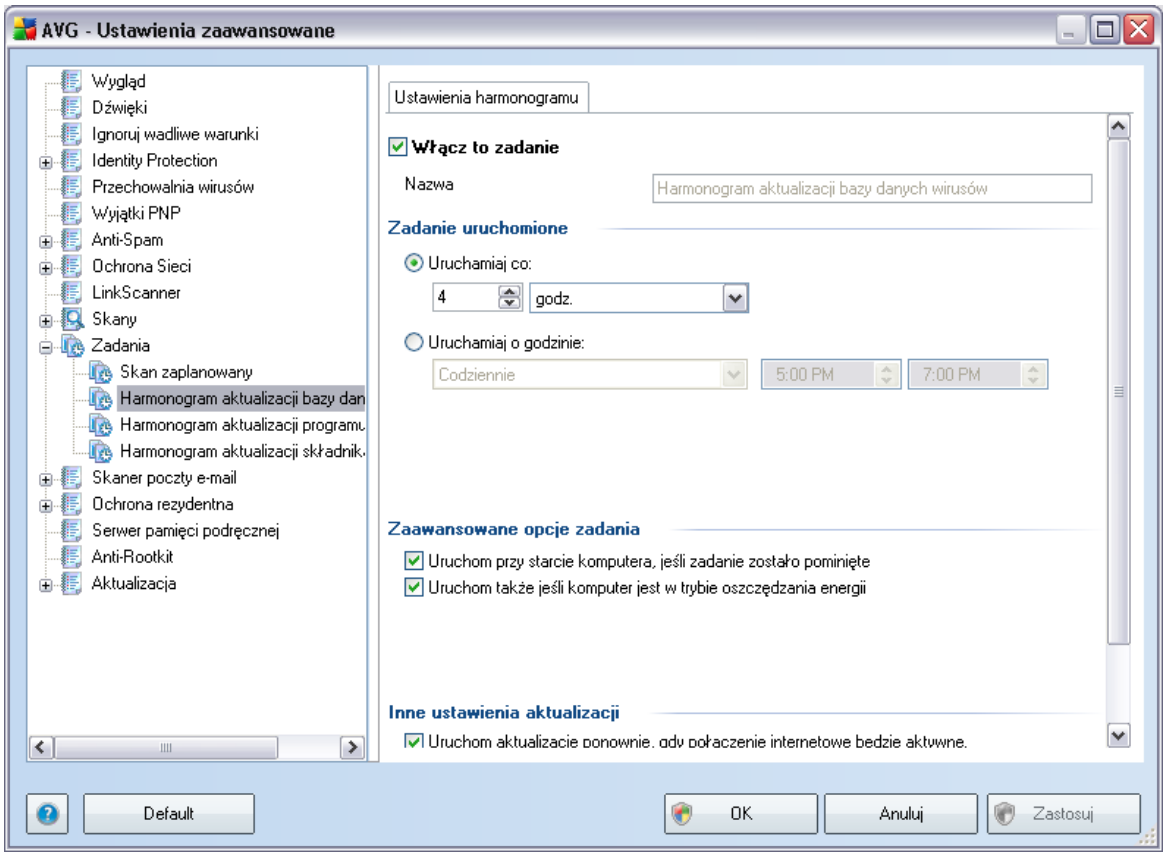
Dodatkowe ustawienia skanowania — link ten pozwala otworzyc nowe okno dialogowe ***Opcje zamykania komputera***, w którym mozna okreslic, czy komputer ma byc zamykany automatycznie po zakonczeniu procesu skanowania. Wybranie tej opcji (***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).


Dodatkowe ustawienia skanowania
Opcje zamykania komputera
Zamknij komputer po ukończeniu skanowania
Wymuś zamknięcie, jeśli komputer jest zablokowany
OK
Anuluj


AVG - Ustawienia zaawansowane
Wygląd
Dźwięki
Ignoruj wadliwe warunki
Identity Protection
Przechowalnia wirusów
Wyjątki PNP
Anti-Spam
Ochrona Sieci
LinkScanner
Skany
Zadania
Skan zaplanowany
Harmonogram aktualizacji bazy dan
Harmonogram aktualizacji programu
Harmonogram aktualizacji składnik
Skaner poczty e-mail
Ochrona rezydentna
Serwer pamięci podręcznej
Anti-Rootkit
Aktualizacja
Ustawienia harmonogramu
Jak skanować?
Co skanować?
Skanuj cały komputer
Skanuj określone pliki lub foldery
Desktop
My Computer
A:\
C:\
D:\
My Network Places
Lokalizacje specjalne
Lokalne dyski twarde
Folder Program Files
Folder Moje dokumenty
Moje dokumenty (wszyscy użytkownicy)
Folder Windows
Inne
Default
OK
Anuluj
Zastosuj

Na karcie ***Co skanowac?*** mozna okreslic, czy planowane jest skanowanie calego komputera, czy skanowanie okreslonych plików lub folderów. W przypadku skanowania okreslonych plików lub folderów, w dolnej czesci okna dialogowego aktywowane jest drzewo katalogów, w którym mozna wybrac obiekty do przeskanowania.

10.11.2. Harmonogram aktualizacji bazy wirusów



Na karcie ***Ustawienia harmonogramu*** mozna odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowana aktualizacje bazy wirusów i wlaczyc ja ponownie dopiero gdy zajdzie taka potrzeba. Podstawowe opcje harmonogramu aktualizacji bazy wirusów dostepne sa w skladniku ***Menedzer aktualizacji***. W niniejszym oknie mozna ustawic szczególowe parametry harmonogramu. W polu tekstowym ***Nazwa*** (*wylaczone dla harmonogramów domyslnych*) jest wyswietlana nazwa przypisana do tego harmonogramu przez producenta programu.

Zadanie uruchomione

W tej sekcji nalezy okreslic interwal dla planowanych aktualizacji bazy danych wirusów. Mozna okreslic, ze uruchamianie aktualizacji bedzie nastepowac stale co pewien czas(***Uruchom co ...***) lub definiujac okreslona date i godzine (***Uruchom o okreslonej godzinie ...***).

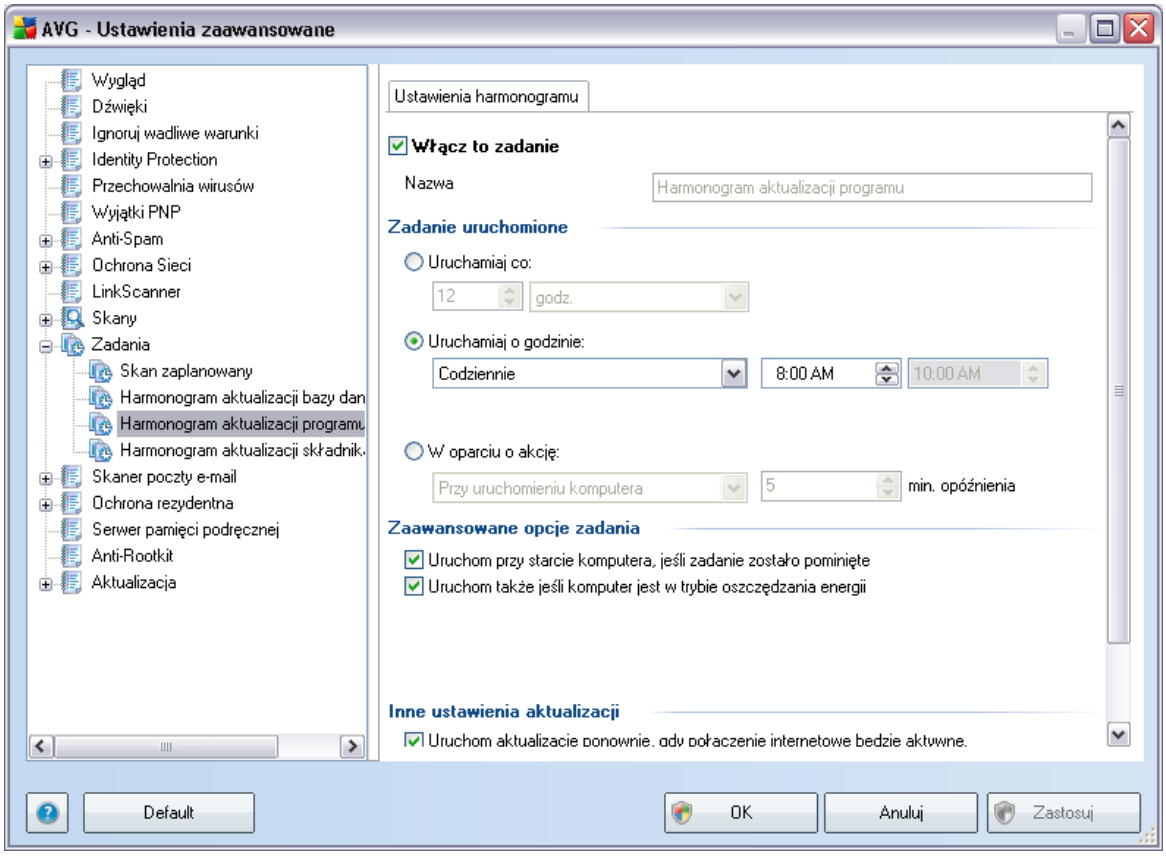
Zaawansowane opcje harmonogramu

Ta sekcja umozliwia zdefiniowanie warunków uruchamiania aktualizacji bazy wirusów w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

Inne ustawienia aktualizacji

Na koniec nalezy zaznaczyc pole wyboru ***Uruchom aktualizacje natychmiast po nawiazaniu polaczenia z internetem***, aby upewnic sie, ze jesli polaczenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie sie, po ponownym polaczeniu z internetem aktualizacja zostanie rozpoczeta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o okreslonej godzinie, nad ikona systemu AVG na pasku systemowym wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wyglad***).



Na karcie ***Ustawienia harmonogramu*** mozna odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowana aktualizacje programu i wlaczyc ja ponownie dopiero gdy zajdzie taka potrzeba. W polu tekstowym ***Nazwa*** (*wylaczone dla harmonogramów domyslnych*) jest wyswietlana nazwa przypisana do tego harmonogramu przez producenta programu.

Zadanie uruchomione

W tym miejscu nalezy okreslic interwal dla nowo zaplanowanych aktualizacji programu. Uruchamianie aktualizacji moze byc powtarzane w okreslonych odstepach czasu (***Uruchamiaj co***) lub w zadanych momentach (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia okreslonego zdarzenia (***akcja powiazana z uruchomieniem komputera***).

Zaawansowane opcje harmonogramu

Ta sekcja umozliwia zdefiniowanie warunków uruchamiania aktualizacji programu w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

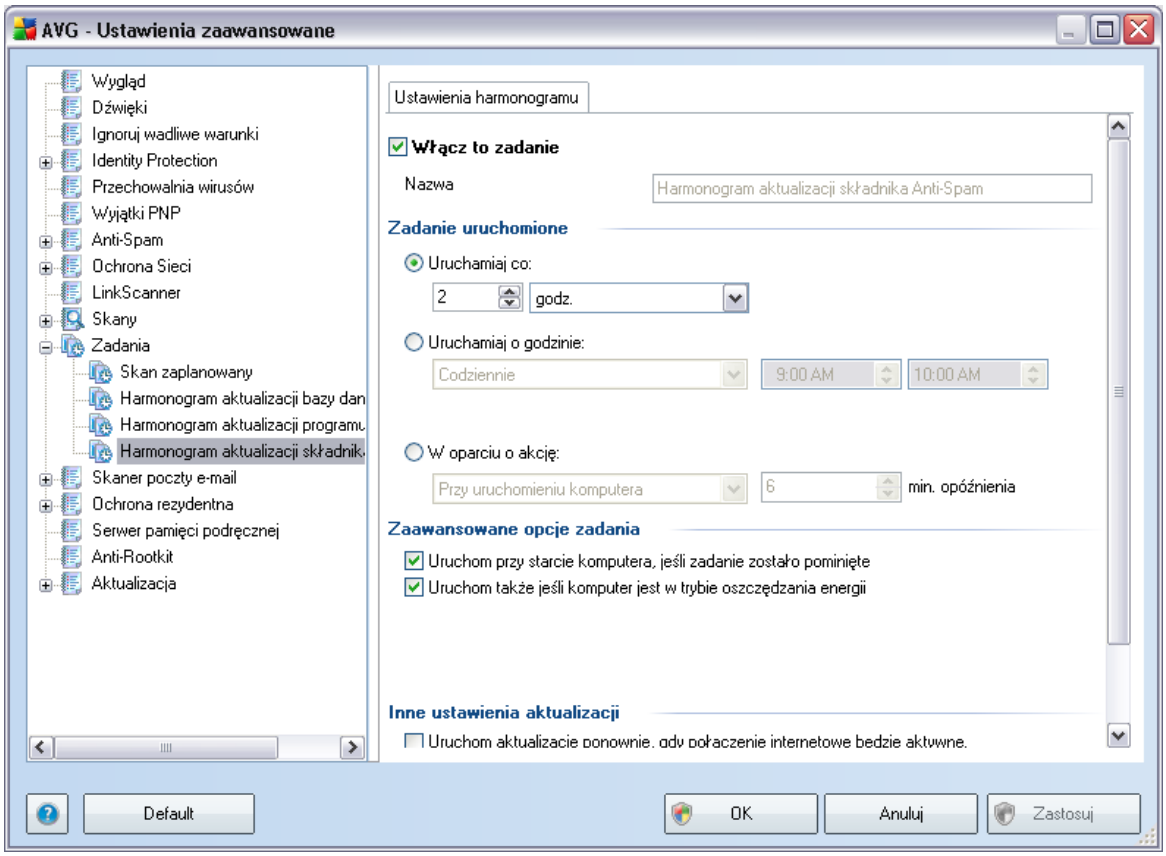
Inne ustawienia aktualizacji

Na koniec nalezy zaznaczyc pole wyboru ***Uruchom aktualizacje natychmiast po nawiazaniu polaczenia z internetem***, aby upewnic sie, ze jesli polaczenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie sie, po ponownym polaczeniu z internetem aktualizacja zostanie rozpoczeta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o okreslonej godzinie, nad ikona systemu AVG na pasku systemowym wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wyglad***).

Uwaga: *Jesli zaplanowane skanowanie i zaplanowana aktualizacja naloza sie, proces aktualizacji bedzie mial pierwszenstwo i skanowanie zostanie przerwane.*

10.11.3. Harmonogram aktualizacji skladnika Anti-Spam



Na karcie ***Ustawienia harmonogramu*** mozna odznaczyc pozycje ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowana ***aktualizacje skladnika*** Anti-Spami wlaczyc ja ponownie dopiero gdy zajdzie taka potrzeba. Podstawowe opcje planowania aktualizacji skladnika ***Anti-Spam*** opisano w interfejsie ***Menedzera aktualizacji***. W niniejszym oknie mozna ustawic szczegółowe parametry harmonogramu aktualizacji. W polu tekstowym ***Nazwa*** (*wylaczone dla harmonogramów domyslnych*) jest wyswietlana nazwa przypisana do tego harmonogramu przez producenta programu.

Zadanie uruchomione

W tym miejscu nalezy okreslic interwaly czasowe uruchamiania nowo zaplanowanych aktualizacji skladnika ***Anti-Spam***. Aktualizacja skladnika ***Anti-Spam***moze byc powtarzana w okreslonych odstepach czasu (***Uruchamiaj co***) lub o zadanej godzinie (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia zdefiniowanego

zdarzenia (***W oparciu o akcje, np. uruchomienie komputera***).

Zaawansowane opcje harmonogramu

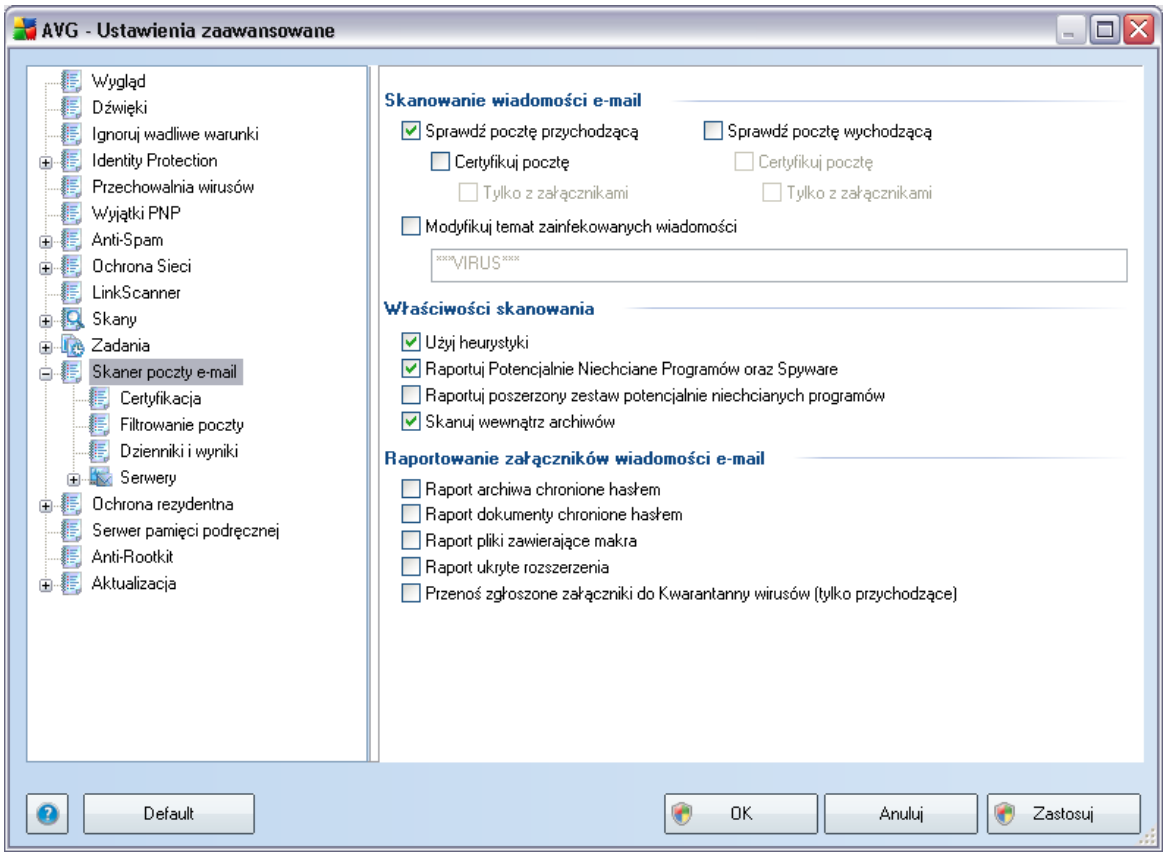
Ta sekcja umozliwia zdefiniowanie warunków uruchamiania aktualizacji skladnika ***Anti-Spam***w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

Inne ustawienia aktualizacji

Na koniec nalezy zaznaczyc pole wyboru ***Uruchom aktualizacje natychmiast po nawiazaniu polaczenia z internetem***, aby upewnic sie, ze jesli polaczenie internetowe zostanie przerwane a proces aktualizacji skladnika ***Anti-Spam*** nie powiedzie sie, po ponownym polaczeniu z internetem aktualizacja zostanie rozpoczeta na nowo.

Po rozpoczeciu zaplanowanego skanowania, nad ikona AVG na pasku zadan wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji* ***Ustawienia zaawansowane/Wyglad***).

10.12. Skaner poczty e-mail



Okno ***Skaner poczty e-mail*** podzielone jest na trzy sekcje:

- ***Skanowanie wiadomosci e-mail*** — w tej sekcji mozna okreslic nastepujace podstawowe ustawienia, dla przychodzacych i/lub wychodzacych wiadomosci e-mail:
    - Czy wiadomosci e-mail maja byc skanowane w poszukiwaniu wirusów.
    - Czy na koncu kazdej wolnej od wirusów wiadomosci e-mail ma byc dodawany tekst certyfikujacy. Tekst moze zostac dostosowany w oknie dialogowym Certyfikacja
    - Czy tekst certyfikacji ma byc dodawany tylko do wiadomosci z zalacznikami.

Aby ***modyfikowac temat zainfekowanych wiadomosci***, nalezy zaznaczyc odpowiednie pole i wpisac zadany tekst. Wartosc ta bedzie dodawana do tematu kazdej zainfekowanej wiadomosci, aby ulatwic jej zidentyfikowanie i odfiltrowanie. Wartosc domyslna to ***WIRUS***; zaleca sie jej zachowanie.

- ***Wlasciwosci skanowania*** — w tej sekcji mozna okreslic sposób skanowania wiadomosci e-mail:
    - ***Uzyj analizy heurystycznej*** — zaznaczenie tego pola umozliwia korzystanie z analizy heurystycznej podczas skanowania wiadomosci e-mail. Gdy ta opcja jest wlaczona, mozliwe jest filtrowanie zalaczników nie tylko wedlug ich rozszerzenia, ale równiez na podstawie ich wlasciwej zawartosci. Opcje filtrów moga zostac dostosowane w oknie Filtrowanie poczty.
    - ***Raportuj zagrozenia potencjalnie niechcianymi programami i oprogramowaniem szpiegujacym*** (*opcja domyslnie wlaczona*) — zaznaczenie tego pola powoduje wlaczenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegujacego (a nie tylko wirusów). Oprogramowanie szpiegujace nalezy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrozenie dla bezpieczenstwa, ale niektóre z takich programów moga zostac zainstalowane umyslnie. Nie zaleca sie wylaczania tej opcji — znaczaco zwieksza ona poziom ochrony komputera.
    - ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** — jesli poprzednia opcja jest aktywna, mozna równiez zaznaczyc to pole, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona.
    - ***Skanuj wewnatrz archiwów*** — zaznaczenie tego pola umozliwia skanowanie zawartosci archiwów dolaczonych do wiadomosci e-mail.
- ***Zglaszanie zalaczników poczty e-mail*** — w tej sekcji mozna skonfigurowac dodatkowe raporty dotyczace potencjalnie niebezpiecznych lub podejrzanych plików. Nalezy zwrócic uwage na fakt, ze Skaner poczty e-mail nie wyswietla zazwyczaj zadnych komunikatów z ostrzezeniem, a jedynie dodaje na koncu wiadomosci tekst certyfikacji. Historie dzialan tego skladnika mozna przejrzec w oknie Zagrozenia wykryte przez Skaner poczty e-mail:

- ***Raportuj archiwa chronione haslem*** — archiwów (ZIP, RAR itp.) chronionych haslem nie mozna skanowac w poszukiwaniu wirusów. Nalezy zaznaczyc to pole wyboru, aby system AVG zglaszal je jako potencjalnie niebezpieczne.

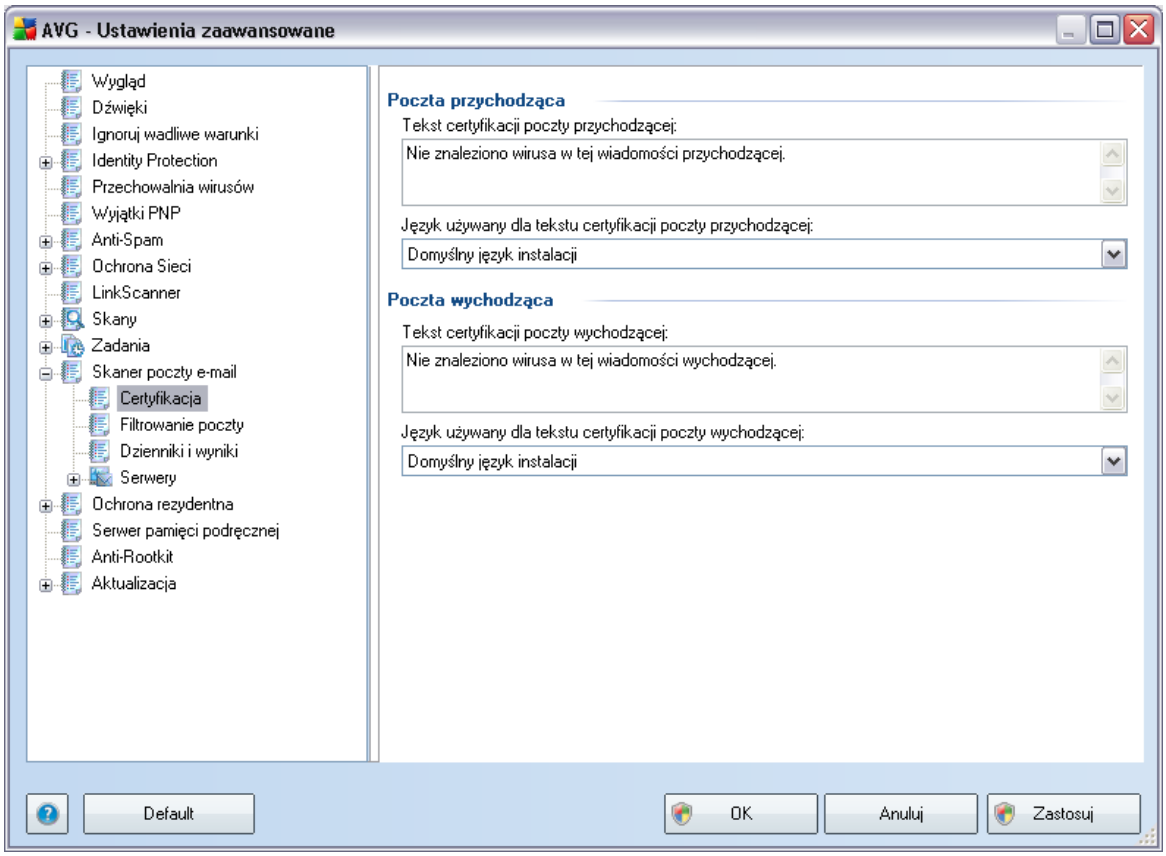
- ***Raportuj dokumenty chronione haslem*** — dokumentów chronionych haslem nie mozna skanowac w poszukiwaniu wirusów. Nalezy zaznaczyc to pole wyboru, aby system AVG zglaszal je jako potencjalnie niebezpieczne.

- ***Raportuj pliki zawierajace makra*** — makro to predefiniowana sekwencja kroków majaca ulatwiac wykonywanie okreslonych czynnosci (szeroko znane sa np. makra programu MS Word). Makra moga byc potencjalnie niebezpieczne — warto zaznaczyc to pole, aby miec pewnosc, ze pliki zawierajace makra beda raportowane jako podejrzane.

- ***Raportuj ukryte rozszerzenia*** — ukryte rozszerzenia moga maskowac podejrzane pliki wykonywalne (np. plik.txt.exe) jako niegrozne pliki tekstowe (np. plik.txt). Nalezy zaznaczyc to pole wyboru, aby zglaszac je jako potencjalnie niebezpieczne.

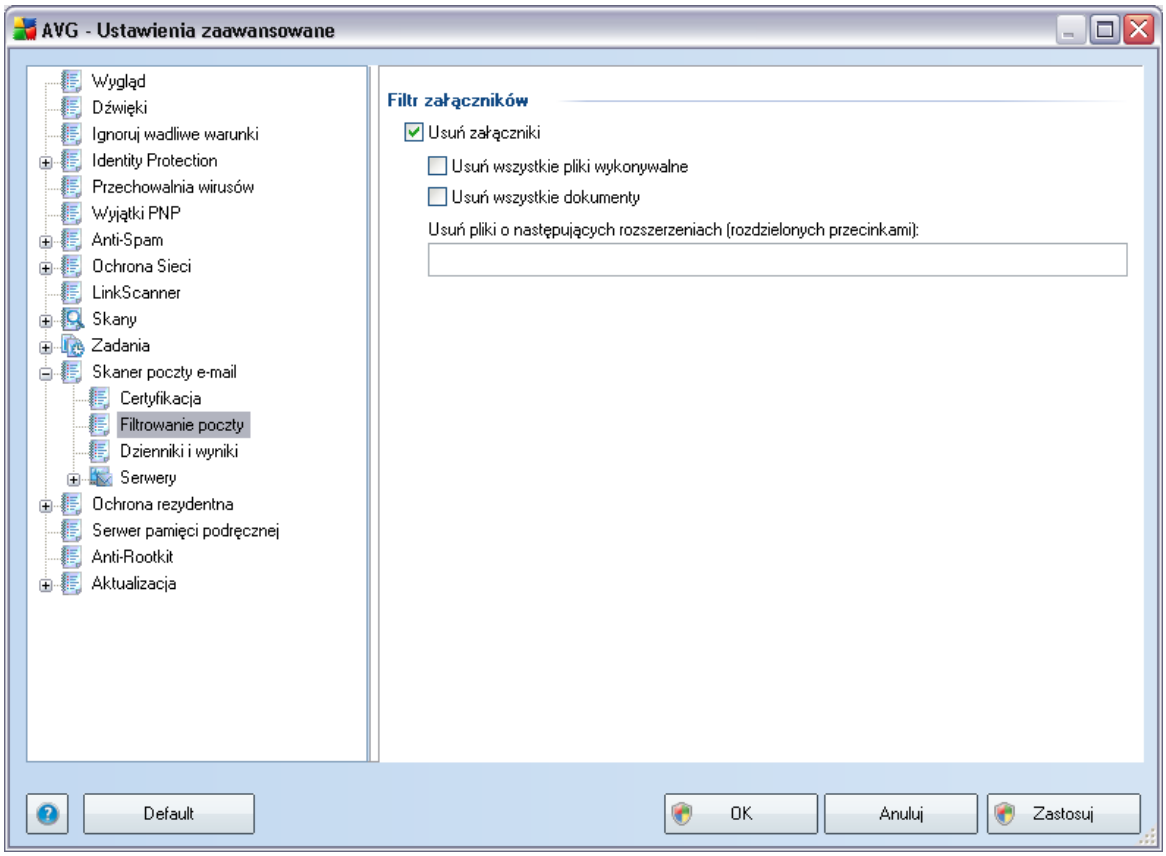
- ***Przenos raportowane zalaczniki do Przechowalni wirusów*** — nalezy okreslic, czy system ma powiadamiac poczta e-mail o archiwach zabezpieczonych haslem, dokumentach zabezpieczonych haslem, plikach zawierajacych makra i/lub plikach o ukrytych rozszerzeniach, które zostana wykryte jako zalaczniki do skanowanych wiadomosci e-mail. Nalezy takze okreslic, czy w przypadku wykrycia takiej wiadomosci podczas skanowania zainfekowany obiekt ma zostac przeniesiony do ***Przechowalni wirusów***.

10.12.1. Certyfikacja



W oknie ***Certyfikacja*** mozna szczególowo okreslic tresc certyfikatu oraz jego jezyk. Ustawienia te nalezy wprowadzic osobno dla ***wiadomosci przychodzacych*** i ***wychodzacych***.

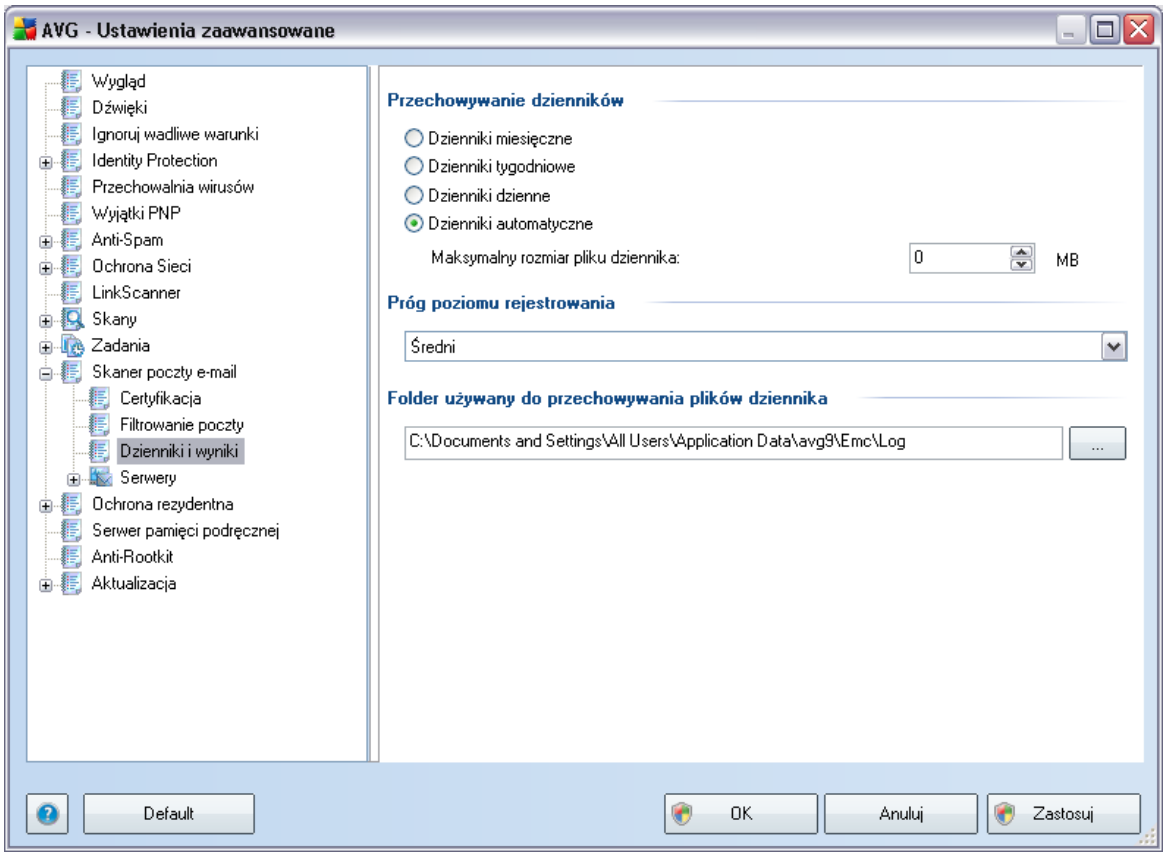
10.12.2. Filtrowanie poczty



W oknie ***Filtr zalaczników*** mozna ustawiac parametry skanowania zalaczników e-mail. Opcja ***Usun zalaczniki*** jest domyslnie wylaczona. Jesli zostanie wlaczona, wszystkie zalaczniki wiadomosci zidentyfikowane jako zainfekowane lub potencjalnie niebezpieczne, beda automatycznie usuwane. Aby okreslic typy zalaczników, które maja byc usuwane, nalezy zaznaczyc odpowiednia opcje:

- ***Usun wszystkie pliki wykonywalne*** — usuniete beda wszystkie pliki *.exe.
- ***Usun wszystkie dokumenty*** — usuniete zostana wszystkie pliki *.doc, *.docx, *.xls, *.xlsx.
- ***Usun pliki o nastepujacych rozszerzeniach oddzielonych przecinkami*** — usuniete beda wszystkie pliki o zdefiniowanych rozszerzeniach.

10.12.3. Dzienniki i Wyniki

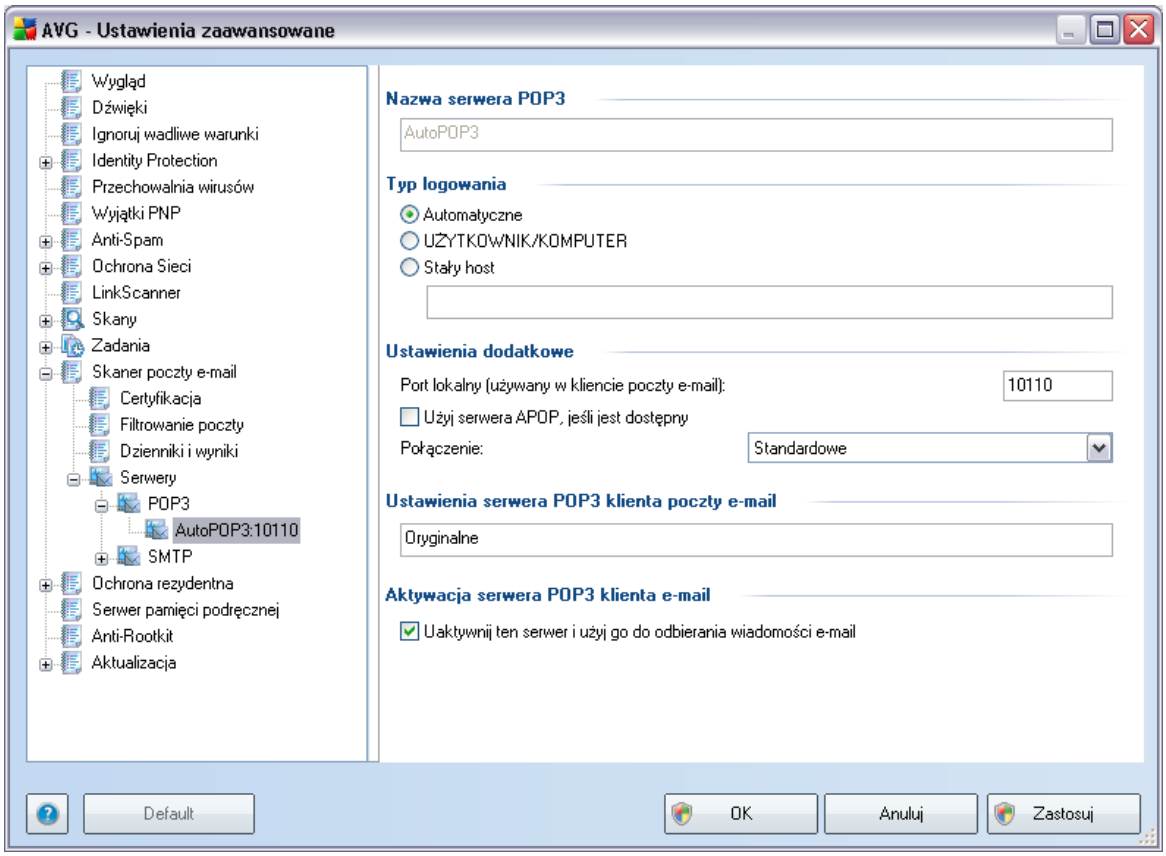


W oknie ***Dzienniki i wyniki*** mozna okreslic parametry przechowywania wyników skanowania poczty e-mail. Okno to podzielone jest na dwa obszary:

- ***Przechowywanie dzienników*** — pozwala zdecydowac, czy informacje o skanowaniu poczty e-mail maja byc rejestrowane codziennie, co tydzien, co miesiac itd.; mozna tu takze okreslic maksymalny rozmiar pliku dziennika (*w MB*).
- ***Próg poziomu rejestrowania*** — domyslnie ustawiony jest poziom sredni; mozna wybrac nizszy (*rejestrowanie podstawowych informacji o polaczeniu*) lub wyzszy (*rejestrowanie calego ruchu*).
- ***Folder uzywany do przechowywania plików dziennika*** — pozwala okreslic, gdzie maja znajdowac sie pliki dziennika.

10.12.4. Serwery

W sekcji ***Serwery*** edytowac mozna parametry wirtualnych serwerów ***Skanera poczty e-mail*** lub zdefiniowac nowy (klikajac przycisk ***Dodaj nowy serwer***).



W tym oknie dialogowym (dostepnym z menu ***Serwery / POP3***) mozna zdefiniowac (na potrzeby ***Skanera poczty e-mail***) nowy serwer poczty przychodzacej, korzystajacy z protokolu POP3:

- ***Nazwa serwera POP3*** — nalezy wpisac nazwe serwera lub zachowac domyslna nazwe AutoPOP3.
- ***Typ logowania*** — definiuje metode okreslania serwera pocztowego dla wiadomosci przychodzacych:
    - ***Automatycznie*** — logowanie jest przeprowadzane automatycznie

zgodnie z ustawieniami klienta poczty e-mail.

- ***UZYTKOWNIK/KOMPUTER*** — najprostsza i najczesciej uzywana metoda ustalania docelowego serwera pocztowego jest metoda proxy. Stosujac te metode, jako czesc loginu uzytkownika nalezy podac jego nazwe lub adres (lub takze port), oddzielajac ja znakiem /. Na przyklad dla konta uzytkownik1 na serwerze pop.domena.com z numerem portu 8200 nalezy stosowac login uzytkownik1/pop.domena.com:8200.

- ***Staly host*** — po wybraniu tej opcji program bedzie zawsze korzystal z serwera okreslonego w tym miejscu. Nalezy podac adres lub nazwe serwera pocztowego. Login uzytkownika pozostaje niezmieniony. Jako nazwy mozna uzyc nazwy domeny (na przyklad pop.acme.com) lub adresu IP (na przyklad 123.45.67.89). Jesli serwer pocztowy uzywa niestandardowego portu, mozna okreslic go po dwukropku zaraz za nazwa serwera (na przyklad pop.domena.com:8200). Standardowym portem protokolu POP3 jest 110.

- ***Ustawienia dodatkowe*** — pozwalaja zdefiniowac bardziej szczegółowe parametry:

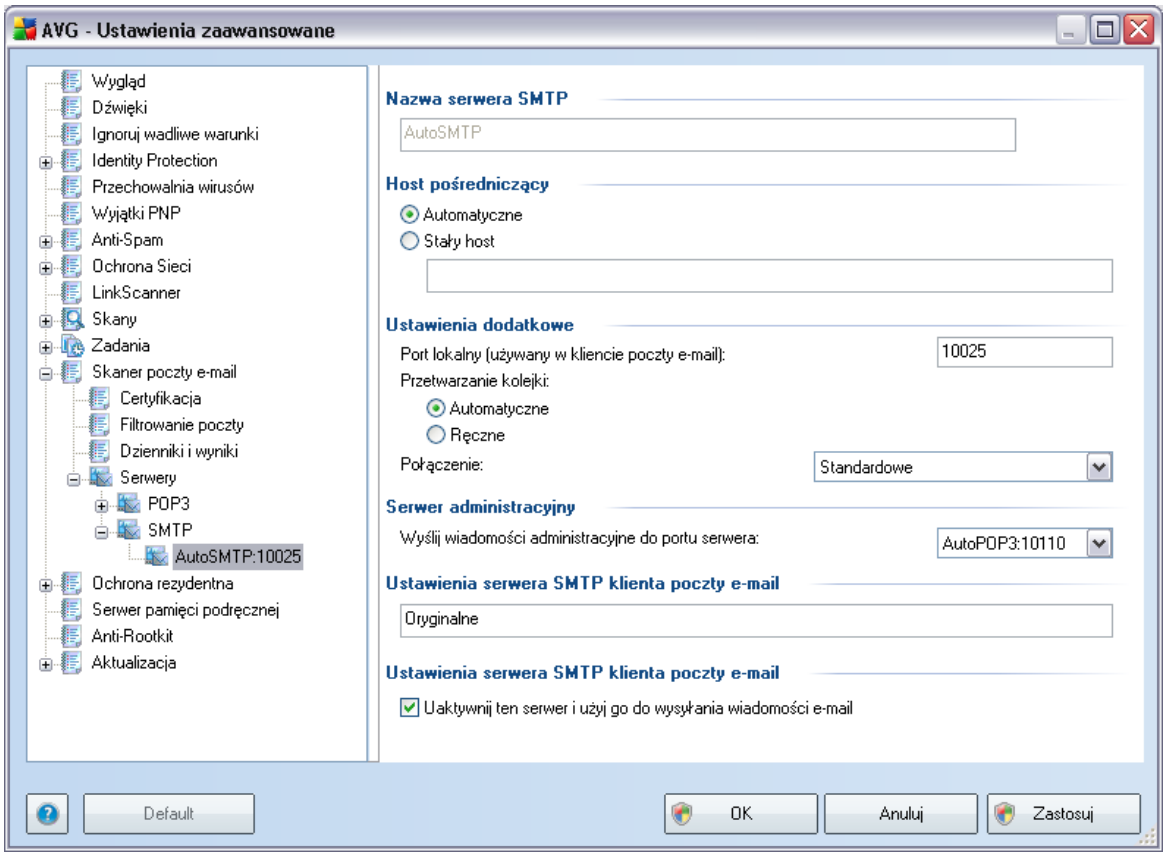
  - ***Port lokalny*** — okresla port nasluchu dla aplikacji pocztowej. Ten sam port nalezy nastepnie okreslic w kliencie poczty jako port docelowy serwera POP3.

  - ***Uzyj serwera APOP, jesli jest dostepny*** — opcja ta zapewnia bezpieczniejsze logowanie na serwerze pocztowym. Gwarantuje to, ze ***Skaner poczty e-mail*** bedzie uzywal alternatywnej metody przekazywania hasla uzytkownika, polegajacej na wysylaniu go w formie zaszyfrowanej, która korzysta ze zmiennego klucza nadeslanego przez serwer. Funkcja ta dostepna jest tylko wtedy, gdy obsluguje ja docelowy serwer pocztowy.

  - ***Polaczenie*** — z menu rozwijanego nalezy wybrac rodzaj uzywanego polaczenia (zwykle/SSL/domyslne SSL). Jesli zostanie wybrane polaczenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostepna jest tylko wtedy, gdy obsluguje ja docelowy serwer pocztowy.

- ***Ustawienia serwera POP3 klienta poczty e-mail*** — w tym obszarze znajduja sie informacje dotyczace poprawnego skonfigurowania ustawien klienta poczty e-mail sluzacych do sprawdzania poczty przychodzacej przez ***Skaner poczty e-mail***. Informacje te stanowia podsumowanie odpowiednich parametrów okreslonych w calej konfiguracji AVG.

- ***Aktywacja serwera POP 3 klienta poczty e-mail*** — opcje te nalezy zaznaczyc/odznaczyc, aby aktywowac/wylaczyc okreslony serwer POP3.



W tym oknie dialogowym (dostepnym z menu ***Serwery / SMTP***) mozna zdefiniowac (na potrzeby ***Skanera poczty e-mail***) nowy serwer poczty przychodzacej, korzystajacy z protokolu SMTP:

- ***Nazwa serwera SMTP —*** nalezy wpisac nazwe serwera lub zachowac domyslna nazwe AutoSMTP.
- ***Host posredniczacy —*** definiuje metode okreslania serwera pocztowego dla wiadomosci wychodzacych:
    - ***Automatyczne*** — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail

- ***Staly host*** — po wybraniu tej opcji program bedzie zawsze korzystal z serwera okreslonego w tym miejscu. Nalezy podac adres lub nazwe serwera pocztowego. Jako nazwy mozna uzyc domeny (na przyklad smtp.domena.com) lub adresu IP (na przyklad 123.45.67.89). Jesli serwer pocztowy uzywa niestandardowego portu, mozna okreslic go po dwukropku zaraz za nazwa serwera (np. smtp.acme.com:8200). Standardowym portem protokolu SMTP jest port 25.

- ***Ustawienia dodatkowe*** — pozwalaja zdefiniowac bardziej szczególowe parametry:

  - ***Port lokalny*** — okresla port nasluchu dla aplikacji pocztowej. Ten sam port nalezy nastepnie okreslic w aplikacji pocztowej jako port komunikacji SMTP.

  - ***Przetwarzanie kolejki*** — okresla zachowanie ***skanera poczty e-mail*** podczas przetwarzania wymagan dotyczacych wysylania wiadomosci e-mail:

    - Automatycznie — poczta wychodzaca jest natychmiast dostarczana (wysylana) do docelowego serwera pocztowego.

    - Reczne — wiadomosci sa umieszczane w kolejce wiadomosci wychodzacych i wysylane w pózniejszym terminie.

  - ***Polaczenie*** — z menu rozwijanego nalezy wybrac rodzaj uzywanego polaczenia (zwykle/SSL/domyslne SSL). Jesli zostanie wybrane polaczenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostepna jest tylko wtedy, gdy obsluguje ja docelowy serwer pocztowy.

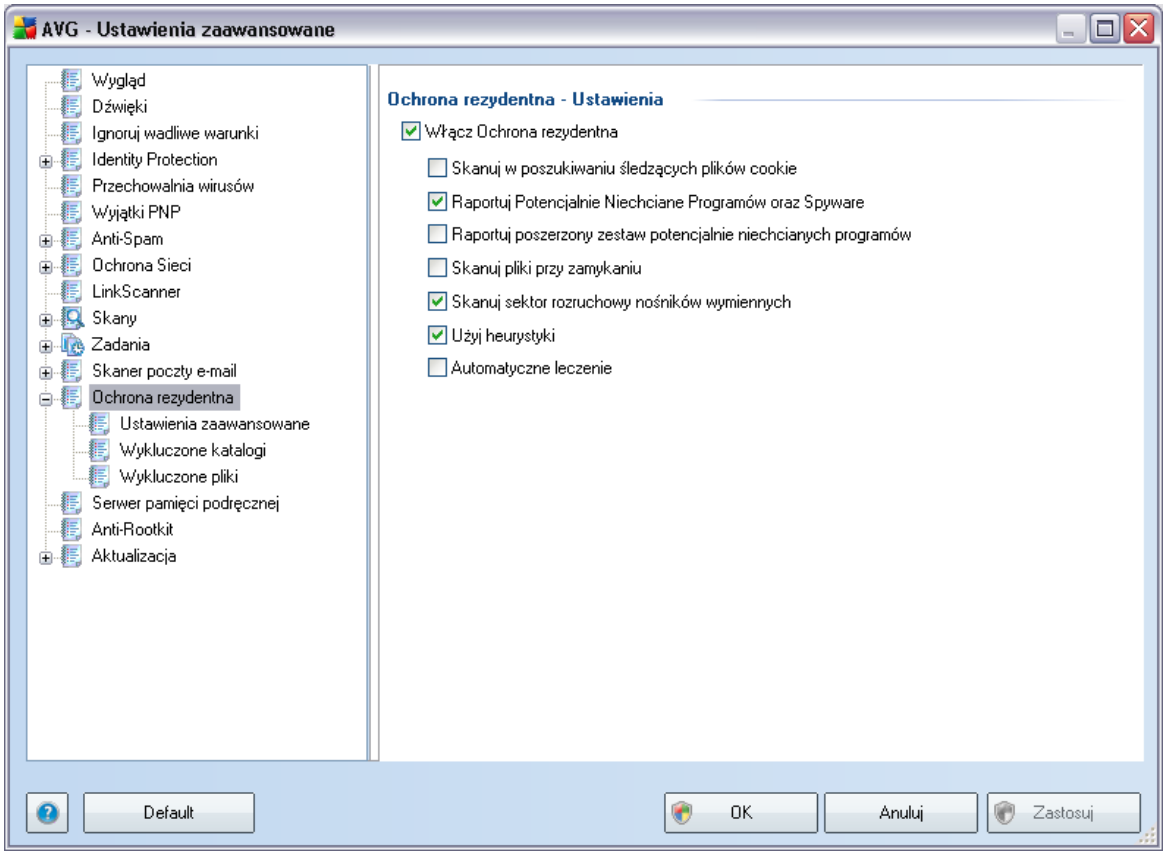
- ***Serwer administracyjny*** — zawiera numer portu serwera uzywanego do zwrotnego dostarczania raportów administracyjnych. Takie wiadomosci sa generowane, kiedy np. serwer docelowy jest niedostepny lub odrzuca wiadomosc wychodzaca.

- ***W sekcji*** Ustawienia serwera SMTP klienta poczty e-mail znajduja sie zalecenia dotyczace takiej konfiguracji klienta poczty, która umozliwi wysylanie wiadomosci do aktualnie modyfikowanego serwera. Informacje te stanowia podsumowanie odpowiednich parametrów okreslonych w calej konfiguracji AVG.

- ***Aktywacja serwera SMTP klienta poczty e-mail*** — zaznacz lub usun zaznaczenie tego pola, aby wlaczyc/wylaczyc okreslony powyzej serwer SMTP.

10.13. Ochrona rezydentna

Skladnik ***Ochrona Rezydentna*** zapewnia aktywna ochrone plików i folderów przed wirusami, oprogramowaniem szpiegujacym i innymi zagrozeniami.



W oknie ***Ustawienia Ochrony rezydentnej*** mozna calkowicie wlaczyc lub wylaczyc ***Ochrone Rezydentna***, zaznaczajac lub odznaczajac pole ***Wlacz Ochrone Rezydentna*** (*opcja ta jest domyslnie wlaczona*). Ponadto, mozna aktywowac tylko wybrane funkcje ***Ochrony Rezydentnej***:

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** — parametr ten okresla, czy w czasie skanowania maja byc wykrywane pliki cookie. (*Pliki cookie w protokole HTTP sa uzywane do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach — np. preferencje dotyczace wygladu witryny lub zawartosc koszyka w sklepach internetowych.*)

- ***Raportuj zagrozenia potencjalnie niechcianymi programami i***

oprogramowaniem szpiegujacym (*opcja domyslnie wlaczona*) — zaznaczenie tego pola powoduje wlaczenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegujacego (a nie tylko wirusów). Oprogramowanie szpiegujace nalezy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrozenie dla bezpieczenstwa, ale niektóre z takich programów moga zostac zainstalowane umyslnie. Nie zaleca sie wylaczania tej opcji — znaczaco zwieksza ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** — jesli poprzednia opcja jest aktywna, mozna równiez zaznaczyc to pole, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona.

- ***Skanuj pliki przy zamykaniu*** — oznacza, ze system AVG skanuje aktywne obiekty (np. aplikacje, dokumenty itp.) nie tylko przy ich otwieraniu, ale takze przy zamykaniu. Funkcja ta pomaga chronic komputer przed pewnymi typami bardziej skomplikowanych wirusów.

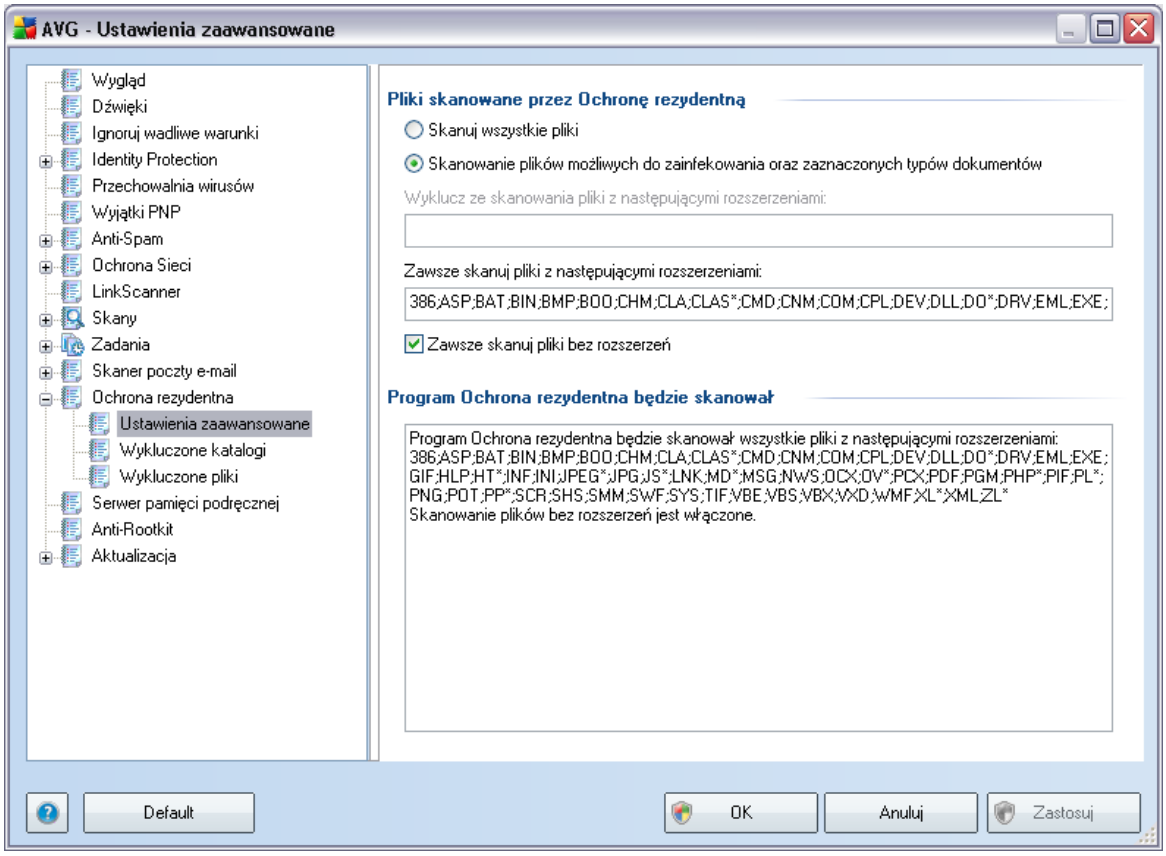
- ***Skanuj sektor rozruchowy nosników wymiennych*** — (*domyslnie wlaczona*)

- ***Uzyj heurystyki*** — (*domyslnie wlaczona*) do wykrywania bedzie uzywana heurystyka (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku maszyny wirtualnej*).

- ***Automatyczne leczenie*** — kazda wykryta infekcja bedzie automatycznie leczona (o ile jest to mozliwe).

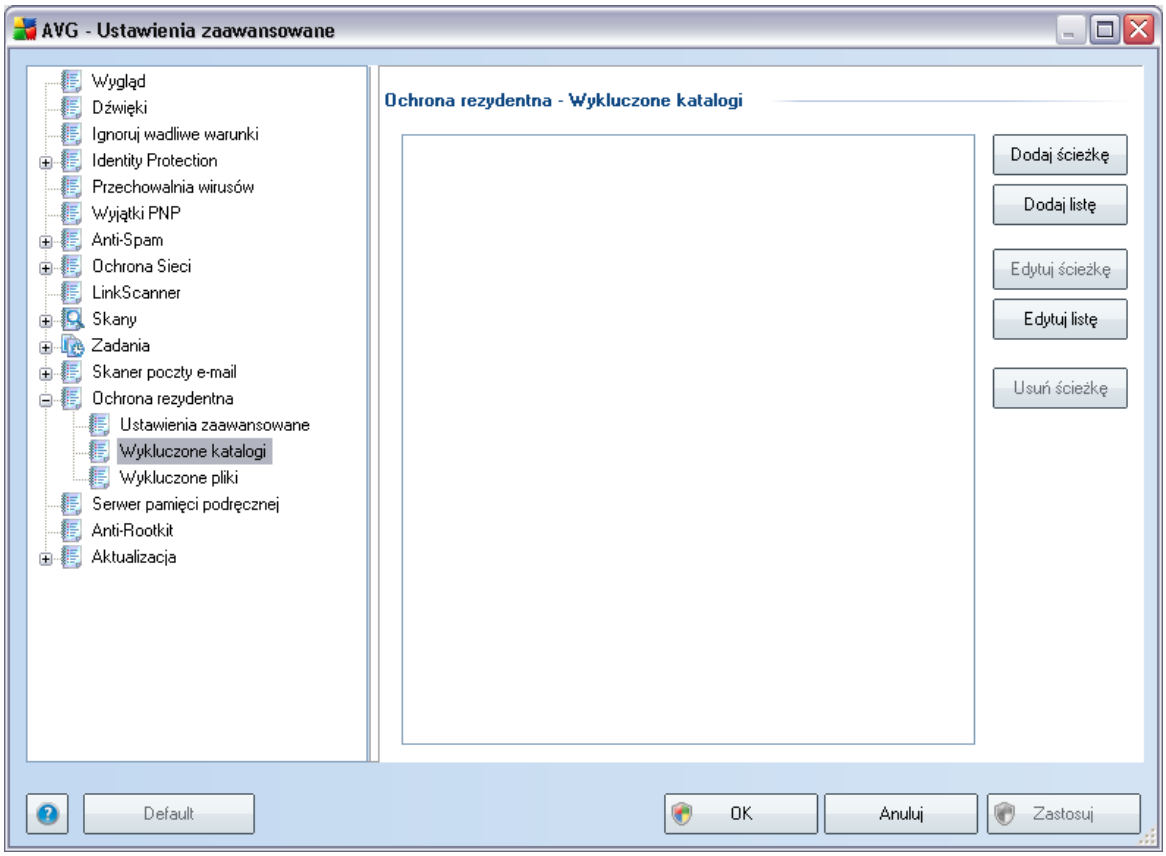
10.13.1. Ustawienia zaawansowane

W oknie ***Pliki skanowane przez Ochrone Rezydentna*** mozna okreslic, które pliki maja byc skanowane (*wedlug ich rozszerzen*):



Zdecyduj, czy chcesz skanowac tylko pliki infekowalne - jesli tak, bedziesz mógl okreslic liste rozszerzen plików, które maja byc wykluczone ze skanowania, oraz liste tych, które maja byc zawsze skanowane.

10.13.2. Wykluczenia katalogów



Okno ***Ochrona rezydentna — Wykluczone katalogi*** pozwala definiowac foldery, które maja byc wykluczone ze skanowania przez ***Ochrone Rezydentna.***

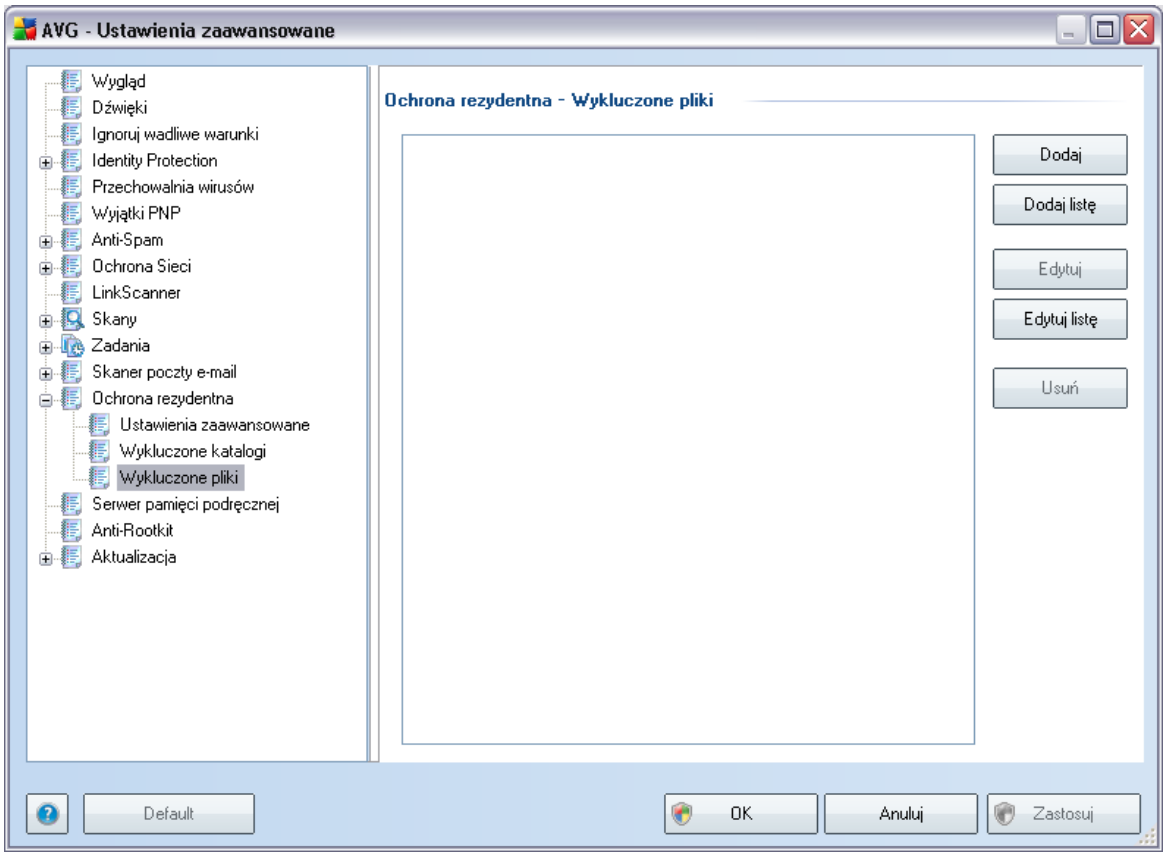
Jesli nie jest to koniecznie, zdecydowanie zalecamy nie wykluczac zadnych katalogów ze skanowania!

W biezacym oknie dostepne sa nastepujace przyciski kontrolne:

- ***Dodaj sciezke***— umozliwia okreslenie folderów, które maja zostac wykluczone ze skanowania, przez wybranie ich kolejno w drzewie obrazujacym strukture katalogów.
- ***Dodaj liste***— umozliwia podanie listy katalogów, które zostana wykluczone ze skanowania przez ***Ochrone Rezydentna***.
- ***Edytuj sciezke***— umozliwia edycje sciezki do wybranego folderu.

- ***Edytuj liste***— umozliwia edycje listy folderów.
- ***Usun sciezke***— umozliwia usuniecie z listy wybranego folderu.

10.13.3. Wykluczone pliki



Okno dialogowe ***Ochrona rezydentna — wykluczone pliki*** zachowuje sie w taki sam sposób co poprzednio opisane okno ***Ochrona rezydentna — wykluczone katalogi***, ale zamiast folderów mozna w nim okreslic pliki, które maja zostac wykluczone ze skanowania przez ***Ochrone rezydentna.***

Jesli nie jest to koniecznie, zdecydowanie zalecamy nie wylaczac zadnych katalogów ze skanowania!

W biezacym oknie dostepne sa nastepujace przyciski kontrolne:

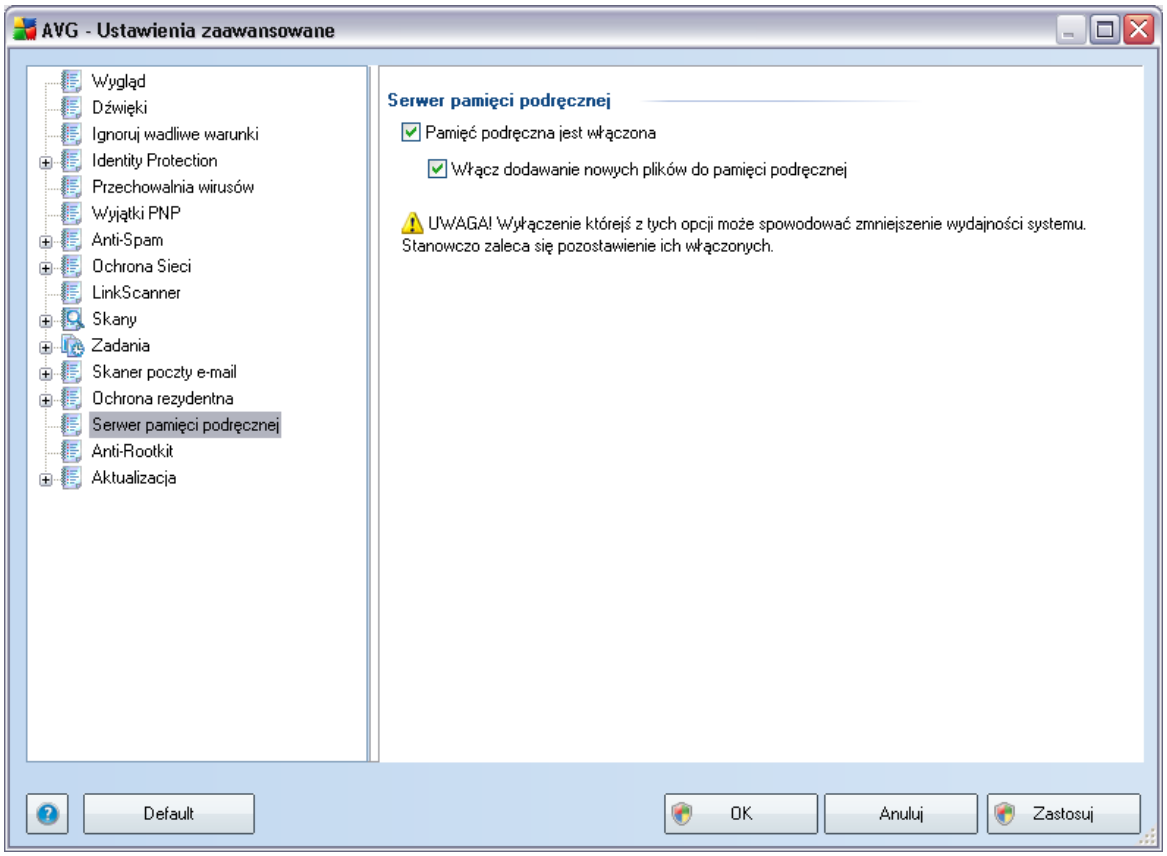
- ***Dodaj***— umozliwia okreslenie katalogów, które maja zostac wykluczone ze

skanowania, przez wybranie ich kolejno w drzewie nawigacyjnym dysku lokalnego.

- ***Dodaj liste***— umozliwia podanie listy plików, które zostana wylaczone ze skanowania przez skladnik ***Ochrona rezydentna***.
- ***Edytuj*** — umozliwia edycje okreslonej sciezki dostepu do wybranego pliku.
- ***Edytuj liste*** — umozliwia edycje listy plików.
- ***Usun***— umozliwia usuniecie z listy sciezki dostepu do wybranego pliku.

10.14. Serwer pamieci podrecznej

Funkcja ***Serwer pamieci podrecznej*** to tak naprawde proces majacy na celu przyspieszenie skanowania (*skanowania na zadanie, zaplanowanego skanowania calego komputera, skanowania skladnika Ochrona rezydentna*). Zbiera i zachowuje informacje na temat bezpiecznych plików (*takich jak pliki systemowe z podpisem cyfrowym itp.*) — pliki te sa wówczas uwazane za bezpieczne i pomijane podczas skanowania.



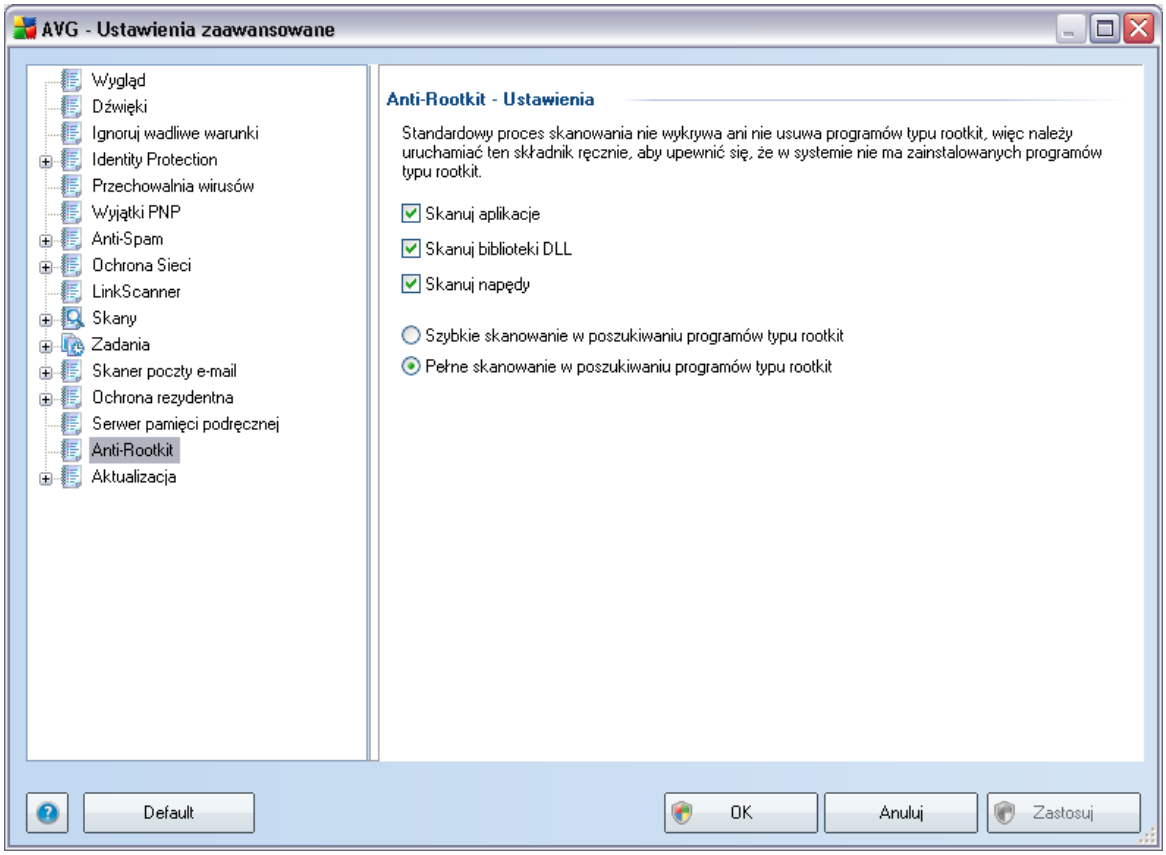
Okno dialogowe ustawien zawiera dwie opcje:

- ***Wlaczona pamiec podreczna*** (*opcja domyslnie wlaczona*) — usuniecie zaznaczenia tego pola powoduje wylaczenie funkcji ***Serwer pamieci podrecznej*** i opróznienie pamieci podrecznej. Nalezy pamietac, ze skanowanie moze spowolnic dzialanie komputera i zmniejszyc jego ogólna wydajnosc, poniewaz kazdy plik uzywany w danej chwili bedzie skanowany w poszukiwaniu wirusów i oprogramowania szpiegujacego.

- ***Wlacz dodawanie nowych plików do pamieci podrecznej*** (*opcja domyslnie wlaczona*) — usuniecie zaznaczenia tego pola umozliwia wylaczenie funkcji dodawania kolejnych plików do pamieci podrecznej. Wszystkie pliki zapisane w pamieci podrecznej sa w niej przechowywane dopóki funkcja nie zostanie zupelnie wylaczona lub do czasu kolejnej aktualizacji bazy danych wirusów.

10.15. Anti-Rootkit

W tym oknie dialogowym mozna edytowac konfiguracje skladnika ***Anti-Rootkit***:



Wszystkie funkcje skladnika ***Anti-Rootkit***dostepne w tym oknie dialogowym mozna takze edytowac bezposrednio w ***interfejsie skladnika Anti-Rootkit***.

Zaznacz odpowiednie pola wyboru, aby okreslic obiekty, które maja byc skanowane:

- ***Skanuj aplikacje***
- ***Skanuj biblioteki DLL***
- ***Skanuj sterowniki***

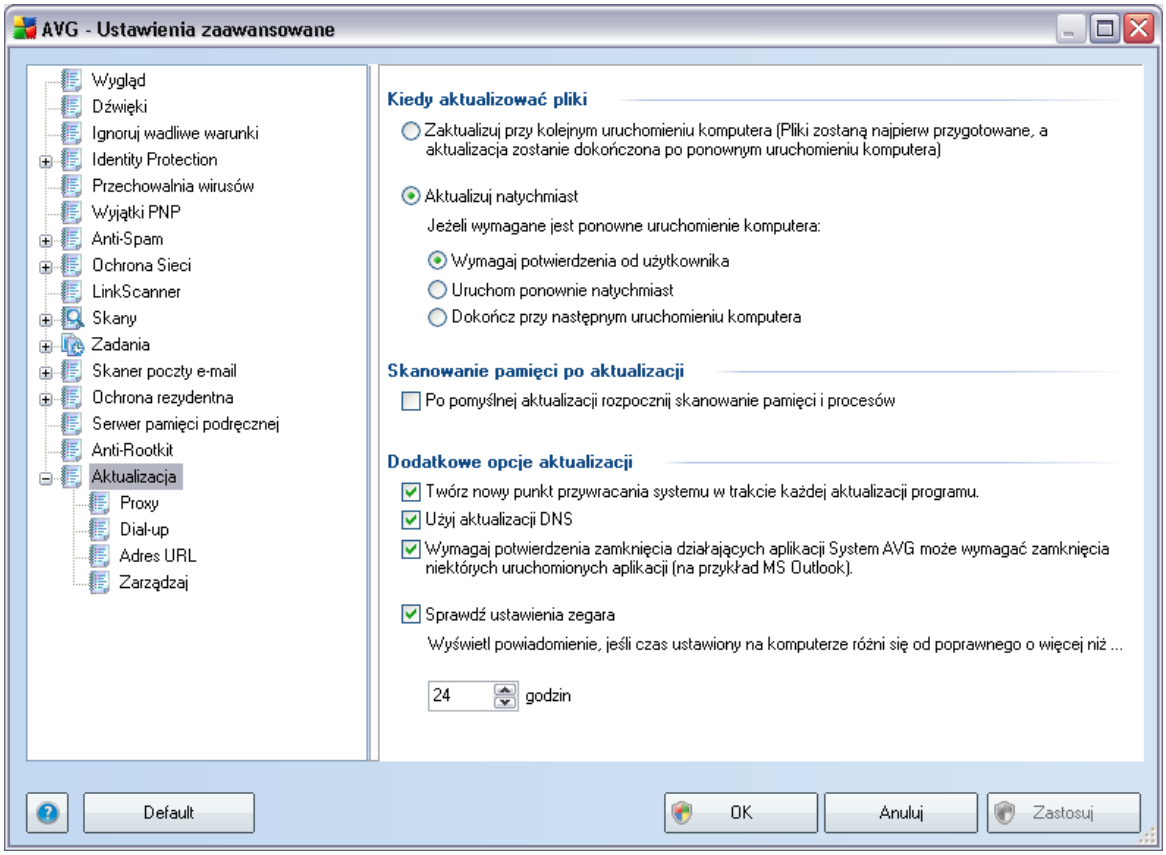
Nastepnie nalezy wybrac tryb skanowania w poszukiwaniu programów typu rootkit:

- ***Szybkie skanowanie w poszukiwaniu programów typu rootkit*** — skanuje

wszystkie uruchomione procesy, zaladowane sterowniki i folder systemowy (*zazwyczaj c:\Windows*)

- ***Pelne skanowanie w poszukiwaniu programów typu rootkit*** — skanuje wszystkie uruchomione procesy, zaladowane sterowniki i folder systemowy (*zazwyczaj c:\Windows*) oraz wszystkie dyski lokalne (*w tym dyski flash, ale bez uwzglednienia napedów dyskietek/plyt CD*)

10.16. Aktualizacja



Klikniecie pozycji ***Aktualizacja*** otwiera nowe okno dialogowe, w którym mozna okreslic ogólne parametry aktualizacji AVG:

Kiedy aktualizowac pliki

W tej sekcji mozna wybrac jedna z dwóch metod: zaplanowanie aktualizacji na

najblizszy restart komputera lub uruchomienie aktualizacji natychmiast. Domyslnie wybrana jest opcja natychmiastowa, poniewaz zapewnia ona maksymalny poziom bezpieczenstwa. Zaplanowanie aktualizacji na kolejne uruchomienie komputera zaleca sie tylko w przypadku, gdy komputer jest regularnie restartowany (co najmniej raz dziennie).

Przy pozostawienia konfiguracji domyslnej (natychmiastowe uruchomienie), mozna okreslic warunki ewentualnego restartu komputera:

- ***Wymagaj potwierdzenia od uzytkownika*** — przed zakonczeniem aktualizacji system zapyta uzytkownika o pozwolenie na restart komputera.

- ***Uruchom ponownie natychmiast*** — komputer zostanie automatycznie zrestartowany zaraz po zakonczeniu procesu aktualizacji — potwierdzenie ze strony uzytkownika nie jest wymagane.

- ***Dokoncz przy nastepnym uruchomieniu komputera*** — zakonczenie aktualizacji zostanie odlozone do najblizszego restartu komputera. Nalezy pamietac, ze opcja ta jest zalecana tylko w przypadku, gdy komputer jest regularnie uruchamiany (co najmniej raz dziennie).

Skanowanie pamieci po aktualizacji

Pole to nalezy zaznaczyc, jesli po kazdej pomyslnej aktualizacji system ma uruchamiac skanowanie pamieci. Pobrana aktualizacja mogla zawierac nowe definicje wirusów, które moga zostac zastosowane podczas takiego skanowania.

Dodatkowe opcje aktualizacji

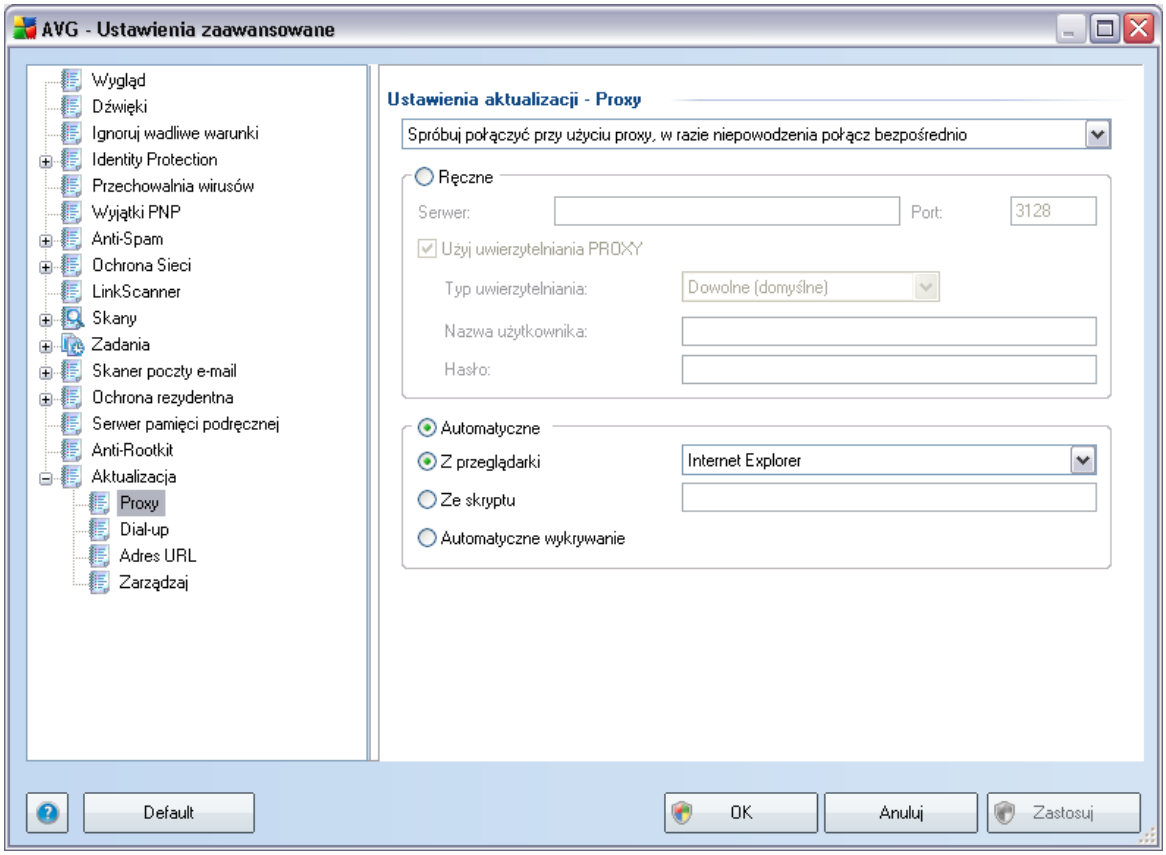
- ***Twórz nowy punkt przywracania systemu po kazdej aktualizacji programu*** — przed kazdym uruchomieniem aktualizacji systemu AVG tworzony bedzie punkt przywracania systemu. Przy jego uzyciu mozliwe bedzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Aby przywrócic system, nalezy wybrac kolejno: Start / Wszystkie programy / Akcesoria / Narzedzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoswiadczonym uzytkownikom! Aby korzystac z tej funkcji, pole wyboru musi pozostac zaznaczone.

- ***Uzyj aktualizacji DNS*** — zaznacz to pole, aby potwierdzic, ze chcesz uzywac metody wykrywania nowych aktualizacji, która ogranicza ilosc danych przesylanych miedzy serwerem aktualizacyjnym a klientem AVG.

- ***Wymagaj potwierdzenia zamkniecia dzialajacych aplikacji*** (*domyslnie wlaczona*) — daje pewnosc, ze zadne dzialajace aplikacje nie zostana zamkniete bez potwierdzenia ze strony uzytkownika, jesli do zakonczenia aktualizacji bedzie wymagane ponowne uruchomienie komputera.

- ***Sprawdz ustawienia zegara*** — zaznacz to pole jesli chcesz, aby program AVG wyswietlil powiadomienie, gdy róznica miedzy wlasciwym a lokalnym czasem komputera przekroczy okreslona wartosc.

10.16.1. Proxy



Serwer proxy jest samodzielnym serwerem lub uruchomiona na komputerze usluga gwarantujaca bezpieczniejsze polaczenie internetowe. Zgodnie z okreslonymi w Twojej sieci zasadami, polaczenie internetowe moze odbywac sie bezposrednio lub poprzez serwer proxy. Mozna takze zezwolic na korzystanie z obu opcji jednoczesnie. Dlatego tez w oknie ***Ustawienia aktualizacji — Proxy*** nalezy najpierw wybrac jedna z dostepnych opcji:

- ***Uzywaj proxy***
- ***Nie uzywaj serwera proxy*** — ustawienia domyslne
- ***Spróbuj polaczyc przy uzyciu proxy, a w razie niepowodzenia polacz bezposrednio***

W przypadku wybrania opcji uzycia serwera proxy nalezy podac dalsze informacje. Ustawienia serwera moga zostac skonfigurowane recznie lub automatycznie.

Konfiguracja reczna

W przypadku wybrania konfiguracji recznej (zaznaczenie *opcji* ***Recznie*** *aktywuje odpowiednia sekcje*) nalezy podac nastepujace informacje:

- ***Serwer*** — okresl adres IP lub nazwe serwera
- ***Port*** — okresl numer portu umozliwiajacego dostep do internetu (*domyslnie jest to port 3128, ale moze byc ustawiony inaczej; w przypadku watpliwosci nalezy skontaktowac sie z administratorem sieci*).

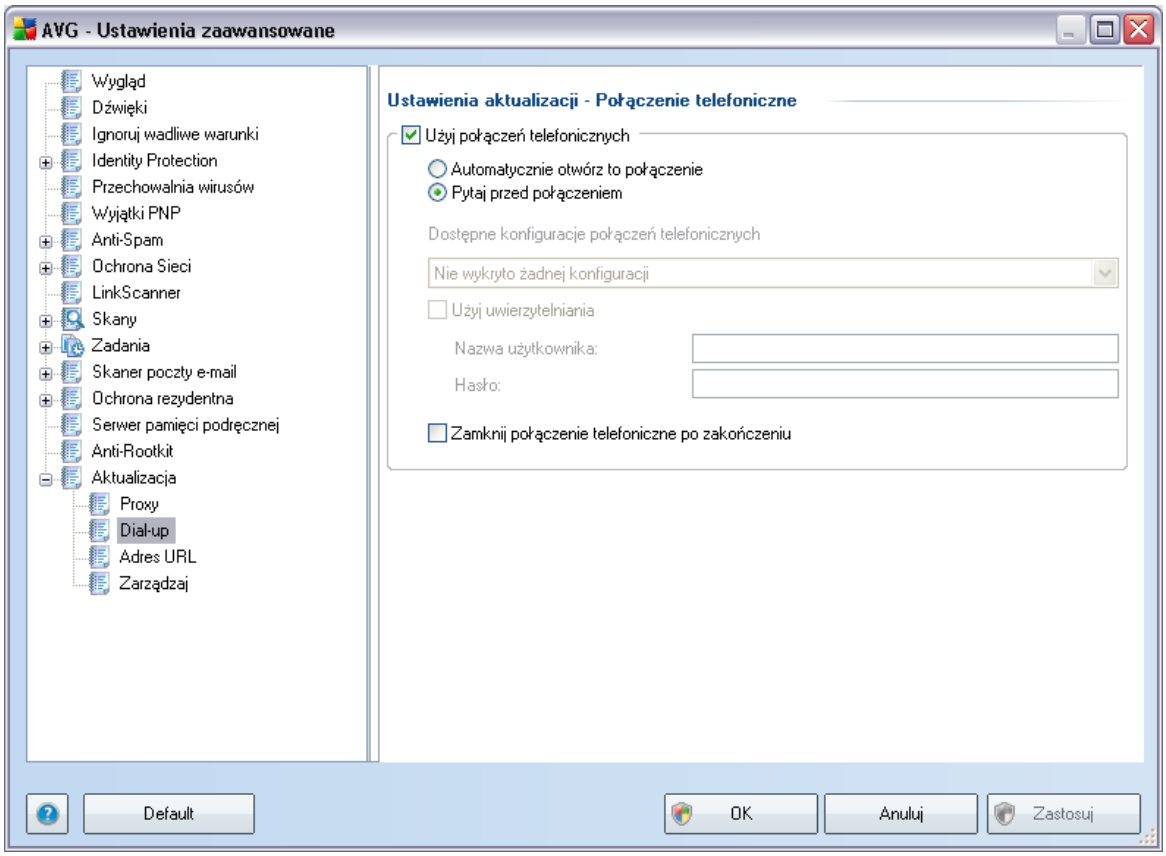
Zdarza sie, ze na serwerze proxy dla kazdego uzytkownika skonfigurowane sa odrebne reguly. Jesli serwer proxy jest skonfigurowany w ten sposób, nalezy zaznaczyc opcje ***Uzyj uwierzytelniania PROXY***, aby serwer weryfikowal nazwe uzytkownika i haslo przed nawiazaniem polaczenia.

Konfiguracja automatyczna

W przypadku wybrania konfiguracji automatycznej (*zaznaczenie opcji* ***Automatycznie*** *aktywuje odpowiedni obszar okna dialogowego*) nalezy wskazac, skad ma zostac pobrana konfiguracja proxy:

- ***Z przegladarki*** — konfiguracja zostanie odczytana z domyslnej przegladarki internetowej.
- ***Ze skryptu*** — konfiguracja zostanie odczytana z pobranego skryptu zawierajacego funkcje zwracajaca adres serwera proxy.
- ***Automatyczne wykrywanie*** — konfiguracja zostanie wykryta automatycznie bezposrednio na serwerze proxy.

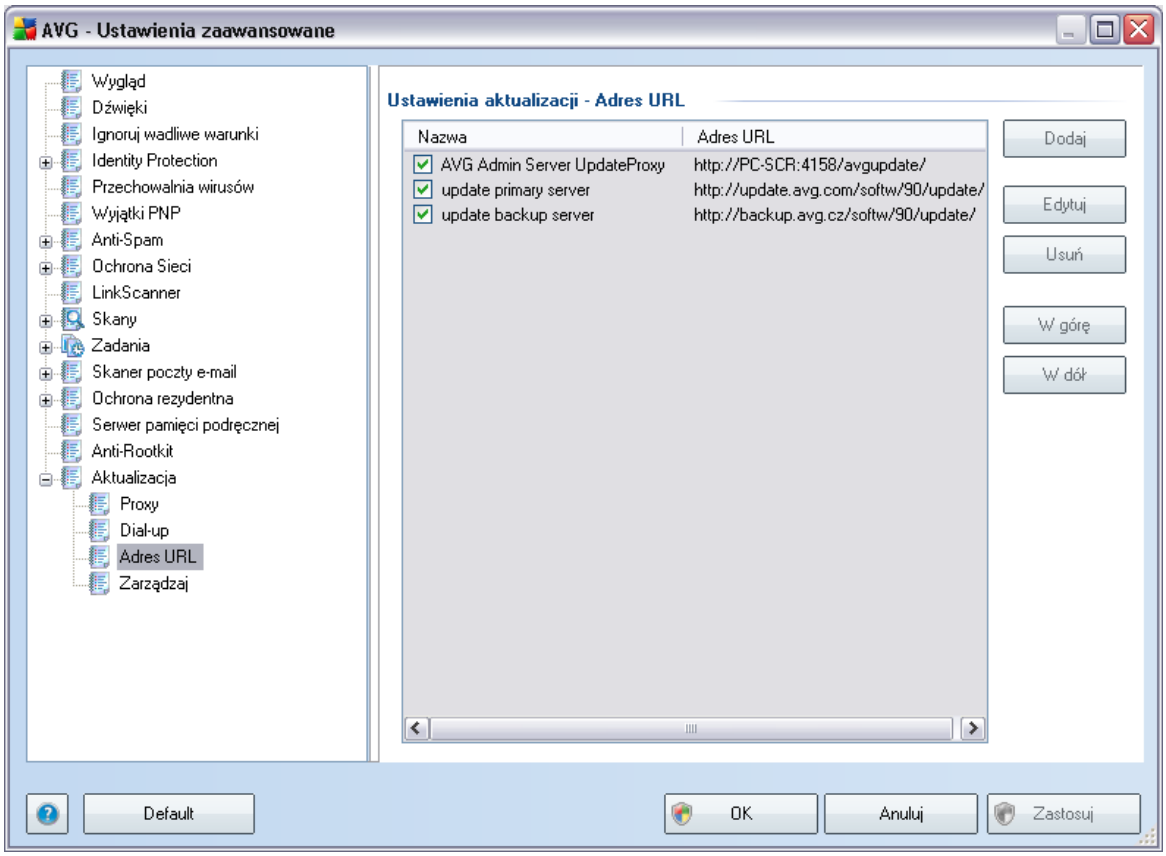
10.16.2. Polaczenie telefoniczne



Wszystkie opcjonalne parametry podawane w oknie ***Ustawienia aktualizacji — Polaczenie telefoniczne*** odnosza sie do polaczenia dial-up z internetem. Pola tego okna pozostaja nieaktywne az do zaznaczenia opcji ***Uzyj polaczen telefonicznych.***

Nalezy okreslic, czy polaczenie z internetem zostanie nawiazane automatycznie (***Automatycznie otwórz to polaczenie***), czy tez realizacje polaczenia nalezy zawsze potwierdzac recznie (***Pytaj przed polaczeniem***). W przypadku laczenia automatycznego nalezy takze okreslic, czy polaczenie ma byc zamykane natychmiast po zakonczeniu aktualizacji (***Zamknij polaczenie telefoniczne po zakonczeniu***).

10.16.3. URL

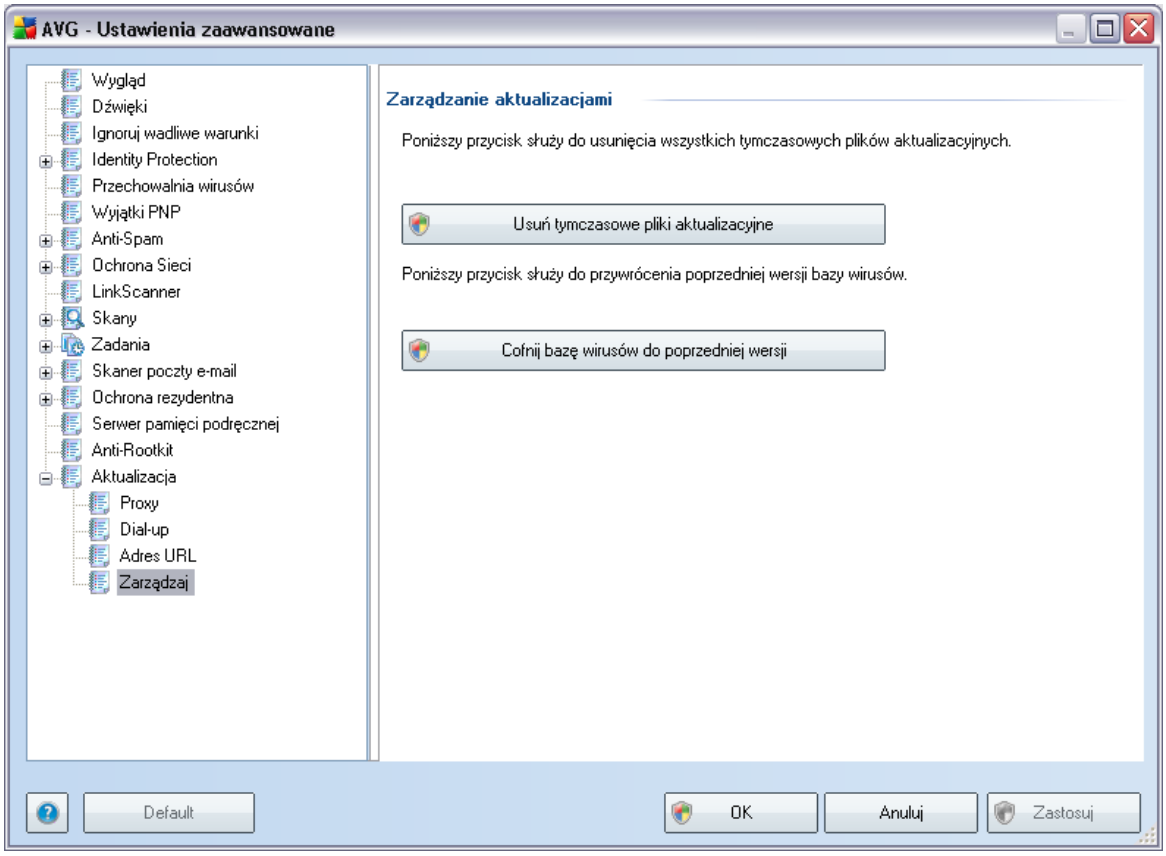


W oknie ***URL*** znajduje sie lista adresów internetowych, z których mozna pobierac pliki aktualizacyjne. Liste i jej elementy mozna modyfikowac za pomoca nastepujacych przycisków kontrolnych:

- ***Dodaj***— powoduje otwarcie okna dialogowego umozliwiajacego okreslenie nowego adresu URL, który zostanie dodany do listy.
- ***Edytuj*** — powoduje otwarcie okna dialogowego umozliwiajacego edycje parametrów wybranego adresu URL.
- ***Usun***— powoduje usuniecie wybranego adresu z listy.
- ***W góre***— przenosi wybrany adres URL o jedna pozycje w góre.
- ***W dól*** — przenosi wybrany adres URL o jedna pozycje w dól.

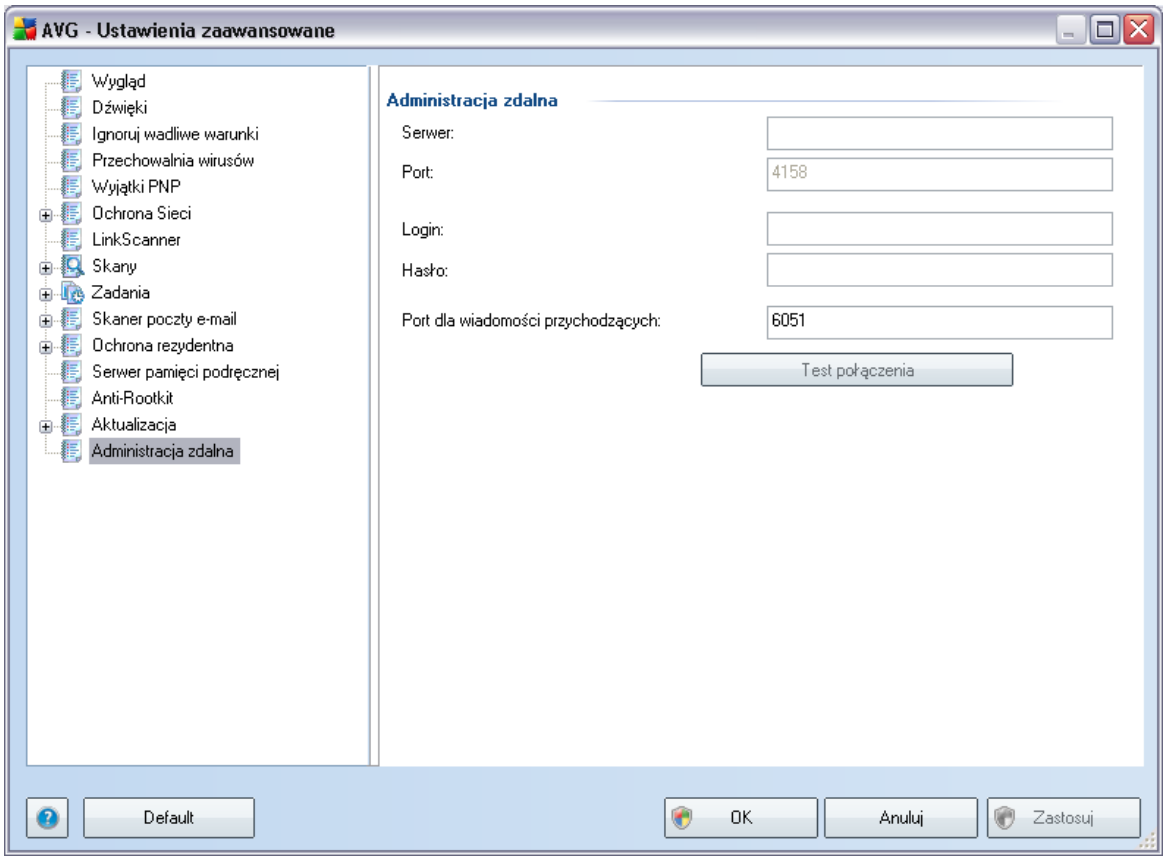
10.16.4. Zarzadzaj

Okno dialogowe ***Zarzadzaj*** zawiera dwa przyciski:



- ***Usun tymczasowe pliki aktualizacyjne*** — pozwala usunac z dysku twardego wszystkie zbedne pliki aktualizacyjne (*sa one domyslnie przechowywane przez 30 dni*)
- ***Cofnij baze wirusów do poprzedniej wersji*** — pozwala usunac z dysku twardego ostatnia wersje bazy wirusów i przywrócic ja do poprzedniego stanu (*nowa baza bedzie czescia najblizszej aktualizacji*)

10.17. Administracja zdalna



Ustawienia ***Administracji zdalnej*** okreslaja sposób laczenia sie stacji roboczej AVG z systemem administracji zdalnej. Jesli dana stacja ma laczyc sie ze zdalnym serwerem administracyjnym, nalezy okreslic nastepujace parametry:

- ***Serwer*** — nazwa (lub adres IP) serwera, na którym zainstalowano oprogramowanie AVG Admin Server.
- ***Port*** — numer portu, przez który klient AVG komunikuje sie z serwerem AVG Admin Server (*za domyslny uwazany jest port 4158 — jesli ma byc uzywany, nie trzeba go wprowadzac*).
- ***Nazwa logowania*** — jesli uzywana jest opcja bezpiecznej komunikacji miedzy klientem AVG i oprogramowaniem AVG Admin Server, nalezy podac nazwe uzytkownika ...

- ***Haslo*** — wymagane, jesli podano login.
- ***Port dla wiadomosci przychodzacych*** — numer portu, na którym klient AVG odbiera wiadomosci od serwera AVG Admin Server.

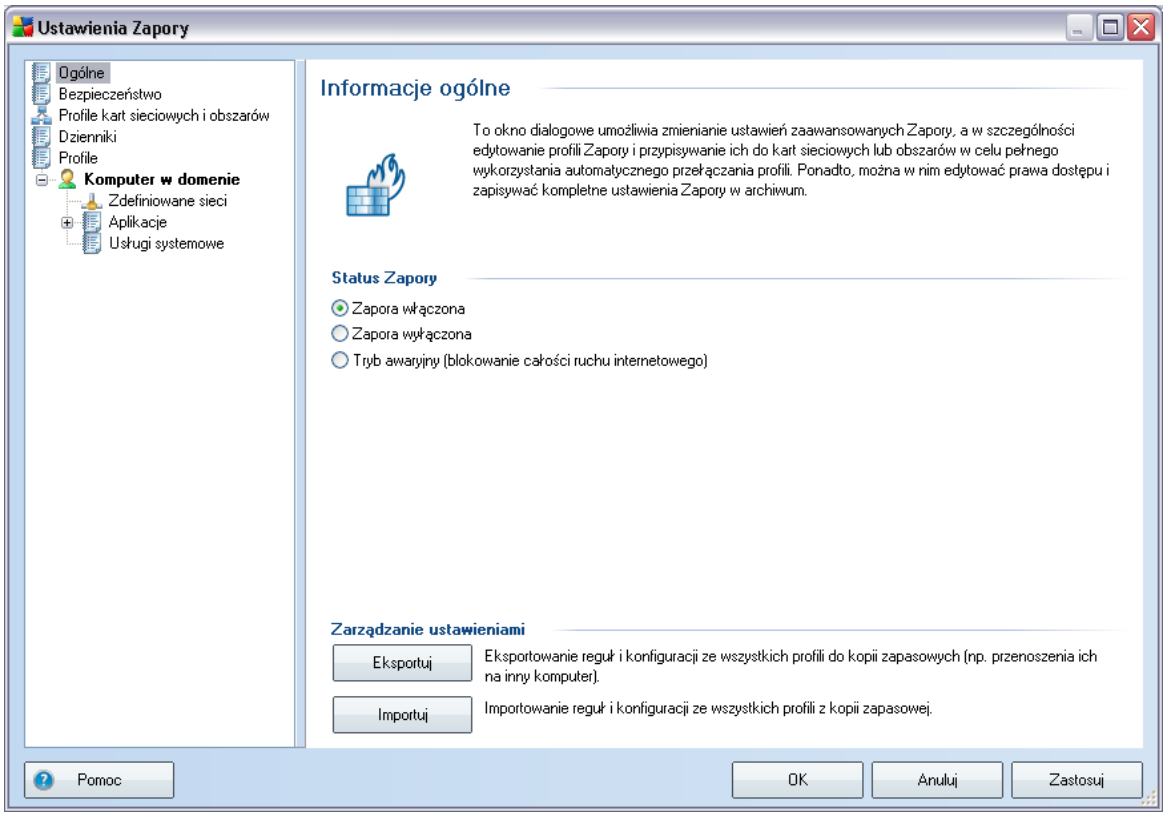
Przycisk·***Testuj polaczenie*** pozwala sprawdzic, czy wszystkie powyzsze dane sa prawidlowe i zapewnia pomyslne polaczenie z baza danych DataCenter.

Uwaga: *Szczegółowy opis funkcji administracji zdalnej zawiera dokumentacja programu AVG Network Edition.*

11. Ustawienia Zapory

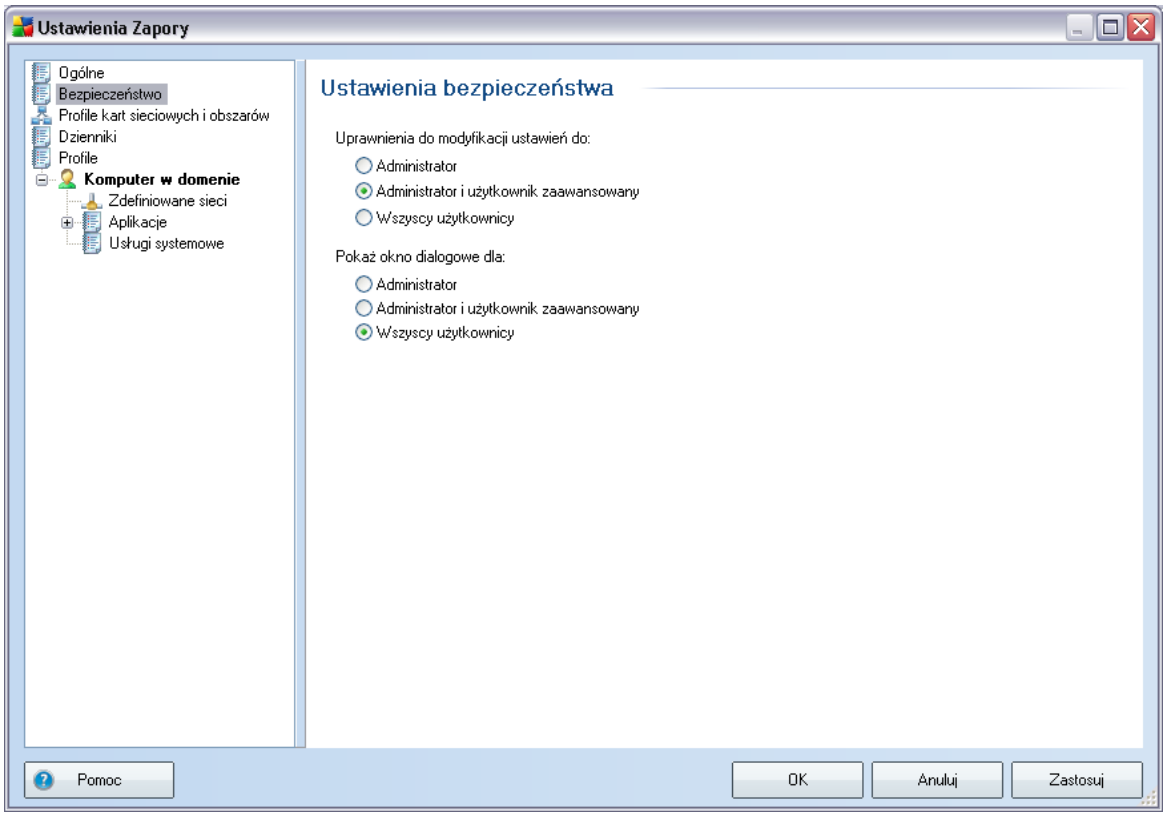
Konfiguracja ***Zapory*** otwierana jest w nowym oknie, gdzie w kilku sekcjach mozna okreslic nawet najbardziej zaawansowane parametry tego skladnika. ***Jednakze edycja zaawansowanej konfiguracji powinna byc dokonywana jedynie przez ekspertów i doswiadczonych uzytkowników.***

11.1. Ogólne



W oknie ***Informacje ogólne*** mozna***wyeksportowac*** / ***zaimportowac******konfiguracje*** Zapory, tzn. wyeksportowac zdefiniowane reguly i ustawienia ***Zapory*** do pliku kopii zapasowej lub tez zaimportowac do programu caly plik tego typu.

11.2. Bezpieczenstwo



W oknie ***Ustawienia bezpieczenstwa*** mozna zdefiniowac ogólne reguly zachowania ***Zapory*** niezaleznie od wybranego profilu:

- ***Pozwól modyfikowac ustawienia:*** — nalezy okreslic, kto moze zmieniac konfiguracje skladnika ***Zapora***.
- ***Pokaz okno dialogowe:*** — nalezy okreslic, komu mozna wyswietlac okna potwierdzen Zapory (*okna dialogowe z prosba o podjecie decyzji w sytuacji nieobjetej zadna regula* ***Zapory***).

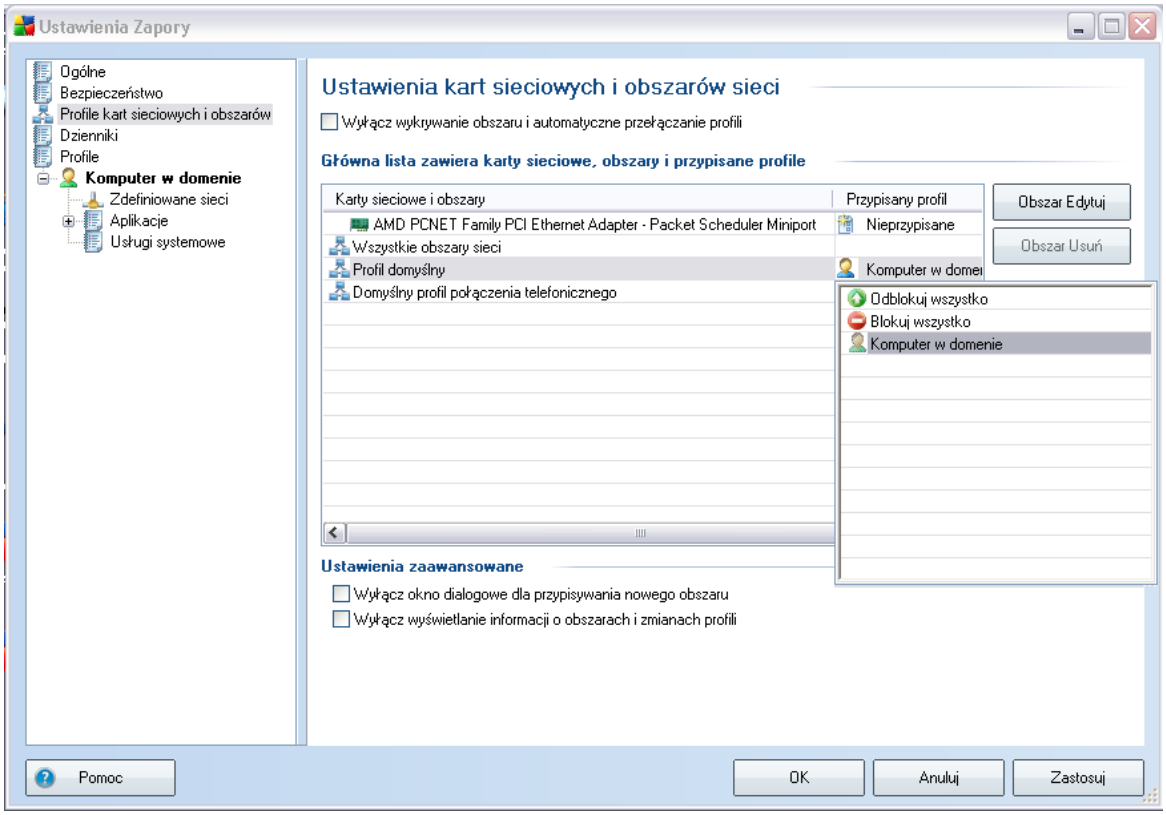
W obu wypadkach mozna przypisac konkretne uprawnienie jednej z nastepujacych grup uzytkowników:

- ***Administratorom*** — posiadaja oni calkowita kontrole nad komputerem i mozliwosc przydzielania uzytkowników do grup z okreslonymi uprawnieniami.

- ***Administratorom i uzytkownikom uprzywilejowanym*** — administrator moze przydzielic dowolnego uzytkownika do uprzywilejowanej grupy (*Uzytkownicy uprzywilejowani*) oraz okreslic uprawnienia jej czlonków.

- ***Wszyscy uzytkownicy*** — pozostali uzytkownicy (nie przydzieleni do zadnej konkretnej grupy).

11.3. Profile kart sieciowych i obszarów



W oknie ***Ustawienia kart sieciowych i obszarów*** mozna edytowac ustawienia zwiazane z przypisywaniem zdefiniowanych profili do konkretnych kart i sieci:

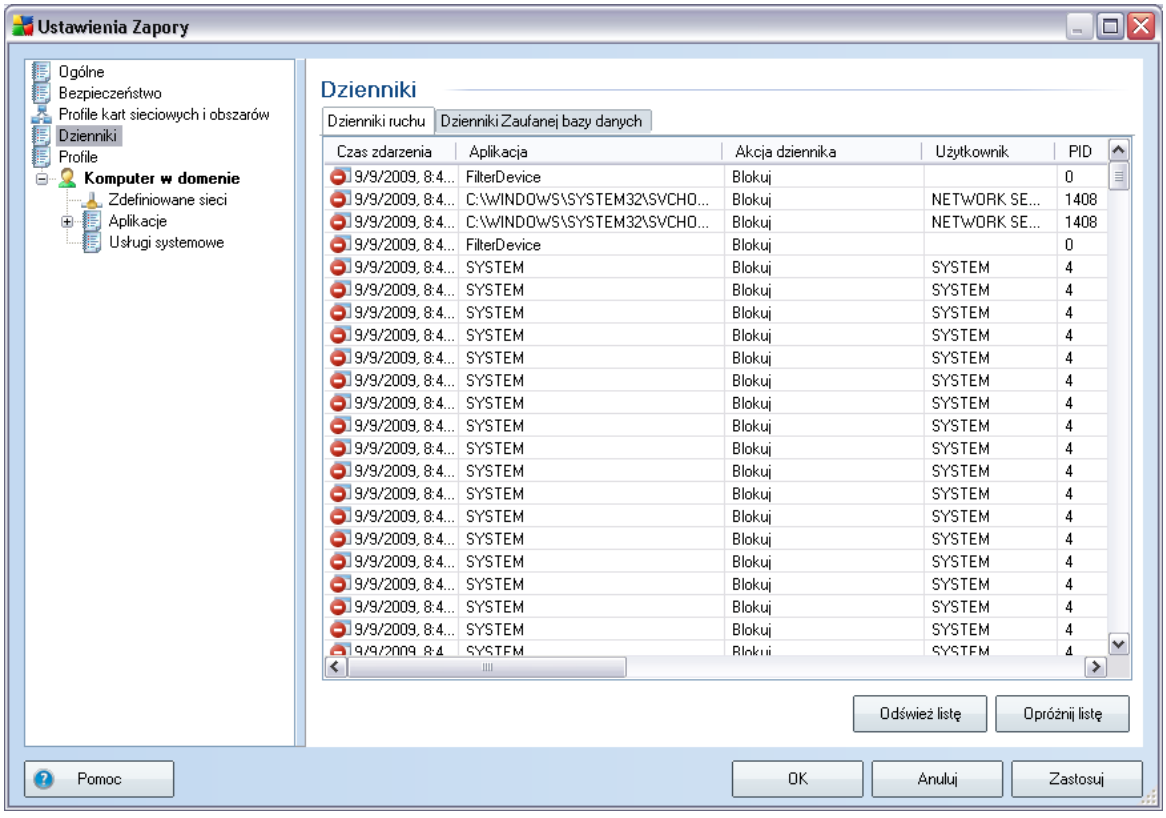
- ***Wylacz wykrywanie obszaru i automatyczne przelaczanie profili*** — do kazdego typu interfejsu sieciowego mozna przypisac jeden ze zdefiniowanych profili (odpowiednio dla poszczególnych obszarów). Jesli nie chcesz tworzyc wlasnych, konkretnych profili, uzywany bedzie jeden wspólny profil zdefiniowany na podstawie typu komputera i sposobu polaczenia z internetem okreslonych podczas ***procesu instalacji***. Jesli jednak postanowisz zróznicowac

profile i przypisac je do konkretnych kart i obszarów, a nastepnie — z jakiegos powodu — zechcesz tymczasowo zmienic to przypisanie, zaznacz opcje ***Wylacz wykrywanie obszaru i automatyczne przelaczanie profili***.

- ***Lista kart sieciowych, obszarów i przypisanych profili*** — na tej liscie mozna znalezc przeglad wykrytych kart i obszarów. Do kazdego z nich mozna przypisac okreslony profil z menu zdefiniowanych profili. Aby otworzyc to menu, kliknij odpowiedni element na liscie kart sieciowych i wybierz profil.

- ***Ustawienia zaawansowane*** — zaznaczenie odpowiednich opcji spowoduje wylaczenie komunikatów informacyjnych.

11.4. Dzienniki



Okno dialogowe ***Dzienniki*** umozliwia przeglad listy wszystkich dzialan podjetych przez ***Zapore*** oraz zwiazanych z nia wydarzen wraz ze szczegółowym opisem odpowiednich parametrów (*godzina zdarzenia, nazwa aplikacji, odpowiednia akcja dziennika, nazwa uzytkownika, PID, kierunek komunikacji, typ protokolu, numery zdalnych i lokalnych*

portów itp.) na dwóch nastepujacych kartach:

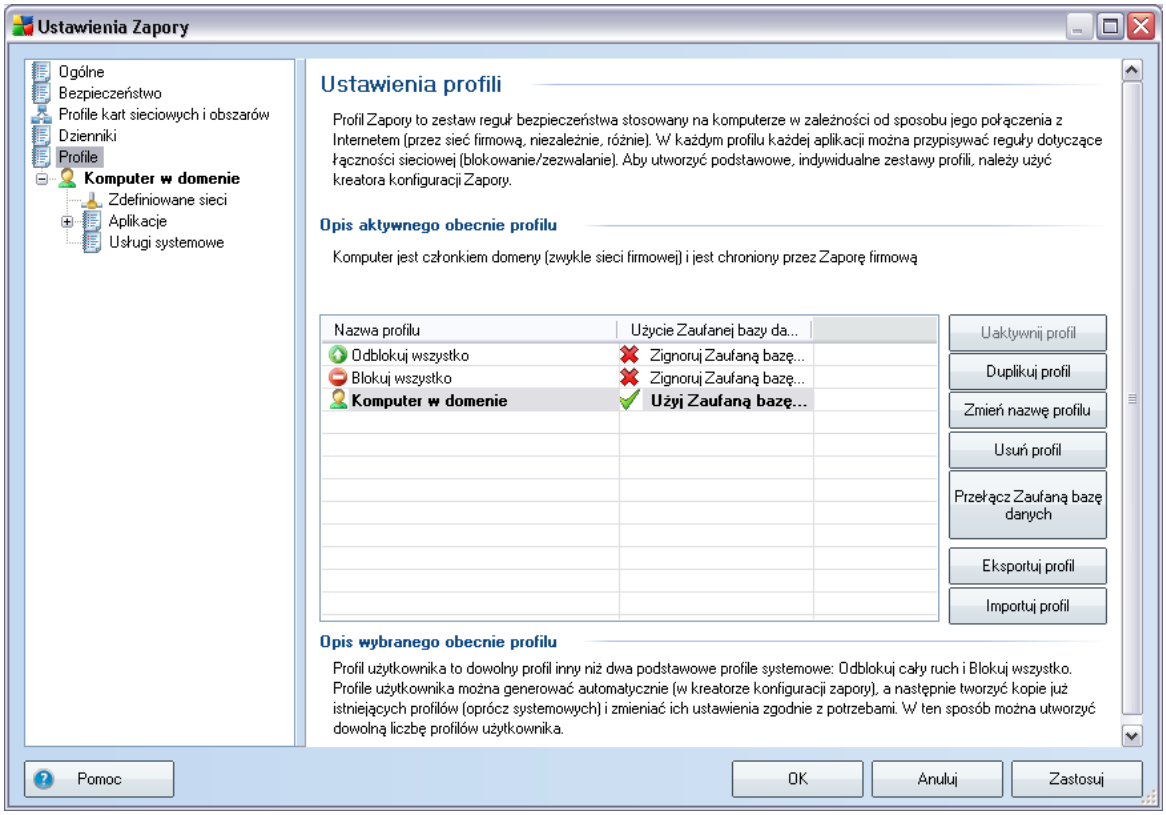
- ***Dzienniki sieciowe*** — zawiera informacje o aktywnosci wszystkich aplikacji, które próbowaly polaczyc sie z siecia.
- ***Dzienniki Trusted Database*** — *Trusted Database* to wewnetrzne baza danych systemu AVG zbierajaca informacje na temat certyfikowanych i zaufanych aplikacji, dla których komunikacja w trybie online jest zawsze dozwolona. Za pierwszym razem, kiedy nowa aplikacja próbuje sie polaczyc z siecia (*np. gdy jeszcze nie zostala utworzona regula zapory dla tej aplikacji*), konieczna jest decyzja, czy zezwolic na komunikacje sieciowa. Najpierw system AVG przeszukuje baze *Trusted Database*. Jesli aplikacja znajduje sie na liscie, dostep do sieci zostanie jej automatycznie umozliwiony. Dopiero wtedy, gdy w naszej bazie danych nie ma zadnych informacji na temat tej aplikacji, zostanie wyswietlone oddzielne okno dialogowe z pytaniem, czy dostep do sieci powinien zostac odblokowany.

Przyciski kontrolne

- ***Pomoc*** — otwiera okno dialogowe z powiazanymi tematami pomocy.
- ***Odswiez liste*** — wszystkie zarejestrowane parametry mozna uporzadkowac wedlug wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) — wystarczy kliknac odpowiedni naglówek kolumny. Uzyj przycisku ***Odswiez liste***, aby zaktualizowac wyswietlane informacje.
- ***Opróznij liste*** — pozwala usunac wszystkie wpisy.

11.5. Profile

W oknie ***Ustawienia profili*** mozna znalezc liste dostepnych profili.



Wszystkie profile (prócz systemowych) moga byc edytowane w tym oknie dialogowym przy uzyciu nastepujacych przycisków kontrolnych:

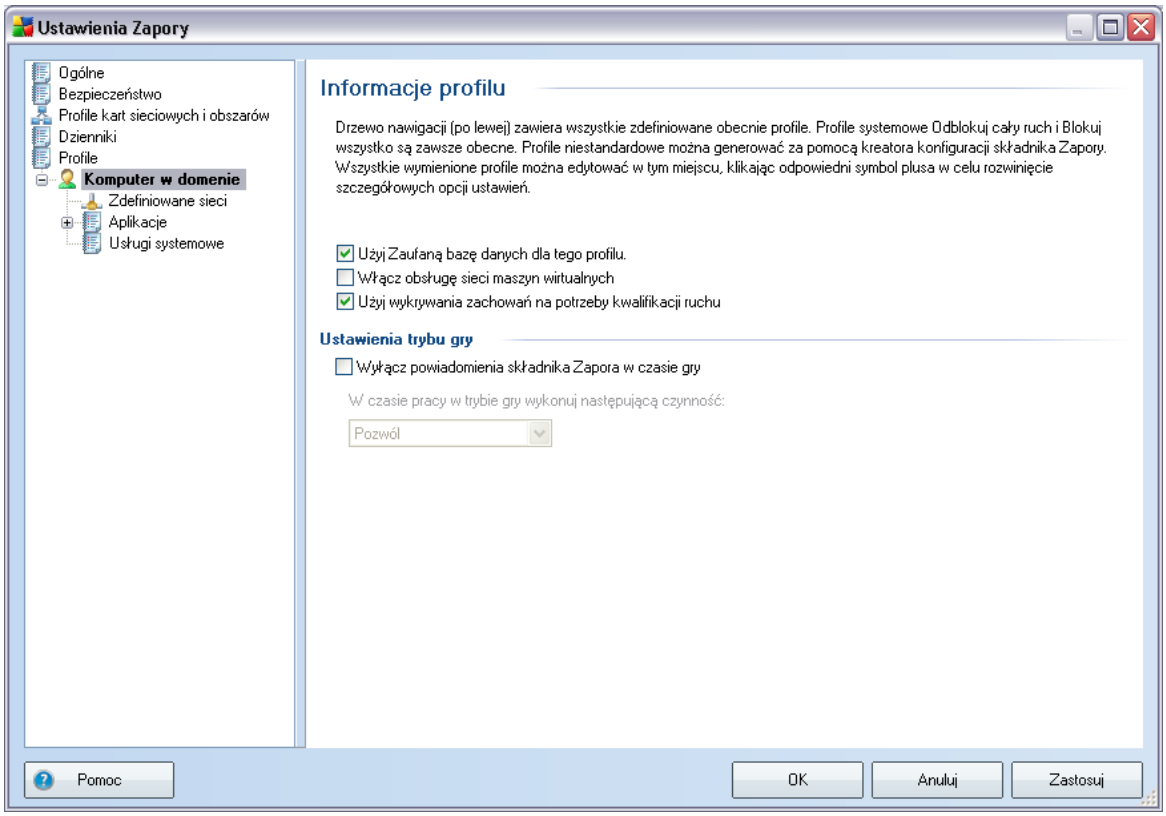
- ***Uaktywnij profil*** — przycisk ten ustawia wybrany profil jako aktywny, co oznacza, ze konfiguracja wybranego profilu bedzie uzywana przez ***Zapore*** do sterowania ruchem w sieci.
- ***Duplikuj profil*** — tworzy kopie wybranego profilu. Później bedzie mozna przeprowadzic edycje i zmienic nazwe kopii, aby utworzyc nowy profil na podstawie istniejacego.
- ***Zmien nazwe profilu*** — umozliwia zdefiniowanie nowej nazwy dla wybranego profilu.

- ***Usun profil*** — usuwa wybrany profil z listy.
- ***Wlacz/wylacz Trusted Database*** — umozliwia danemu profilowi korzystanie z bazy *Trusted Database* (*Trusted Database to wewnetrzne baza danych AVG, zbierajaca informacje na temat certyfikowanych i zaufanych aplikacji, którym bez obaw mozna zezwolic na polaczenie z internetem.*)
- ***Eksportuj profil*** — zapisuje konfiguracje wybranego profilu w pliku, którego bedzie mozna uzyc w przyszlosci.
- ***Importuj profil*** — konfiguruje ustawienia wybranego profilu na podstawie danych zapisanych w pliku konfiguracyjnym.
- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.

W dolnej czesci okna dialogowego mozna znalezc opis profilu wybranego z powyzszej listy.

Menu nawigacyjne znajdujace sie po lewej stronie zmienia odzwierciedla liste profili wyswietlona w oknie ***Profile***. Kazdy zdefiniowany profil tworzy jedna galaz nalezaca do grupy ***Profile***. Konkretne profile mozna edytowac w kolejnych oknach dialogowych (*identycznych dla wszystkich profili*):

11.5.1. Informacje o profilu



Okno dialogowe ***Informacje o profilu*** to pierwsze z okien sekcji, w której mozna edytowac konfiguracje wybranego profilu w osobnych oknach dialogowych dotyczacych jego okreslonych parametrów.

- ***Dla tego profilu uzyj bazy Trusted Database*** (*opcja domyslnie wlaczona*) — te opcje nalezy zaznaczyc, aby aktywowac baze *Trusted Database* (*czyli wewnetrzna baze danych systemu AVG zbierajaca informacje o zaufanych i certyfikowanych aplikacjach korzystajacych z komunikacji online. Jesli dla danej aplikacji nie ma jeszcze okreslonych regul, konieczne jest sprawdzenie, czy aplikacja moze uzyskac dostep do sieci. System AVG przeszukuje najpierw baze Trusted Database i jezeli dana aplikacja jest na liscie, zostanie uznana za bezpieczna i bedzie jej umozliwiona komunikacja poprzez siec. W innym przypadku zostanie wyswietlone zapytanie, czy komunikacja przez siec dla danej aplikacji powinna zostac odblokowana*) dla okreslonego profilu.

- ***Wlacz obsluge sieci maszyn wirtualnych*** (*domyslnie wylaczone*) — zaznaczenie tej pozycji pozwala maszynom wirtualnym WMware laczyc sie

bezposrednio z siecia.

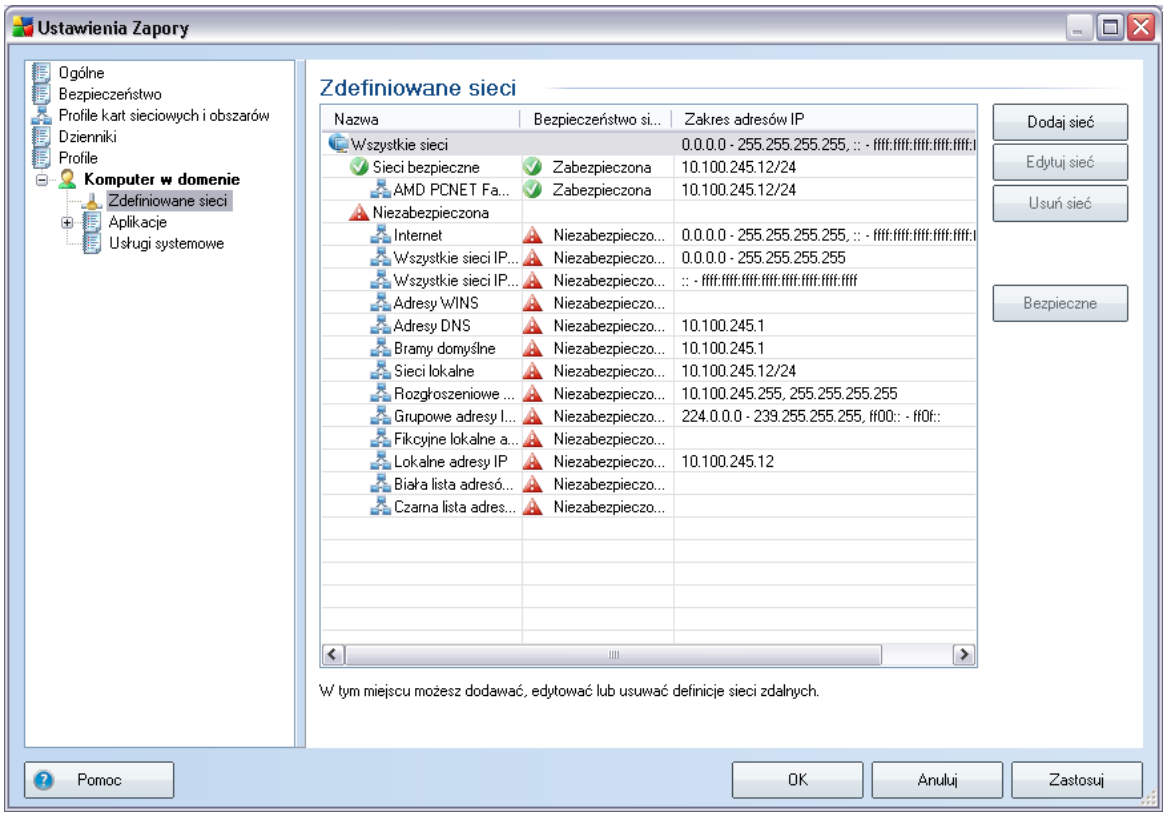
- ***Uzyj analizy behawioralnej przy ocenie ruchu sieciowego*** (*domyslnie wlaczone*) — zaznaczenie tej opcji pozwala ***Zaporze*** na korzystanie z funkcji skladnika ***Identity Protection*** podczas oceniania aplikacji — skladnik Identity Protection*** umozliwia stwierdzenie, czy aplikacja wykazuje jakiekolwiek podejrzane zachowania, czy tez mozna jej zaufac i zezwolic na komunikacje online.

Ustawienia trybu gry

W sekcji ***Ustawienia trybu gry*** mozna okreslic czy komunikaty ***Zapory*** maja byc wyswietlane nawet podczas dzialania aplikacji pelnoekranowych (*sa to na ogól gry, ale dotyczy to równiez wszelkich innych aplikacji, takich jak np. prezentacje PPT*). Komunikaty informacyjne moga byc w pewnym stopniu irytujace.

Jesli zostanie zaznaczona opcja ***Wylacz powiadomienia Zapory w czasie gry***, z menu rozwijanego znajdujacego sie ponizej nalezy wybrac akcje, która ma podjac Zapora, gdy nowa aplikacja spróbuje nawiazac polaczenie z siecia (*aby nie wyswietlac komunikatu z pytaniem o dostep*). Wszystkie takie aplikacje moga byc odblokowane lub zablokowane.

11.5.2. Zdefiniowane sieci

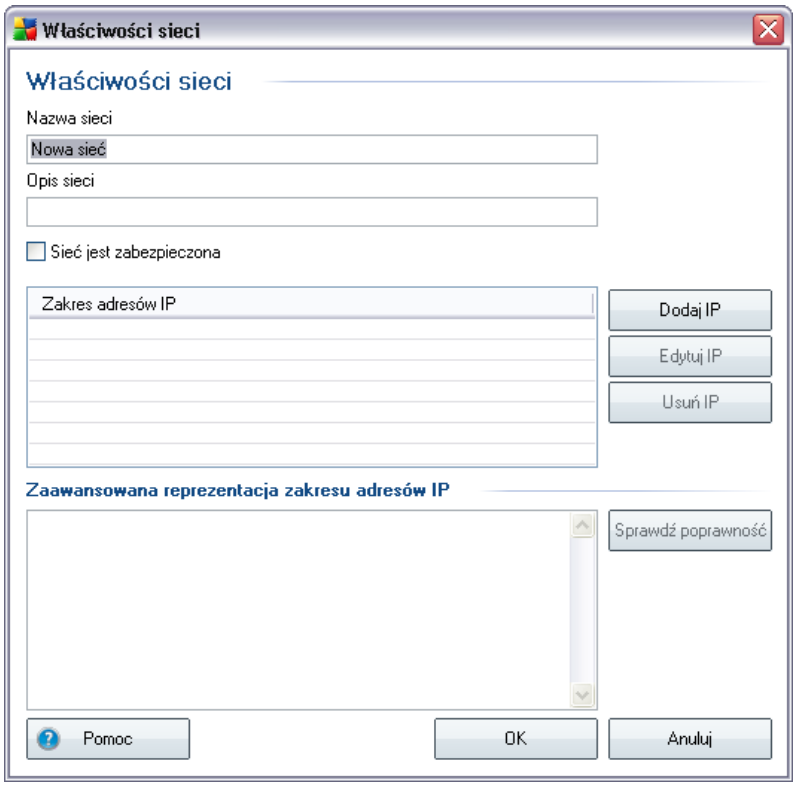


Okno dialogowe ***Zdefiniowane sieci*** zawiera liste wszystkich sieci, z którymi polaczony jest Twój komputer. Dla kazdej wykrytej sieci wyswietlane sa nastepujace informacje:

- ***Sieci*** — lista nazw wszystkich sieci, do których podlaczony jest komputer.
- ***Bezpieczenstwo sieci*** — domyslnie wszystkie sieci uwazane sa za niebezpieczne i tylko w przypadku pewnosci, ze dana siec (i odpowiednia karta sieciowa) jest godna zaufania, mozna przypisac jej takie ustawienie (*w tym celu nalezy kliknac na liscie pozycje odpowiadajaca tej sieci i wybrac z menu kontekstowego opcje Bezpieczna*). Wszystkie bezpieczne karty sieciowe i odpowiadajace im sieci zostana wziete pod uwage przy przyznawaniu dostepu aplikacjom, dla których zastosowano regule Odblokuj bezpieczne
- ***Zakres adresów IP*** — kazda siec zostanie automatycznie wykryta i okreslona w formie zakresu adresów IP

Przyciski kontrolne

- ***Dodaj siec*** — otwiera okno dialogowe ***Wlasciwosci sieci*** , w którym mozna edytowac parametry nowo zdefiniowanej sieci:



Mozliwe jest w nim okreslenie ***nazwy sieci***, wprowadzenie ***opisu sieci*** i zdecydowanie, czy oznaczyc ja jako bezpieczna. Adres sieci moze byc okreslony recznie w odrebnym oknie dialogowym otwieranym za pomoca przycisku ***Dodaj adres IP*** (mozna tez uzyc przycisków ***Edytuj adres IP***/ ***Usun adres IP***). W tym oknie mozna okreslic siec, podajac zakres adresów IP lub maske.

W wypadku duzej liczby sieci, które maja byc zdefiniowane jako czesci nowo utworzonej sieci, mozna uzyc opcji ***Zaawansowana reprezentacja zakresu adresów IP***: nalezy w tym celu wpisac liste wszystkich sieci do odpowiedniego pola tekstowego (*obslugiwane sa wszystkie standardowe formaty*) i kliknac przycisk ***Sprawdz***, aby upewnic sie, ze format zostal rozpoznany. Nastepnie nalezy kliknac przycisk ***OK***, aby potwierdzic i

zapisac dane.

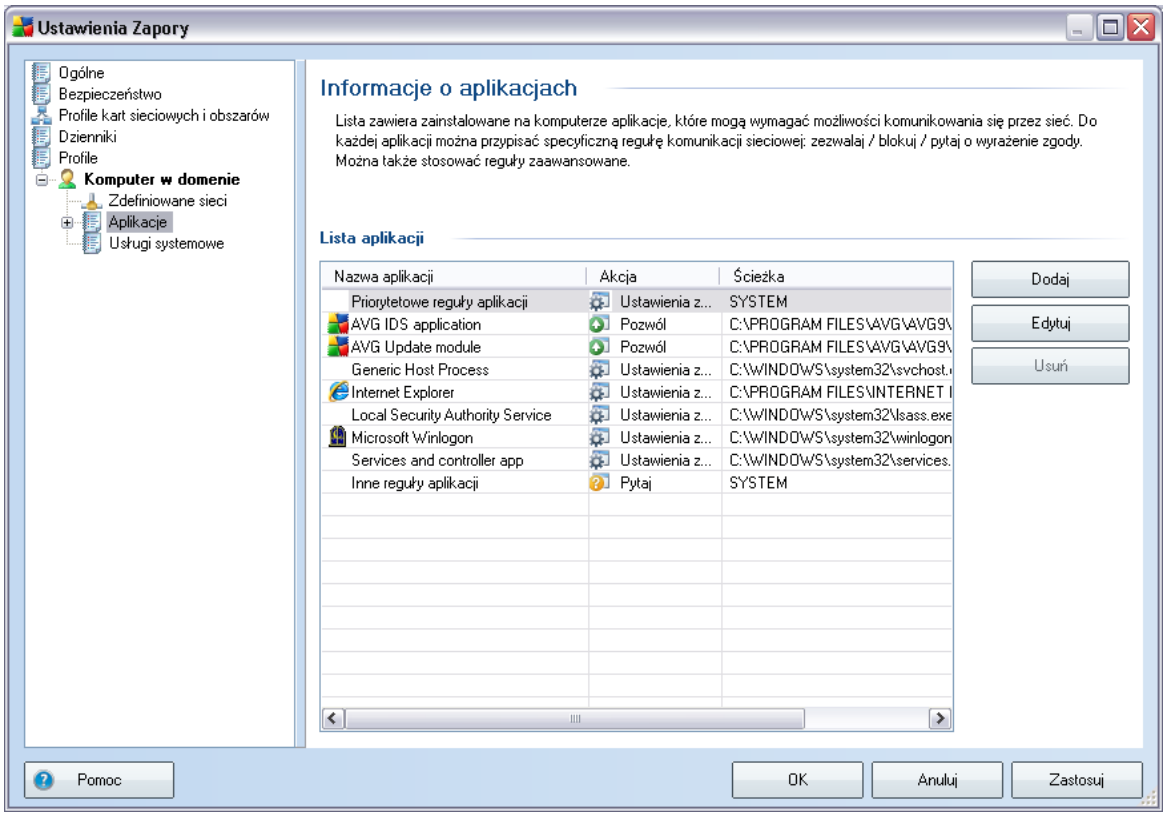
- ***Edytuj siec*** — powoduje otwarcie okna dialogowego ***Wlasciwosci sieci*** (*patrz wyzej*). w którym mozna edytowac parametry zdefiniowanej sieci (*okno to jest identyczne jak podczas dodawania nowej sieci. Zobacz opis w poprzednim akapicie*).

- ***Usun siec*** — usuwa zapis dotyczacy wybranej sieci z listy sieci.

- ***Oznacz jako bezpieczna*** — domyslnie wszystkie sieci uwazane sa za niebezpieczne i tylko w przypadku pewnosci, ze dana siec jest godna zaufania, mozna przypisac jej takie ustawienie (*i na odwrót: gdy siec zostala oznaczona jako bezpieczna, tekst przycisku zostaje zmieniony na "Oznacz jako niezabezpieczona"*).

- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.

11.5.3. Aplikacje



W oknie dialogowym ***Informacje o aplikacjach*** wyswietlana jest lista wszystkich zainstalowanych aplikacji, które komunikuja sie z siecia, oraz ikony reprezentujace przypisane do nich akcje:

- Odblokuj komunikacje dla wszystkich sieci
- Odblokuj komunikacje tylko dla sieci zdefiniowanych jako bezpieczne
- Zablokuj komunikacje
- Wyswietlaj zapytanie w oknie dialogowym (*uzytkownik bedzie mógl w okreslonym momencie podjac decyzje o odblokowaniu lub zablokowaniu komunikacji*)
- Zdefiniowano ustawienia zaawansowane

Aplikacje wyswietlane na liscie zostaly wykryte na komputerze (*i przypisano im odpowiednie akcje*) podczas wyszukiwania przeprowadzanego przez ***kreatora konfiguracji skladnika Firewall*** albo pózniej (w przypadku nieznanej lub nowo zainstalowanej aplikacji).

Uwaga: Nalezy pamietac, ze tylko aplikacje juz zainstalowane moga zostac wykryte, wiec dla zainstalowanej pózniej nowej aplikacji konieczne bedzie zdefiniowanie regul. Domyslnie, kiedy nowa aplikacja próbuje polaczyc sie z siecia po raz pierwszy, Zapora automatycznie utworzy dla niej regule na podstawie bazy Trusted Database lub zapyta, czy komunikacja ma zostac odblokowana. W tym drugim przypadku mozliwe bedzie zapisanie odpowiedzi jako stalej reguly (która wówczas zostanie dodana do listy w tym oknie dialogowym).

Mozna tez zdefiniowac reguly dla nowej aplikacji natychmiast, uzywajac w tym oknie dialogowym przycisku ***Dodaj*** i podajac szczegóły aplikacji.

Poza aplikacjami na liscie wyswietlane sa jeszcze dwie pozycje specjalne:

- ***Priorytetowe reguly aplikacji*** (*u góry listy*) sa wybierane jako pierwsze i stosowane zawsze przed regulami okreslonej aplikacji.
- ***Inne reguly aplikacji*** (*na dole listy*) sluza jako „rezerwa”, gdy nie sa stosowane zadne okreslone reguly, np. dla nieznanych lub niezdefiniowanych aplikacji.

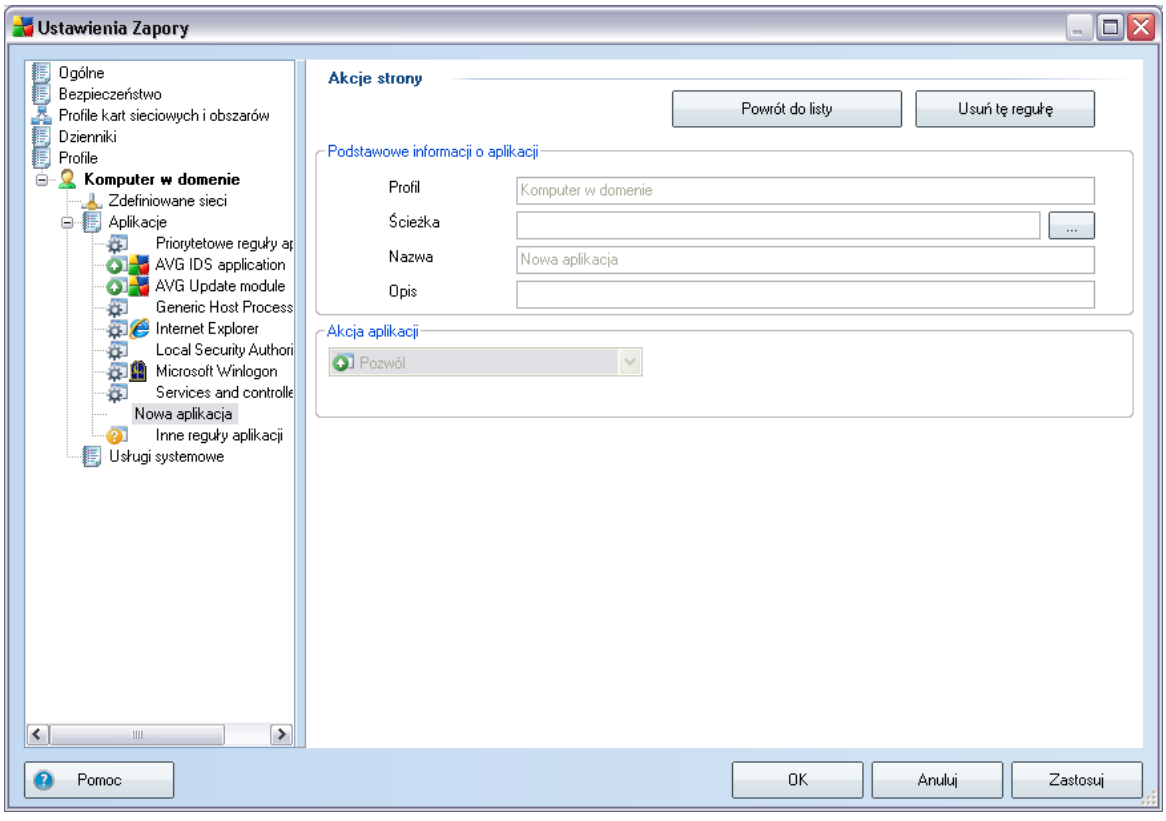
Te pozycje maja inne opcje niz zwykle ustawienia aplikacji i sa przeznaczone tylko dla doswiadczonych uzytkowników. Stanowczo zalecamy

niemodyfikowanie tych ustawien

Przyciski kontrolne

Liste mozna edytowac przy uzyciu nastepujacych przycisków kontrolnych:

- ***Dodaj*** — otwiera puste okno dialogowe ***Akcje strony*** w celu zdefiniowania nowych regul aplikacji.
- ***Edytuj*** — otwiera to samo okno dialogowe ***Akcje strony*** z odpowiednimi danymi w celu edytowania istniejacego zestawu regul aplikacji.
- ***Usun*** — usuwa wybrany zbiór regul z listy.
- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.



To okno dialogowe sluzy do szczególowego definiowania ustawien dla odpowiednich

aplikacji.

Akcje strony

- Przycisk ***Powrót do listy*** umozliwia wyswietlenie przegladu wszystkich zdefiniowanych regul aplikacji.
- Przycisk ***Usun te regule*** umozliwia usuwanie wyswietlanej w danej chwili reguly aplikacji. Nalezy pamietac, ze tej czynnosci nie da sie cofnac!

Podstawowe informacje o aplikacji

W tej sekcji nalezy wprowadzic ***nazwe*** aplikacji oraz jej ***opis*** *(opcjonalny krótki komentarz do wlasnego uzytku*). W polu ***Sciezka*** nalezy wprowadzic pelna sciezke dostepu do aplikacji (*pliku wykonywalnego*) na dysku; aplikacje mozna latwo zlokalizowac w drzewie katalogów, klikajac przycisk „***...***”.

Akcja aplikacji

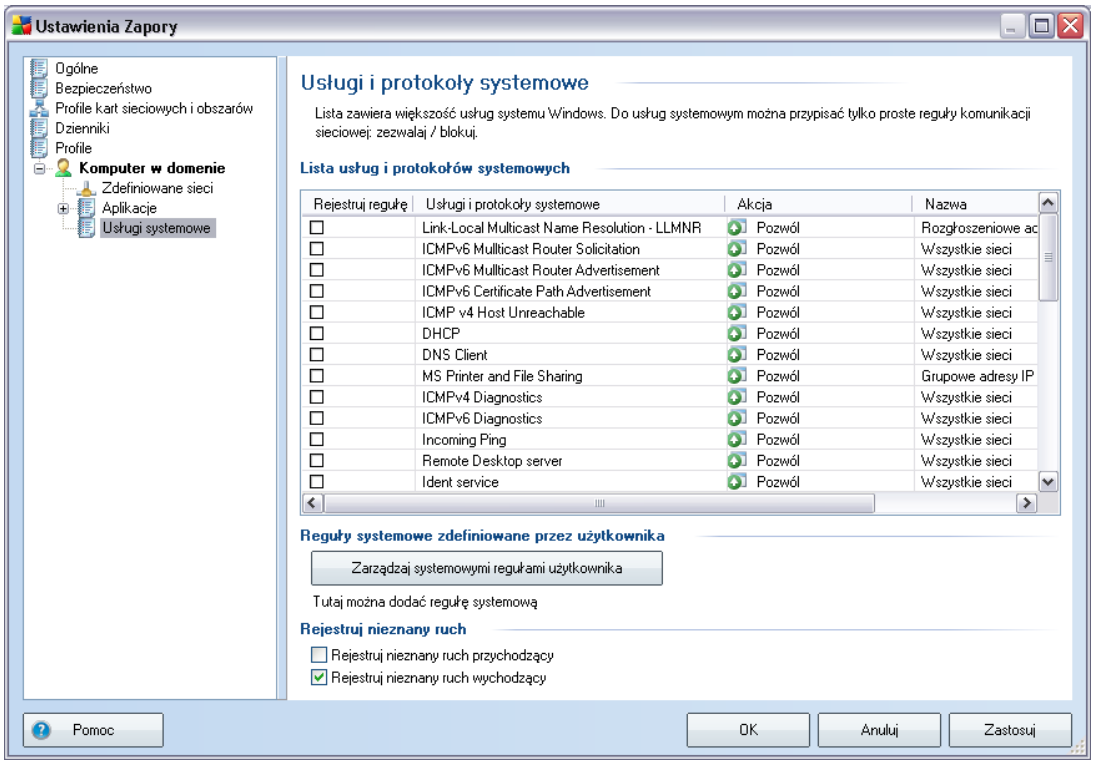
Z rozwijanego menu mozna wybrac regule Zapory dla danej aplikacji, tj. jaka akcje powinien wykonac skladnik, gdy aplikacja próbuje polaczyc sie z siecia.

- ***Odblokuj wszystkie*** — umozliwia wszystkim aplikacjom dowolna komunikacje ze zdefiniowanymi sieciami i kartami sieciowymi (bez zadnych ograniczen).
- ***Odblokuj bezpieczne*** — umozliwia aplikacji dostep tylko do sieci zdefiniowanych jako bezpieczne (godne zaufania).
- ***Blokuj*** — automatycznie blokuje komunikacje; aplikacja nie bedzie mogla uzyskac dostepu do zadnej sieci.
- ***Pytaj*** — powoduje wyswietlanie okna dialogowego pozwalajacego zdecydowac, czy próba polaczenia ma zostac w danym momencie odblokowana czy zablokowana.
- ***Ustawienia zaawansowane*** — powoduje wyswietlenie dalszych opcji ustawien szczególowych w dolnej czesci okna dialogowego, w sekcji ***Szczególowe reguly aplikacji***. Ustawienia szczególowe beda stosowane

zgodnie z kolejnoscia ich wyswietlania na liscie, w zwiazku z czym mozna je ***przesuwac w góre*** lub ***w dól*** zgodnie z pozadana kolejnoscia ich przetwarzania przez Zapore. Po kliknieciu wybranej reguly z listy w dolnej czesci okna dialogowego zostanie wyswietlony przeglad szczegółów tej reguly. Wszystkie sposród wartosci podkreslonych na niebiesko moga zostac zmienione w odpowiednich oknach dialogowych. Aby usunac zaznaczona regule, wystarczy kliknac przycisk ***Usun***. Aby zdefiniowac nowa regule, kliknij przycisk ***Dodaj***, który spowoduje otwarcie okna dialogowego ***Zmien szczegól reguly*** umozliwiajacego okreslenie niezbednych szczegółów.

11.5.4. Uslugi systemowe

Wszelkie zmiany w konfiguracji uslug i protokolów systemowych powinny byc wprowadzane JEDYNIE·przez doswiadczonych uzytkowników.



W oknie dialogowym ***Uslugi i protokoly systemowe*** dostepna jest lista standardowych uslug i protokolów systemu Windows, które moga wymagac komunikacji poprzez siec. Tabela zawiera nastepujace kolumny:

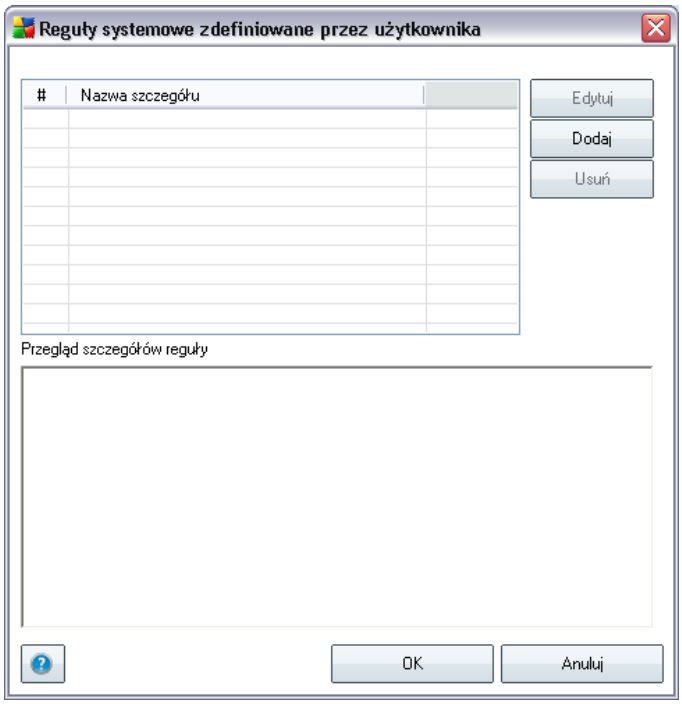
- ***Rejestruj uzycie regul*** — to pole pozwala wlaczyc funkcje zapisywania

kazdego uzycia reguly w Dziennikach.

- ***Uslugi i protokoly systemowe*** — w tej kolumnie wyswietlana jest nazwa odpowiedniej uslugi systemowej.
- ***Akcja*** — w tej kolumnie wyswietlana jest ikona przypisanej akcji:
  -  Odblokuj komunikacje dla wszystkich sieci
  -  Odblokuj komunikacje tylko dla sieci zdefiniowanych jako bezpieczne
  -  Zablokuj komunikacje
- ***Sieci*** — w tej kolumnie wyswietlane sa informacje o tym, której sieci dotyczy dana regula systemowa.

Lista (*w tym przypisane akcje*) moze byc edytowana przy uzyciu nastepujacych przycisków:

- Aby edytowac ustawienia dowolnej pozycji z listy (*w tym przypisanych akcji*), nalezy kliknac te pozycje prawym przyciskiem myszy i wybrac polecenie ***Edytuj*** .
- Aby otworzyc nowe okno dialogowe pozwalajace definiowac wlasne reguly uslug systemowych (*patrz ilustracja ponizej*), kliknij przycisk ***Zarzadzaj wlasnymi regulami systemowymi***. Górna sekcja okna dialogowego ***Reguly systemowe zdefiniowane przez uzytkownika*** zawiera przeglad wszystkich szczegółów edytowanej w danej chwili reguly systemowej. W dolnej sekcji wyswietlany jest wybrany szczegól. Szczegóły reguly zdefiniowanej przez uzytkownika moga byc edytowane, dodawane lub usuwane za pomoca odpowiednich przycisków. Reguly zdefiniowane przez producenta moga byc jedynie edytowane:



Ostrzezenie: *Nalezy pamietac, ze szczególowe ustawienia reguly sa ustawieniami zaawansowanymi i kierowane sa przede wszystkim do administratorów sieci, którzy wymagaja pelnej kontroli nad konfiguracja Zapory. W przypadku braku wystarczajacej wiedzy o typach protokolów, numerach portów sieciowych, adresach IP itp. nie nalezy modyfikowac tych ustawien! Jesli istnieje uzasadniona potrzeba zmiany tej konfiguracji, szczególowe informacje mozna znalezc w plikach pomocy dostepnych w poszczególnych oknach dialogowych.*

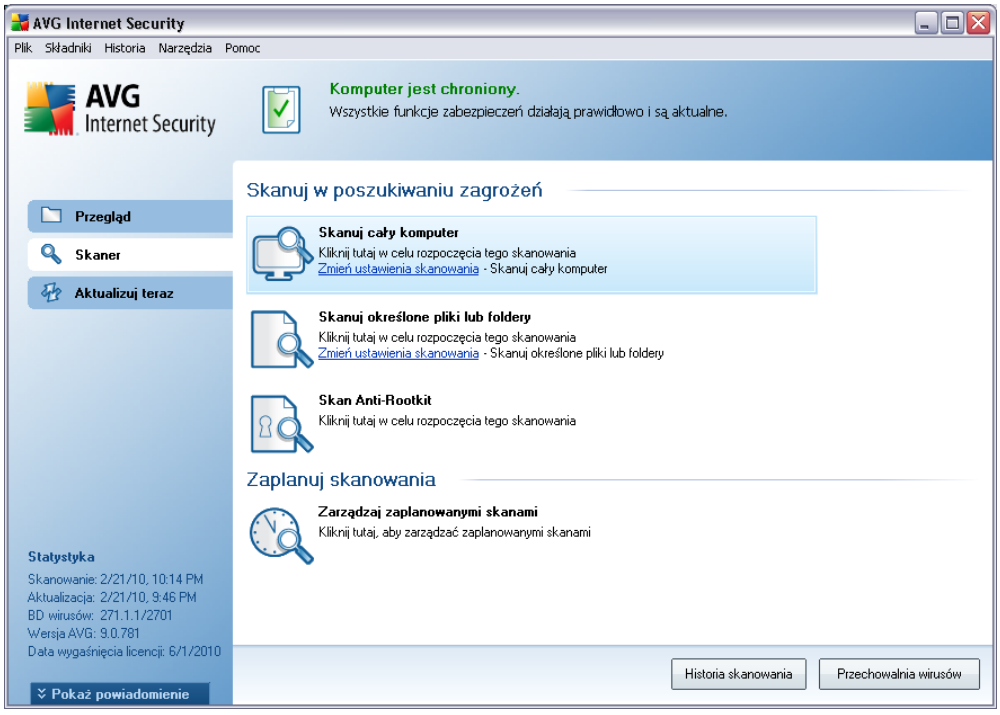
Rejestruj nieznany ruch

- ***Rejestruj nieznany ruch przychodzacy*** — to pole wyboru nalezy zaznaczyc, aby zapisywac w dziennikach kazda nieznana próbe polaczenia sie z zewnatrz z tym komputerem.
- ***Rejestruj nieznany ruch wychodzacy*** — to pole wyboru nalezy zaznaczyc, aby zapisywac w dziennikach kazda nieznana próbe polaczenia sie z tego komputera z zewnetrzna lokalizacja.

12. Skanowanie AVG

Skanowanie jest podstawowym elementem funkcjonowania systemu **AVG 9 Internet Security**. Mozliwe jest uruchamianie testów na zadanie lub planowanie ich okresowego przeprowadzania o odpowiednich porach.

12.1. Interfejs skanowania



Interfejs skanera AVG dostepny jest za posrednictwem linku ***Skaner****. Kliknięcie go otwiera okno ***Skanuj w poszukiwaniu zagrozen***. Okno to zawiera nastepujace elementy:

- przeglad wstepnie zdefiniowanych testów — trzy·typy testów (zdefiniowane przez dostawce oprogramowania) sa gotowe do uzycia na zadanie lub wedlug utworzonego harmonogramu:
    - ***Skan calego komputera***
    - ***Skan okreslonych plików lub folderów***
    - ***Skan Anti-rootkit***

- Planowanie testów — w tym obszarze mozna definiowac nowe testy i tworzyc nowe harmonogramy w zaleznosci od potrzeb.

Przyciski kontrolne

Interfejs skanera zawiera nastepujace przyciski kontrolne:

- ***Historia skanowania*** — wyswietla okno dialogowe Przeglad wyników skanowania, które zawiera pelna historie testów.
- ***Przechowalnia wirusów*** — otwiera nowe okno z zawartoscia Przechowalni wirusów, w której izolowane sa wykryte infekcje.

12.2. Wstepnie zdefiniowane testy

Jedna z glównych funkcji systemu **AVG 9 Internet Security** jest skanowanie na zadanie. Testy na zadanie sluza do skanowania konkretnych obszarów komputera, gdy uzytkownik podejrzewa obecnosc wirusa. Stanowczo zaleca sie jednak wykonywanie tych testów regularnie, nawet w przypadku, gdy nie ma takich podejrzen.

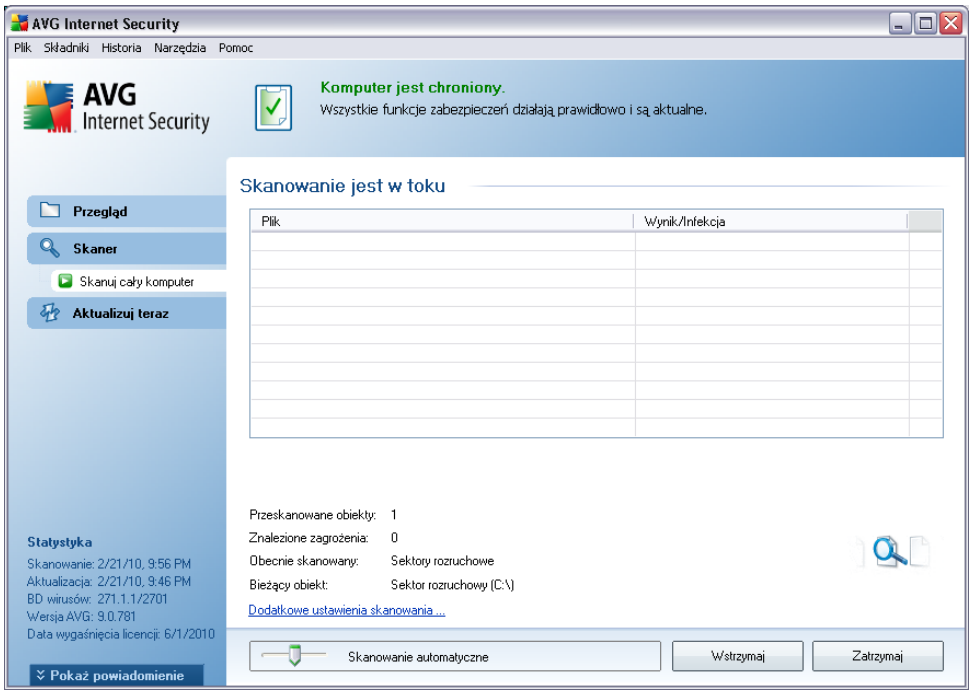
W systemie **AVG 9 Internet Security** dostepne sa dwa typy skanowania zdefiniowane wstepnie przez producenta oprogramowania:

12.2.1. Skan calego komputera

Skanuj caly komputer — skanuje caly komputer w poszukiwaniu mozliwych infekcji i/ lub potencjalnie niechcianych programów. Test ten obejmuje wszystkie dyski twarde komputera. Wykryte infekcje sa leczone lub przenoszone do ***Przechowalni wirusów***. Skanowanie calego komputera powinno byc regularnie przeprowadzane co najmniej raz na tydzien.

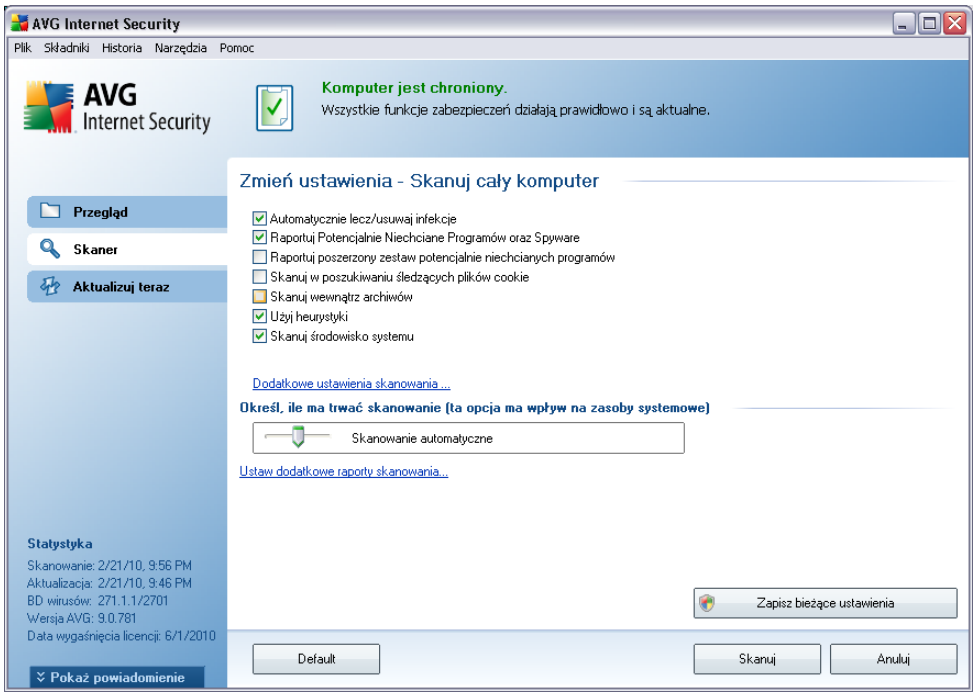
Uruchamianie skanowania

Skanowanie calego komputera mozna uruchomic bezposrednio z poziomu interfejsu skanera, klikajac ikone odpowiedniego testu. Dla tego skanowania nie mozna okreslac dalszych ustawien; jest ono uruchamiane od razu w oknie dialogowym ***Skanowanie w toku***. (*patrz ilustracja*). W razie potrzeby skanowanie mozna tymczasowo przerwac (***Wstrzymaj***) lub anulowac (***Zatrzymaj***).



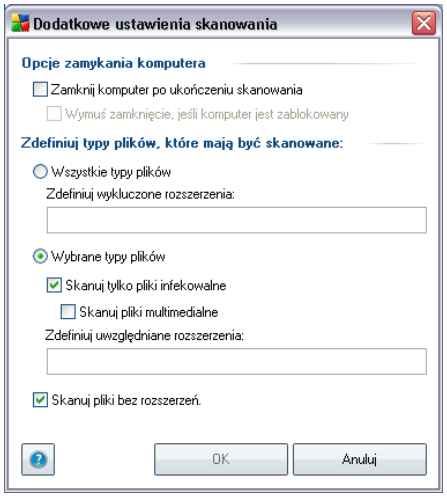
Edycja konfiguracji skanowania

Wstepne, domyslne ustawienia testu ***Skan calego komputera*** mozna latwo edytowac. Kliknięcie linku ***Zmien ustawienia skanowania*** powoduje otwarcie okna dialogowego ***Zmien ustawienia skanu calego komputera. Zaleca sie nie zmieniac ustawien domyslnych, jesli nie jest to konieczne!***



- ***Parametry skanowania*** — na liscie parametrów skanowania mozna wlaczyc/ wylaczyc okreslone parametry w zaleznosci od potrzeb. Wiekszosc parametrów jest domyslnie wlaczona i automatycznie uzywana podczas skanowania.

- ***Dodatkowe ustawienia skanowania*** — link do okna dialogowo ***Dodatkowe ustawienia skanowania***, w którym mozna okreslic nastepujace parametry:



- ***Opcje wylaczania komputera*** — okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).

- ***Zdefiniuj typy plików do skanowania*** — nalezy zdecydowac, które z ponizszych elementów maja byc skanowane:

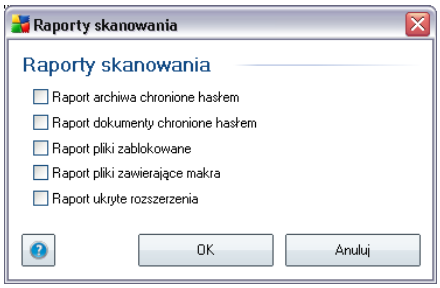
  - ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen plików, który nie powinny byc skanowane;

  - ***Wybrane typy plików*** — skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowanie skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

  - Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

- ***Priorytet procesu skanowania*** — za pomoca suwaka mozna zmienic priorytet procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- ***Ustaw dodatkowe raporty skanowania*** — link ten pozwala otworzyc nowe okno dialogowe ***Raporty skanowania***, w którym mozna okreslic elementy lub zdarzenia, które maja byc zglaszane:



Ostrzezenie: *Ustawienia te sa identyczne jak domyslne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale* ***Skanowanie AVG / Planowanie skanowania / Jak skanowac****. Jesli jednak domyslna konfiguracja testu* ***Skan calego komputera*** *zostanie zmieniona, nowe ustawienia mozna zapisac jako konfiguracje domyslna, aby byly uzywane we wszystkich przyszlych skanach calego komputera.*

12.2.2. Skan okreslonych plików lub folderów

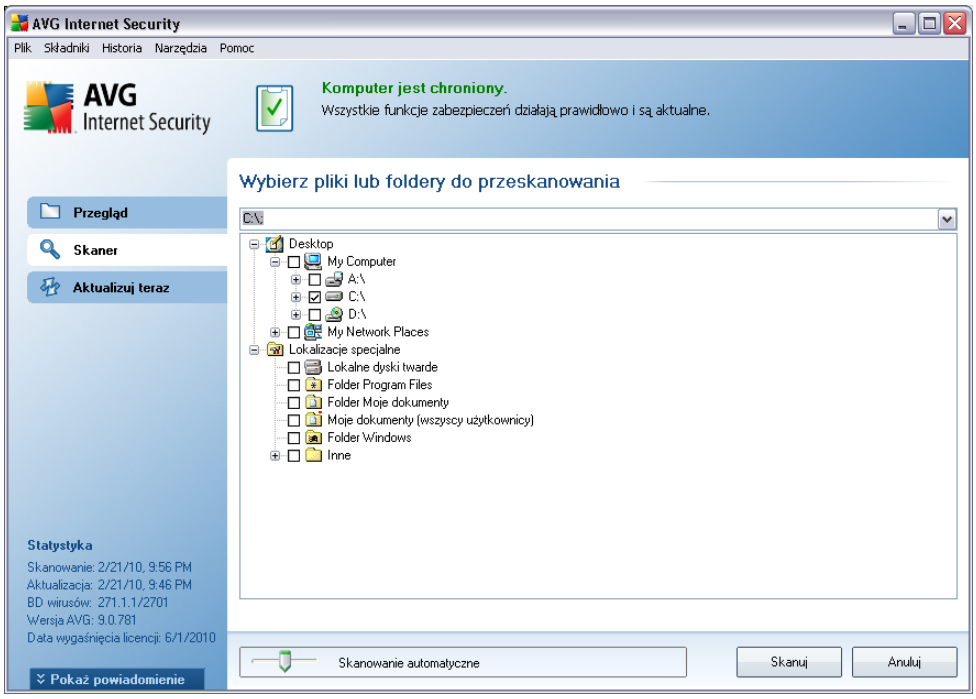
Skan okreslonych plików lub folderów — skanowane sa tylko wskazane obszary komputera (wybrane foldery, a takze dyski twarde, pamieci flash, CD itd).). Postepowanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu calego komputera: kazdy znaleziony wirus jest leczony lub przenoszony do ***Przechowalni***. Skanowanie okreslonych plików lub folderów moze posluzyc do utworzenia wlasnych testów i planowania ich zgodnie z konkretnymi potrzebami.

Uruchamianie skanowania

Skanowanie okreslonych plików lub folderów mozna uruchomic bezposrednio z poziomu interfejsu skanera, klikajac ikone testu. Wyswietlone zostanie nowe okno dialogowe ***Wybierz pliki lub foldery do przeskanowania***. W drzewie katalogów nalezy wybrac te, które maja zostac przeskanowane. Sciezki do wszystkich wybranych folderów zostana wygenerowane automatycznie i wyswietlone w polu tekstowym w górnej czesci okna dialogowego.

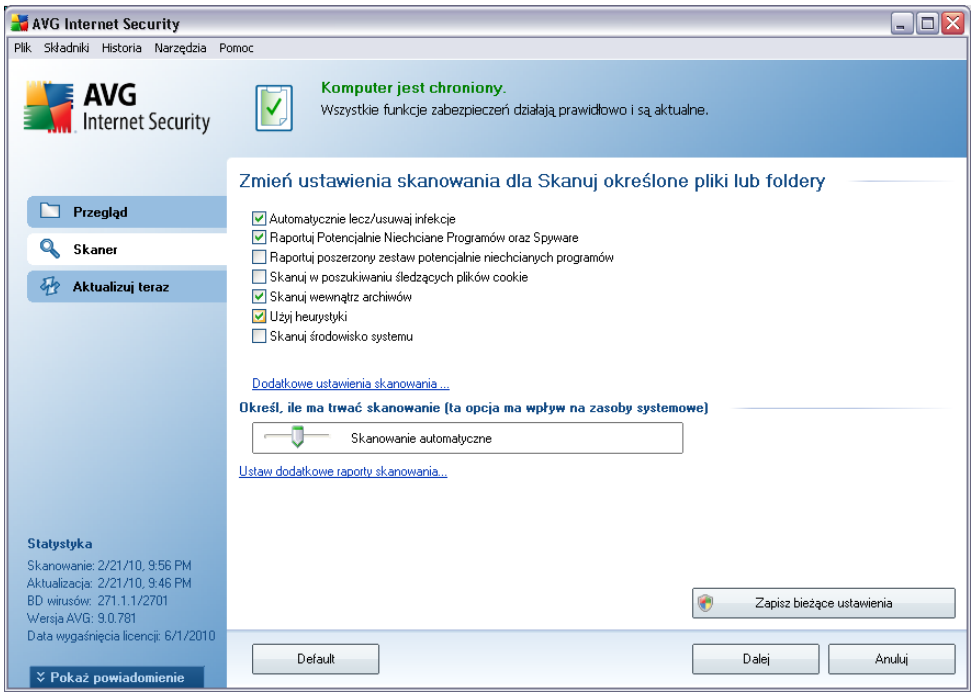
Mozna takze przeskanowac wybrany folder, wykluczajac jednoczesnie ze skanowania wszystkie jego podfoldery: nalezy wprowadzic znak minus „**-**” przed jego nazwa w wygenerowanej sciezce (*patrz ilustracja*). Aby wykluczyc caly folder ze skanowania, nalezy uzyc parametru „!”.

Na koniec, aby uruchomic skanowanie, nalezy nacisnac przycisk ***Rozpocznij skanowanie***; proces skanowania jest w zasadzie taki sam jak skanowanie calego komputera.



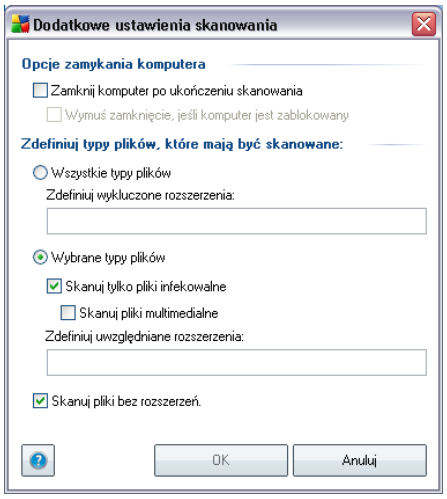
Edycja konfiguracji skanowania

Wstepne, domyslne ustawienia testu ***Skan okreslonych plików lub folderów*** mozna latwo edytowac. Kliknięcie linku ***Zmien ustawienia skanowania*** powoduje otwarcie okna dialogowego ***zmiany ustawien dla skanowania okreslonych plików lub folderów***. ***Zaleca sie nie zmieniac ustawien domyslnych, jesli nie jest to konieczne!***



- ***Parametry skanowania*** — na liscie parametrów skanowania mozna wlaczac/wylaczac okreslone parametry w zaleznosci od potrzeb *(szczególowy opis tych ustawien zawiera rozdzial Zaawansowane ustawienia AVG / Skany / Skanowanie okreslonych plików lub folderów)*.

- ***Dodatkowe ustawienia skanowania*** — link do okna dialogowo Dodatkowe ustawienia skanowania, w którym mozna okreslic nastepujace parametry:



- ***Opcje wylaczania komputera*** — okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).

- ***Zdefiniuj typy plików do skanowania*** — nastepnie nalezy zdecydowac, czy skanowane maja byc:

  - ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;

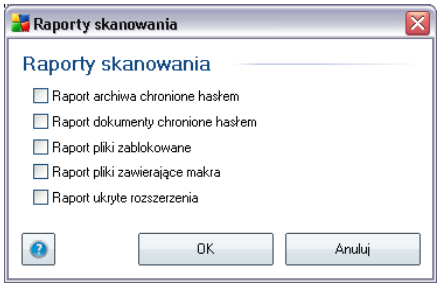
  - ***Wybrane typy plików*** — skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe niewykonywalne*), z uwzglednieniem multimediów (*plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

  - Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

- ***Priorytet procesu skanowania*** — za pomoca suwaka mozna zmienic priorytet

procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- ***Ustaw dodatkowe raporty skanowania*** — link ten pozwala otworzyc nowe okno dialogowe ***Raporty skanowania***, w którym mozna okreslic elementy lub zdarzenia, które maja byc zglaszane:



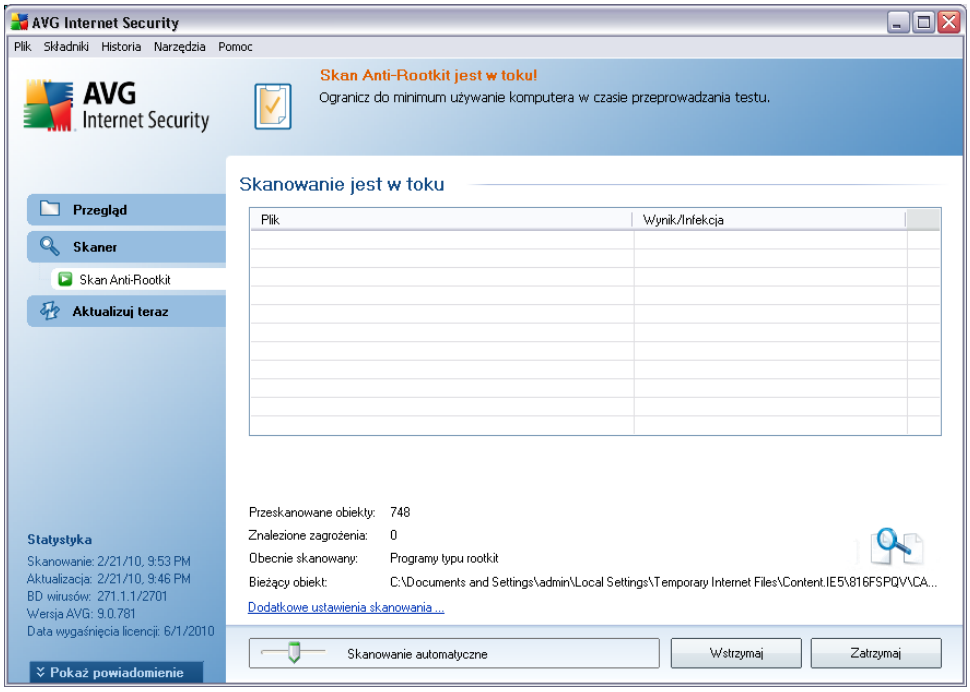
Ostrzezenie: *Ustawienia te sa identyczne jak domyslne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale* ***Skanowanie AVG / Planowanie skanowania / Jak skanowac****. Jesli jednak domyslna konfiguracja testu* ***Skan okreslonych plików lub folderów*** *zostanie zmieniona, nowe ustawienia bedzie mozna zapisac jako konfiguracje domyslna, która bedzie uzywana we wszystkich zdefiniowanych w przyszlosci Skanach okreslonych plików lub folderów. Stanie sie ona równiez szablonem dla wszystkich nowych skanów zaplanowanych (wszystkie testy uzytkownika oparte sa na biezacej konfiguracji Skanu okreslonych plików lub folderów).*

12.2.3. Skan Anti-Rootkit

Skan Anti-Rootkit przeszukuje komputer w poszukiwaniu obecnych na nim programów typu rootkit (*aplikacji oraz technologii, które moga maskowac dzialanie szkodliwego oprogramowania na tym komputerze*). Wykrycie programu typu rootkit nie jest równoznaczne z tym, ze komputer jest zainfekowany. W niektórych przypadkach pewne sterowniki lub elementy zwyklych aplikacji moga omylkowo zostac zaklasyfikowane jako programy typu rootkit.

Uruchamianie skanowania

Skan skladnika Anti-Rootkit moze zostac uruchomiony bezposrednio z poziomu interfejsu skanera poprzez klikniecie ikony skanowania. Dla tego skanowania nie mozna okreslac dalszych ustawien; jest ono uruchamiane od razu w oknie dialogowym ***Skanowanie w toku***. (*patrz ilustracja*). W razie potrzeby skanowanie mozna tymczasowo przerwac (***Wstrzymaj***) lub anulowac (***Zatrzymaj***).

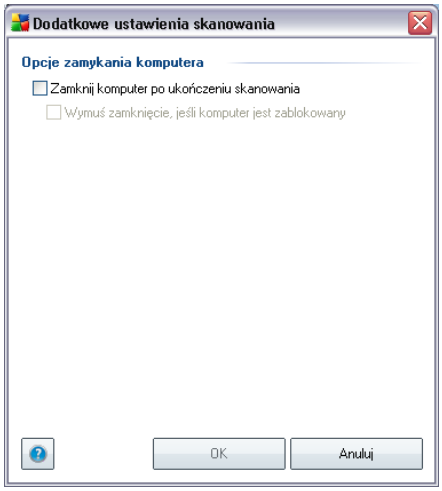


Edycja konfiguracji skanowania

Skan skladnika Anti-Rootkit jest zawsze uruchamiany z ustawieniami domyslnymi, a edycja parametrów skanowania jest dostepna tylko w oknie dialogowym ***Zaawansowane ustawienia systemu AVG / skladnik Anti-Rootkit***. Z poziomu interfejsu skanera dostepne sa tylko nastepujace opcje konfiguracji:

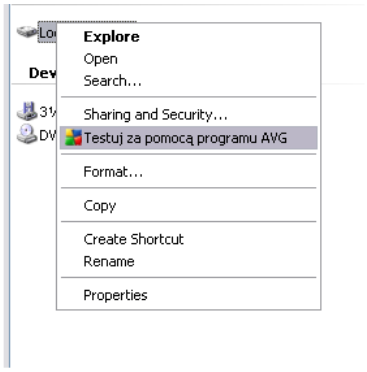
- ***Skanowanie automatyczne*** — za pomoca suwaka mozna zmienic priorytet procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- ***Dodatkowe ustawienia skanowania*** — to lacze umozliwia otwarcie nowego okna dialogowego ***Dodatkowe ustawienia skanowania***, w którym dostepne sa opcje wylaczenia komputera zwiazane ze ***skanowaniem skladnika Anti-Rootkit*** (***Zamknij komputer po zakonczeniu skanowania*** *oraz* ***Wymus zamkniecie, jesli komputer jest zablokowany***):



12.3. Skan z poziomu eksploratora systemu Windows

Oprócz wstepnie zdefiniowanych skanów obejmujacych caly komputer lub wybrane obszary, system **AVG 9 Internet Security** oferuje takze mozliwosc skanowania okreslonych obiektów bezposrednio z interfejsu Eksploratora Windows. Jesli nie ma pewnosci co do zawartosci pliku, który ma zostac otwarty, mozna przeskanowac go „na zadanie”. W tym celu nalezy wykonac nastepujace kroki:



- W Eksploratorze Windows zaznacz plik (lub folder), który chcesz sprawdzic.

- Kliknij go prawym przyciskiem myszy, aby wyswietlic menu kontekstowe.
- Wybierz polecenie ***Testuj za pomoca programu AVG***, aby system AVG przeskanowal obiekt.

12.4. Skan z poziomu wiersza polecen

System **AVG 9 Internet Security** posiada opcje uruchamiania skanowania z poziomu wiersza polecen. Opcji tej mozna uzywac na przyklad na serwerach lub w czasie tworzenia skryptu wsadowego, który ma byc uruchamiany po restarcie komputera. Uruchamiajac skanowanie z wiersza polecen, mozna uzywac wiekszosci parametrów dostepnych w graficznym interfejsie uzytkownika AVG.

Aby uruchomic skanowanie z poziomu wiersza polecen, nalezy uzyc nastepujacego polecenia w folderze, w którym zainstalowano system AVG:

- ***avgscanx*** — w przypadku 32-bitowych systemów operacyjnych
- ***avgscana*** — w przypadku 64-bitowych systemów operacyjnych

Skladnia polecenia

Skladnia polecenia jest nastepujaca:

- ***avgscanx /parametr*** ... np. ***avgscanx /comp*** w celu przeskanowania calego komputera
- ***avgscanx /parametr /parametr*** .. — jesli uzywanych jest wiele parametrów, nalezy wpisac je w jednym wierszu, rozdzielajac spacjami i ukosnikami
- jesli parametry wymagaja podania okreslonych wartosci, (np. parametr ***/scan*** wymaga informacji o wybranych do przeskanowania obszarach komputera — nalezy wskazac dokladna sciezke), nalezy je rozdzielac przecinkami, na przyklad: ***avgscanx /scan=C:\,D:***

Parametry skanowania

Aby wyswietlic pelny przeglad dostepnych parametrów, nalezy wpisac odpowiednie polecenie oraz parametr /? lub /HELP (np. ***avgscanx /?***). Jedynym wymaganym parametrem jest /SCAN, który pozwala okreslic, jakie obszary komputera maja byc skanowane. Bardziej szczególowe informacje na temat opcji zawiera przeglad parametrów wiersza polecen.

Aby uruchomic skanowanie, nalezy nacisnac klawisz ***Enter***. Skanowanie mozna zatrzymac, naciskajac kombinacje klawiszy ***Ctrl+C*** lub ***Ctrl+Pause***.

Skanowanie z poziomu wiersza polecen uruchamiane za pomoca interfejsu graficznego

Gdy komputer dziala w trybie awaryjnym, skanowanie z poziomu wiersza polecen mozna równiez uruchomic za pomoca interfejsu graficznego uzytkownika. Skanowanie zostanie uruchomione z wiersza polecen, a okno dialogowe ***Kompozytor wiersza polecen*** umozliwi jedynie okreslenie wiekszosci parametrów skanowania w wygodnym interfejsie graficznym.

Poniewaz okno to jest dostepne tylko w trybie awaryjnym, jego szczegółowy opis mozna znalezc w pliku pomocy dostepnym bezposrednio z tego okna.

12.4.1. Parametry skanowania z wiersza polecen

Ponizej przedstawiono liste wszystkich parametrów dostepnych dla skanowania z wiersza polecen:

- ***/SCAN*** Skanuj okreslone pliki lub foldery /SCAN=sciezka;sciezka (np. /SCAN=C:\;D:\)
- ***/COMP*** Skanuj caly komputer
- ***/HEUR*** Uzyj analizy heurystycznej***
- ***/EXCLUDE*** Wyklucz ze skanowania sciezki lub pliki
- ***/@*** Plik polecenia /nazwa pliku/
- ***/EXT*** Skanuj te rozszerzenia /na przyklad EXT=EXE,DLL/
- ***/NOEXT*** Nie skanuj tych rozszerzen /na przyklad NOEXT=JPG/
- ***/ARC*** Skanuj archiwa
- ***/CLEAN*** Czysc automatycznie
- ***/TRASH*** Przenies zainfekowane pliki do Przechowalni wirusów***
- ***/QT*** Szybki test
- ***/MACROW*** Raportuj pliki zawierajace makra

- ***/PWDW*** Raportuj pliki chronione haslem
- ***/IGNLOCKED*** Ignoruj pliki zablokowane
- ***/REPORT*** Raportuj do pliku /nazwa pliku/
- ***/REPAPPEND*** Dopisz do pliku raportu
- ***/REPOK*** Raportuj niezainfekowane pliki jako OK
- ***/NOBREAK*** Nie zezwalaj na przerwanie klawiszami CTRL-BREAK
- ***/BOOT*** Wlacz sprawdzanie MBR/sektora rozruchowego
- ***/PROC*** Skanuj aktywne procesy
- ***/PUP*** Raportuj potencjalnie niechciane programy
- ***/REG*** Skanuj rejestr
- ***/COO*** Skanuj pliki cookie
- ***/?*** Wyswietl pomoc na ten temat
- ***/HELP*** Wyswietl pomoc na ten temat
- ***/PRIORITY*** Ustaw priorytet skanowania /Niski, Automatyczny, Wysoki/ (zobacz Ustawienia zaawansowane/ Skany)
- ***/SHUTDOWN*** Zamknij komputer po ukonczeniu skanowania
- ***/FORCESHUTDOWN*** Wymus zamkniecie komputera po ukonczeniu skanowania
- ***/ADS*** Skanuj alternatywne strumienie danych (tylko NTFS)

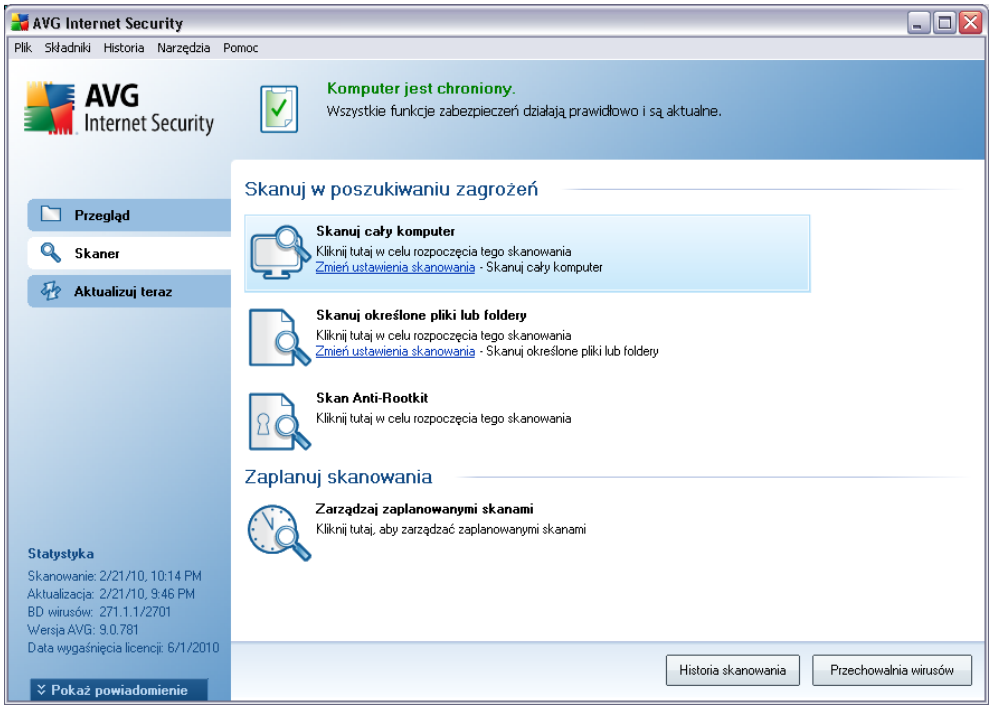
12.5. Planowanie skanowania

System **AVG 9 Internet Security** pozwala uruchamiac skanowanie na zadanie (na przyklad gdy podejrzewa sie infekcje komputera) lub zgodnie z zalozonym harmonogramem. Stanowczo zaleca sie korzystac z harmonogramu: ten sposób daje pewnosc, ze komputer jest chroniony przed infekcjami i zwalnia uzytkownika z obowiazku pamietania o regularnych testach.

Skan calego komputera nalezy uruchamiac regularnie co najmniej raz na tydzien. Jesli

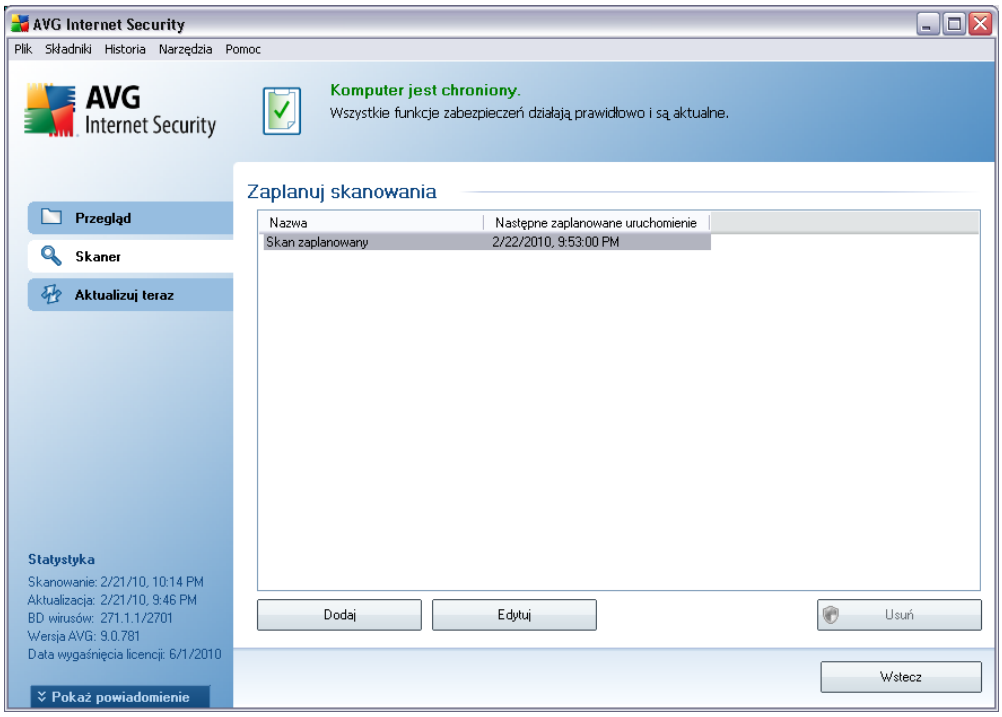
jest to mozliwe, nalezy skanowac komputer codziennie — zgodnie z domyslna konfiguracja harmonogramu skanowania. Jesli komputer dziala 24 godziny na dobe, mozna zaplanowac skanowanie poza czasem pracy. Jesli komputer jest czasami wylaczany, pominiete z tego powodu skany uruchamiane sa po ponownym wlaczeniu komputera.

Aby utworzyc nowe harmonogramy, skorzystaj z przycisku znajdujacego sie w dolnej czesci interfejsu skanera AVG, w sekcji ***Zaplanuj skanowania***:



Zaplanuj skanowania

Kliknij ikone w sekcji ***Zaplanuj skanowania***, aby otworzyc nowe okno dialogowe ***planowania skanowania***, które zawiera liste wszystkich zaplanowanych testów:

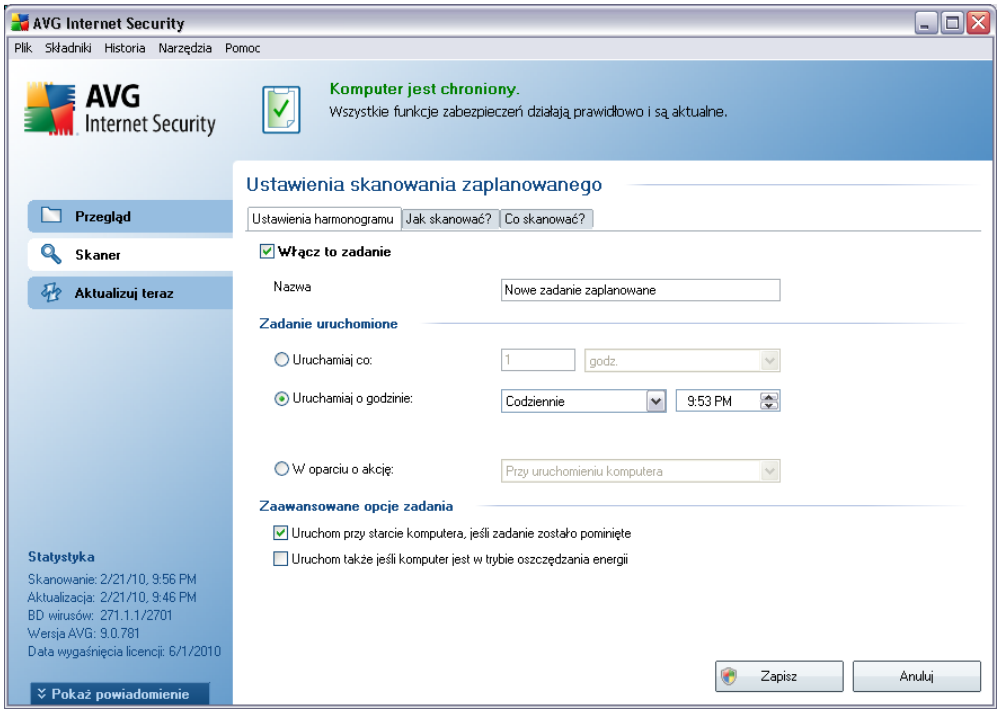


Zawartosc okna mozna edytowac, uzywajac nastepujacych przycisków:

- ***Dodaj*** — otwiera okno ***Ustawienia skanowania zaplanowanego***, a w nim karte ***Ustawienia harmonogramu***. W oknie tym mozna okreslic parametry definiowanego testu.
- ***Edytuj*** — jest aktywny tylko, jesli wybrano istniejacy test na liscie zaplanowanych testów. W takim przypadku klikniecie przycisku powoduje przejscie do okna dialogowego ***Ustawienia skanowania zaplanowanego***, na karte ***Ustawienia harmonogramu***. Parametry wybranego testu sa juz okreslone i mozna je edytowac.
- ***Usun*** — jest aktywny tylko, jesli wybrano istniejacy test na liscie zaplanowanych skanów. Klikniecie przycisku spowoduje usuniecie wybranej pozycji z listy. Usuwac mozna jedynie testy zdefiniowane przez uzytkownika; nie da sie usunac domyslnego ***Skanu zaplanowanego*** .
- ***Wstecz*** — pozwala wrócic do interfejsu skanera AVG

12.5.1. Ustawienia harmonogramu

Aby zaplanowac nowy test i uruchamiac go regularnie, nalezy przejsc do okna dialogowego ***Ustawienia zaplanowanego testu*** (*klikajac przycisk* ***Dodaj harmonogram skanowania*** *w oknie dialogowym* ***Planowanie skanowania***). Okno dialogowe jest podzielone na trzy karty: ***Ustawienia harmonogramu*** — *zobacz ilustracja ponizej (karta otwierana domyslnie),* ***Jak skanowac*** i ***Co skanowac***.



Na karcie ***Ustawienia harmonogramu*** mozna zaznaczyc/odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowany test lub wlaczyc go ponownie, gdy zajdzie taka potrzeba.

Nastepnie nalezy nazwac nowo tworzony skan. Nazwe mozna wpisac w polu tekstowym obok etykiety ***Nazwa.*** Nalezy uzywac krótkich, opisowych nazw, aby ulatwic rozpoznawanie ich przez innych uzytkowników w przyszlosci.

Przyklad: *Nazwy takie jak „Nowy skan” lub „Mój skan” nie sa odpowiednie, poniewaz nie informuja o tym, co jest przedmiotem skanowania. Przykladem dobrej, opisowej nazwy jest „Skan obszarów systemowych”. Ponadto, nie ma potrzeby okreslac w nazwie skanowania, czy skanowany jest caly komputer, czy tylko jego wybrane obszary — wlasne testy uzytkownika sa zawsze specyficznym skanowaniem okreslonych plików lub folderów.*

W tym samym oknie mozna szczególowo okreslic nastepujace parametry skanowania:

- ***Zadanie uruchomione*** — nalezy okreslic interwal przeprowadzanych testów. Skanowanie moze byc powtarzane w okreslonych odstepach czasu (***Uruchamiaj co***) lub o zadanej godzinie (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia zdefiniowanego zdarzenia (***W oparciu o akcje, np. uruchomienie komputera***).

- ***Zaawansowane opcje zadania*** — ta sekcja umozliwia zdefiniowanie warunków skanowania w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

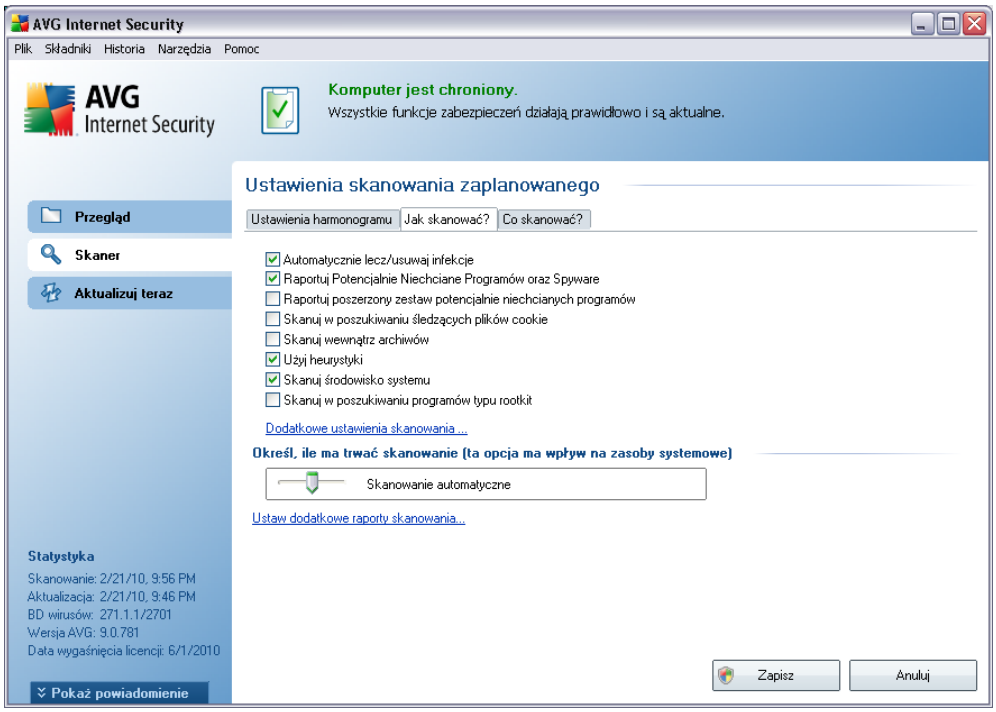
Przyciski kontrolne konfiguracji harmonogramu

Na trzech zakladkach okna dialogowego ***Ustawienia zaplanowanego skanowania*** dostepne sa trzy przyciski sterujace (***Ustawienia harmonogramu***, ***Jak skanowac*** i ***Co skanowac***). Dzialanie tych przycisków jest takie samo na kazdej zakladce:

- ***Zapisz*** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyslnego okna Interfejsu uzytkownika AVG. Oznacza to, ze aby zapisac nowe parametry testów na wszystkich kartach, nalezy kliknac ten przycisk po zakonczeniu wprowadzania ustawien.

- ***Anuluj*** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do Interfejsu uzytkownika AVG.

12.5.2. Jak skanowac?



Karta ***Jak skanowac?*** zawiera liste parametrów testu, które mozna wlaczyc lub wylaczyc. Domyslnie wiekszosc funkcji jest wlaczona, a odpowiadajace im ustawienia sa stosowane podczas skanowania. Ustawienia te nalezy zmieniac tylko w uzasadnionych przypadkach, w pozostalych zachowujac wstepnie zdefiniowana konfiguracje:

- ***Automatycznie lecz/usuwaj infekcje*** — (*domyslnie wlaczona*) jezeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jesli zainfekowanego pliku nie mozna wyleczyc, lub jesli opcja ta zostanie wylaczona, system powiadomi o wykryciu wirusa i zapyta o sposób reakcji na infekcje. Zalecana czynnoscia jest przeniesienie zainfekowanego pliku do ***Przechowalni wirusów***.

- ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyslnie wlaczona*) — zaznaczenie tego pola powoduje wlaczenie silnika ***Anti-Spyware*** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegujacego (a nie tylko wirusów). Oprogramowanie szpiegujace nalezy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrozenie dla bezpieczenstwa, ale niektóre z takich programów moga zostac zainstalowane umyslnie. Nie zaleca sie wylaczania tej opcji — znaczaco zwieksza ona poziom

ochrony komputera

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** — jesli poprzednia opcja jest aktywna, mozna równiez zaznaczyc to pole, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona.

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** — (*domyslnie wlaczone*) ten parametr skladnika ***Anti-Spyware*** okresla, czy wykrywane maja byc pliki cookie (*uzywane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach, np. preferencji wygladu witryny i zawartosc koszyków w sklepach internetowych*).

- ***Skanuj wewnatrz archiwów*** — (*domyslnie wlaczona*) parametr ten okresla, czy skanowanie ma obejmowac pliki znajdujace sie wewnatrz niektórych typów archiwów, np. ZIP, RAR itd.

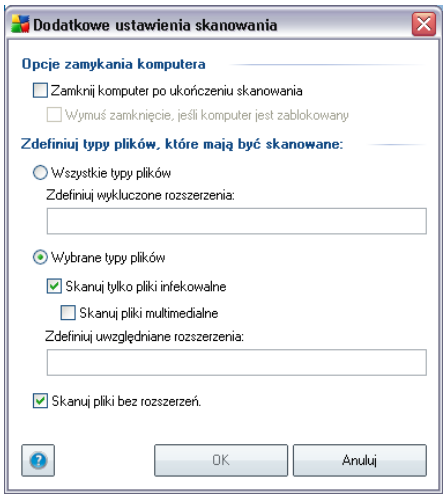
- ***Uzyj heurystyki*** — (*domyslnie wlaczona*) analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku wirtualnej maszyny*) jest jedna z metod wykrywania wirusów w czasie rzeczywistym.

- ***Skanuj srodowisko systemu*** — (*domyslnie wlaczona*) skanowanie obejmie takze obszary systemowe komputera.

- ***Skanuj w poszukiwaniu programów typu rootkit*** — zaznaczenie tej pozycji pozwala dolaczyc wykrywanie programów typu rootkit do operacji skanowania calego komputera. Test Anti-Rootkit mozna takze uruchomic niezaleznie, dzieki interfejsowi skladnika ***Anti-Rootkit***

Nastepnie mozna zmienic konfiguracje skanowania zgodnie z ponizszym opisem:

- ***Dodatkowe ustawienia skanowania*** — link do okna dialogowo ***Dodatkowe ustawienia skanowania***, w którym mozna okreslic nastepujace parametry:



- ***Opcje wylaczania komputera*** — okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).

- ***Zdefiniuj typy plików do skanowania*** — nalezy zdecydowac, które z ponizszych elementów maja byc skanowane:

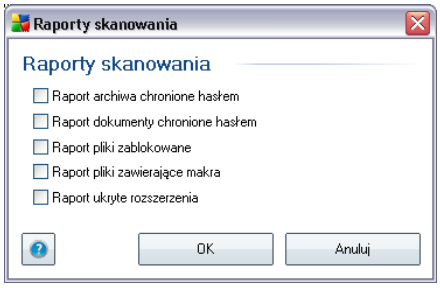
  - ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;

  - ***Wybrane typy plików*** — skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowanie skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

  - Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** — ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

- ***Priorytet procesu skanowania*** — za pomoca suwaka mozna zmienic priorytet procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- ***Ustaw dodatkowe raporty skanowania*** — link ten pozwala otworzyc nowe okno dialogowe ***Raporty skanowania***, w którym mozna okreslic elementy lub zdarzenia, które maja byc zglaszane:



Uwaga: *Domyslnie konfiguracja jest ustawiona pod katem optymalnej wydajnosci. Konfiguracje skanowania nalezy zmieniac tylko w uzasadnionych sytuacjach. Stanowczo zaleca sie stosowanie wstepnie zdefiniowanych ustawien. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Wiecej opcji dostepne jest w oknie* ***Ustawienia zaawansowane****, (****Menu glówne/Plik/ Ustawienia zaawansowane****).*

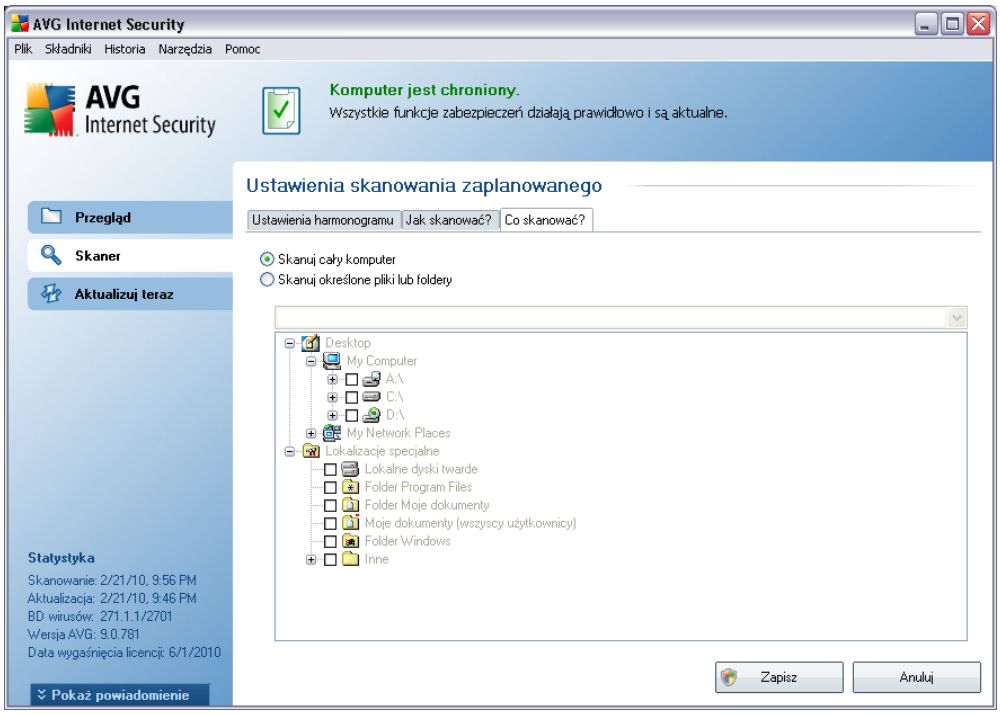
Przyciski kontrolne

Na wszystkich trzech kartach okna z ***konfiguracja skanu zaplanowanego*** (***Ustawienia harmonogramu***, ***Jak skanowac?*** i***Co skanowac?***) dostepne sa dwa przyciski kontrolne. Ich dzialanie na kazdej karcie jest takie samo:

- ***Zapisz*** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyslnego okna Interfejsu uzytkownika AVG. Oznacza to, ze aby zapisac nowe parametry testów na wszystkich kartach, nalezy kliknac ten przycisk po zakonczeniu wprowadzania ustawien.

- ***Anuluj*** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do Interfejsu uzytkownika AVG.

12.5.3. Co skanowac?



Na karcie ***Co skanowac?*** mozna okreslic, czy planowane jest skanowanie calego komputera, czy skanowanie okreslonych plików lub folderów.

Jesli zostanie wybrane skanowanie okreslonych plików lub folderów, w dolnej czesci tego okna dialogowego zostanie aktywowane okno katalogów, które umozliwi wybranie folderów do skanowania (*rozwijaj pozycje, klikajac znak plusa, dopóki nie znajdziesz folderu, który ma zostac przeskanowany*). Zaznaczajac wiecej pól, mozna wybrac kilka folderów. Wybrane foldery zostana wyswietlone w polu tekstowym u góry okna dialogowego, a historia wybranych skanów bedzie przechowywana w rozwijanym menu do pózniejszego uzytku. Opcjonalnie mozna wprowadzic recznie pelna sciezke dostepu wybranego folderu (*w przypadku kilku sciezek nalezy je rozdzielic srednikiem bez dodatkowej spacji*).

Drzewo katalogów zawiera równiez galaz ***Lokalizacje specjalne***. Ponizej znajduje sie lista tych lokalizacji; beda one skanowane, jesli zostanie obok nich zaznaczone odpowiednie pole wyboru:

- ***Lokalne dyski twarde*** — wszystkie dyski twarde na tym komputerze
- ***Program Files*** — C:\:\Folder Program Files\

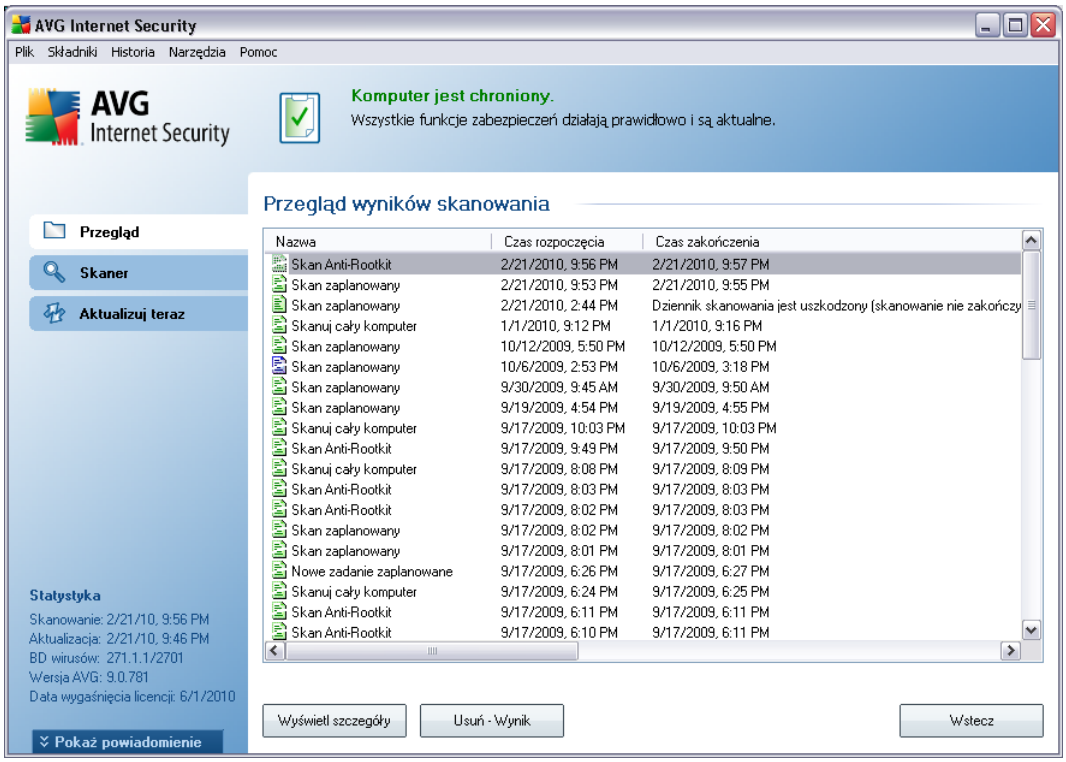
- ***Folder Moje dokumenty*** — C:\Documents and Settings\User\My Documents\
- ***Udostepniane dokumenty*** — C:\Documents and Settings\All Users\Documents\
- ***Folder Windows*** — C:\Windows\
- ***Inne***
    - *Dysk systemowy* — dysk twardy, na którym zainstalowany jest system operacyjny (zazwyczaj C:)
    - *Folder systemowy* — Windows/System32
    - *Folder plików tymczasowych* — Documents and Settings/User/Local Settings/Temp
    - *Folder tymczasowych plików internetowych* — Documents and Settings/User/Local Settings/Temporary Internet Files

Przyciski kontrolne konfiguracji harmonogramu

Na trzech zakladkach okna dialogowego ***Ustawienia zaplanowanego skanowania*** dostepne sa trzy przyciski sterujace (***Ustawienia harmonogramu***, ***Jak skanowac*** i ***Co skanowac***). Dzialanie tych przycisków jest takie samo na kazdej zakladce:

- ***Zapisz*** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyslnego okna Interfejsu uzytkownika AVG. Oznacza to, ze aby zapisac nowe parametry testów na wszystkich kartach, nalezy kliknac ten przycisk po zakonczeniu wprowadzania ustawien.
- ***Anuluj*** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do Interfejsu uzytkownika AVG.

12.6. Przeglad wyników skanowania



Dostep do okna ***Przeglad wyników skanowania*** mozliwy jest z poziomu Interfejsu skanera AVG, przez kliknięcie przycisku ***Historia skanowania***. Okno to zawiera liste wszystkich wczesniejszych testów oraz informacje o ich wynikach:

- ***Nazwa*** — oznaczenie skanowania; moze to byc nazwa jednego ze wstepnie zdefiniowanych skanów lub nazwa nadana przez uzytkownika jego skanowi zaplanowanemu. Kazdej nazwie towarzyszy ikona okreslajaca wynik skanowania:

  — zielona oznacza, ze nie wykryto zadnych infekcji;

  — niebieska ikona oznacza, ze wykryto infekcje, ale zainfekowany obiekt zostal automatycznie usuniety.

  — czerwona oznacza, ze wykryto infekcje i nie udalo sie jej usunac.

  Kazda z ikon moze byc widoczna w calosci lub „przerwana” — jesli ikona jest cala, skanowanie zostalo prawidlowo ukonczone; w przeciwnym

razie skanowanie zostalo anulowane lub przerwane.

Uwaga: *Szczególowe informacje na temat kazdego testu zawiera okno* ***Wyniki skanowania*** *dostepne po kliknieciu przycisku* ***Wyswietl szczegóły*** *(w dolnej czesci okna).*

- ***Czas rozpoczecia*** — data i godzina uruchomienia testu.
- ***Czas zakonczenia*** — data i godzina zakonczenia skanowania.
- ***Przetestowano obiektów*** — liczba obiektów sprawdzonych podczas skanowania.
- ***Infekcje*** — liczba infekcji wirusowych, które zostaly wykryte/usuniete.
- ***Oprogramowanie szpiegujace*** — liczba programów szpiegujacych, które zostaly wykryte/usuniete.

- ***Ostrzezenia*** — liczba wykrytych podejrzanych obiektów
- ***Programy typu rootkit*** — liczba wykrytych programów typu rootkit

- ***Informacji w dzienniku skanowania*** — informacje dotyczace przebiegu i wyniku skanowania (zwykle o jego zakonczeniu lub przerwaniu).

Przyciski kontrolne

Przyciski kontrolne dostepne w oknie ***Przeglad wyników skanowania*** to:

- ***Wyswietl szczegóły*** — kliknięcie tego przycisku powoduje przelaczenie sie do okna dialogowego ***Wyniki skanowania***, w którym mozna przejrzec szczegółowe dane dotyczace wybranego skanowania.
- ***Usun wynik*** — kliknięcie tego przycisku powoduje usuniecie wybranej pozycji z przegladu wyników skanowania.
- ***Wstecz*** — otwiera ponownie domyslne okno Interfejsu skanera AVG.

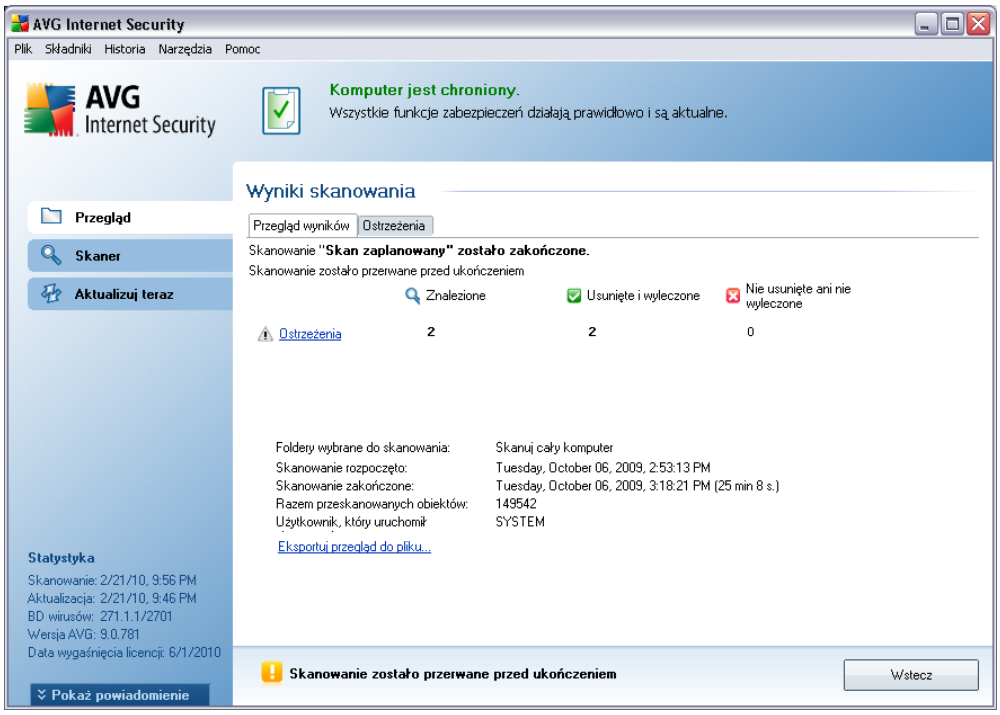
12.7. Szczegóły wyników skanowania

Po wybraniu w oknie ***Przeglad wyników skanowania*** któregos z testów, mozna kliknac przycisk ***Wyswietl szczegóły***, aby przejsc do okna ***Wyniki skanowania***, które zawiera dodatkowe informacje o jego przebiegu.

Okno to podzielone jest na kilka kart:

- ***Przeglad wyników*** — karta jest zawsze wyswietlana; zawiera statystyki dotyczace przebiegu skanowania.
- ***Infekcje*** — karta jest wyswietlana tylko, jesli w czasie skanowania wykryto co najmniej jedna infekcje wirusowa.
- ***Oprogramowanie szpiegujace*** — karta jest wyswietlana tylko, jesli w czasie skanowania wykryto oprogramowanie szpiegujace.
- ***Ostrzezenia*** — ta karta jest wyswietlana na przyklad, jesli podczas skanowania wykryto pliki cookie.
- ***Programy typu rootkit*** — karta jest wyswietlana tylko, jesli w czasie skanowania wykryto programy typu rootkit.
- ***Informacje*** **—** karta jest wyswietlana tylko, jesli w czasie skanowania wykryto potencjalne zagrozenia, których nie mozna bylo zakwalifikowac do powyzszych kategorii; dla kazdego znalezionego obiektu wyswietlany jest komunikat ostrzegawczy. Dodatkowo, sa tu wyswietlane informacje o obiektach, które nie mogly zostac przeskanowane (np. archiwa chronione haslem).

12.7.1. Karta "Przeglad wyników"



Na karcie ***Wyniki skanowania*** mozna znalezc szczególowe statystyki oraz informacje o:

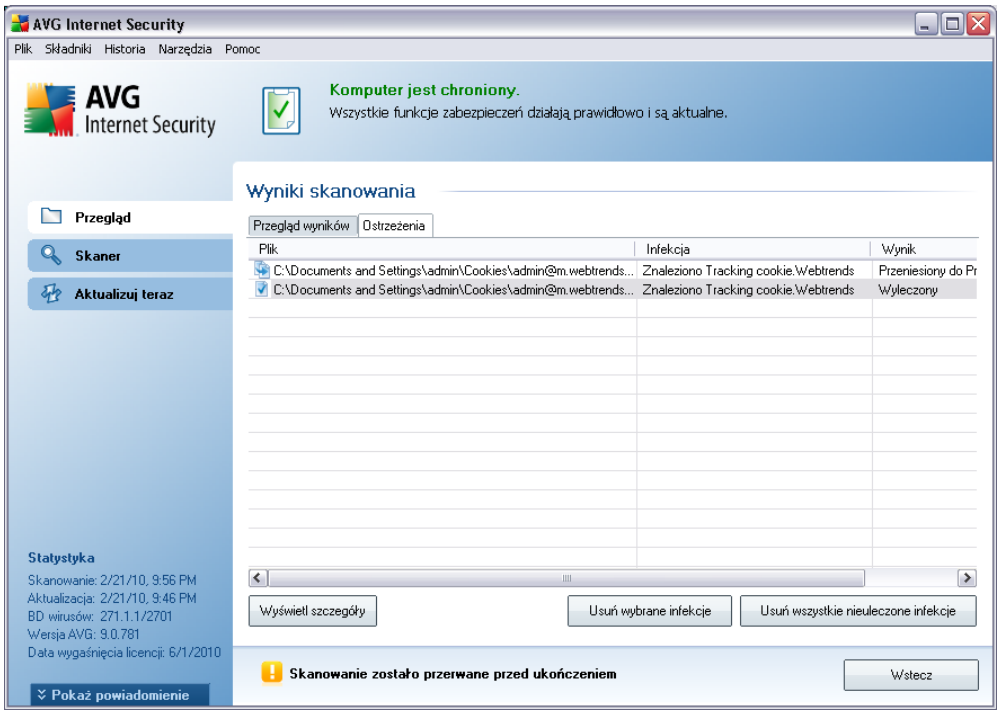
- wykrytych infekcjach wirusowych/programach szpiegujacych
- usunietychinfekcjach wirusowych/programach szpiegujacych
- liczbie infekcji wirusowych/programów szpiegujacych, których nie udalo sie usunac ani wyleczyc.

Ponadto, znajduja sie tu informacje o dacie i dokladnej godzinie uruchomienia testu, lacznej liczbie przeskanowanych obiektów, czasie trwania oraz liczbie napotkanych bledów.

Przyciski kontrolne

Okno to zawiera tylko jeden przycisk kontrolny. Kliknięcie przycisku ***Zamknij wyniki*** powoduje powrót do ***Przegladu wyników skanowania***.

12.7.2. Karta "Infekcje"



Karta ***Infekcje*** jest wyswietlana w oknie dialogowym ***Wyniki skanowania*** tylko, jesli podczas skanowania wykryto wirusa. Karta jest podzielona na trzy obszary, które zawieraja nastepujace informacje:

- ***Plik*** — pelna sciezka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** — nazwa wykrytego wirusa (*szczególowe informacje na temat wirusów zawiera Encyklopedia Wirusów dostepna online*).
- ***Wynik*** — okresla biezacy stan zainfekowanego obiektu, który wykryto podczas skanowania:
  - ***Zainfekowany*** — zainfekowany obiekt zostal wykryty i pozostawiony w oryginalnej lokalizacji (*np. jesli wylaczono opcje automatycznego leczenia w szczególowych ustawieniach skanowania).*
  - ***Wyleczony*** — zainfekowany obiekt zostal automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
  - ***Przeniesiony do Przechowalni*** — zainfekowany obiekt zostal

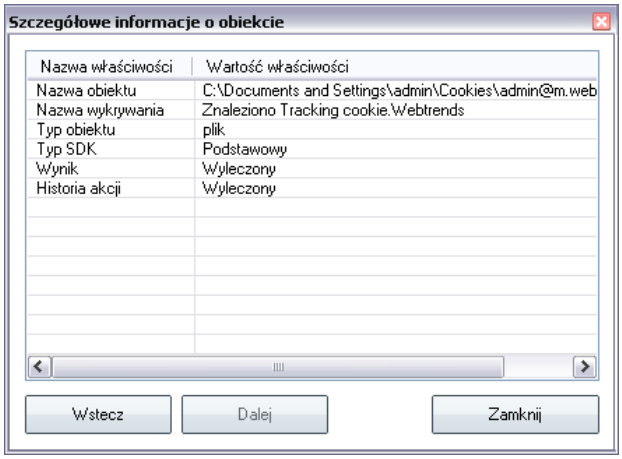
przeniesiony do ***Przechowalni wirusów***.

- ***Usuniety*** — zainfekowany obiekt zostal usuniety.
- ***Dodany do listy wyjatków PNP*** — znaleziony obiekt zostal uznany za wyjatek i dodany do listy wyjatków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie* ***Wyjatki PNP***).
- ***Plik zablokowany - nie testowany*** — obiekt jest zablokowany i program AVG nie mógl go przeskanowac.
- ***Obiekt potencjalnie niebezpieczny*** — obiekt zostal uznany za potencjalnie niebezpieczny, ale nie zainfekowany (*moze na przyklad zawierac makra*); informacje te nalezy traktowac wylacznie jako ostrzezenie.
- ***Wymagany restart systemu*** — aby calkowicie usunac zainfekowany obiekt, nalezy ponownie uruchomic komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

- ***Wyswietl szczegóły*** — otwiera nowe okno ze ***szczególowymi informacjami o wyniku testu***:



Mozna w nim znalezc informacje o lokalizacji wykrytego pliku (***Nazwa wlasciwosci***). Za pomoca przycisków ***Wstecz*** / ***Dalej*** mozna wyswietlac

informacje o wybranych znalezionych obiektach. Przycisk ***Zamknij*** zamyka okno.

- ***Usun wybrane infekcje*** — pozwala przeniesc wybrane obiekty do ***Przechowalni wirusów.***
- ***Usun wszystkie niewyleczone pliki*** — pozwala usunac wszystkie znalezione obiekty, których nie mozna wyleczyc ani przeniesc do ***Przechowalni wirusów.***
- ***Zamknij wyniki*** — powoduje zamkniecie szczególowych wyników i powrót do okna ***Przeglad wyników skanowania***.

12.7.3. Karta "Oprogramowanie szpiegujace"

Karta ***Oprogramowanie szpiegujace*** jest wyswietlana w oknie dialogowym ***Wyniki skanowania*** tylko, jesli podczas skanowania wykryto oprogramowanie szpiegujace. Karta jest podzielona na trzy obszary, które zawieraja nastepujace informacje:

- ***Plik*** — pelna sciezka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** — nazwa wykrytego oprogramowania szpiegujacego (*szczególowe informacje na temat wirusów zawiera* ***Encyklopedia Wirusów*** *dostepna online*).
- ***Wynik*** — okresla biezacy stan obiektu, który wykryto podczas skanowania:
  - ***Zainfekowany*** — zainfekowany obiekt zostal wykryty i pozostawiony w oryginalnej lokalizacji (np. jesli wylaczono opcje automatycznego leczenia w szczególowych ustawieniach skanowania).
  - ***Wyleczony*** — zainfekowany obiekt zostal automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
  - ***Przeniesiony do Przechowalni*** — zainfekowany obiekt zostal przeniesiony do ***Przechowalni wirusów.***
  - ***Usuniety*** — zainfekowany obiekt zostal usuniety.
  - ***Dodany do listy wyjatków PNP*** — znaleziony obiekt zostal uznany za wyjatek i dodany do listy wyjatków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie* ***Wyjatki PNP***).
  - ***Plik zablokowany - nie testowany*** — obiekt jest zablokowany i program AVG nie mógl go przeskanowac.

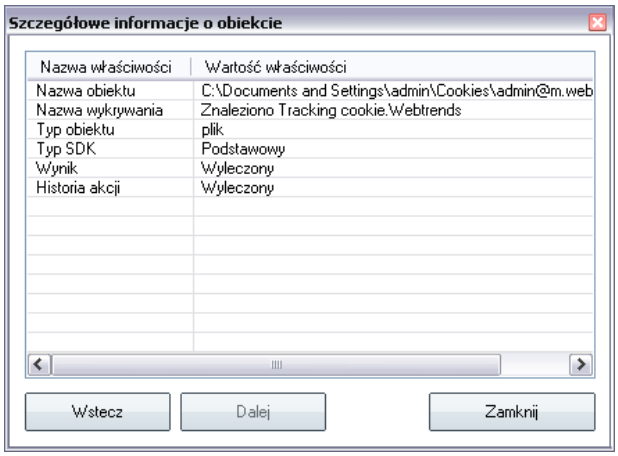
- o ***Obiekt potencjalnie niebezpieczny*** — obiekt zostal uznany za potencjalnie niebezpieczny, ale nie zainfekowany (moze np. zawierac makra); informacja ta jest wylacznie ostrzezeniem.

- o ***Wymagany restart systemu*** — aby calkowicie usunac zainfekowany obiekt, nalezy ponownie uruchomic komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

- ***Wyswietl szczegóły*** — otwiera nowe okno ze ***szczególowymi informacjami o wyniku testu***:



  Mozna w nim znalezc informacje o lokalizacji wykrytego pliku (***Nazwa wlasciwosci***). Za pomoca przycisków ***Wstecz*** / ***Dalej*** mozna wyswietlac informacje o wybranych znalezionych obiektach. Przycisk ***Zamknij*** zamyka okno.

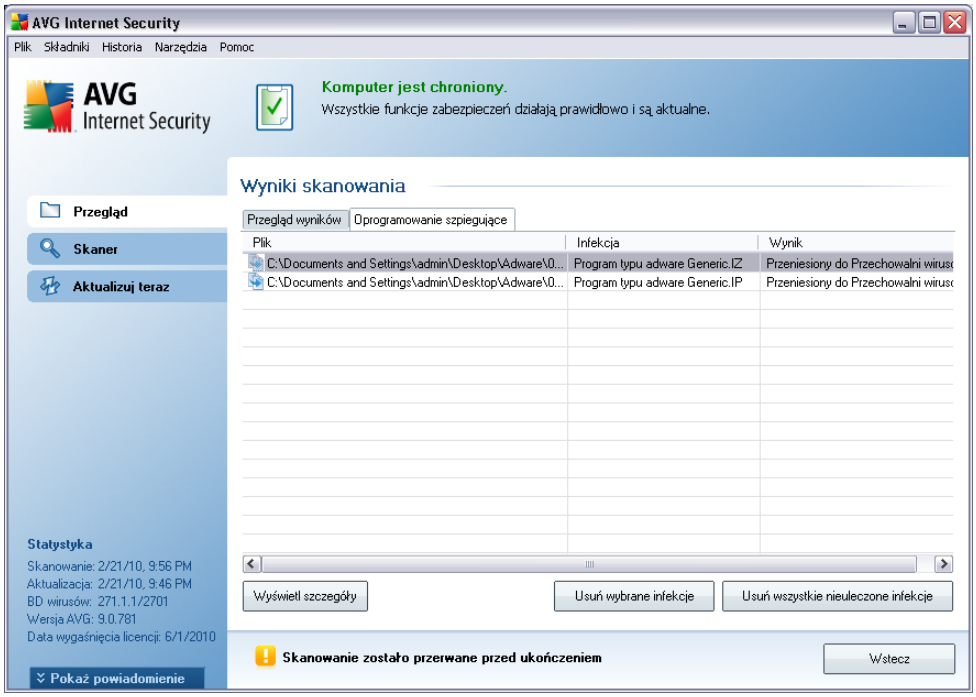
- ***Usun wybrane infekcje*** — pozwala przeniesc wybrane obiekty do ***Przechowalni wirusów.***

- ***Usun wszystkie niewyleczone pliki*** — pozwala usunac wszystkie znalezione obiekty, których nie mozna wyleczyc ani przeniesc do ***Przechowalni wirusów.***

- ***Zamknij wyniki*** — powoduje zamkniecie szczególowych wyników i powrót do okna ***Przeglad wyników skanowania***.

12.7.4. Karta "Ostrzezenia"

Karta ***Ostrzezenia*** zawiera informacje o „podejrzanych" obiektach (*zwykle plikach*) wykrytych podczas skanowania. Gdy ***Ochrona Rezydentna*** wykryje takie pliki, zazwyczaj blokuje do nich dostep. Typowe przyklady obiektów tego typu to: ukryte pliki, cookies, podejrzane klucze rejestru, zabezpieczone haslem archiwa i dokumenty itp.Pliki te nie stanowia zadnego bezposredniego zagrozenia dla bezpieczenstwa komputera i uzytkownika. Informacje o nich przydatne sa jednak w wypadku wykrycia na komputerze oprogramowania reklamowego lub szpiegujacego. Jesli podczas testu AVG pojawily sie tylko ostrzezenia, nie jest konieczne podejmowanie jakichkolwiek dzialan.



Oto krótki opis najbardziej popularnych obiektów tego typu:

- ***Pliki ukryte*** Pliki ukryte sa domyslnie niewidoczne dla uzytkownika w systemie Windows. Niektóre wirusy moga próbowac uniknac wykrycia przez wykorzystanie tej wlasciwosci. Jesli system AVG zglasza obecnosc ukrytego pliku, który moze byc szkodliwy, mozna przeniesc go do ***Przechowalni wirusów AVG***.

- ***Pliki cookie*** Pliki cookie to pliki tekstowe wykorzystywane przez strony internetowe do przechowywania informacji wlasciwych dla danego

uzytkownika. Sa one pózniej uzywane do ladowania witryn internetowych dostosowanych do wymagan uzytkownika, itp.

- ***Podejrzane klucze rejestru*** Niektóre szkodliwe oprogramowanie przechowuje informacje w rejestrze systemu Windows, aby uruchamiac sie podczas ladowania systemu lub rozszerzyc zakres swojego dzialania.

12.7.5. Karta "Rootkity"

Karta ***Programy typu rootkit*** zawiera informacje na temat programów typu rootkit wykrytych podczas skanowania, jesli uruchomiono ***skanowanie skladnika Anti-Rootkit*** lub dodano te opcje recznie do konfiguracji ***skanu calego komputera*** (*opcja jest domyslnie wylaczona*).

Program typu rootkit to wirus zaprojektowany w celu przejecia calkowitej kontroli nad systemem komputerowym bez zgody jego wlascicieli czy upowaznionych administratorów. Bezposredni dostep do sprzetu jest rzadko wymagany, poniewaz programy typu rootkit w pelni zdalnie kontroluja system operacyjny komputera. Zwykle ukrywaja one swoja obecnosc mylac lub unikajac standardowych mechanizmów bezpieczenstwa systemu operacyjnego. Wiele z nich jest jednoczesnie konmi trojanskimi, które dodatkowo staraja sie przekonac uzytkowników, ze ich systemy sa bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorujacymi) oraz plików lub danych przed samym systemem operacyjnym.

Struktura tej karty jest w zasadzie taka sama jak kart ***Infekcje*** i ***Oprogramowanie szpiegujace***.

12.7.6. Karta "Informacje"

Karta ***Informacje*** zawiera dane dotyczace znalezionych obiektów, których nie mozna zakwalifikowac jako infekcje, oprogramowanie szpiegujace itp. Obiektów tych nie mozna w stu procentach uznac za niebezpieczne, ale czesto wymagaja one uwagi uzytkownika. Skaner AVG jest w stanie wykryc pliki, które moga nie byc zainfekowane, ale sa podejrzane. Zglaszane beda one jako ***lub*** Informacja.

Informacje o zagrozeniu moga byc zglaszane z jednego z nastepujacych powodów:

- ***Plik kompresowany w czasie rzeczywistym*** - Plik zostal skompresowany przy uzyciu jednego z mniej popularnych programów kompresujacych w czasie wykonania, co moze wskazywac na próbe uniemozliwienia skanowania takiego pliku. Nie kazde zgloszenie takiego pliku oznacza obecnosc wirusa.

- ***Plik rekurencyjnie kompresowany w czasie rzeczywistym*** - Podobny do powyzszego, ale rzadziej spotykany wsród zwyklego oprogramowania. Takie

pliki sa podejrzane i nalezy rozwazyc ich usuniecie lub przeslanie do analizy.

- ***Archiwum lub dokument chroniony haslem*** - Pliki chronione haslem nie moga byc skanowane przez program AVG (*ani generalnie przez zaden inny program chroniacy przed szkodliwym oprogramowaniem*).

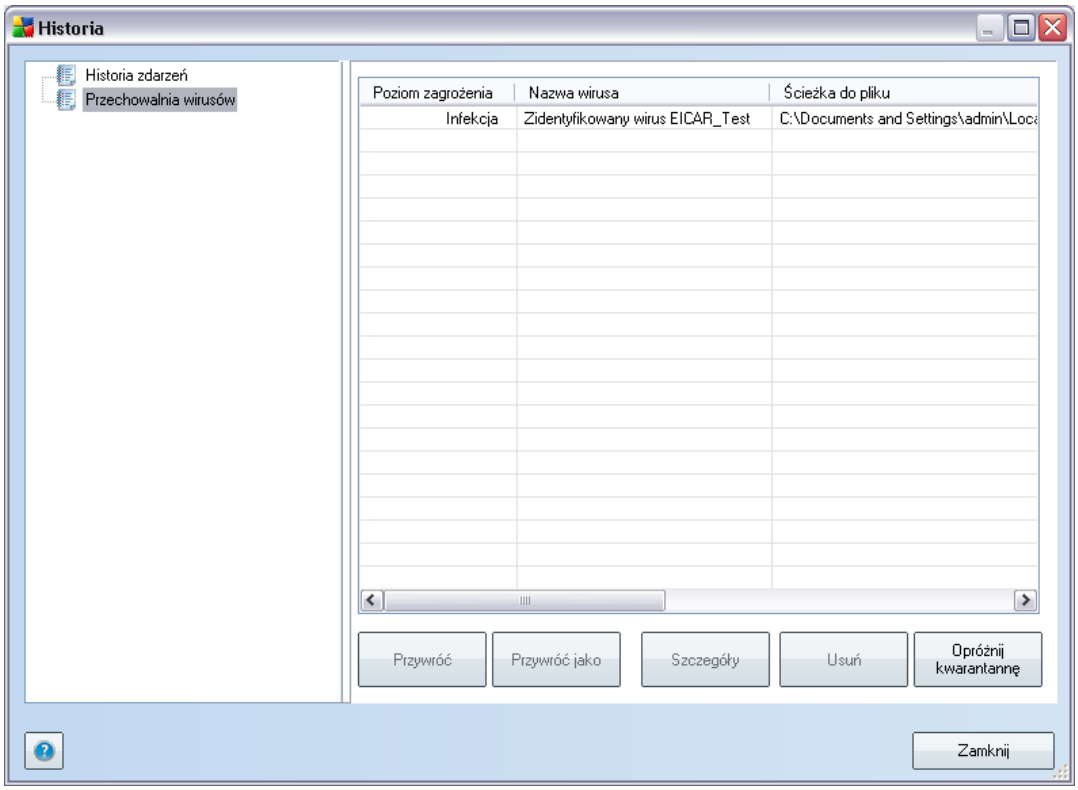
- ***Dokument zawierajacy makra*** — zgloszone dokumenty zawieraja makra, które moga byc szkodliwe.

- ***Ukryte rozszerzenie*** — pliki z ukrytymi rozszerzeniami moga udawac np. obrazy, podczas gdy w rzeczywistosci sa plikami wykonywalnymi (*np. "obrazek. jpg.exe"*). Drugie rozszerzenie jest w systemie Windows domyslnie niewidoczne. Program AVG zglasza takie pliki, aby zapobiec ich przypadkowemu uruchomieniu.

- ***Niewlasciwa sciezka do pliku*** — jezeli jakis wazny plik systemowy jest uruchamiany z innej sciezki niz domyslna (*np. plik "winlogon.exe" jest uruchamiany z folderu innego niz Windows*), system AVG zglasza te niezgodnosc. W niektórych przypadkach wirusy uzywaja nazw standardowych procesów systemowych, aby ich obecnosc w systemie byla trudniejsza do wychwycenia przez uzytkownika.

- ***Plik zablokowany*** — raportowany plik jest zablokowany, dlatego nie moze zostac przeskanowany przez system AVG. Oznacza to zazwyczaj, ze dany plik jest stale uzywany przez system (*np. plik wymiany*).

12.8. Przechowalnia wirusów



Kwarantanna to bezpieczne srodowisko przeznaczone do zarzadzania podejrzanymi/ zainfekowanymi obiektami, które zostaly wykryte podczas testów przeprowadzonych przez AVG. Po wykryciu zainfekowanego obiektu podczas skanowania (w przypadku, gdy AVG nie jest w stanie automatycznie go wyleczyc), uzytkownik zostanie poproszony o wybranie reakcji na to zagrozenie. Zalecanym rozwiazaniem jest przeniesienie obiektu do ***kwarantanny***, skad mozna bedzie podjac dalsze dzialanie zwiazane z analiza, wyleczeniem lub usunieciem pliku. Głównym zadaniem ***kwarantanny*** jest przechowywanie wszelkich usunietych plików przez okreslony czas, aby mozliwe bylo upewnienie sie, ze plik nie jest wymagany w swojej pierwotnej lokalizacji. Jesli brak pliku powoduje problemy, mozna go wyslac wraz z pytaniem do analizy lub przywrócic do pierwotnej lokalizacji.

Interfejs ***kwarantanny*** jest otwierany w nowym oknie i zawiera przeglad informacji o izolowanych, zainfekowanych obiektach:

- ***Zagrozenie*** — jesli w systemie ***zostal zainstalowany skladnik*** Identity Protection**AVG 9 Internet Security**, w tej sekcji wyswietlana bedzie graficzna

identyfikacja poziomu zagrozenia odpowiednich obiektów — od "nieistotne" (■□□□) do "bardzo niebezpieczne" (■■■■); dostepne beda również informacje na temat typu infekcji (*zgodnie z ich poziomem zainfekowania — wszystkie obiekty na liscie moga byc zainfekowane faktycznie lub potencjalnie*).

- ***Nazwa wirusa*** — nazwa wykrytej infekcji pochodzaca z Encyklopedii wirusów (online).
- ***Sciezka do pliku*** — pelna sciezka do oryginalnej lokalizacji zainfekowanego pliku.
- ***Pierwotna nazwa obiektu*** — wszystkie wykryte obiekty na liscie zostaly oznaczone standardowymi nazwami okreslanymi przez AVG w trakcie skanowania. W przypadku gdy obiekt mial okreslona nazwe, która jest znana (*np. nazwa zalacznika wiadomosci e-mail, która nie odpowiada faktycznej zawartosci zalacznika*), jest ona podawana w tej kolumnie.
- ***Data zachowania*** — data i godzina wykrycia podejrzanego pliku i przeniesienia go do ***kwarantanny.***

Przyciski kontrolne

Interfejs ***kwarantanny*** zawiera nastepujace przyciski kontrolne:

- ***Przywróc*** — przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- ***Przywróc jako*** — jesli zainfekowany obiekt ma zostac przeniesiony poza ***kwarantanne***, do okreslonego folderu, ten przycisk pozwala zapisac obiekt z nazwa inna niz pierwotna. Jesli nazwa pierwotna nie jest znana, uzyta zostanie nazwa standardowa.
- ***Szczegóły*** — ten przycisk moze byc uzywany tylko dla zagrozen wykrytych przez skladnik ***Identity Protection***. Jego klikniecie wyswietla porównawczy przeglad szczegółów zagrozen (*zainfekowane pliki/procesy, charakterystyka procesów itp.*). Nalezy zawrócic uwage na fakt, ze dla wszystkich pozycji innych niz wykryte przez skladnik IDP ten przycisk pozostanie szary i nieaktywny!
- ***Usun*** — nieodwracalnie usuwa zainfekowany plik z ***kwarantanny***.
- ***Opróznij kwarantanne*** — usuwa bezpowrotnie cala zawartosc ***kwarantanny***. Usuniecie plików z kwarantanny oznacza calkowite i nieodwracalne ich usuniecie z dysku (nie sa przenoszone do kosza).

13. Aktualizacje AVG

Zapewnienie aktualnosci programu AVG jest niezbedne, poniewaz tylko w ten sposób wszystkie nowo pojawiajace sie wirusy beda wykrywane we wlasciwym czasie.

Podczas procesu instalacji systemu AVG mozliwe jest okreslenie, jak czesto on ma byc aktualizowany. Dostepne opcje to ***Co 4 godziny*** lub ***Codziennie*** (zobacz okno dialogowe ***Planowanie regularnego skanowania i pobierania aktualizacji***). Poniewaz Aktualizacje systemu AVG nie sa publikowane zgodnie z jakimkolwiek harmonogramem (powstaja jako reakcja na pojawiajace sie zagrozenia), zalecamy sprawdzanie dostepnosci aktualizacji przynajmniej raz dziennie. Sprawdzanie co 4 godziny zagwarantuje ciagla aktualnosc systemu**AVG 9 Internet Security**.

13.1. Poziomy aktualizacji

Program AVG oferuje dwa poziomy aktualizacji:

- ***Aktualizacja definicji*** zawiera uzupelnienia niezbedne do zapewnienia niezawodnej ochrony antywirusowej, antyspamowej i przed szkodliwym oprogramowaniem. Na ogól nie zawiera modyfikacji programu i aktualizuje tylko baze definicji. Ta aktualizacja powinna zostac zastosowana, gdy tylko bedzie dostepna.

- ***Aktualizacja programu*** zawiera rózne zmiany w programie glównym, oraz poprawki i udoskonalenia.

Podczas planowania aktualizacji mozna wybrac poziom priorytetu aktualizacji, które maja zostac pobrane i zastosowane.

Uwaga: *Jesli zaplanowane skanowanie i zaplanowana aktualizacja naloza sie, proces aktualizacji bedzie mial pierwszenstwo i skanowanie zostanie przerwane.*

13.2. Typy aktualizacji

Mozna wyróznic dwa typy aktualizacji:

- ***Aktualizacja na zadanie*** — natychmiastowa aktualizacja oprogramowania AVG, której mozna dokonac w dowolnym momencie, w razie wystapienia takiej koniecznosci.

- ***Aktualizacja zaplanowana*** — system AVG umozliwia przygotowanie harmonogramu aktualizacji. Aktualizacja zaplanowana jest wykonywana regularnie, zgodnie z ustawiona konfiguracja. Gdy dostepne sa nowe pliki aktualizacyjne, AVG pobiera je bezposrednio z internetu lub katalogu

sieciowego. W przypadku braku nowych aktualizacji proces ten konczy sie, nie dokonujac zadnych zmian.

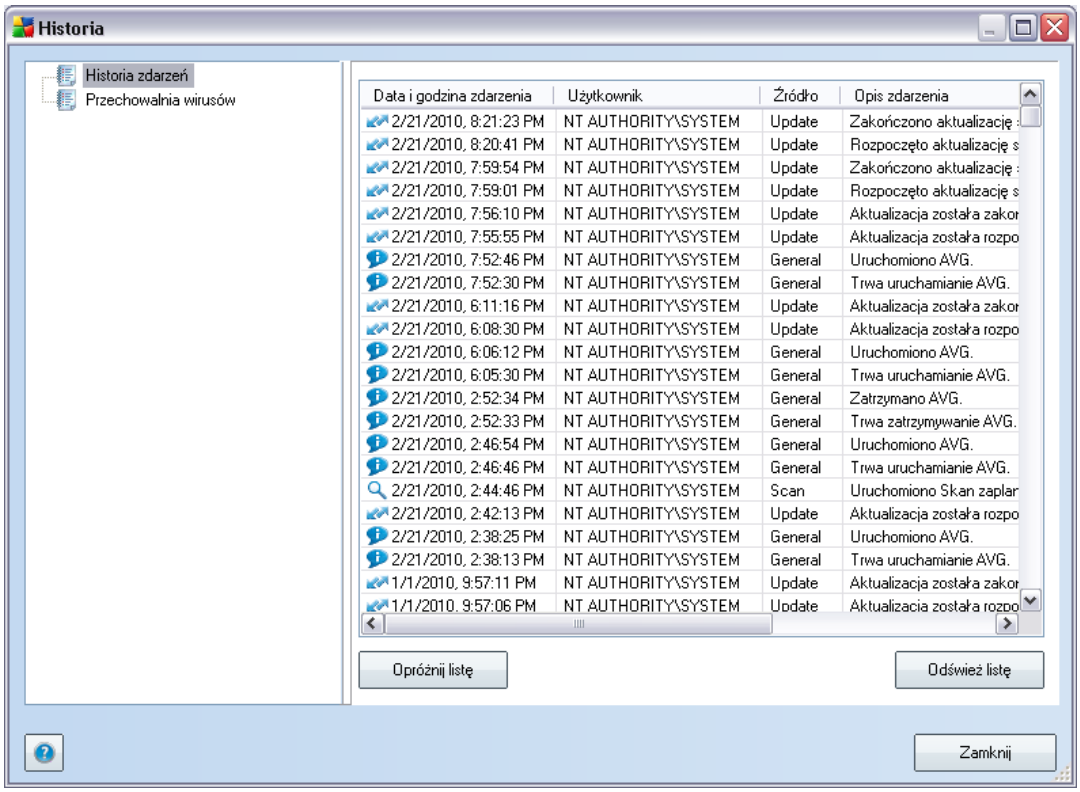
13.3. Proces aktualizacji

Proces aktualizacji mozna uruchomic natychmiast, gdy jest ona potrzebna, klikajac szybki link ***Aktualizuj teraz***. Link ten jest zawsze dostepny w głównym oknie interfejsu uzytkownika AVG. Mimo to, zaleca sie regularne aktualizowanie systemu, zgodnie z harmonogramem, który mozna edytowac za pomoca Menedzera aktualizacji.

Po uruchomieniu tego procesu program AVG sprawdza, czy dostepne sa nowe pliki aktualizacyjne. Jesli tak, system pobiera je i uruchamia wlasciwy proces aktualizacji. W tym czasie otwierany jest interfejs ***Aktualizacja*** , w którym mozna sledzic przedstawiony graficznie postep aktualizacji oraz przegladac szereg parametrów (*rozmiar pliku aktualizacji, ilosc odebranych danych, szybkosc pobierania, czas pobierania itd., ...*).

***Uwaga**: Przed zaktualizowaniem programu AVG tworzony jest punkt odtwarzania systemu. Przy jego uzyciu mozliwe bedzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Funkcja ta jest dostepna po kolejnym wybraniu opcji: Start / Wszystkie programy / Akcesoria / Narzedzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoswiadczonym uzytkownikom!*

14. Historia zdarzen



Do interfejsu ***Historii zdarzen*** mozna dostac sie poprzez menu glówne ***Historia/ Dziennik historii zdarzen***. Okno to zawiera podsumowanie najwazniejszych wydarzen, które wystapily w czasie pracy systemu **AVG 9 Internet Security**. ***Dziennik historii zdarzen*** zawiera rekordy odpowiadajace nastepujacym typom zdarzen:

- Informacje o aktualizacjach oprogramowania AVG;
- Uruchomienie, zakonczenie lub wstrzymanie testu (lacznie z testami wykonywanymi automatycznie);
- Zdarzenia powiazane z wykryciem wirusa (przez Ochrone Rezydentna lub podczas zwyklego skanowania), wraz ze wskazaniem lokalizacji zainfekowanego pliku;
- Inne wazne zdarzenia.

Przyciski kontrolne

- ***Opróznij liste*** — powoduje usuniecie wszystkich wpisów z listy zdarzen.
- ***Odswiez liste*** — powoduje odswiezenie zawartosci listy zdarzen.

15. FAQ i pomoc techniczna

W przypadku jakichkolwiek problemów z oprogramowaniem AVG (w kwestiach handlowych lub technicznych) nalezy skorzystac z sekcji ***FAQ*** witryny systemu AVG (http://www.avg.com/).

Jesli pomoc ta okaze sie niewystarczajaca, zalecamy kontakt z dzialem pomocy technicznej za posrednictwem poczty e-mail. Zachecamy do skorzystania z formularza kontaktowego, dostepnego po wybraniu polecenia menu systemowego ***Pomoc/ Uzyskaj pomoc online***.